Ej: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <nombre de archivo de entrada>: Entrada de la lista de hosts/redes

-iR <num hosts>: elige objetivos aleatorios

--exclude <host1[,host2][,host3],...>: Excluir hosts/redes

--excludefile <exclude\_file>: Excluir lista del archivo

DESCUBRIMIENTO DEL ANFITRIÓN:

-sL: Escaneo de lista: simplemente enumera los objetivos para escanear

-sn: Ping Scan - deshabilitar el escaneo de puertos

-Pn: Trata a todos los hosts como si estuvieran en línea - omite el descubrimiento de hosts

-PS/PA/PU/PY[lista de puertos]: descubrimiento TCP SYN/ACK, UDP o SCTP en puertos determinados

-PE/PP/PM: sondas de descubrimiento de solicitudes de eco, marca de tiempo y máscara de red ICMP

-PO[lista de protocolos]: Ping de protocolo IP

-n/-R: Nunca resolver DNS/Resolver siempre [predeterminado: a veces]

--dns-servers <serv1[,serv2],...>: Especifica servidores DNS personalizados

--system-dns: utiliza el solucionador de DNS del sistema operativo

--traceroute: rastrea la ruta del salto a cada host

TÉCNICAS DE ESCANEO:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon explora

-sU: Escaneo UDP

-sN/sF/sX: escaneos TCP nulos, FIN y Navidad

--scanflags <flags>: personaliza los indicadores de escaneo TCP

-sI <host zombie[:probeport]>: escaneo inactivo

-sY/sZ: escaneos SCTP INIT/COOKIE-ECHO

-sO: escaneo de protocolo IP

-b <host de retransmisión FTP>: escaneo de rebote FTP

ESPECIFICACIÓN DEL PUERTO Y ORDEN DE ESCANEO:

-p <rangos de puertos>: solo escanea los puertos especificados

Ej: -p22; -p1-65535; -pU:53,111,137,T:21-25,80,139,8080,S:9

--exclude-ports <rangos de puertos>: excluye los puertos especificados del escaneo

-F: Modo rápido: escanea menos puertos que el escaneo predeterminado

-r: escanea puertos secuencialmente, no aleatorizar

--top-ports <número>: escanea <número> puertos más comunes

--port-ratio <ratio>: escanea puertos más comunes que <ratio>

DETECCIÓN DE SERVICIO/VERSIÓN:

-sV: Sondear puertos abiertos para determinar información de servicio/versión

--version-intensity <nivel>: Establecer de 0 (ligero) a 9 (pruebe todas las sondas)

--version-light: Limitar a las sondas más probables (intensidad 2)

--version-all: Pruebe cada sonda (intensidad 9)

--version-trace: muestra la actividad de escaneo de versiones detallada (para depuración)

ESCANEO DEL GUIÓN:

-sC: equivalente a --script=predeterminado

--script=<scripts Lua>: <scripts Lua> es una lista separada por comas de

directorios, archivos de script o categorías de script

--script-args=<n1=v1,[n2=v2,...]>: proporciona argumentos a los scripts

--script-args-file=nombre de archivo: proporciona argumentos de script NSE en un archivo

--script-trace: muestra todos los datos enviados y recibidos

--script-updatedb: actualiza la base de datos del script.

--script-help=<scripts de Lua>: muestra ayuda sobre los scripts.

<Lua scripts> es una lista de archivos de script separados por comas o

categorías de script.

DETECCIÓN DEL SO:

-O: Habilitar la detección del sistema operativo

--osscan-limit: limita la detección del sistema operativo a objetivos prometedores

--osscan-guess: Adivina el sistema operativo de forma más agresiva

TIEMPO Y RENDIMIENTO:

Las opciones que toman <tiempo> están en segundos o agregan 'ms' (milisegundos),

's' (segundos), 'm' (minutos) o 'h' (horas) al valor (por ejemplo, 30 m).

-T<0-5>: Establecer plantilla de tiempo (cuanto más alto, más rápido)

--min-hostgroup/max-hostgroup <tamaño>: tamaños de grupos de exploración de hosts paralelos

--min-parallelism/max-parallelism <numprobes>: paralelización de sondas

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <tiempo>: Especifica

Tiempo de ida y vuelta de la sonda.

