METASPLOITABLE 2 ENUMERACIÓN

En este tutorial de Metasploit vamos a enumerar la máquina virtual de Metasploitable 2 para recopilar información útil para una evaluación de vulnerabilidades. Enumeración en matemáticas o informática se refiere a contabilizar un número de elementos en un conjunto. Enumeración en el contexto de hacking es el proceso de recuperar nombres de usuario, recursos compartidos, servicios, directorios web, grupos, ordenadores en una red. También se denomina enumeración de la red. Durante este proceso también recopilaremos otra información útil relacionada con la red para llevar a cabo una prueba de penetración. Una parte importante del proceso de enumeración de Metasploitable 2 es el proceso de escaneo de puertos y huellas digitales. El escaneo de puertos se utiliza para sondear un servidor o host en busca de puertos TPC y UDP abiertos. El fingerprinting es el proceso de identificar los servicios conectados a esos puertos. Una herramienta muy popular utilizada para la enumeración de redes, escaneo de puertos y huellas digitales es NMap (Network Mapper), que utilizaremos a lo largo de este tutorial. También utilizaremos una herramienta de enumeración llamada enum4linux. Enum4linux es una herramienta utilizada para enumerar información de hosts Windows y Samba.

Después de haber completado con éxito la enumeración de la VM Metasploitable 2 vamos a hacer una evaluación de la vulnerabilidad en el lado de la red en el siguiente tutorial. Con la información recuperada del proceso de enumeración, por ejemplo, la versión del sistema operativo y los servicios en ejecución con su versión, buscaremos vulnerabilidades conocidas en estos servicios. Para ello utilizaremos la Open Source Vulnerability Database (OSVDB) y la Common Vulnerabilities and Exposures (CVE). El último paso es escanear el host de destino en busca de estas vulnerabilidades con un escáner de vulnerabilidades llamado OpenVAS.

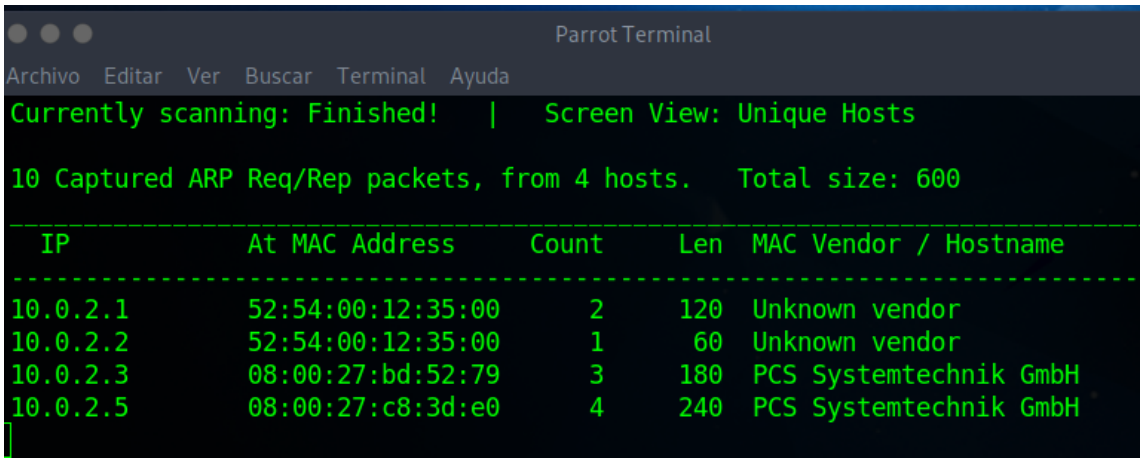
METASPLOITABLE 2 ENUMERACIÓN Y ESCANEO DE PUERTOS

En esta parte del tutorial de enumeración de Metasploitable 2 enumeraremos los servicios en ejecución, las cuentas y realizaremos un escaneo de puertos abiertos. Utilizaremos NMap para escanear la máquina virtual en busca de puertos abiertos e identificaremos los servicios conectados. En este tutorial sólo nos centraremos en enumerar el lado de red de la máquina Metasploitable 2. Cubriremos el lado web posteriormente. Cubriremos la parte web en otro tutorial donde enumeraremos aplicaciones y directorios web, realizaremos ataques de inyección SQL y explotaremos los servicios web vulnerables.

