HERRAMIENTAS DE EXPLOTACIÓN LINUX

Jordi Masó Pla

INDICE

1 DESCUBRIMIENTO

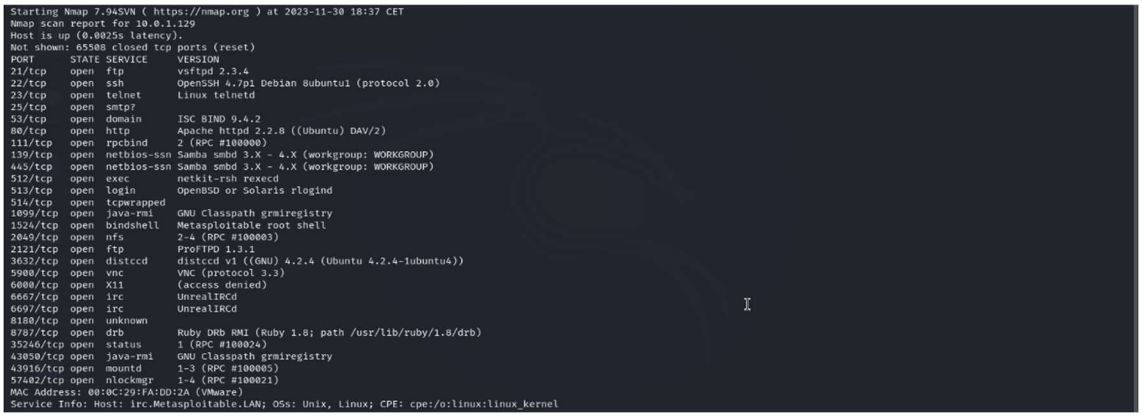
En este ejercicio realizaremos las pruebas de explotación de los servicios en la maquina Metasplotable 2, utilizado técnicas manuales como automáticas.

1.1 ARP-SCAN

Con arp-scan procedemos a encontrar la dirección ip de nuestra maquina victima a la que vamos atacar. En nuestro caso es la ip 10.0.1.129 ya que las demás son reservadas por el programa VMware.

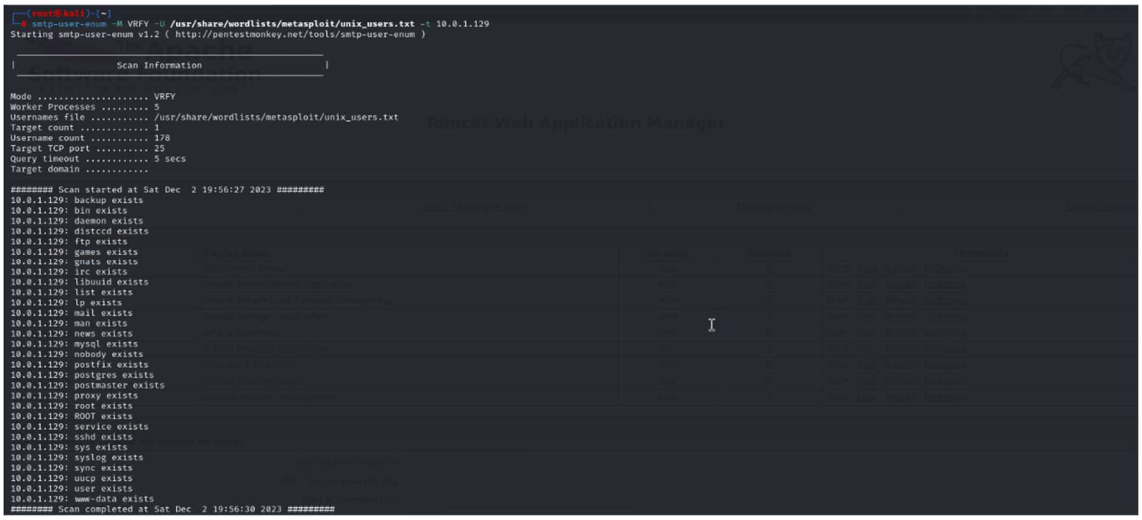
1.2 NMAP

Empezamos el descubrimiento de la maquina con la herramienta nmap para saber qué servicios están corriendo en esta máquina. Tenemos una variedad de puertos abiertos con muchos servicios activos, de los cuales se explotando para ir comprometiendo la maquina y el servicio en sí mismo.



1.3 SMTP

Con el servicio de smpt del puerto 25 y el comando smtp-user-enum y el módulo VRFY con un pequeño diccionario podemos descubrir algunos usuarios y ficheros de la propia máquina.