--max-retries <tries>: Limita el número de retransmisiones de sondas de escaneo de puertos.

--host-timeout <tiempo>: Renuncia al objetivo después de tanto tiempo

--scan-delay/--max-scan-delay <tiempo>: Ajusta el retraso entre sondas

--min-rate <número>: envía paquetes a una velocidad no inferior a <número> por segundo

--max-rate <número>: envía paquetes a una velocidad no superior a <número> por segundo

EVASIÓN Y SPOOFING DE FIREWALL/IDS:

-F; --mtu <val>: fragmenta paquetes (opcionalmente con MTU dada)

-D <decoy1,decoy2[,ME],...>: Ocultar un escaneo con señuelos

-S <Dirección\_IP>: Dirección de origen falsa

-e <iface>: utiliza la interfaz especificada

-g/--source-port <portnum>: utilizar el número de puerto dado

--proxies <url1,[url2],...>: Retransmite conexiones a través de proxies HTTP/SOCKS4

--data <cadena hexadecimal>: agrega una carga útil personalizada a los paquetes enviados

--data-string <cadena>: agrega una cadena ASCII personalizada a los paquetes enviados

--data-length <num>: agrega datos aleatorios a los paquetes enviados

--ip-options <opciones>: envía paquetes con opciones de IP especificadas

--ttl <val>: establece el campo de tiempo de vida de IP

--spoof-mac <dirección mac/prefijo/nombre del proveedor>: falsifica tu dirección MAC

--badsum: envía paquetes con una suma de comprobación TCP/UDP/SCTP falsa

PRODUCCIÓN:

-oN/-oX/-oS/-oG <archivo>: Escaneo de salida en normal, XML, s|<rIpt kIddi3,

y formato Grepable, respectivamente, al nombre de archivo dado.

-oA <nombre base>: Salida en los tres formatos principales a la vez

-v: aumenta el nivel de detalle (use -vv o más para un mayor efecto)

-d: aumenta el nivel de depuración (use -dd o más para un mayor efecto)

--reason: muestra el motivo por el que un puerto se encuentra en un estado particular

--open: solo muestra puertos abiertos (o posiblemente abiertos)

--packet-trace: muestra todos los paquetes enviados y recibidos

--iflist: imprime rutas e interfaces de host (para depuración)

--append-output: Agregar a archivos de salida especificados en lugar de bloquearlos

--resume <nombre de archivo>: reanudar un análisis cancelado

--noninteractive: deshabilita las interacciones en tiempo de ejecución mediante keyb

tabla

--stylesheet <ruta/URL>: hoja de estilo XSL para transformar la salida XML a HTML

--webxml: hoja de estilo de referencia de Nmap.Org para XML más portátil

--no-stylesheet: Evita la asociación de hojas de estilos XSL con salida XML

MISC:

-6: Habilitar escaneo IPv6

-A: habilitar la detección de sistema operativo, detección de versión, escaneo de scripts y traceroute

--datadir <dirname>: especifica la ubicación del archivo de datos Nmap personalizado

--send-eth/--send-ip: envío utilizando tramas Ethernet sin formato o paquetes IP

--privileged: asume que el usuario tiene todos los privilegios

--unprivileged: se supone que el usuario carece de privilegios de socket sin formato

-V: número de versión de impresión

-h: imprime esta página de resumen de ayuda.

EJEMPLOS:

nmap -v -A scanme.nmap.org

nmap -v -sn 192.168.0.0/16 10.0.0.0/8

nmap -v -iR 10000 -Pn -p 80

CONSULTE LA PÁGINA MAN (https://nmap.org/book/man.html) PARA OBTENER MÁS OPCIONES Y EJEMPLOS

Lista de todas las opciones de nmap

Nmap es una poderosa herramienta de código abierto para el escaneo de redes y la auditoría de seguridad. Aquí están algunas de las opciones más comunes de Nmap junto con sus descripciones:

1. \*\*-sS (TCP SYN scan)\*\*: Este escaneo envía un paquete SYN TCP al puerto de destino. Si se recibe un paquete SYN/ACK de respuesta, indica que el puerto está abierto. Si se recibe un RST/ACK, indica que el puerto está cerrado.