Asumo que ya has instalado la máquina virtual Metasploitable del tutorial anterior y si no se está ejecutando ahora es el momento de encenderla. Cuando inicies sesión en el host vulnerable con msfadmin como nombre de usuario y contraseña puedes utilizar el comando ifconfig para determinar su dirección IP. También puede utilizar netdiscover en la máquina Kali linux para escanear un rango de direcciones IP para el host de destino. Utilice el siguiente comando en el terminal:

```
netdiscover -r 192.168.111.0/24
```

Este comando devolverá todos los hosts vivos en el rango IP dado, en este ejemplo será el rango 10.0.2.0/24 que consiste en IP 10.0.2.0.0 a 10.0.2.255. Por supuesto deberías escanear el rango de IPs en el que se encuentra tu instalación de Metasploitable 2 VM en tu propia red.



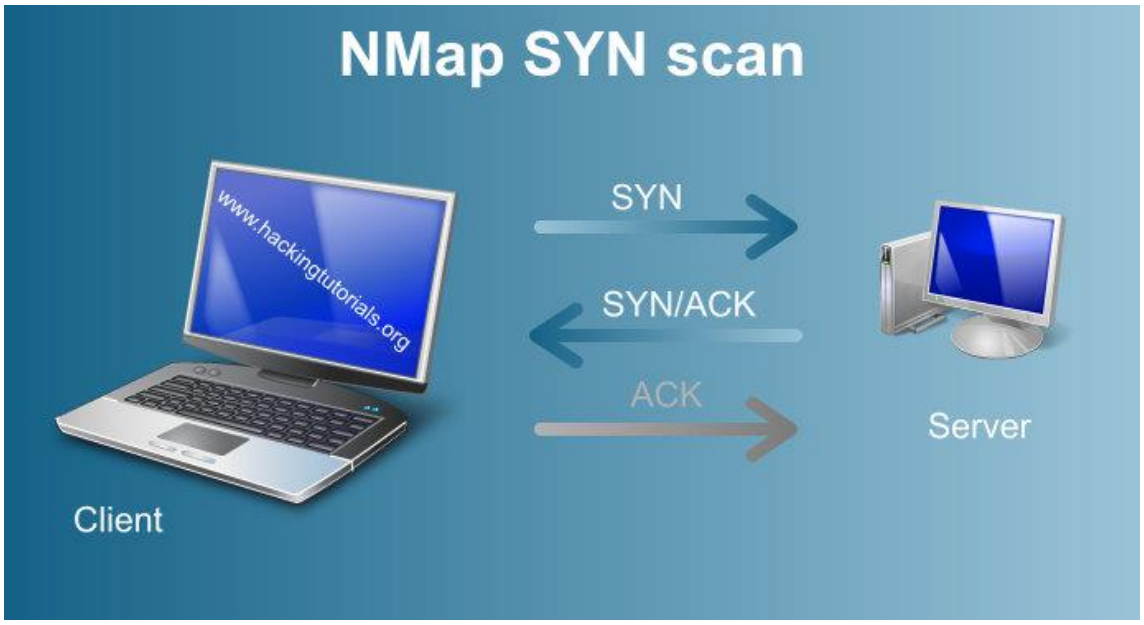
El comando netdiscover -r 10.0.2.0/24 descubre todas las direcciones IP en el rango dado.

ESCANEO DE PUERTOS NMAP Y ESCANEO DE SERVICIOS

Comenzaremos el escaneo de puertos abiertos escaneando el host de destino con NMap. Utilizaremos un escaneo TCP SYN para este propósito y luego escanearemos el objetivo en busca de puertos UDP abiertos. El escaneo SYN es conocido como un escaneo de puertos sigiloso porque no termina el handshake TCP completo. Una conexión TCP completa comienza con un handshake de tres vías donde un paquete SYN es enviado por NMap como la primera parte del handshake. Cuando un puerto de la máquina de destino está abierto, responderá con un paquete SYN-ACK. Cuando no hay respuesta del objetivo al primer paquete SYN, el puerto se cierra o es filtrado por un cortafuegos. El tercer paso en este proceso es la máquina anfitriona que debe responder al SYN-ACK con un paquete ACK para completar el TCP handshake. En el caso de un escaneo SYN nunca lo hace y por lo tanto se llama sigiloso.

