

Servicios de enumeración en una máquina de destino

La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos compartidos de recursos de red y servicios de un sistema.

Objetivos del laboratorio

El objetivo de este laboratorio es ayudar a los estudiantes a comprender y realizar la enumeración en una red objetivo utilizando diversas técnicas para:

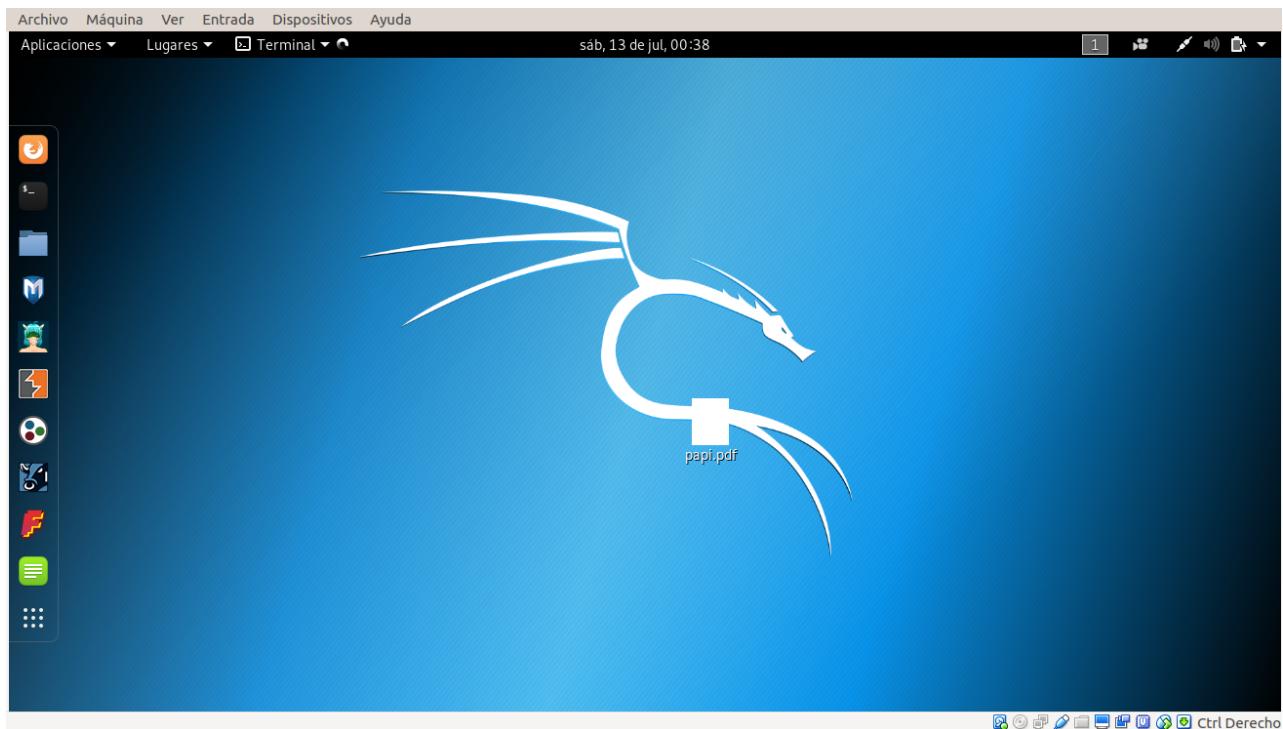
- Escanee todas las máquinas en una red dada o una subred
- Lista de máquinas que están en funcionamiento
- Determine los puertos abiertos en un nodo dado
- encontrar si alguno de los puertos tiene restricción de firewall
- Enumere todos los servicios que se ejecutan en el puerto junto con sus respectivas versiones.