2. \*\*-sT (TCP connect scan)\*\*: Este escaneo realiza una conexión TCP completa con el puerto de destino. Si se establece la conexión, el puerto está abierto. Sin embargo, este método es más fácil de detectar que otros escaneos.

3. \*\*-sU (UDP scan)\*\*: Escanea los puertos UDP para determinar si están abiertos, cerrados o filtrados. Este tipo de escaneo es más lento y menos confiable debido a la naturaleza no orientada a la conexión de UDP.

4. \*\*-sN, -sF, -sX (NULL, FIN, Xmas scan)\*\*: Estos escaneos envían paquetes TCP con los bits de control NULL, FIN o URG activados. Se utilizan para eludir ciertos tipos de firewalls y sistemas de detección de intrusos.

5. \*\*-sA (ACK scan)\*\*: Este escaneo envía un paquete ACK TCP al puerto de destino. Se utiliza para determinar si un firewall está filtrando los paquetes de retorno.

6. \*\*-sV (Service Version Detection)\*\*: Intenta determinar la versión y el servicio de los servicios en los puertos abiertos.

7. \*\*-O (OS detection)\*\*: Intenta determinar el sistema operativo del host objetivo basándose en las respuestas del escaneo.

8. \*\*-p (Port specification)\*\*: Permite especificar los puertos a escanear. Puede ser un solo puerto, un rango de puertos o una lista separada por comas.

9. \*\*-A (Aggressive scan)\*\*: Activa un conjunto de opciones que incluyen detección de sistemas operativos, detección de servicios y scripts de secuencias de comandos integrados.

10. \*\*-T (Timing Template)\*\*: Controla el tiempo de espera y el tiempo de respuesta de los escaneos. Los valores van de 0 (paranoico) a 5 (insensato).

11. \*\*--script (Script scanning)\*\*: Permite ejecutar scripts Nmap sobre los puertos de destino. Estos scripts pueden realizar tareas como detectar vulnerabilidades o recopilar información adicional.

12. \*\*-oA (Output to All Formats)\*\*: Guarda los resultados del escaneo en tres formatos diferentes: XML, formato greppable y formato normal.

Claro, aquí tienes algunas opciones adicionales de Nmap junto con sus descripciones:

13. \*\*-v (Verbose mode)\*\*: Activa el modo detallado, que muestra información adicional durante el escaneo, como cada paso que realiza Nmap y más detalles sobre los puertos y servicios detectados.

14. \*\*-vv (Very verbose mode)\*\*: Activa un modo aún más detallado que el modo verbose normal. Proporciona una salida aún más exhaustiva con información detallada sobre el progreso del escaneo.

15. \*\*-Pn (No ping)\*\*: Omite la fase de detección de hosts activos, lo que puede ser útil cuando se sabe que los hosts objetivo no responden a los paquetes de ping.

16. \*\*-iL (Input from list)\*\*: Permite especificar un archivo que contiene una lista de direcciones IP o nombres de host para escanear. Útil para realizar escaneos en múltiples objetivos de forma simultánea.

17. \*\*-oN (Normal output)\*\*: Guarda los resultados del escaneo en un formato normal para su visualización posterior. Este formato es fácilmente legible por humanos.

18. \*\*-oX (XML output)\*\*: Guarda los resultados del escaneo en formato XML, lo que facilita su procesamiento posterior por parte de herramientas de análisis.

19. \*\*-oG (Grepable output)\*\*: Guarda los resultados del escaneo en un formato greppable, que puede ser fácilmente analizado por herramientas de filtrado y búsqueda como grep.

20. \*\*-D (Decoy scan)\*\*: Especifica direcciones IP adicionales para incluir en el escaneo como señuelos (decoys), lo que puede ayudar a ocultar la identidad del escáner y confundir al objetivo.

