En esta entrada vamos a prender un poco de herramientas del red team practicando con la maquina Cap de HTB

Para iniciar con esta máquina iniciamos como con cualquier otra, con el reconocimiento de puertos para identificar cuales son los servicios que tiene abiertos esta máquina.

Para el reconocimiento usaremos `nmap`

```console

nmap -p- --open -n -sV -T5 10.10.10.245

```

Para que sirven cada uno de los parámetros que usamos en nmap

\* -p- es para que escanee todos los puertos del servidor

\* --open nos muestra solo los puertos abiertos

\* -n para que no nos haga resolución de domino

\* -sV nos regresa el nombre y versión de los servicios

\* -T5 es para que haga el escaneo rápido y ruidoso

Texto

Descripción generada automáticamente

Con nmap encontramos que el servidor tiene tres puertos abiertos el 21 con ftp, 22 con ssh y el 80 con http.

Cuando veo que en las maquinas de ctf tienen servicio de ftp siempre intento conectarme con el usuario Anonymous pero en este caso no es posible conectarse, así que no lo intentaremos en este posts

Nos vamos directo al servicio http,

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

Explorando la pagina llegamos a la uri /data/1 en la cual podemos descargar archivos pcap de la máquina de las interacciones que nosotros hacemos en la máquina, por ejemplo, use nikto para investigar la maquina y ahí en esos archivos encontré esa información, en esta página podemos investigar si podemos descargar más archivos además del 1 y encontramos el uri /data/0 el cual es de antes que nosotros iniciáramos a trabajar en la máquina.

Captura de pantalla de un celular

Descripción generada automáticamente

Por suerte el archivo es muy pequeño y podemos encontrar a simple vista trafico ftp, el cual no esta encriptado y podemos ver en texto plano la comunicación entre cliente y servidor. Aplicamos en el filtro ftp para que solo nos muestre los paquetes de ese protocolo.

Captura de pantalla de computadora

Descripción generada automáticamente

Es aquí donde encontramos un usuario y contraseña estos son para el servicio ftp pero usaremos para ver si también son las del servicio ssh

Texto

Descripción generada automáticamente

Y funciono, con un ls encontramos el user.txt

Ahora vamos por el root

Vamos a intentar escalar privilegios, iniciamos con el descubrimiento para reconocer los posibles vectores de ataque que podemos usar, a mi me gusta usar un script llamado linpeas.sh, que nos sirve investigar todo esto de una forma automatizada, lo descargamos del repositorio oficial y lo subimos al servidor con scp.

```console

#From github

curl <https://raw.githubusercontent.com/carlospolop/privilege-escalation-awesome-scripts-suite/master/linPEAS/linpeas.sh>

scp linpeas.sh nathan@10.10.10.245:/home/nathan/

```

Texto

Descripción generada automáticamente

Nos vamos al servidor hacemos un ls para ver si se encuentra ahí el archivo. Ejecutamos con sh el script

```console

sh linpeas.sh

```

Interfaz de usuario gráfica

Descripción generada automáticamente

En la información del script nos dice que tenemos que poner atención a el texto rojo remarcado en amarillo tenemos un 95% para usar ese vector

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Y lo encontramos en los archivos con capacidades en el cual nos dice que con python3.8 podemos conseguir un SUID, aquí tenemos que investigar en Google para encontrar algo, en i casso con una simple búsqueda en Google encontré <https://useful.adindrabkin.com/hacker-mode/privilege-escalation/linux-privilege-escalation-checklist> ese link en el que nos explican como conseguir el usuario root

```console

python3 -c 'import os;os.setuid(0);os.system("/bin/bash")'

```

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Listo…

En este momento tenemos acceso root

Solo queda ver el archivo root.txt

```console

cat /root/root.txt

```