Resumen de Enumeracion

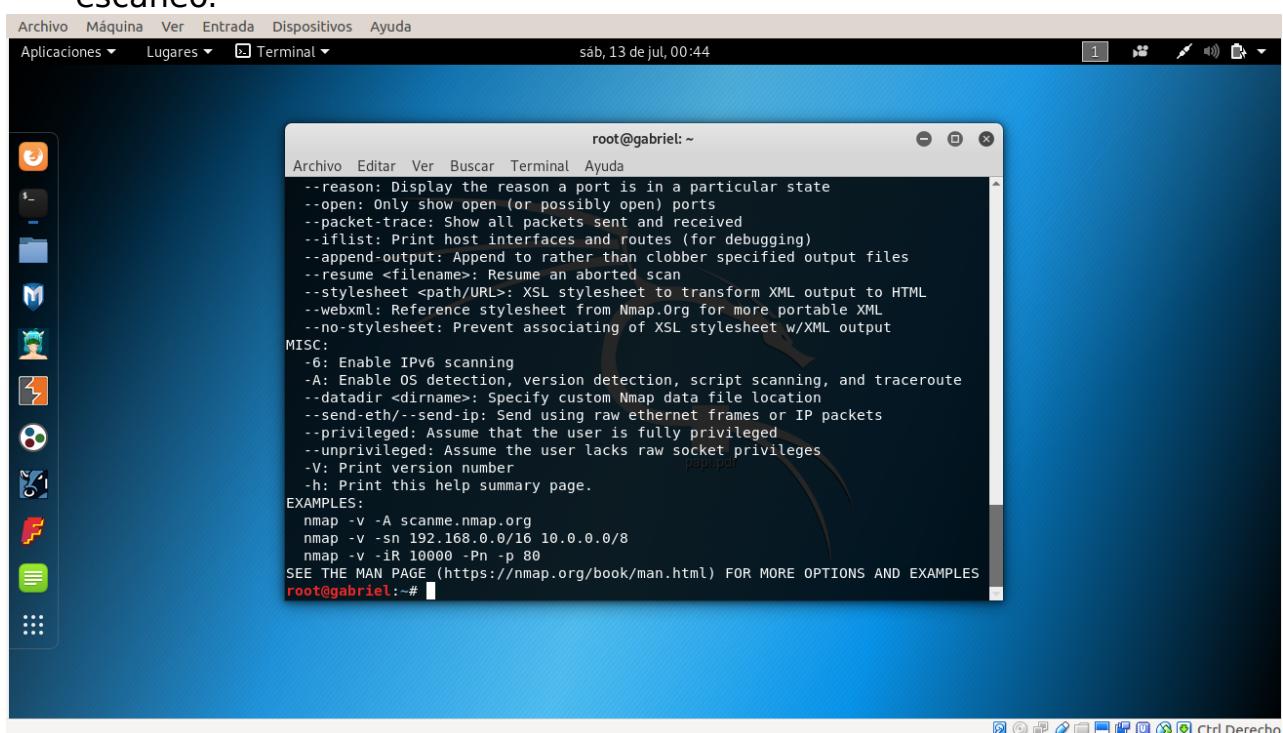
La enumeración es el proceso de extracción de nombres de usuarios, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema. Las técnicas de enumeración se realizan en un entorno de intranet.

