THE-WALL:1

1. Búsqueda y descarga

Buscamos la máquina que queramos vulnerar en vunhulb, en este caso la the-wall 1. Tras encontrarla la descargamos y la importamos a la máquina virtual, en este caso estamos usando la máquina virtual VM virtualBox.

Abrimos la máquina virtual y le damos a importar, buscamos donde hemos descargado la máquina virtual y la importamos, esto tardará unos segundos. Tras esto antes de iniciarla es importante que configuremos unos parámetros para que la máquina funcione perfectamente.

- Nos vamos a la configuración de esta máquina al apartado de red, y cambiamos la parte de “Conectado a:” de NAT, a Adaptador puente.
- En esta misma pestaña de red, en el apartado de advanced en la parte de “Modo promiscuo:” pasamos de denegar, a permitir todo.

¿Por qué hemos cambiado el tipo de red? Por que si dejamos NAP, la máquina virtual no sería visible desde la red local, al cambiarla a adaptador puente permite que la máquina obtenga su propia IP para interactuar con esta.

¿Por qué hemos cambiado el modo advanced? Esto se hace ya que si no la máquina no va a procesar paquetes externos, solo procesaría los que sean destinados a su dirección MAC. Esto se hace para que se pueda analizar el tráfico de la red, o simular ataques a la máquina.

Tras haber hecho los pasos anteriores y comprendido el porqué de esos cambios, iniciamos la máquina descargada y configurada.
Posteriormente iniciamos la máquina atacante, es decir, la máquina desde donde vamos a intentar vulnerar nuestra máquina the-wall. Esta máquina atacante es Kali-lunix, y la iniciamos desde VMware.

2. Antes de comenzar

Vamos a dejar nuestro espacio de trabajo lo más limpio posible, así que por si hemos ejecutado algo anterior que puede interferir.

- Nos movemos al directorio escritorio para poder tener accesible todo lo que necesitemos. Esto se hace mediante el comando “cd desktop”
- Tras situarnos en este lugar eliminamos todo lo que podamos haber creado en un intento de vulnerar otra máquina. Esto se hace mediante el comando “rm -r *”

Tras limpiarlo lo idóneo es crear un nuevo directorio con el nombre de la máquina para ir dejando ahí todos los recursos que vayamos a usar. Esto se hace gracias al comando “mkdir the-wall”. Después de crearlo nos movemos a ese directorio con el comando “cd the-wall”.

3. Primera fase

La primera fase para vulnerar una máquina virtual consiste en ver si la máquina es accesible en nuestra red tras iniciarla ya que a veces puede haber fallos. Esto lo hacemos mediante el comando “arp-scan -I eth0 –localnet”. En este comando hay un detalle importante que es el “eth0”, esto lo ponemos ya que si ejecutamos el comando “ifconfig”, vemos que en la interfaz eth0 está nuestra dirección IP, por eso debemos ejecutar el comando con esa pequeña modificación.

Que puede suceder cuando ejecutemos el comando, que no muestre nada, tras unos intentos lo que nos puede indicar que la máquina a la que queremos atacar no se ha conectado bien, en este caso lo que hay que hacer es reiniciar la máquina, en la barra de opciones selecciona “Máquina” y le aplicamos un reinicio. Si esto no funciona podemos cambiar uno de los parámetros de configuración del principio, en concreto el de advanced, poniendo en vez de permitir en todos, permitir MVs. Para hacer esto hay que apagar la máquina primero. Con esto permitimos únicamente máquinas virtuales para acceder a nuestra máquina que va a ser atacada.

Tras cambiar esto al ejecutar el comando arp-scan mencionado anteriormente veremos cómo aparece la dirección de nuestra máquina. Es importante apuntar esta dirección en algún lado.

Con la dirección de la máquina apuntada ejecutamos el comando “nmap -p- –open -sS -sC -sV –min-rate 5000 -vvv -n -Pn dirección -oN fichero”.

- El parámetro -p: puertos abiertos.
- El parámetro –open: que de verdad estén abiertos.
- El parámetro -sS: Para que el escaneo no sea muy detectable.
- El parámetro -sC: Conjunto de scripts de nmap para que nos busque más información.
- El parámetro -sV: versión de cada entorno de los puertos.
- El parámetro -min-rate: Para que aumente la velocidad.
- El parámetro 5000: Velocidad del min-rate.
- El parámetro -vvv: Se conoce como triple vervose, para que a medida que me encuentre algo me lo reporte.
- El parámetro -n: Que no ejecute resolución DNS para ahorrar tiempo.
- El parámetro -Pn: Para que no haga ping a la hora de buscar información, así evitamos que bloquee trazas icmp.
- El parámetro -oN: Guardar los datos del escaneo en el archivo fichero (se le puede poner otro nombre).

