HackMyVM - Alzheimer's

WriteUP (Spanish)

d4t4s3c Jan 29 · 2 min read

Author: sML **Twitter:** @ x6cx61x63x61x73

Operating System: Linux

Difficulty: Easy

. . .

- discovering **IP** via **ARP**

```
/HackMyVM/Alzheimer ✔ # arp-scan -l | grep "PCS" | awk '{print $1}'
192.168.1.142
```

- detecting open ports with **nmap**

```
/HackMyVM/Alzheimer ✔ # nmap -n -sS -p- --min-rate 5000 192.168.1.142 | grep "open"
```

```
21/tcp open     ftp
```

- parsing the only open port with **nmap**

```
/HackMyVM/Alzheimer ✓ # nmap -n -sV -sC -p21 192.168.1.142
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-28 23:08 CET
Nmap scan report for 192.168.1.142
Host is up (0.00039s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.111
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
MAC Address: 08:00:27:D1:F3:B6 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

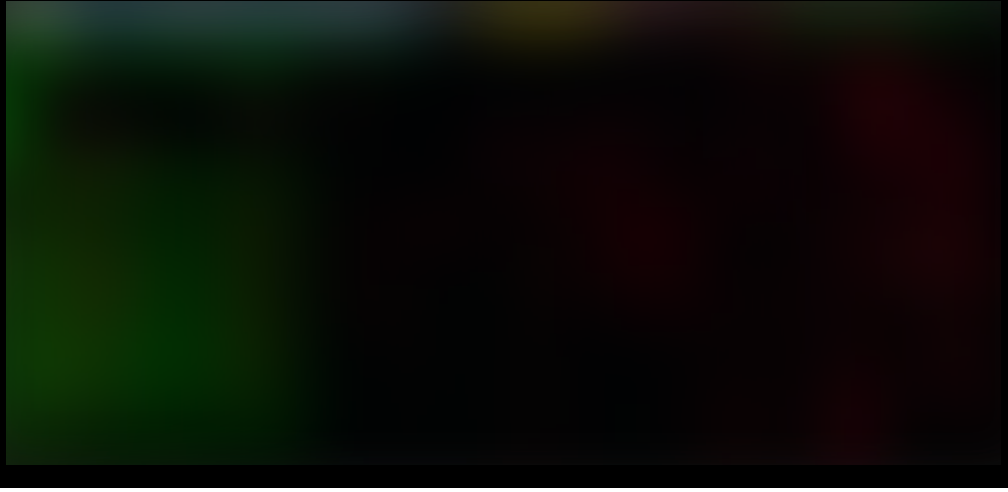
. . .

- **Port: 21 (FTP)**

has **anonymous** user enabled

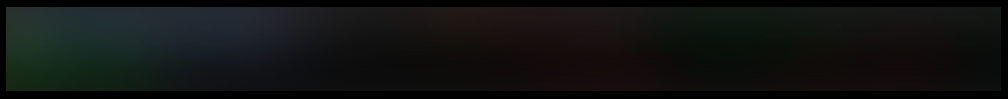
```
/HackMyVM/Alzheimer ✓ # ftp 192.168.1.142
Connected to 192.168.1.142.
220 (vsFTPd 3.0.3)
Name (192.168.1.142:d4t4s3c): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        113          4096 Oct 03 05:01 .
drwxr-xr-x    2 0        113          4096 Oct 03 05:01 ..
-rw-r--r--    1 0        0              70 Oct 03 05:01 .secretnote.txt
226 Directory send OK.
ftp> mget .*
mget .secretnote.txt? y
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .secretnote.txt (70 bytes).
226 Transfer complete.
70 bytes received in 0.00 secs (27.1267 kB/s)
ftp> exit
221 Goodbye.
```

I find a hidden file called **.secretnote.txt**



contains a sequence for a port knocking **(Port Knocking)**

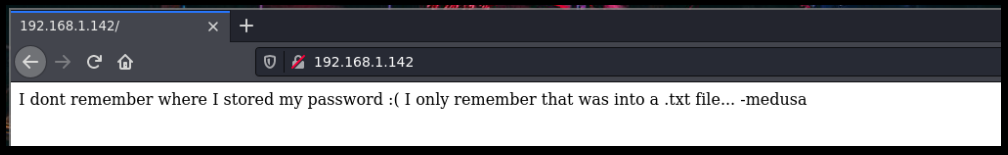
inicio el golpeo de puertos con la secuencia encontrada



tras el golpeo, detecto dos puertos nuevos abiertos (**22 SSH y 80 HTTP**)

. . .

- **Puerto: 80 (HTTP)**



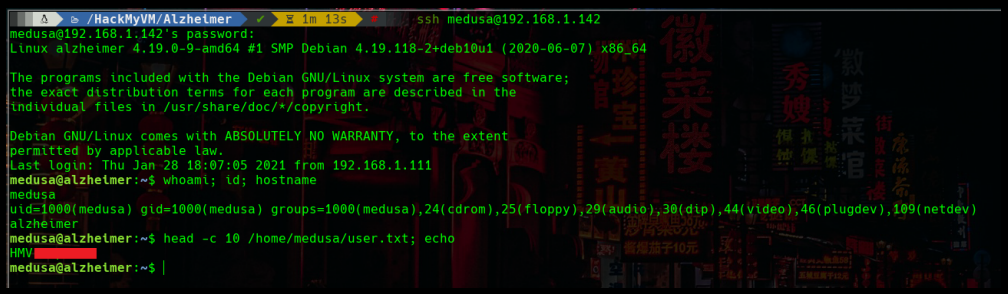
encuentro un texto que dice lo siguiente:

> *No recuerdo dónde guardé mi contraseña :(Solo recuerdo que estaba en un archivo .txt … -medusa*

. . .

- **Puerto: 22 (SSH)**

accedo al sistema como **medusa** con las credenciales encontradas en **.secretnote.txt** y puedo leer la **flag** de **user.txt**



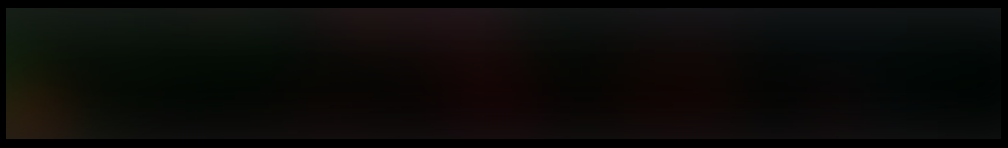
. . .

- **Elevación de Privilegios**

medusa tiene permisos **SUID** sobre el binario de **capsh**

(puede ejecutar temporalmente el binario como su propietario "**root**")

get or a **shell** as **root** and I can read the **flag root.txt**



so far the **Alzheimer's** machine

Offensive Security | Pentesting | Hacking | Cybersecurity | Ctf Writeup