Tareas del laboratorio

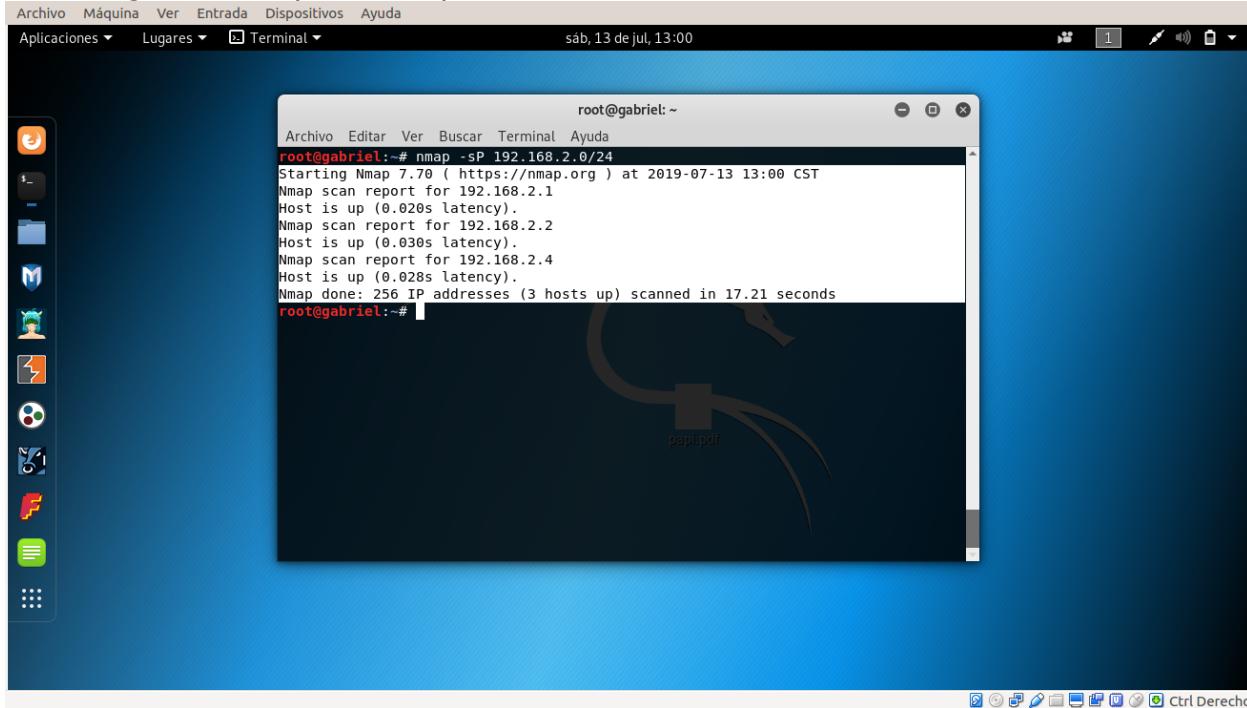
1. Inicie la máquina virtual Kali Linux desde el Administrador de Hyper-V e inicie sesión en ella.
2. Aparece el escritorio de la máquina Kali Linux, como se muestra en la siguiente captura de pantalla.



3. Seleccione **Aplicaciones -> Kali Linux -> Las 10 herramientas de seguridad principales -> nmap**. Esto lanza la aplicación nmap.
4. La aplicación Nmap aparece en un terminal de línea de comando, mostrando todos los interruptores, que pueden usarse para realizar el escaneo.



- Escriba **nmap -sP 192.168.2.0/24** y presione **Enter** para iniciar la exploración de barrido de ping.
- Nmap escanea todos los nodos en el rango de red dado y comienza a mostrar todos los hosts que están en funcionamiento junto con su respectiva dirección MAC e información del dispositivo, como se muestra en la siguiente captura de pantalla:



The screenshot shows a Linux desktop environment with a blue theme. A terminal window is open in the center, displaying the output of an Nmap scan. The command entered was `nmap -sP 192.168.2.0/24`. The output shows that three hosts are up: 192.168.2.1, 192.168.2.2, and 192.168.2.4. The scan took 17.21 seconds. The desktop interface includes a dock with various icons on the left and a taskbar at the bottom.

```
root@gabriel:~# nmap -sP 192.168.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-13 13:00 CST
Nmap scan report for 192.168.2.1
Host is up (0.020s latency).
Nmap scan report for 192.168.2.2
Host is up (0.030s latency).
Nmap scan report for 192.168.2.4
Host is up (0.028s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 17.21 seconds
root@gabriel:~#
```

- El escaneo puede tomar comparativamente más tiempo para completar. Después de obtener la cantidad suficiente de máquinas en el resultado del escaneo, puede terminar el escaneo presionando **Ctrl + C**.
- Ahora, elija una dirección IP del resultado del escaneo y realice un escaneo **sincronizado de sincronización**. Para hacerlo, escriba **nmpa -ss 192.168.2.2** y presione **Entrar**. La dirección IP utilizada en este laboratorio es **192.168.2.2** y esta dirección pertenece a Windows Server 2016.
- Al emitir el comando, se iniciará un análisis de sincronización silencioso.
- Nmap realiza un análisis oculto de sincronización y enumera todos los puertos abiertos que se ejecutan en el servidor de Windows 2016 Máquina, como se muestra en la captura de pantalla.

```
root@gabriel:~# nmap -sS 192.168.2.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-13 13:38 CST
Nmap scan report for 192.168.2.2
Host is up (0.055s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
root@gabriel:~#
```