Cuando se inicia un escaneo SYN (y cualquier otro escaneo de puertos) desde NMap sin especificar el rango de puertos, NMap escaneará sólo los primeros 1.000 puertos que se consideran los más importantes en lugar de todos los 65.535 puertos. Para escanear todos los puertos debe utilizar el indicador -p-. La orden Nmap SYN scan utiliza la bandera -sS como se utiliza en la siguiente orden para SYN scan del puerto 1 al puerto 65.535:

```
nmap -sS -p- [dirección IP taget]
```



El sondeo SYN de Nmap a menudo se denomina sondeo sigiloso, lo que implica que pasa desapercibido. Esto es cierto para cortafuegos antiguos, que sólo registran conexiones TCP completas, pero no para cortafuegos modernos que también registran conexiones TCP no completadas.

¿SON VULNERABLES LOS PUERTOS ABIERTOS?

Que un puerto esté abierto no significa que el software subyacente sea vulnerable. Necesitamos conocer la versión del sistema operativo y los servicios en ejecución. Con esta información podemos determinar si existen vulnerabilidades conocidas que puedan ser explotadas. El resultado del escaneo de servicios y del sistema operativo nos dará la información adecuada para investigar más a fondo durante la evaluación de vulnerabilidades. Para obtener esta información ejecutaremos el sondeo de puertos con la opción -sV para la detección de versiones y la opción -O para la detección de SO para recuperar las versiones de los servicios en ejecución y del SO. El sondeo de versiones y SO de Nmap completa el TCP handshake y utiliza técnicas como banner grabbing para obtener información de los servicios en ejecución.

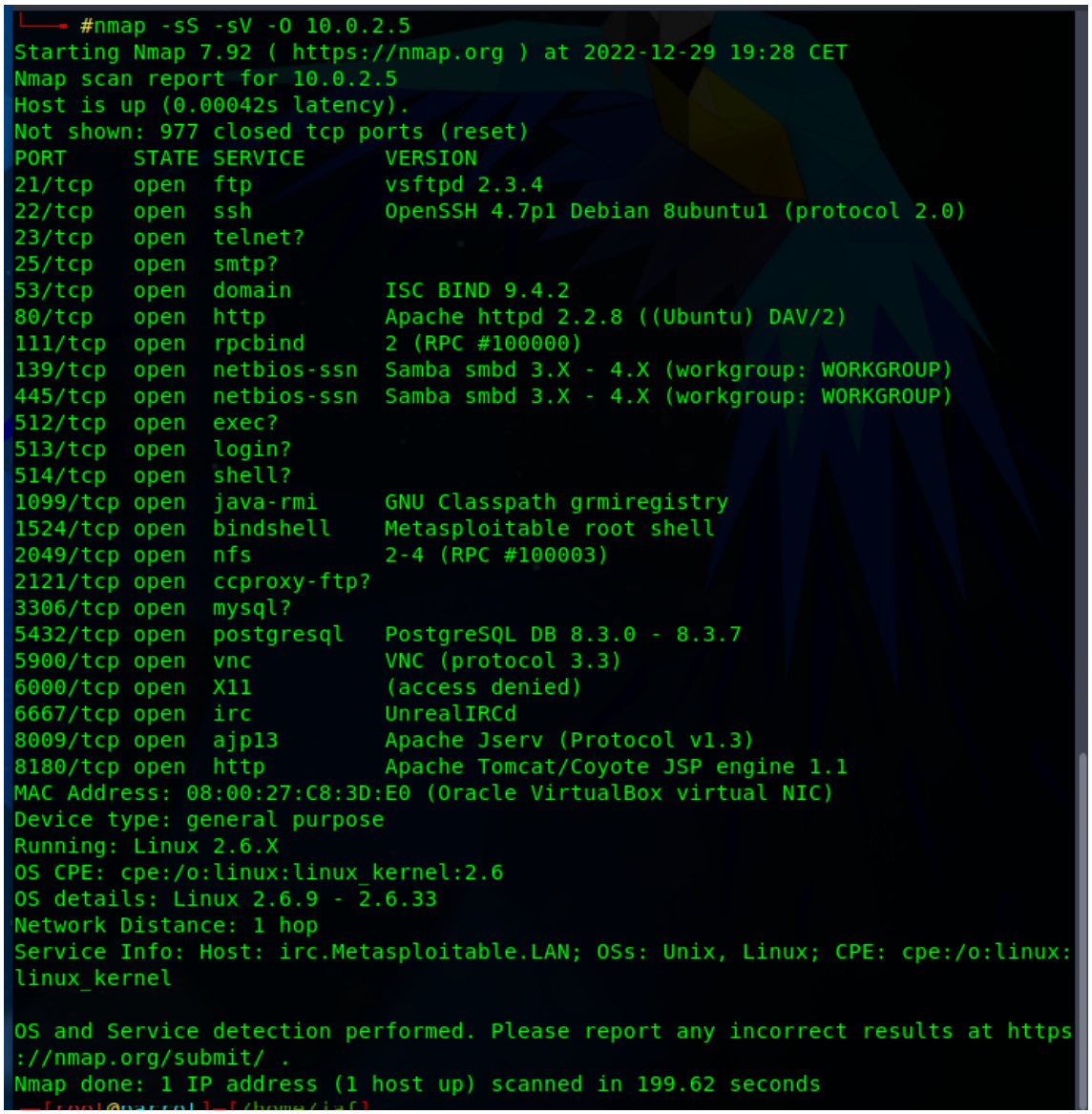
También puede utilizar la opción -A en lugar de -O para activar la detección de SO, la detección de versiones, el escaneo de scripts y la ruta de rastreo todo a la vez. Esta no es una forma sigilosa de escanear.

