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 80 y 21, que corresponden a http y ftp respectivamente.

FASE DE PROFUNDIZACIÓN

Comenzamos explorando el 80, este nos lleva a una web, revisando su código fuente no encontramos nada y no hay elementos que llamen la atención, salvo un botón para buscar.

Pulsando en buscar vemos que en la url de la web tenemos "**ipMaquinaVictima/sitio/busque.php?buscar=**", probamos a poner cualquier comando a la derecha del igual como "**pwd**" (muestra el directorio en el que estamos trabajando) y nos devuelve efectivamente, el directorio en el que "estamos". Si vemos el código fuente de esta página vemos un código en php "**<?php system($_GET['buscar']); ?>**" esto nos indica que va a obtener lo que pongamos a la derecha del igual en la url y nos lo va a devolver, es decir, que cada comando que pongas que exista y que tengas permisos para ejecutar funcionará. Probamos a enviarle el comando "**netstat -antopu | grep LISTEN**" que nos detecta el puerto 22 como filtrado.

Si aplicamos FUZZING e la url para detectar posibles directorios, obtenemos el directorio "**/backup**". Donde vemos datos relacionados con una base de datos que apuntamos.

Probamos el usuario y contraseña encontrados en la base de datos en el servidor ftp del puerto 21 y tenemos acceso. Podríamos intentar usar la shell del navegador pero no funcionaría porque si en la ventana de buscar, introducimos el comando "**id**" vemos que los permisos del usuario están muy limitados.

Así que aprovechamos este FTP al que tenemos acceso para subir algún fichero que podamos aprovechar para proporcionarnos acceso al ssh o al Mysql que vimos previamente.

Para eso usaremos reGeorg*, crearemos un proxy socks en la máquina destino que nos permitirá acceder a cualquier puerto local de la máquina y que no esté accesible directamente.

Por un lado subimos el fichero "tunnel.nosocket.php", que se encuentra ubicado dentro del directorio de reGeorg, al FTP como "tunnel.php", en el directorio destino /tmp. Y le damos permisos para que el usuario www-data pueda copiarlo dentro de /site/.

Y con esto ya podríamos acceder al ssh. Una vez dentro encontraríamos la Flag de usuario.

Contenido de apoyo:

Ciberseguridad.blog

Leyenda:

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