11. Ahora que hemos obtenido todos los puertos abiertos, junto con los servicios que se ejecutan en ellos, intentaremos determinar / enumerar las versiones de cada uno de los servicios que se ejecutan en los puertos realizando una exploración de sincronización con el interruptor de detección de versión habilitado.
12. Para enumerar la versión de los servicios obtenidos, escriba el comando **nmap -sSV -O 192.168.2.2** y presione **Entrar**. La dirección IP utilizada en este laboratorio es **192.168.2.2**, y esta dirección pertenece a **Windows Server 2016**.
13. Al emitir este comando, se iniciará un análisis de sincronización silencioso con detección de versión junto con detección de SO.
14. Nmap realiza la exploración y muestra las versiones de los servicios, junto con una huella digital del sistema operativo, como se muestra en la captura de pantalla.

Archivo Máquina Ver Entrada Dispositivos Ayuda

Aplicaciones ▾ Lugares ▾ Terminal ▾

sáb, 13 de jul, 13:49

root@gabriel: ~

Archivo Editar Ver Buscar Terminal Ayuda

```
root@gabriel:~# nmap -sSV -O 192.168.2.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-13 13:45 CST
Nmap scan report for 192.168.2.2
Host is up (0.036s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
80/tcp    open  http         Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-07-13 19:45:44Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows NetBIOS-SSN
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WS20160)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=7/13%T=5D2A34EC%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"%0\x1e\%0\x06\x81\%0\x01\%0\%0\%0\x07%version\
SF:\x04bind\%0\x10\%0\x03";
Aggressive OS guesses: Microsoft Windows Server 2016 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft Windows 10 1511 (95%), Microsoft Windows Vista Home Premium SP1, Windows 7, or Windows Server 2008 (92%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (90%), Microsoft Windows Server 2012 or Server 2012 R2 (89%), Microsoft Windows 7 SP1 (88%), Microsoft Windows 8 (88%), Microsoft Windows 10 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: WS2016; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.24 seconds
```

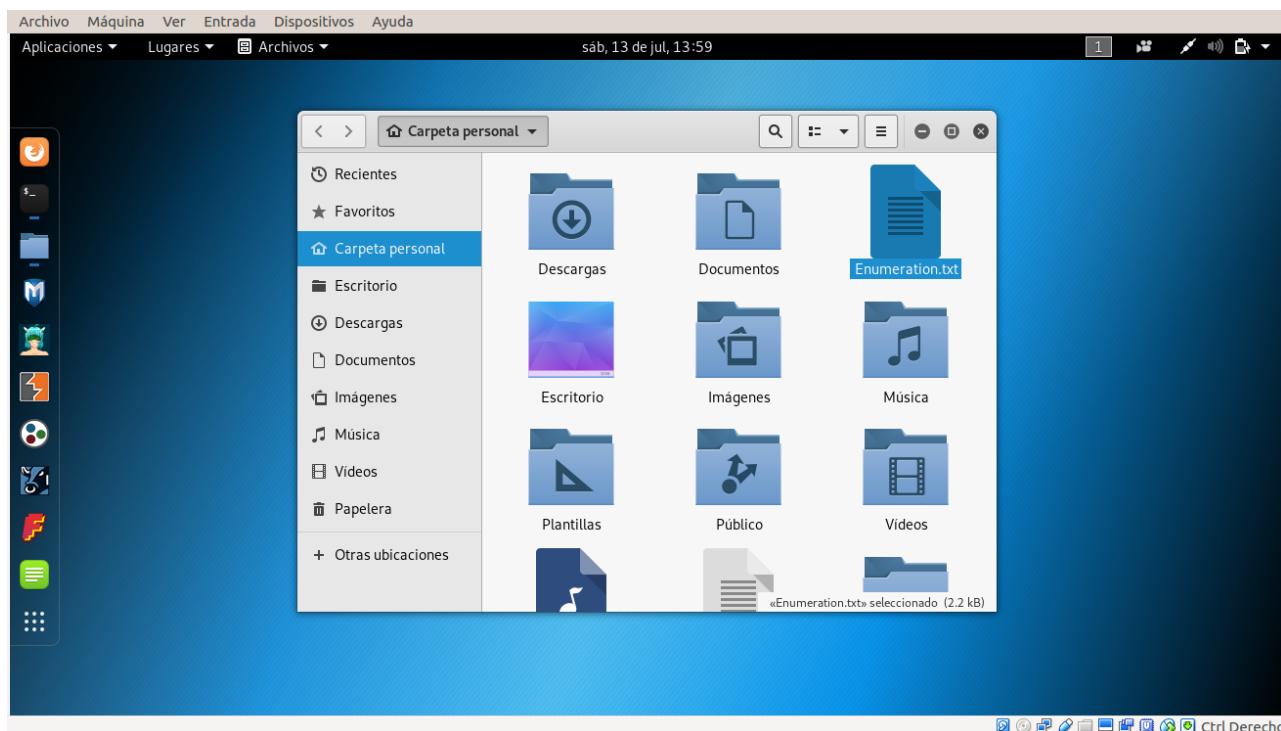
15. Ahora que ha obtenido el resultado enumerado, puede guardar este resultado de escaneo para futuras referencias.