EXPLORACIÓN DEL SERVICIO NMAP CON DETECCIÓN DEL SO

Utilice la siguiente orden para iniciar el sondeo de puertos de Nmap con detección de servicios y SO:

```
Nmap -sS -sV -O [dirección IP de destino].
```

Después de ejecutar este comando NMap devolverá una lista de puertos abiertos y los servicios conectados:



El escaneo de puertos y servicios de Nmap devuelve un montón de puertos abiertos, servicios a la escucha y la versión del sistema operativo. El host objetivo está ejecutando Linux 2.6.9 - 2.6.33 como sistema operativo. Podemos ver que el host está ejecutando un servicio SSH usando OpenSSH, un servicio telnet, un servidor web Apache 2.2.8, 2 servidores SQL y algunos servicios más. Vamos a sumar todos los servicios con versión y puerto en una lista que utilizaremos próximamente donde haremos una evaluación de vulnerabilidades y buscaremos vulnerabilidades comunes:

- Vsftpd 2.3.4 en puerto abierto 21
- OpenSSH 4.7p1 Debian 8ubuntu 1 (protocolo 2.0) en el puerto abierto 22
- Servicio telnetd de Linux en el puerto abierto 23
- Postfix smtpd en el puerto 25
- ISC BIND 9.4.2 en el puerto abierto 53
- Apache httpd 2.2.8 Ubuntu DAV/2 en el puerto 80
- Un servicio RPCbind en el puerto 111
- Samba smbd 3.X en los puertos 139 y 445
- 3 servicios r en los puertos 512, 513 y 514
- GNU Classpath grmiregistry en el puerto 1099
- Metasploitable root shell en el puerto 1524

- Un servicio NFS en el puerto 2049
- ProFTPD 1.3.1 en el puerto 2121
- MySQL 5.0.51a-3ubuntu5 en el puerto 3306
- PostgreSQL DB 8.3.0 - 8.3.7 en el puerto 5432
- Protocolo VNC v1.3 en el puerto 5900
- Servicio X11 en el puerto 6000
- Unreal ircd en el puerto 6667
- Apache Jserv protocolo 1.3 en el puerto 8009
- Motor JSP Apache Tomcat/Coyote 1.1 en el puerto 8180

La mayoría de los servicios en ejecución escaneados por Nmap serán probablemente vulnerables.