21. \*\*--randomize-hosts (Randomize target hosts)\*\*: Escanea los objetivos en un orden aleatorio, lo que puede ayudar a evitar la detección y el bloqueo por parte de sistemas de defensa de red.

22. \*\*-S (Spoof source address)\*\*: Especifica una dirección IP de origen falsificada para usar en el escaneo. Puede ayudar a ocultar la identidad del escáner.

23. \*\*--badsum (Bad checksum)\*\*: Envía paquetes con sumas de comprobación incorrectas. Puede ser útil para evadir algunos tipos de firewalls y sistemas de detección de intrusiones.

24. \*\*-f (Fragment packets)\*\*: Divide los paquetes de escaneo en fragmentos más pequeños, lo que puede ayudar a evitar la detección por parte de algunos dispositivos de seguridad.

25. \*\*--reason (Host and port state reasons)\*\*: Proporciona información adicional sobre el estado de los hosts y puertos, incluidas las razones por las que se determinó que estaban abiertos, cerrados o filtrados.

Por supuesto, aquí tienes más opciones de Nmap junto con sus descripciones:

26. \*\*--open (Show only open ports)\*\*: Muestra solo los puertos que se determinan como abiertos durante el escaneo, ignorando los puertos cerrados o filtrados.

27. \*\*--max-retries (Set maximum retries)\*\*: Especifica el número máximo de reintentos que Nmap realizará cuando no recibe una respuesta del host objetivo.

28. \*\*--scan-delay (Set scan delay)\*\*: Establece un retraso entre los paquetes de escaneo enviados, lo que puede ayudar a evitar la detección por parte de sistemas de prevención de intrusiones (IPS) o sistemas de detección de intrusiones (IDS).

29. \*\*--max-rate (Set maximum scan rate)\*\*: Limita la velocidad de escaneo máxima, controlando el número de paquetes enviados por segundo. Puede ser útil para reducir el impacto en la red y evitar la detección.

30. \*\*--script (Script execution)\*\*: Ejecuta scripts Nmap específicos durante el escaneo para realizar tareas como detección de vulnerabilidades, enumeración de servicios o recopilación de información adicional.

31. \*\*--script-args (Script arguments)\*\*: Permite especificar argumentos adicionales para los scripts Nmap que se ejecutan durante el escaneo.

32. \*\*--traceroute (Perform traceroute)\*\*: Realiza un traceroute al host objetivo antes de iniciar el escaneo, mostrando la ruta que los paquetes de escaneo seguirán a través de la red.

33. \*\*--spoof-mac (Spoof MAC address)\*\*: Especifica una dirección MAC falsificada para usar en el escaneo. Puede ayudar a ocultar la identidad del escáner.

34. \*\*--source-port (Specify source port)\*\*: Especifica el puerto de origen a utilizar en los paquetes de escaneo. Puede ser útil para eludir ciertos tipos de firewalls.

35. \*\*--data-length (Append random data)\*\*: Agrega datos aleatorios a los paquetes de escaneo para intentar evadir la detección por parte de sistemas de defensa de red.

36. \*\*--send-eth (Send Ethernet frame)\*\*: Envía paquetes de escaneo directamente en el nivel Ethernet en lugar de a través de IP. Puede ser útil para escanear redes locales.

37. \*\*--append-output (Append to output file)\*\*: Agrega los resultados del escaneo a un archivo de salida existente en lugar de sobrescribirlo.

38. \*\*--exclude (Exclude hosts/networks)\*\*: Excluye hosts o redes específicas del escaneo, lo que puede ser útil para evitar escanear áreas sensibles o no deseadas.

39. \*\*--iflist (List interfaces and routes)\*\*: Muestra una lista de interfaces de red disponibles y sus configuraciones, así como las tablas de enrutamiento del sistema.

Por supuesto, aquí tienes más opciones de Nmap junto con sus descripciones:

40. \*\*--ip-options (Set IP options)\*\*: Permite especificar opciones personalizadas de IP para incluir en los paquetes de escaneo, como el tipo de servicio o el tiempo de vida (TTL).

