ASICI

Asociación Internacional de Ciberseguridad

Guía del Comando nmap

Comando nmap

`nmap` (Network Mapper) es una herramienta de código abierto fundamental para la exploración de redes y la auditoría de seguridad. Permite a los administradores de sistemas y a los profesionales de la seguridad descubrir hosts y servicios en una red, escanear puertos, identificar versiones de sistemas operativos y aplicaciones, y detectar posibles vulnerabilidades.

Sintaxis Básica

La sintaxis básica de `nmap` es simple:

nmap [Tipo de Escaneo] [Opciones] {Especificación del Objetivo}

1. Especificación de Objetivos

Puedes especificar uno o más objetivos de diversas maneras:

- **Host único:** `nmap 192.168.1.1`
- **Múltiples hosts (separados por espacio):** `nmap 192.168.1.1 192.168.1.5`
- **Rango de direcciones IP:** `nmap 192.168.1.1-10`
- **Subred (notación CIDR):** `nmap 192.168.1.0/24`
- **Excluir hosts:** Puedes usar `--exclude <host1,host2>` para omitir hosts específicos de un rango.
    - Ejemplo: `nmap 192.168.1.0/24 --exclude 192.168.1.5`
- **Lista de objetivos desde un archivo:** `-iL <archivo_de_lista>`
    - Ejemplo: `nmap -iL objetivos.txt` (donde `objetivos.txt` contiene una lista de IPs o nombres de host, uno por línea).

2. Tipos de Escaneo (Scan Techniques)

Estas opciones determinan cómo Nmap interactúa con los puertos del objetivo para determinar su estado (abierto, cerrado, filtrado).

- **`-sS` (TCP SYN Scan / Escaneo sigiloso):** El escaneo por defecto y el más popular. Envía un paquete SYN y espera la respuesta. Si recibe SYN/ACK, sabe que el puerto está abierto. Si recibe RST, está cerrado. Si no hay respuesta o un error ICMP, el puerto está filtrado. Es "sigiloso" porque no completa la conexión TCP.
- **`-sT` (TCP Connect Scan):** El escaneo por defecto si el usuario no tiene permisos de raw-sockets (por ejemplo, si no es root en Linux). Realiza una conexión TCP completa (establece la sesión SYN, SYN/ACK, ACK). Es más ruidoso y menos sigiloso que el SYN scan.
- **`-sU` (UDP Scan):** Escanea puertos UDP. Envía un paquete UDP vacío o específico para algunos puertos comunes. Si no hay respuesta, el puerto podría estar abierto o

filtrado. Si recibe un "ICMP Port Unreachable", el puerto está cerrado. Puede ser muy lento.
- **`-sA` (ACK Scan):** Diseñado para mapear reglas de firewall. Envía paquetes ACK. Si recibe un RST, el puerto no está filtrado. Si no hay respuesta o ICMP, el puerto está filtrado. No determina si el puerto está abierto o cerrado.
- **`-sW` (Window Scan):** Similar al ACK scan, pero explota un detalle en el tamaño de la ventana TCP para determinar si un puerto está abierto o cerrado en algunos sistemas.
- **`-sM` (Maimon Scan):** Envía paquetes FIN/ACK. Si no hay respuesta, el puerto está abierto. Si hay RST, el puerto está cerrado.
- **`-sN` (Null Scan):** Envía paquetes TCP sin ningún flag activado (NULL). Los puertos cerrados responden con RST. Los puertos abiertos/filtrados no responden.
- **`-sF` (FIN Scan):** Envía solo el flag FIN. Los puertos cerrados responden con RST. Los puertos abiertos/filtrados no responden.
- **`-sX` (Xmas Scan):** Envía paquetes TCP con los flags FIN, URG y PSH activados. Los puertos cerrados responden con RST. Los puertos abiertos/filtrados no responden.
    - *Nota sobre Null, FIN, Xmas Scans:* Estos son efectivos para evadir firewalls sencillos que solo monitorean el flag SYN.
- **`--scanflags <flags>`:** Permite personalizar los flags TCP enviados (ej. `--scanflags SYNPSHFINURG`).
- **`-b <hostrelé>` (FTP Bounce Scan):** Utiliza un servidor FTP vulnerable como proxy para realizar el escaneo, ocultando el origen del escaneo.

3. Detección de Hosts (Host Discovery / Ping Scans)

Estas opciones controlan cómo Nmap detecta si un host está en línea antes de escanearlo.

- **`-Pn` (No Ping):** No realiza ningún descubrimiento de hosts. Asume que todos los hosts están en línea y los escanea directamente. Útil si sabes que los hosts están activos o si un firewall bloquea los pings.
- **`-PS [lista de puertos]` (TCP SYN Ping):** Envía un paquete SYN a un puerto específico (por defecto 80). Si recibe SYN/ACK o RST, el host está activo.
- **`-PA [lista de puertos]` (TCP ACK Ping):** Similar a `-PS`, pero envía un paquete ACK.
- **`-PU [lista de puertos]` (UDP Ping):** Envía un paquete UDP a un puerto específico (por defecto 40125).
- **`-PE` (ICMP Echo Request Ping):** El ping ICMP tradicional.
- **`-PP` (ICMP Timestamp Request Ping):** Envía un paquete ICMP de solicitud de marca de tiempo.
- **`-PM` (ICMP Netmask Request Ping):** Envía un paquete ICMP de solicitud de máscara de red.
- **`-PO [lista de protocolos]` (IP Protocol Ping):** Envía cabeceras de paquetes IP para protocolos específicos.
- **`-n` (No DNS Resolution):** No resuelve los nombres de host (más rápido).