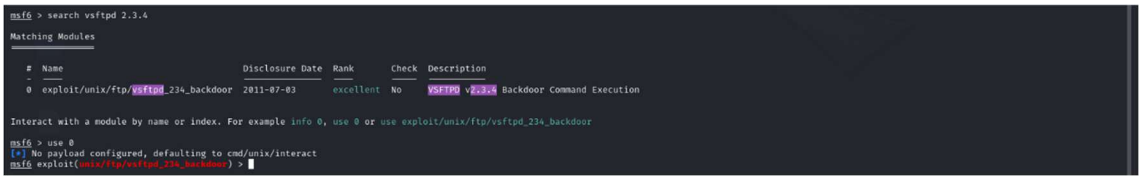
2 EXPLOTACION DE LOS SERVICIOS

En esta fase realizaremos la explotación de los servicios y comprometer la maquina de su integridad, confidencialidad y disponibilidad.

2.1 FTP

En el puerto 21 corre el servicio vsftpd 2.3.4, se hace una búsqueda en searchsploit y encontramos, que este servicio tiene un backdoor y es explotable con Mestasploit.

Abrimos Mestasploit buscamos el exploit para esta vulnerabilidad y configuramos los requisitos que nos solicita este exploit para realizar el ataque, como la ip de la víctima.



Una vez configurado el exploit con los requisitos que nos solicita lo lanzamos, comprobamos que se nos abre un Shell con permisos de superusuario o root, podemos acceder a todo el sistema de archivos.

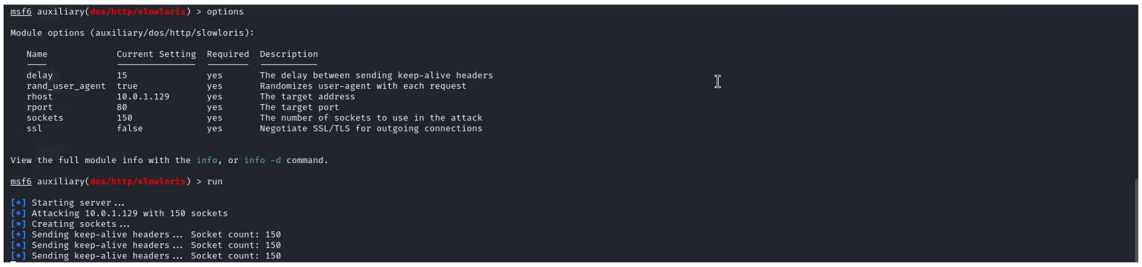
Con los privilegios adquiridos accedemos al archivo /etc/passwd para ver los usuarios registrados en el sistema.

2.2 TELNET

El servicio telnet que corren en el puerto 23 se puede acceder directamente e incluso al acceder al servicio la propia maquina nos indica como podemos logear cono usuario “msfadmin” y password “msfadmin” sin ningún tipo de seguridad por parte de este servicio.

2.3 APACHE HTTP

El servicio web es vulnerable a un ataque de denegación de servicio. Con Metasploit realizamos un ataque Dos a este servicio con el Slowloris, configuramos el auxiliar para realizar el ataque y lo lanzamos. En efecto el servicio no se puede acceder.



2.4 SAMBA SMBD

El protocolo samba del puerto 139 que tiene la versión 3.x -4.x tiene varias vulnerabilidades que se pueden explotar con Metasploit, con el exploit multi/samba/usermap_script podemos explotar este servicio y obtener privilegios de root. Como podemos ver in las capturas de pantalla

2.5 RLOGIN

Este servicio corre sobre los puertos 512, 513 y 514. Estos puertos son utilizados para la comunicación remota entre cliente y servidor. Estos servicios están mal configurados y por ello, podemos comunicarnos remotamente desde cualquier máquina, logeandonos como root.

2.6 JAVA-RMI

El puerto 1099 se puede atacar con un exploit de Metasploit consiguiendo credenciales de root. Con el exploit multi/misc/java_rmi_server configuramos la ip de la victima y ejecutamos el exploit obtenemos la Shell con Meterpreter y usuario root.

2.7 BINDSHELL

En el puerto 1524 se puede conectar al host simplemente utilizando netcat y acceder con privilegios de root, sin ningún tipo de contraseña.