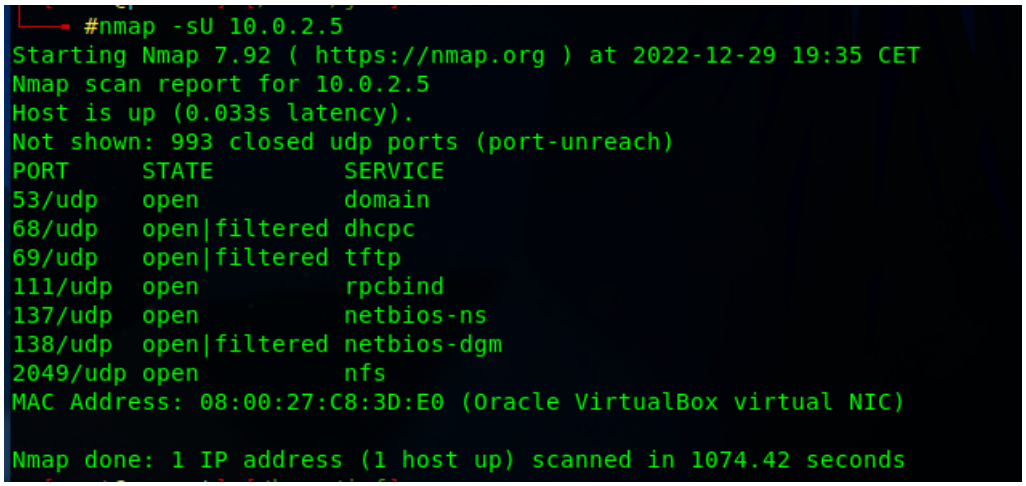
Por supuesto, sabemos que la máquina virtual Metasploitable 2 es intencionadamente vulnerable. Por lo tanto, uno sólo puede sospechar que la mayoría, si no todos, de los servicios contienen vulnerabilidades, puertas traseras, etc. Aquí sólo cubriremos tácticas de enumeración, escaneo de puertos y evaluación de vulnerabilidades en la red. En el siguiente tutorial de Metasploitable explotaremos las vulnerabilidades. Continuemos con la enumeración de usuarios.

ESCANEO UDP DE NMAP

Hasta ahora sólo hemos analizado los puertos TCP abiertos, que es el valor por omisión de Nmap, y no los puertos UDP abiertos. Utilicemos el siguiente comando para iniciar un sondeo UDP:

```
nmap -sU 10.0.2.5
```

También podemos utilizar la bandera -p para definir los puertos a escanear. El sondeo UDP tardará algo más de tiempo en finalizar que un sondeo TCP. Nmap devuelve la siguiente información sobre los puertos UDP abiertos que ha encontrado:



Tenga en cuenta que los escaneos UDP pueden causar muchos falsos positivos. Los falsos positivos pueden ocurrir porque UDP carece de un equivalente de un paquete TCP SYN. Cuando un puerto UDP escaneado está cerrado, el sistema responderá con un mensaje ICMP de puerto inalcanzable. La ausencia de dicho paquete indica que el puerto UDP está abierto para muchas herramientas de escaneo. Cuando hay un cortafuegos en el host de destino que bloquea el mensaje ICMP inalcanzable, todos los puertos UDP parecen estar abiertos. Cuando el cortafuegos bloquea un único puerto, el escáner también informará falsamente de que el puerto está abierto.

METASPLOITABLE 2 ENUMERACIÓN DE USUARIOS

La enumeración de usuarios es un paso importante en toda prueba de penetración y debe realizarse de forma exhaustiva. Con la enumeración de usuarios, la persona que realiza la prueba de penetración puede ver qué usuarios tienen acceso al servidor y qué usuarios existen en la red. Otro propósito de la enumeración de usuarios es obtener acceso a la máquina utilizando técnicas de fuerza bruta. Dado que el nombre de usuario ya es conocido por el probador de penetración, lo único que queda por forzar es la contraseña. Existen múltiples formas de enumerar usuarios en un sistema Linux. Veremos 2 métodos diferentes:

1. Enumerar usuarios usando un script de Nmap llamado smb-enum-users.
2. Enumerar usuarios a través de una sesión nula usando rpclient.