Al ejecutar esto vemos que no está escuchando nada, asi que comprobamos si esta hablando, esto lo hacemos a través de una herramienta Wireshark , esta herramienta lo que hace es capturar paquetes de la red en tiempo real, para ello y que sea más efectivo buscamos en la red con el comando => ip.src == “172.16.231.142”, o campiando la ip a la que tengas en ese momento. Tras esperar un rato nos saca lo siguiente:

- 90 7.203252830 172.16.231.129 172.16.231.142 TCP 54 1337 → 21344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Gracias a esto vemos que está buscando conectarse al puerto 1337, así que lo hacemos mediante el comando nc -lvp 1337. Tras esto vemos que el wireshark también nos dio otra información:

- 3558 241.470595714 172.16.231.142 172.16.231.129 HTTP 605 HTTP/1.1 200 OK (text/html)

Gracias a esta información podemos ver que tiene una solicitud http, podemos concluir que tras la conexión del puerto 1337 se ha iniciado esta solicitud, así que probamos otra vez el nmap y vemos que tiene los puertos 80 y 1965 abiertos.

El puerto 1965 requiere de un usuario y una contraseña, así que como no las tenemos seguimos mirando por el puerto 80. En este puerto encontramos una imagen de Pink Floyd, y al inspeccionarla y ver su código observamos una serie de números que podrían ser hexadecimal, pero para cumplir esto necesita ser una serie de valores separados por espacio.

- “737465673d333331313537333064626262333730666362653937323066653633326 5633035”

Para lograr esto con un simple código en python vale =>

```
import sys
a='737465673d333331313537333064626262333730666362653937323066536333265633
035'
for i in range(0, len(a), 2):
   sys.stdout.write(chr(int(a[i:i+2], 16)))
print()
```

Este código muestra como resultado esta cadena =>

- steg=33115730dbbb370fcbe9720fe632ec05

Gracias a esta cadena podemos sacar dos cosas, con la palabra steg, que la imagen tiene esteganografía, y el resto de caracteres es un hash (“33115730dbbb370fcbe9720fe632ec05”) que lo podemos descifrar gracias a la herramienta en línea Crackstation, el hash descodificado que nos da es “divisionbell”.

Mediante esta contraseña ya podemos acceder al archivo oculto que hay dentro de la imagen la cual requiere una contraseña, con el comando =< steghide extract -p divisionbell -sf pink_floyd.jpg, sacamos todos los datos en un archivo txt llamado pink_floyd_syd.txt. Al hacer cat sobre este archivo nos revela una pista en la cual hay una key en base64 y otro hash, se puede deducir que uno será el usuario y otro a contraseña para acceder a la máquina.

Para el usuario usamos este comando => “echo U3lkQmFycmV0dA== | base64 -d”, que nos arroja el user => “SydBarrett”, y para la contraseña podemos usar la misma herramienta que antes Crackstation que nos arroja la password => “pinkfloydrocks”.

Intentamos conectarnos con ssh a la máquina mediante el comando => “ssh SydBarrett@172.16.231.142 -p 1965”, esto nos dice que no acepta conexiones ssh si no sftp, así que probamos con el comando => “sftp -P 1965 SydBarrett@172.16.231.142”, lo que nos pide la contraseña la podemos y ya nos deja acceder a la máquina.

4. Escalada de privilegios

Al estar en la máquina hacemos ls -la y vemos que tiene varios directorios, una imagen, la cual no es relevante, una biografía y una carpeta .mail. En el correo se dicen varias cosas como que el material lo debe usar con bisturí lo que se refiere a que debe haber algún archivo oculto. Así que entramos en la carpeta -mail y hacemos ls -la para ver si hay archivos ocultos, lo que nos lleva a encontrar una carpeta .stash que contiene un archivo comprimido. Este archivo se extrae con el comando tar xzf archivo.tar.gz. Tras la extracción, aparece un archivo .lsd, que parece ser un sistema de archivos en formato FAT16.
Para analizarlo, utilizamos Scalpel, una herramienta de recuperación forense, que nos permite extraer archivos eliminados o perdidos dentro del sistema FAT16. Ejecutamos el siguiente comando: scalpel archivo.lsd -o recuperados/. Esto hará que Scalpel recupere los archivos y los guarde en la carpeta recuperados/.
Después de ejecutar Scalpel, revisamos los archivos recuperados dentro de la carpeta recuperados/. Para ver las imágenes extraídas, usamos el comando ls recuperados/*.jpg. En este caso, encontramos que la imagen jpg-3-0 contiene la contraseña "Roger Waters". Para verificar su contenido, podemos abrirla con un visor de imágenes como eog recuperados/jpg-3-0 en un sistema con entorno gráfico o con feh recuperados/jpg-3-0 si usamos terminal. Si estamos en un sistema sin interfaz gráfica, podemos extraer texto oculto dentro de la imagen utilizando el comando strings recuperados/jpg-3-0 | less.
Con la contraseña encontrada, podemos acceder a la máquina remota a través de SSH usando el puerto 1965, con el comando ssh RogerWaters@172.16.231.142 -p 1965. Si la contraseña es correcta, ingresamos al sistema con éxito.