41. \*\*--ttl (Set time-to-live)\*\*: Especifica el TTL (Tiempo de Vida) a utilizar en los paquetes de escaneo. Puede ser útil para simular el tráfico desde diferentes tipos de dispositivos o sistemas operativos.

42. \*\*--mtu (Set MTU value)\*\*: Especifica el valor del MTU (Unidad de Transmisión Máxima) a utilizar en los paquetes de escaneo. Puede ser útil para probar la fragmentación de paquetes y la capacidad de los dispositivos de red para manejar diferentes tamaños de paquetes.

43. \*\*--reason (Host and port state reasons)\*\*: Proporciona información adicional sobre el estado de los hosts y puertos, incluidas las razones por las que se determinó que estaban abiertos, cerrados o filtrados.

44. \*\*--packet-trace (Trace packets)\*\*: Muestra una traza detallada de los paquetes de escaneo enviados y recibidos, lo que puede ser útil para depurar problemas de conectividad o entender cómo funciona el escaneo.

45. \*\*--scanflags (Custom TCP scan flags)\*\*: Permite especificar banderas TCP personalizadas para incluir en los paquetes de escaneo, lo que puede ser útil para pruebas avanzadas de seguridad de red.

46. \*\*--badsum (Bad checksum)\*\*: Envía paquetes con sumas de comprobación incorrectas. Puede ser útil para evadir algunos tipos de firewalls y sistemas de detección de intrusiones.

47. \*\*--ttl (Set time-to-live)\*\*: Especifica el TTL (Tiempo de Vida) a utilizar en los paquetes de escaneo. Puede ser útil para simular el tráfico desde diferentes tipos de dispositivos o sistemas operativos.

48. \*\*--dns-servers (Set custom DNS servers)\*\*: Especifica servidores DNS personalizados a utilizar para la resolución de nombres durante el escaneo.

49. \*\*--script-updatedb (Update script database)\*\*: Actualiza la base de datos de scripts Nmap a la última versión disponible.

50. \*\*--exclude-ports (Exclude ports)\*\*: Excluye puertos específicos del escaneo, lo que puede ser útil para enfocar el escaneo en rangos específicos de puertos.

Mis disculpas por la repetición. Continuemos desde donde nos quedamos:

91. \*\*--excludefile (Exclude hosts/networks file)\*\*: Especifica un archivo que contiene una lista de hosts o redes para excluir del escaneo.

92. \*\*--datadir (Custom data directory)\*\*: Especifica un directorio personalizado donde Nmap buscará scripts, bases de datos y otros archivos necesarios.

93. \*\*--dns-servers (Set custom DNS servers)\*\*: Especifica servidores DNS personalizados a utilizar para la resolución de nombres durante el escaneo.

94. \*\*--script-updatedb (Update script database)\*\*: Actualiza la base de datos de scripts Nmap a la última versión disponible.

95. \*\*--exclude-ports (Exclude ports)\*\*: Excluye puertos específicos del escaneo, lo que puede ser útil para enfocar el escaneo en rangos específicos de puertos.

96. \*\*--randomize-hosts (Randomize target hosts)\*\*: Escanea los objetivos en un orden aleatorio, lo que puede ayudar a evitar la detección y el bloqueo por parte de sistemas de defensa de red.

97. \*\*--spoof-mac (Spoof MAC address)\*\*: Especifica una dirección MAC falsificada para usar en el escaneo. Puede ayudar a ocultar la identidad del escáner.

98. \*\*--source-port (Specify source port)\*\*: Especifica el puerto de origen a utilizar en los paquetes de escaneo. Puede ser útil para eludir ciertos tipos de firewalls.

99. \*\*--data-length (Append random data)\*\*: Agrega datos aleatorios a los paquetes de escaneo para intentar evadir la detección por parte de sistemas de defensa de red.

100. \*\*--send-eth (Send Ethernet frame)\*\*: Envía paquetes de escaneo directamente en el nivel Ethernet en lugar de a través de IP. Puede ser útil para escanear redes locales.

Espero que esta continuación sea útil. Si tienes más preguntas o necesitas más detalles sobre alguna opción específica, no dudes en preguntar. Estoy aquí para ayudar.