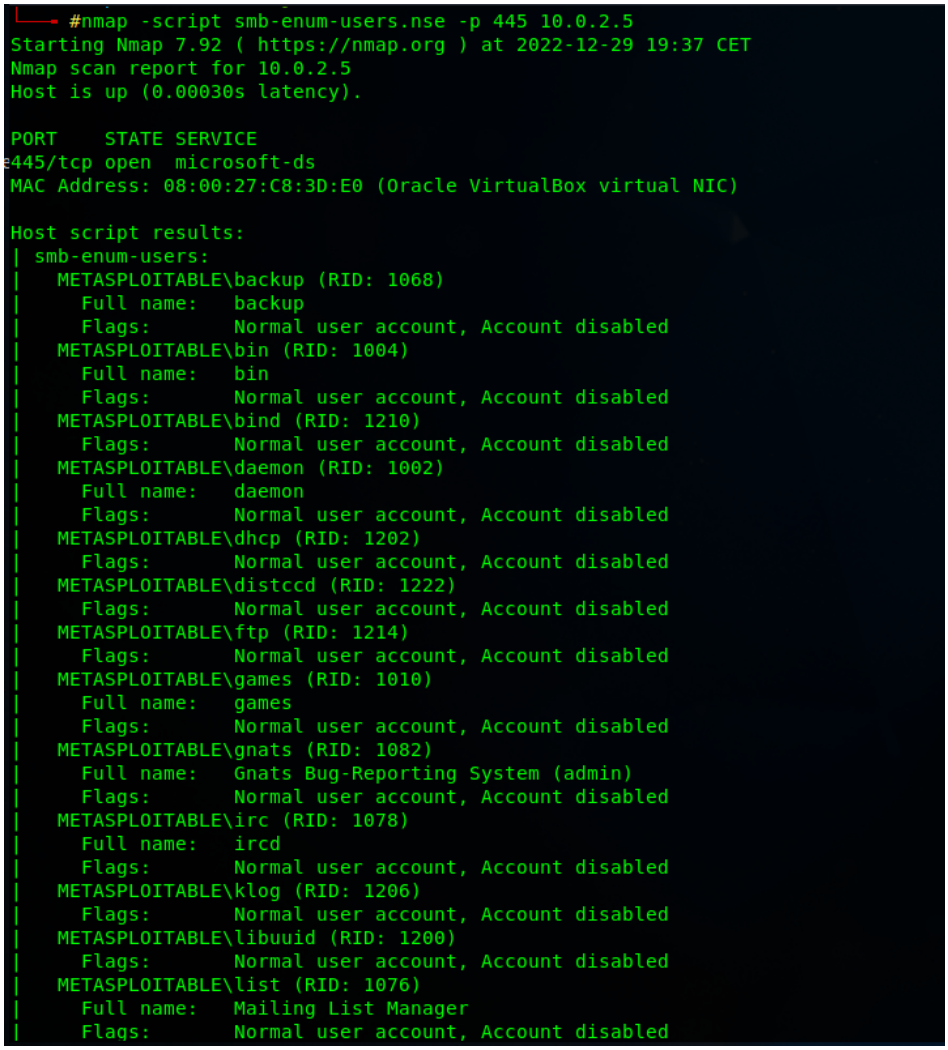
Comencemos con la enumeración de usuarios usando el script NMap.

