Monitoring: 1

1. Búsqueda y descarga

Buscamos la máquina que queramos vulnerar en vunhulb, en este caso la Monitorging: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 Monitorging. 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 Monitorging”. Después de crearlo nos movemos a ese directorio con el comando “cd Monitorging”.

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 puerto 80 con una web apache corriendo en protocolo http, el puerto 443 con otra web y el puerto 389. 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 las webs.

El puerto 80 nos lleva a una web llamada nagios, que es una aplicación para el monitoreo de redes y servidores que suelen usar muchas empresas, podemos probar con usuarios por defecto que tiene esta app para ver si el administrador los ha cambiado buscando en google vemos que las credenciales por defecto son user: nagiosadmin y password: admin, las probamos y da la casualidad de que nos deja entrar.

Esta página para monitorear tiene una vulnerabilidad muy grande ya que una vez dentro podemos ejecutar un código en el servidor. Para explotar esta vulnerabilidad usamos metasploit la cual incluye un módulo específico para atacar a nagios.
Para usar este meta exploit necesitamos tener instalado metasploit, se instala con el comando => “sudo apt update && sudo apt install metasploit-framework -y”. Una vez instalado lo iniciamos con msfconsole, y buscamos si tenemos algún exploit para nagios con el comando => “search nagios”, esto nos da un resultado. Usamos el comando => “use exploit/linux/http/nagios_xi_authenticated_rce”, para ejecutar el exploit. Esto nos pedira que lo configuremos así que usamos el comando => “set RHOSTS <IP_objetivo>”, y ponemos la ip de la máquina, y el usuario con el que vamos a autenticarnos => “set USERNAME nagiosadmin” y su contraseña “set PASSWORD admin”. Tras eso ejecutamos el exploit con => “run”.

Esto nos debería dejar acceder a la máquina con el usuario, y para escalar privilegios podemos usar el comando => “shell” y después el comando => python -c ‘import pty; pty.spawn(“/bin/bash”)’”, con esto nos da acceso a root y si hacemos cd encontramos el archivo proof que contiene la flag =>
“SunCSR.Team.3.af6d45da1f1181347b9e2139f23c6a5b”