-----------------------------------------------------------------------------------------------------------------

**🔍 1. Escaneo con Scripts de Enumeración (RPC y SMB)**

**📌 Enumerar información de RPC**

bash

CopiarEditar

nmap --script=rpcinfo -p 135 192.168.0.8

**Explicación:**

* Muestra los servicios RPC disponibles en la máquina.
* Indica los programas y versiones de RPC activos en el puerto **135**.

**📌 Enumerar usuarios de SMB**

bash

CopiarEditar

nmap --script=smb-enum-users -p 445 192.168.0.8

**Explicación:**

* Lista los usuarios locales y del dominio en un sistema Windows.
* Requiere acceso anónimo o credenciales válidas.

**📌 Listar recursos compartidos de SMB**

bash

CopiarEditar

nmap --script=smb-enum-shares -p 445 192.168.0.8

**Explicación:**

* Muestra los recursos compartidos de SMB (por ejemplo, C$, ADMIN$, etc.).
* Si los recursos están configurados con acceso anónimo, podrás verlos sin autenticación.

**📌 Obtener información del sistema Windows (SMB OS Discovery)**

bash

CopiarEditar

nmap --script=smb-os-discovery -p 445 192.168.0.8

**Explicación:**

* Identifica la versión del sistema operativo Windows.
* Puede revelar detalles como **nombre del host, dominio y versión de SMB**.

**📌 Detectar dominios de Windows (Active Directory)**

bash

CopiarEditar

nmap --script=smb-enum-domains -p 445 192.168.0.8

**Explicación:**

* Identifica dominios en una red Windows.
* Es útil si el objetivo es parte de **Active Directory**.

**⚠️ 2. Escaneo de Vulnerabilidades en SMB**

**📌 Detectar EternalBlue (MS17-010)**

bash

CopiarEditar

nmap --script=smb-vuln-ms17-010 -p 445 192.168.0.8

**Explicación:**

* Busca la vulnerabilidad **EternalBlue**, que permite ejecución remota de código en Windows.
* Si es vulnerable, podrías explotarlo con **Metasploit o un exploit manual**.

**📌 Detectar vulnerabilidades en SMBv2**

bash

CopiarEditar

nmap --script=smb-vuln-ms10-054,smb-vuln-ms10-061 -p 445 192.168.0.8

**Explicación:**

* **MS10-054:** Ataques de denegación de servicio en SMBv2.
* **MS10-061:** Permite escalamiento de privilegios en Windows Vista y Server 2008.

**📌 Detectar si SMB1 está habilitado (para ataques antiguos)**

bash

CopiarEditar

nmap --script=smb-protocols -p 445 192.168.0.8

**Explicación:**

* Indica qué versiones de **SMB (SMB1, SMB2, SMB3)** están activas.
* SMB1 es vulnerable a varios ataques como **EternalBlue**.

**📌 Detectar vulnerabilidad en Netlogon (CVE-2020-1472 - Zerologon)**

bash

CopiarEditar

nmap --script=smb-vuln-cve-2020-1472 -p 445 192.168.0.8

**Explicación:**

* Verifica si el controlador de dominio es vulnerable a **Zerologon**, lo que permite **tomar el control total** del dominio.

**🛠 3. Escaneo Completo con Scripts en RPC y SMB**

bash

CopiarEditar

nmap --script=rpcinfo,smb-os-discovery,smb-enum-users,smb-enum-shares,smb-vuln-ms17-010,smb-protocols -p 135,139,445 192.168.0.8

**Explicación:**

* **rpcinfo** → Enumera servicios RPC activos.
* **smb-os-discovery** → Detecta versión de Windows y dominio.
* **smb-enum-users** → Lista usuarios de SMB.
* **smb-enum-shares** → Muestra carpetas compartidas.
* **smb-vuln-ms17-010** → Busca **EternalBlue**.
* **smb-protocols** → Identifica si SMB1 está habilitado.

Estos comandos te permitirán enumerar servicios, detectar usuarios y encontrar vulnerabilidades en un sistema Windows con RPC y SMB abiertos. 🚀