- **`-R` (Reverse DNS Resolution):** Siempre resuelve los nombres de host.

4. Especificación de Puertos

Controla qué puertos se escanean.

- **`-p <rango de puertos>`:** Especifica los puertos a escanear.
  - Ejemplos:
    - `-p 80` (solo puerto 80)
    - `-p 22,80,443` (puertos específicos)
    - `-p 1-1024` (rango)
    - `-p U:53,T:21-25` (UDP puerto 53, TCP puertos 21-25)
    - `-p-` (todos los 65535 puertos)
    - `-p 80,443,139,445,U:53` (mezcla de TCP y UDP)
- **`--exclude-ports <rango de puertos>`:** Excluye puertos específicos del escaneo.
- **`-F` (Fast Scan / Escaneo Rápido):** Escanea solo los 100 puertos más comunes (definidos en `nmap-services`).
- **`--top-ports <número>`:** Escanea los N puertos más comunes.
  - Ejemplo: `nmap --top-ports 200 google.com` (escanea los 200 puertos TCP más comunes).

5. Detección de Servicios/Versiones y Sistemas Operativos

- **`-sV` (Version Detection):** Intenta determinar el servicio y la versión que se ejecuta en los puertos abiertos. Esto incluye el nombre de la aplicación, el número de versión, y a veces el sistema operativo subyacente.
  - **`--version-intensity <0-9>`:** Controla la intensidad de la detección de versiones. 0 es la más ligera, 9 es la más completa (por defecto 7).
  - **`--version-light`:** Intensidad 2 (más rápido).
  - **`--version-all`:** Intensidad 9 (más lento).
- **`-O` (OS Detection):** Intenta determinar el sistema operativo y el tipo de dispositivo (router, switch, etc.) del objetivo. Puede ser menos preciso con firewalls.
  - **`--osscan-limit`:** Limita la detección de SO a hosts que tienen al menos un puerto abierto y uno cerrado.
  - **`--osscan-guess`:** Nmap adivinará el SO incluso si la confianza es baja.
- **`-A` (Aggressive Scan):** Habilita varias opciones de escaneo avanzadas, incluyendo detección de SO (`-O`), detección de versiones (`-sV`), escaneo de scripts predeterminado (`-sC`), y traceroute (`--traceroute`). Es un escaneo ruidoso pero muy informativo.

6. Rendimiento y Opciones de Temporización (Timing and Performance)

Estas opciones ajustan la velocidad y la agresividad del escaneo.

- `-T<0-5>` **(Timing Template):** Establece una plantilla de temporización predefinida.
  - `T0` (Paranoid): Muy lento, evasivo, para evitar detección de IDS/IPS.
  - `T1` (Sneaky): Lento, para evadir detección.
  - `T2` (Polite): Reduce la tasa de escaneo para no sobrecargar la red/hosts.
  - `T3` (Normal): Por defecto, equilibrio entre velocidad y evasión.
  - `T4` (Aggressive): Más rápido, asume una red rápida y confiable.
  - `T5` (Insane): Muy rápido, puede causar errores en redes lentas.
- `--min-hostgroup <tamaño>`**:** Agrupa hosts para escaneo en paralelo.
- `--max-hostgroup <tamaño>`**:** Máximo de hosts en un grupo.
- `--min-rtt-timeout <tiempo>ms`**:** Tiempo mínimo de espera para respuestas.
- `--max-rtt-timeout <tiempo>ms`**:** Tiempo máximo de espera para respuestas.
- `--initial-rtt-timeout <tiempo>ms`**:** Tiempo de espera inicial.
- `--max-retries <reintentos>`**:** Número máximo de reintentos para un puerto.
- `--host-timeout <tiempo>ms`**:** Abandona el escaneo de un host si no responde en el tiempo especificado.
- `--scan-delay <tiempo>ms`**:** Retraso entre cada sondeo para evitar inundar el objetivo.
- `--max-scan-delay <tiempo>ms`**:** Máximo retraso entre sondeos.
- `--min-rate <tasa>`**:** Envía paquetes a una tasa mínima por segundo.
- `--max-rate <tasa>`**:** Limita la tasa máxima de envío de paquetes por segundo.
- `--defeat-rst-ratelimit`**:** Ajusta la temporización para evitar la limitación de velocidad de RST.

