Walkthrough

FASE INICIAL

Empezamos descargando la máquina desde Vulnhub, una vez descargada lo que haremos será importarla en VirtualBox/VMWare/UTM o similares, la inicializamos y nos pasamos a nuestra máquina Kali linux.

Una vez en la máquina Kali, abrimos la terminal y con un **arp-scan -I eth0 --localnet** escaneamos nuestra red. (Tenemos que tener en cuenta que ambas máquinas deben tener configuradas las redes con tipo Bridged*). Veremos que aparecerán varias direcciones IP, nos quedaremos con aquella que esté en la misma máquina virtual que nosotros.

Una vez conocida la IP de la máquina “víctima”, haremos un ping para verificar la conectividad, esto además nos dará información sobre qué tipo de máquina es gracias al TTL*. Vemos que TTL = 64, por lo que es una máquina Linux.

FASE DE ESCANEO

Usaremos la herramienta nmap* y realizaremos un escaneo de todos los puerto con el siguiente comando:
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn IpMaquinaVictima -oG nombreFichero

Con este comando indicamos que, usando nmap, queremos escanear los todos los puertos existentes (-p-), de entre estos, descubrir solamente los que estén abiertos (--open), con el tipo de escaneo TCP SYN port Scan (-sS)*, indicando que quieres tramitar paquetes no más lentos que 5000 paquetes por segundo (--min-rate 5000), con triple verbose (-vvv) para que a medida que vaya detectando puertos abiertos los vaya reportando por consola, que no aplique resolución DNS (-n), ya que ralentiza el escaneo, desactivaremos la detección de hosts, asumiendo que este está activo, ya que el ping anterior ha sido exitoso (-Pn), y lo exportaremos en formato grepeable (formato que permite filtrar con Regex) al fichero correspondiente (-oG).

(Esta configuración permite un escaneo rápido, sigiloso y violento que no detecta falsos positivos/negativos.)

Cuando ha finalizado nuestro escaneo, mostramos el contenido que nos ha reportado con cat nombreFichero y vemos que tenemos los puertos 21,80 y 55077 que corresponden a ftp, http y ssh respectivamente.

FASE DE PROFUNDIZACIÓN

Vamos a intentar acceder al servicio ftp, como no tenemos usuario o contraseña, intentamos acceder de forma anónima. FTP permite este tipo de accesos. Entramos y si listamos el contenido que hay en el directorio al que nos lleva el ftp, vemos un archivo "**cred.txt**", si mostramos su contenido vemos "**Y2hhbXA6cGFzc3dvcmQ=**". Tras hacer unas búsquedas llegamos a la conclusión de que las credenciales están codificadas en base64, el cual podemos decodificar con "**base64 decode**", que nos devuelve "**champ:password**". De momento no podemos hacer nada más aquí así que pasamos al puerto 80, que nos lleva a una página web con un panel de login, en el que probamos las credenciales obtenidas anteriormente. Esto funciona y nos redirige a una página llamada "CTF Machine".

En la página vemos varios botones, uno de ellos llamado "About Us", el cual nos descarga un archivo cuando lo pulsamos, ese archivo contiene:

"**funny.bmp**
funny.jpg
sudo"

Vemos que sudo es un .txt que cuando lo leemos muestra: "**Did you notice the file name? Isn't is interesting?**"

Ahora usando la herramienta "**steghide**" inspeccionamos ambas imágenes en busca de más información y obtenemos esta cadena en funny.bmp: "**jgs:guvf bar vf n fvzcyr bar**" y esta otra en la otra imagen: "**This is not a python file but you are revolving around. well, try_ to rotate some words too.**"

Esto nos está indicando que el cifrado usado para la cadena de funny.bmp puede involucrar el rotado de letras, uno de los cifrados más comunes de este tipo es el cifrado César, tras probar varios posibles rotados, vemos en en rotado 13 la cadena toma sentido y nos dice:

"**wtf:this one is a simple one**"

Si probamos esto en el puerto ssh nos permite el acceso.

FASE DE ESCALADO

Ahora lo que nos toca es hacernos con el usuario root, investigando por la máquina hemos encontrado que hay tres usuarios: "wtf", "noob" y "root".

Nos movemos al directorio "rooot" y si listamos el contenido vemos que hay un archivo llamado "flag.txt" pero no tenemos permisos para mostrarlo, sin embargo, si hacemos "**sudo su**" para intentar convertirnos en usuarios root, nos lo permite y ya si que podemos listar la flag:

“**RW5kb3JzZSBtZSBvbiBsaW5rZWRpbiA9PiBodHRwczovL3d3dy5saW5rZWRpbi5jb20vaW4vZGV1cGFrLWFoZWVyCg==**”

Leyenda:

Comandos usados
Referencias a la máquina víctima
Passwords
Flags obtenidas
Las palabras con * están definidas en el documento de definiciones