Tras estar en la máquina listamos el resto de usuarios con el comando getent passwd; el cual nos arroja todos los nombres de usuarios. Buscamos uno por uno los archivos relevantes con el comando => “find / -user “username” 2> /dev/null”, con el usuario NickMason encontramos un binario con SUID en la dirección /usr/local/bin/brick, tras ejecutarlo con el comando XXXX nos pregunta que ¿Quién es el único miembro de la banda que aparece en todos los álbumes?, si hacemos una rápida búsqueda en internet sobre pink floyd descubrimos que la respuesta es Nick Manson, esto nos da acceso al usuario al instante.

Una vez dentro de este nuevo usuario buscamos si hay algún archivo que nos pueda arrojar información, y encontramos bio.txt que contiene información que nos manda a su foto de perfil la cual es una archivo ogg que hay que recuperar para escuchar más allá de los tonos de piano, ya que de fondo se escucha lo que podría parecer morse pasamos este sonido

por un filtro de paso alto en el que apuntamos los puntos y líneas del código morse para pasarlo por un traductor de morse que nos arroja => “aRICHARDWRIGHT1943FARFISA” Esto parece ser la contraseña del usuario Richard, pero al intentar acceder no nos deja, asi que volvemos a logearnos como Roger y usamos el comando => “su username” para entrar como Richard.

Una vez dentro observamos el directorio y encontramos un correo que le mandó David el cual nos manda a /usr/local/bin/shineon, el cual si lo ejecutamos nos da comandos básicos de linux, los cuales tienen que ejecutarse con una ruta, todos menos el de mail, el cual si lo ejecutamos busca el binario en los directorios listados en $PATH. Al no tener ruta absoluta se puede manipular para hacer que ejecute un archivo por nosotros. Para ello primero haces un enlace simbólico con el comando => “ln -s /bin/sh /tmp/mail”, despues cambiamos el $PATH para que busque primero en el temp con el comando => “export PATH=/tmp:${PATH}”.
Ahora ejecutamos “/usr/local/bin/shineon”, como hemos hecho antes solo que al seleccionar la opción 4 que es el mail nos introduce a la máquina con el usuario DavidGilmour.

Con este nuevo usuario volvemos a revisar los directorios encontrando pinkfloyd1965newblogsite50yearscelebration-temp/index.php, y una imagen who_are_you_and_who_am_i. Como no podemos hacer ssh primero tenemos que volver al usuario Roger y luego usar el comando su a David, al abrir la imagen y editarla con una aplicación y subir su contraste y brillo se obtiene la url para probar accesos. Esta URL da fallo pero si nos fijamos da un valor con número hexadecimales los cuales al convertirlos nos da lo que parece ser una contraseña “PinkFloyd50Years”, usamos esta contraseña para explorar algunos archivos del usuario en la dirección /var/www/htdocs/, en la que se encuentra un directorio llamado welcometothemachine, donde hay un binario con permisos que pide una contraseña, probamos la que hemos descubierto pero no funciona, asi que probamos la cadena hexadecimal completa “50696e6b466c6f796435305965617273” y funciona.
Con esta acción ha cambiado algo en sistema lo comprobamos con el comando => “find / -mmin 2 2>/dev/null”, el cual nos dice que se ha modificado el archivo => “/etc/sudoers”. Esto indica que el usuario en el que estamos tiene permisos de sudo, asi que ejecutamos sudo su, y obtenemos acceso como ROOT a la máquina, y en la carpeta principal tenemos el archivo flag.txt. Que nos da el mensaje de la victoria, en este caso la flag es el mensaje no hay ningún código.