16. Escriba **nmap -sSV -O 192.168.2.2 -oN Enumeration.txt** y presione Entrar.

17. Este comando realiza el **Stealthy Syn Scan** con **detección de versión** y **detección de SO** y guarda el resultado en el directorio de inicio (raíz) con el nombre Enumeration.txt

18. Al finalizar el laboratorio, vaya a **Lugares -> Carpeta de inicio**.

19. Aparece la carpeta de inicio, que muestra el archivo **Enumeration.txt** guardado. En su lugar, puede hacer doble clic en el archivo para ver el mismo resultado.

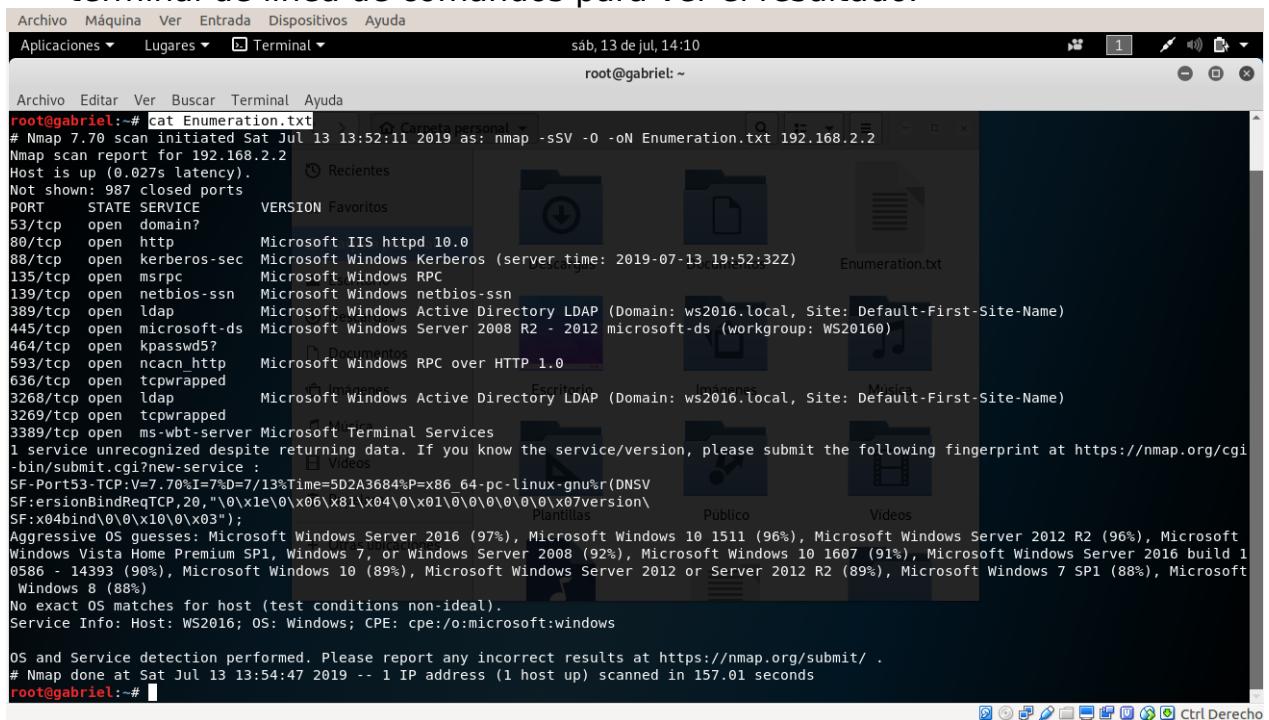


20. El resultado del escaneo aparece en un archivo de texto, como se muestra en la siguiente captura de pantalla.

```
# Nmap 7.70 scan initiated Sat Jul 13 13:52:11 2019 as: nmap -sSV -O -oN Enumeration.txt 192.168.2.2
Nmap scan report for 192.168.2.2
Host is up (0.0275 latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
53/tcp      open  domain?
80/tcp      open  http        Microsoft IIS httpd 10.0
88/tcp      open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-07-13 19:52:32Z)
135/tcp     open  msrpc       Microsoft Windows RPC
139/tcp     open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp     open  ldap        Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
445/tcp     open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WS20160)
464/tcp     open  kpasswd5?
593/tcp     open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp     open  tcpwrapped
3268/tcp    open  ldap        Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
3269/tcp    open  tcpwrapped
3389/tcp    open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=7/13%T=5D2A3684%P=x86_64-pc-linux-gnu%R%DNSV
SF:versionBindReqTCP,20,"0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\x07%version\
SF:x04bind\0\0\x10\0\x03";
Aggressive OS guesses: Microsoft Windows Server 2016 (97%), Microsoft Windows 10 1511 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft Windows Vista Home Premium SP1, Windows 7, or Windows Server 2008 (92%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (90%), Microsoft Windows 10 (89%), Microsoft Windows Server 2012 or Server 2012 R2 (89%), Microsoft Windows 7 SP1 (88%), Microsoft Windows 8 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: WS2016; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 13 13:54:47 2019 -- 1 IP address (1 host up) scanned in 157.01 seconds