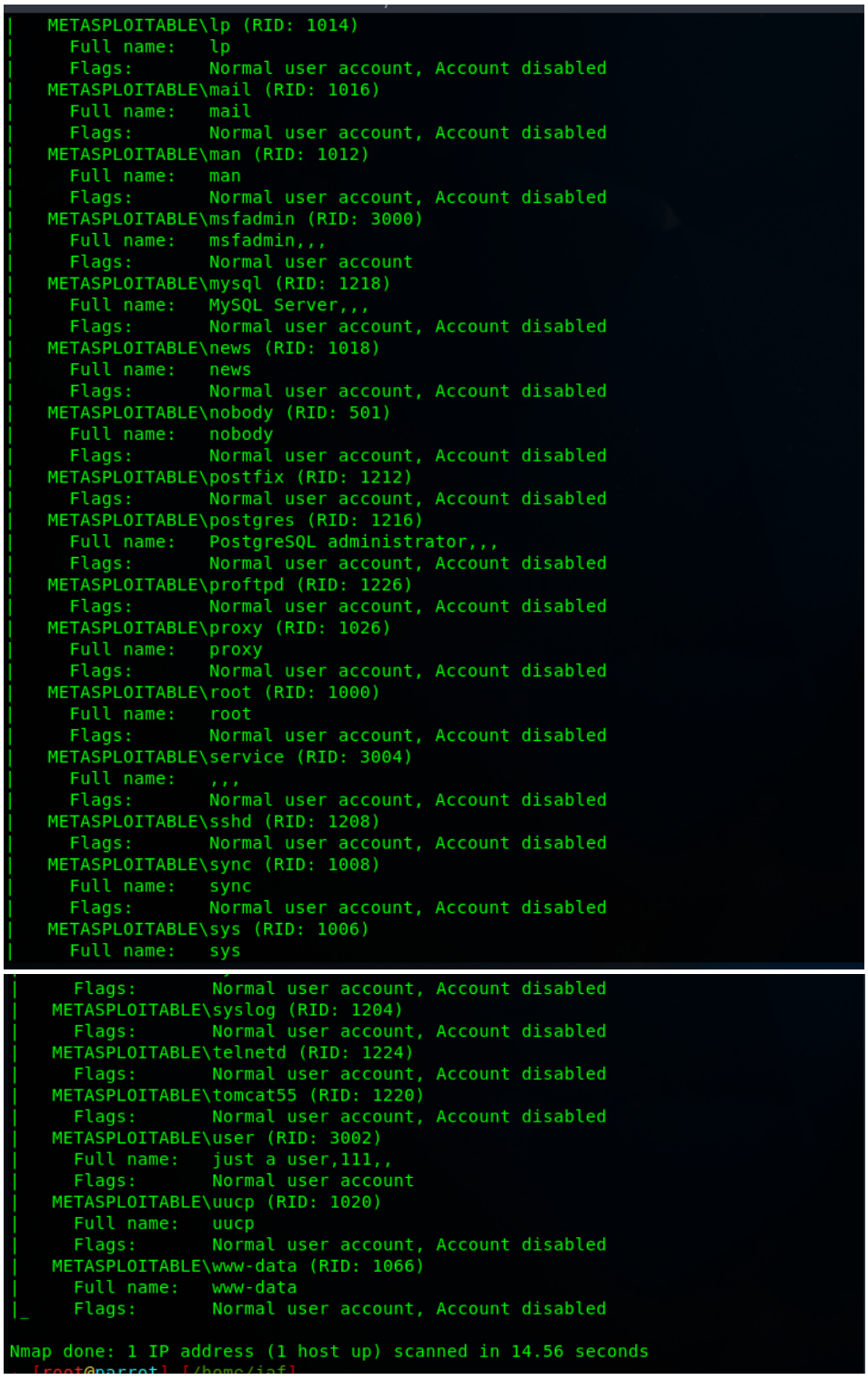
ENUMERACIÓN DE USUARIOS CON NMAP

Para enumerar las cuentas de usuario disponibles en la máquina objetivo, utilizaremos el siguiente script de Nmap: smb-enum-users. Podemos ejecutar el script NMap utilizando el siguiente comando:

```
nmap -script smb-enum-users.nse -p 445 [host de destino]
```

La salida del script es una larga lista de usuarios disponibles en el host:





Como se puede ver hay un montón de nombres de usuario en la máquina Metasploitable 2. Entre ellos hay un montón de cuentas de servicio y la cuenta de administrador que se llama msfadmin. Veamos el segundo método para recuperar una lista de cuentas de usuario del servidor Metasploitable 2 utilizando una sesión nula en el servidor Samba.

ENUMERACIÓN CON ENUM4LINUX

Enum4linux se utiliza para enumerar hosts Windows y Samba y está escrito en Perl. La herramienta es básicamente una envoltura para smbclient, rpcclient, net y nmblookup. Echemos un vistazo a cómo usar

enum4linux y ejecutarlo en Metasploitable 2. A continuación se muestran las opciones más comunes utilizadas en enum4linux. Para obtener una visión general de las diferentes opciones utilice la bandera -help.

```
Uso: ./enum4linux.pl [opciones]ip
```

-U obtener lista de usuarios

-M lista de máquinas

-S obtener lista compartida

-P obtener información de la política de contraseñas

-G lista de grupos y miembros

-d detallado, se aplica a -U y -S

-u user especifica el nombre de usuario a utilizar (por defecto "")

-p pass especificar la contraseña a utilizar (por defecto "")

-a Hacer todas las enumeraciones simples (-U -S -G -P -r -o -n -i).