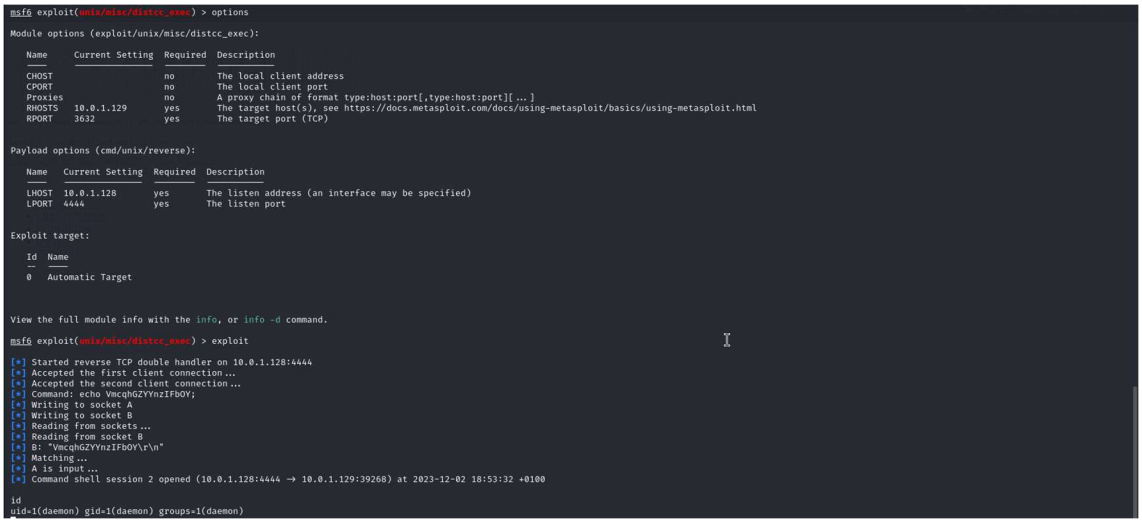
2.8 PROFTPD

En el puerto 2121 corre el servicio proftpd, utilizamos hydra con un pequeño diccionario para encontrar las credenciales de este servicio y poder entrar en el sistema.

Comprobamos las credenciales encontradas por hydra y vemos que son correctas, se puede acceder al servicio ftp del puerto 2121.

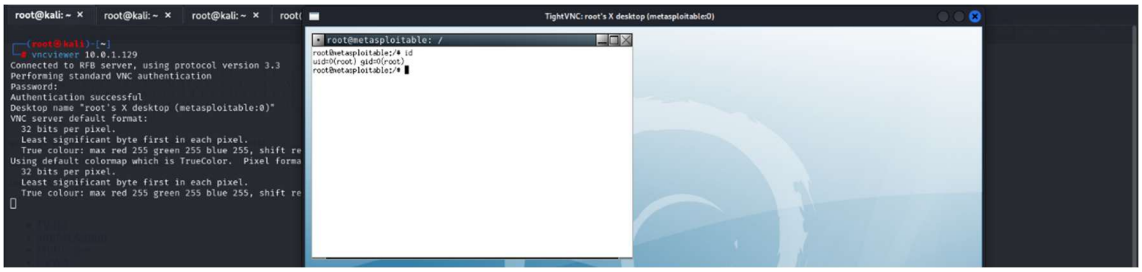
2.9 DISTCCD

El puerto 3632 esta abierto y corre el servicio distccd con un exploit de Metasploit se puede explotar este servicio obteniendo credenciales de usuario. Configuramos el exploit unix/misc/distcc_exec con los requisitos necesarios, accedemos con un usuario con privilegios elevados.



2.10 VNC PROTOCOLO

El protocolo vnc que corren en el puerto 5900 es vulnerable a un ataque de diccionario como vimos en ejercicio anteriores con Hydra o Medusa, solo hace falta la contraseña de acceso que es “password” para acceder como usuario root.

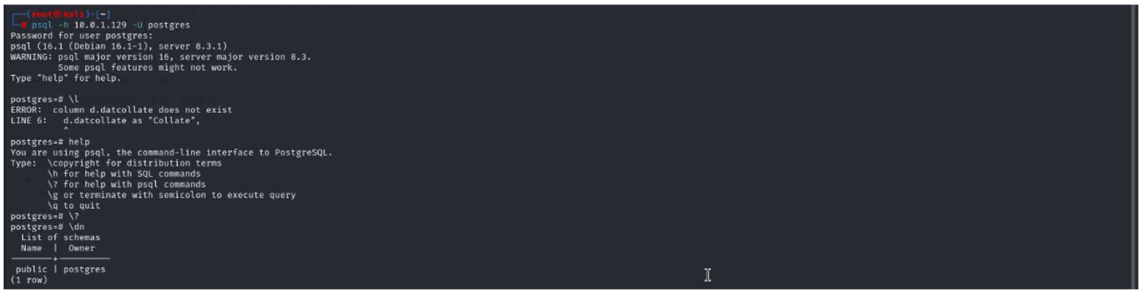


2.11 UNREALIRCD

Según el análisis de Nessus realizado anteriormente el servicio unrealIRCd contiene un backdoor que con un exploit de Metasploit es factible obtener una Shell con privilegios root. Configuramos el exploit unix/irc/unreal_ircd_3281_backdoor con las opciones necesarias y ejecutamos el exploit para obtener una Shell como root.

2.12 POSTGRES

En el puerto 5432 hay el servicio postgres con unas credenciales por defecto que vimos con el análisis de Nessus, que tiene como usuario “postgres” y de password “postgres”. Accedemos al servicio sin ningún tipo de impedimento pudiendo hacer cualquier tipo de modificación.



2.13 APACHE TOMCAT

En le puerto 8180 corre un servicio apache tomcat que podemos atacar con un exploit de Metasploit y conseguir una sesión con Meterpreter. El exploit utilizado es multi/http/tomcat_mgr_upload para subir código malicioso y obtener una Shell reversa de java, con las credenciales de root.

Con la Shell obtenida podemos acceder a todos los archivos del sistema con credenciales de root.