```

21. Alternativamente, puede emitir el comando cat Enumeration.txt en un terminal de línea de comandos para ver el resultado.



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and it displays the command "root@gabriel:~# cat Enumeration.txt". The output of the command is a detailed report from the Nmap 7.70 scan. It lists various ports and services found on the host 192.168.2.2, including Microsoft IIS, Microsoft Windows Kerberos, Microsoft Windows RPC, Microsoft Windows netbios-ssn, Microsoft Windows Active Directory LDAP, Microsoft Windows Server 2008 R2, and Microsoft Windows Terminal Services. The report also includes OS fingerprinting results, suggesting Microsoft Windows Server 2016 as the most likely OS. The desktop background shows a dark-themed file manager window with icons for documents, images, videos, and music.

```
# Nmap 7.70 scan initiated Sat Jul 13 13:52:11 2019 as: nmap -sSV -O -oN Enumeration.txt 192.168.2.2
Nmap scan report for 192.168.2.2
Host is up (0.027s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
80/tcp    open  http         Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-07-13 19:52:32Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WS20160)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: ws2016.local, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=7/13%Time=5D2A3684%P=x86_64-pc-linux-gnu%R(DNSV
SF:ersionBindReqTCP,20,""\0\x1e\0\x6\0\x81\0\x04\0\x01\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03";
Aggressive OS guesses: Microsoft Windows Server 2016 (97%), Microsoft Windows 10 1511 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft Windows Vista Home Premium SP1, Windows 7 or Windows Server 2008 (92%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2016 build 1 0586 - 14393 (90%), Microsoft Windows 10 (89%), Microsoft Windows Server 2012 or Server 2012 R2 (89%), Microsoft Windows 7 SP1 (88%), Microsoft Windows 8 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: WS2016; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 13 13:54:47 2019 -- 1 IP address (1 host up) scanned in 157.01 seconds
root@gabriel:~#
```

Al realizar la enumeración de servicios, un atacante podría intentar encontrar una vulnerabilidad asociada con esa aplicación en particular y explotarla para obtener acceso a la máquina de destino.