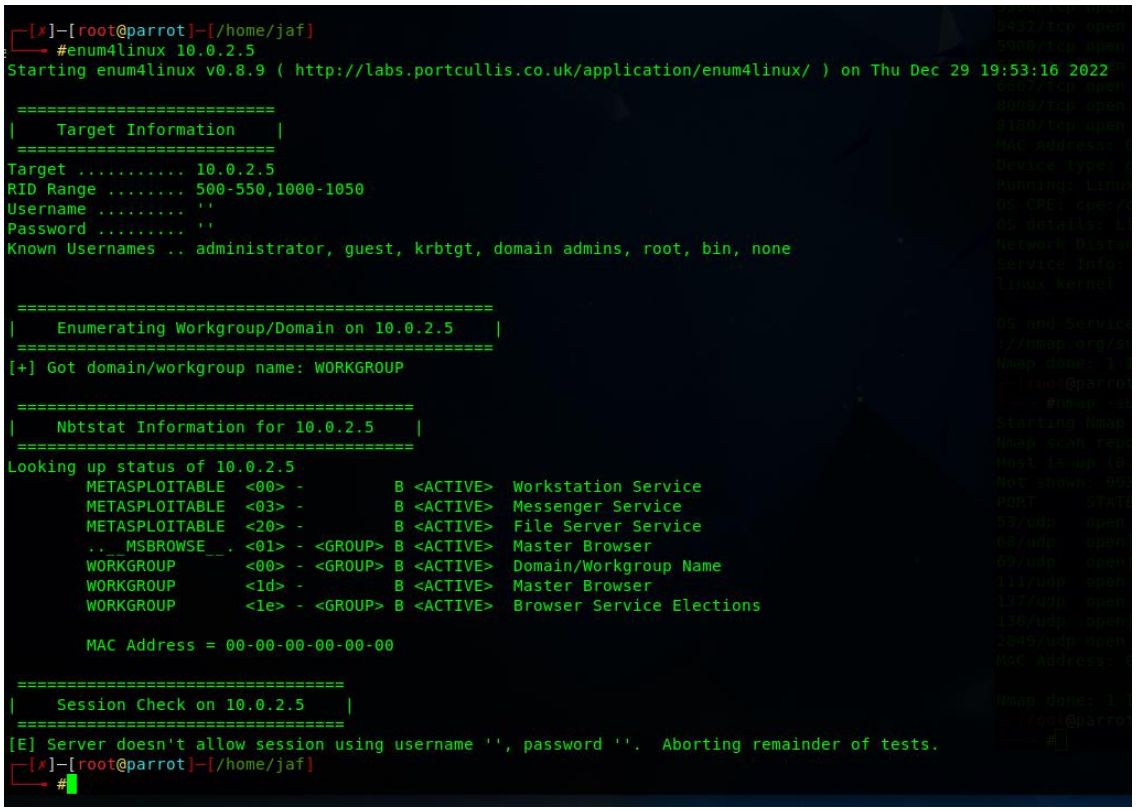
-o Obtener información del sistema operativo

-i Obtener información de la impresora

Vamos a ejecutar enum4linux en Metasploitable 2 con todas las opciones usando el siguiente comando:

```
enum4linux 10.0.2.5
```

Después de que enum4linux haya terminado nos devuelve un montón de información útil. Tenemos una visión general de los recursos compartidos disponibles en nuestro host de destino:



Y también una visión general de los usuarios disponibles.

Y información sobre el sistema operativo.

Hasta ahora hemos recopilado información sobre el sistema operativo, las cuentas de usuario, los puertos abiertos y los servicios en ejecución con los números de versión en este tutorial de enumeración de Metasploitable 2. También hemos recopilado información sobre la política de contraseñas (no hay ninguna) lo que plantea dudas sobre la fortaleza de las contraseñas utilizadas que investigaremos durante la fase de explotación. Hemos utilizado herramientas como Nmap, rpcclient y enum4linux para recopilar toda esta información.