7. Opciones de Detección de Firewall/Evasión (Firewall/IDS Evasion and Spoofing)

- `-f` **(Fragment IP packets):** Fragmenta los paquetes IP en partes más pequeñas para evadir firewalls.
- `-D <decoy1,decoy2,ME,...>` **(Decoy):** Envía paquetes desde direcciones IP falsas (decoy) mezcladas con tu IP real (`ME`).
- `-S <dirección IP de origen>` **(Spoof Source Address):** Establece la dirección IP de origen a una falsa (requiere `-Pn` y puede que no muestre resultados).
- `-e <interfaz>` **(Specify Network Interface):** Especifica la interfaz de red a usar.
- `-g <número de puerto>` / `--source-port <número de puerto>` **(Spoof Source Port):** Utiliza un puerto de origen específico.
- `--data-length <número>`**:** Añade datos aleatorios a los paquetes enviados para hacerlos parecer menos sospechosos.
- `--mtu <tamaño>`**:** Establece el tamaño de la unidad de transmisión máxima del paquete.
- `--badsum`**:** Envía paquetes con una checksum TCP/UDP incorrecta.
- `--randomize-hosts`**:** Aleatoriza el orden de los hosts escaneados.

8. Salida (Output)

Controla cómo Nmap muestra los resultados del escaneo.

- **`-oN <archivo>` (Normal Output):** Guarda la salida normal en un archivo.
- **`-oX <archivo>` (XML Output):** Guarda la salida en formato XML (útil para procesamiento con otras herramientas).
- **`-oS <archivo>` (ScRipT Kiddie Output):** Salida "divertida" con formato de "script kiddie".
- **`-oG <archivo>` (Grepable Output):** Salida en un formato fácil de parsear con herramientas como `grep`.
- **`-oA <basename>` (All Formats):** Guarda la salida en los formatos normal, XML y grepable, usando el mismo nombre base.
- **`-v` (Verbose):** Aumenta el nivel de detalle de la salida. Puedes usar `-vv` para aún más detalle.
- **`-d` (Debugging):** Aumenta el nivel de depuración.
- **`--reason`:** Muestra la razón por la que un puerto está en un estado particular.
- **`--open`:** Muestra solo los puertos que se consideran abiertos.
- **`--packet-trace`:** Muestra todos los paquetes enviados y recibidos.

9. Nmap Scripting Engine (NSE)

El NSE permite a los usuarios escribir (y compartir) scripts simples para automatizar una amplia variedad de tareas de red.

- **`-sC` (Default Script Scan):** Realiza un escaneo usando una selección de scripts NSE predeterminados considerados seguros y útiles.
- **`--script <script | categoría | directorio | expresion>`:** Ejecuta scripts específicos o scripts de una categoría.
    - Ejemplos de categorías: `auth`, `broadcast`, `brute`, `default`, `discovery`, `dos`, `exploit`, `external`, `fuzzer`, `intrusive`, `malware`, `safe`, `version`, `vuln`.
    - Ejemplo: `nmap -sV -sC 192.168.1.1` (escanea con scripts por defecto y detección de versiones).
    - Ejemplo: `nmap --script http-enum 192.168.1.1` (ejecuta el script **http-enum**).
    - Ejemplo: `nmap --script "http-*" 192.168.1.1` (ejecuta todos los scripts que empiezan por "http-").
    - Ejemplo: `nmap --script vuln 192.168.1.1` (ejecuta todos los scripts de la categoría **vuln**).
- **`--script-args <clave=valor,clave2=valor2,...>`:** Pasa argumentos a los scripts.
    - Ejemplo: `nmap --script http-put --script-args http-put.url='/uploads/test.txt',http-put.file='localfile.txt' 192.168.1.1`
- **`--script-help <script>`:** Muestra información y argumentos de un script.

    - Ejemplo: `nmap --script-help http-enum`
- **`--script-trace`:** Muestra la comunicación enviada y recibida por los scripts.
- **`--script-updatedb`:** Actualiza la base de datos de scripts de Nmap.

10. Misceláneos

- **`-6` (IPv6):** Habilita el escaneo de IPv6.
- **`--datadir <directorio>`:** Especifica el directorio de datos de Nmap.
- **`--send-eth` / `--send-ip`:** Envía paquetes a nivel de Ethernet o IP.
- **`--privileged`:** Asume que el usuario tiene todos los privilegios.
- **`--unprivileged`:** Asume que el usuario no tiene privilegios de raw sockets.
- **`--disable-arp-ping`:** Deshabilita el ping ARP (útil en entornos donde el ARP puede ser ruidoso).
- **`--proxies <proxyurl>`:** Encadena conexiones a través de un proxy HTTP/SOCKS4.
- **`--dns-servers <serv1,serv2>`:** Especifica servidores DNS personalizados.
- **`--system-dns`:** Usa los resolvedores DNS del sistema.
- **`--router-lifetime <tiempo>`:** Especifica el tiempo de vida de la entrada del router.
- **`--disable-arp-ping`:** Deshabilita el descubrimiento de hosts mediante ARP.
- **`--reason`:** Muestra la razón por la que un puerto está en un estado particular.
- **`-h` (Help):** Muestra la página de ayuda de Nmap.