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 20 y 80 abiertos, el 20 se corresponde con el puerto SSH y el 80 con el HTTP.

FASE DE PROFUNDIZACIÓN

Cuando entramos en la ip de la máquina vemos la página por defecto de un servidor Apache. Con esta información tenemos realmente poco que hacer, por lo que vamos a intentar ver si sacamos posibles directorios con la herramienta “**feroxbuster**”*
Usaremos el comando “**feroxbuster -u http://192.168.147.212/ -s200,301 -x html,txt,php**”, de este modo encontramos dos directorios, uno llamado “**/robots.txt**” y otro llamado “**/secret/evil.php**”, si miramos en ambas rutas, la primera nos muestra lo siguiente “**Hello H4x0r**” y en la segunda nos muestra la página en blanco. Por lo tanto, en el próximo paso, se utilizará la técnica de fuzzing de parámetros con el fin de descubrir un parámetro válido para el archivo 'evil.php' con el siguiente comando “**ffuf -c -r -u 'http://192.168.147.212/secret/evil.php?FUZZ=/etc/passwd' -w /usr/share/seclists/Discovery/Web-Content/common.txt -fs 0**” y nos devuelve el parámetro “**command**” entonces si probamos a añadir a la ruta de la página php “**?command=ComandoCualquiera**”, si probamos con “**/etc/passwd**” nos muestra el contenido del archivo, lo que nos indica que el sitio es vulnerable a LFI*. Si inspeccionamos el archivo que hemos logrado ver anteriormente vemos un nombre de usuario “**mowree**” , si investigamos más profundamente encontramos la clave SSH del usuario anterior, ubicada en el directorio "**/home/mowree/.ssh/id_rsa**". La usaremos para entrar en el servidor SSH de este usuario, pero primero la desciframos con la herramienta “**ssh2john**”*.
Usamos el comando “**john --wordlist=/home/usuario/rockyou.txt hash_john**”, siendo “**rockyou.txt**” un diccionario muy conocido. La contraseña para poder acceder al servicio SSH haciendo uso de la clave privada id_rsa para el usuario "**mowree**" es "**unicorn**".
Gracias a esto accedemos a la máquina y vemos la flag en el archivo “**local.txt**”.

Flag de usuario: “**35710821240c7d12fa7f02933faf6cb9**”

FASE DE ESCALADO DE PRIVILEGIOS

En esta fase buscamos obtener la flag del usuario privilegiado (“root”), para ello recabamos información sobre la máquina en la que nos encontramos, como el sistema operativo y su distribución concreto, en este caso no vemos nada relevante por lo que volvemos al archivo “**/etc/passwd**” y tratamos de cambiar la contraseña del archivo root con el comando “**openssl passwd -1**” y ya podemos acceder al super usuario y, por ende, a la flag del archivo “**proof.txt**”

Flag de SuperUsuario: “**21375f04e35d019fa9a8392cdd8b40bf**”

Contenido de apoyo:

Securiters wiki

Leyenda:

Comandos usados
Referencias a la máquina víctima

Passwords

Flags obtenidas

Las palabras con * están definidas en el documento de definiciones