Evasión de Firewalls con NMAP

Guía Básica

techdefense.

Los Firewalls actuales son pilares fundamentales en la defensa, capaces de analizar tráfico en tiempo real, identificar patrones de ataque y bloquear amenazas. Sin embargo, como cualquier tecnología, tienen limitaciones que pueden ser explotadas.

Un NGFW (Next Generation Firewall) no solo filtra tráfico por IP o puerto, sino que también analiza aplicaciones, contenido y comportamiento. Utiliza técnicas como la inspección profunda de paquetes (DPI), sistemas de prevención de intrusiones (IPS) y control de aplicaciones.

En este artículo, exploraremos técnicas ofensivas para poner a prueba estos sistemas, ayudando a las organizaciones a mejorar sus defensas.

Con el fin de realizar una penetración autorizada, durante el escaneo de puertos incluyó la cadena de texto 'Scan performed by Tech Defense Europe'. Es poco probable que alguien note este comentario a menos que esté monitoreando activamente la red utilizando un analizador de paquetes.

nmap --data-string "*Scan performed by Tech Defense Europe*"

Los firewalls modernos pueden estar configurados para detectar y bloquear técnicas de evasión como la fragmentación de paquetes y el cambio de MAC. Por lo tanto, es importante probar múltiples técnicas en función de las capacidades del firewall.

Si bien uno, en lo posible, debe escanear los 65535 puertos que existen tanto en TCP como UDP, un escaneo de puertos completo puede ser muy lento dependiendo de la red y la máquina objetivo, por lo que en muchos casos se realiza un escaneo de puertos comunes.

Puertos TCP:

21 (FTP) – Protocolo de transferencia de archivos.
22 (SSH) – Secure Shell, para acceso remoto seguro.
23 (Telnet) – Protocolo de comunicación para terminal remoto (no seguro).
25 (SMTP) – Protocolo de transferencia de correo.
53 (DNS) – Sistema de nombres de dominio.
69 (TFTP) – Trivial File Transfer Protocol (FTP simplificado y sin seguridad).
80 (HTTP) – Protocolo de transferencia de hipertexto (web).
110 (POP3) – Protocolo de oficina de correos (recepción de correo).
143 (IMAP) – Protocolo de acceso a mensajes de Internet (correo).
161 (SNMP) – Protocolo simple de administración de red.
162 (SNMP Trap) – Usado para recibir notificaciones de eventos SNMP.
443 (HTTPS) – HTTP seguro (web).
445 (Microsoft-DS) – Compartición de archivos e impresión en Windows.
5080 (HTTP Proxy) – Protocolo de servidor proxy web alternativo.
5432 (PostgreSQL) – Base de datos PostgreSQL.
5900 (VNC) – Protocolo de acceso a escritorio remoto (Virtual Network Computing).
8080 (HTTP Proxy) – Servidor web alternativo, generalmente usado para proxies HTTP.
8081 (HTTP Proxy) – Otro puerto para proxies HTTP alternativos.
11211 (Memcached) – Servicio de almacenamiento en caché distribuido.
1433 (MS SQL Server) – Protocolo de Microsoft SQL Server.
1521 (Oracle DB) – Base de datos Oracle.
2049 (NFS) – Sistema de archivos de red de UNIX.
27017 (MongoDB) – Base de datos MongoDB.
3389 (RDP) – Protocolo de escritorio remoto de Microsoft.
50000 (SAP) – Sistema de aplicaciones empresariales SAP.
9100 (Printer Services) – Usado por impresoras y servicios de impresión en red.
1521 (Oracle DB) – Base de datos Oracle.
2000 (Cisco SCCP) – Protocolo de control de llamadas en sistemas de Cisco.

Puertos UDP:

53 (DNS) – Protocolo de nombres de dominio (resolución de nombres).
67 (DHCP) – Protocolo de configuración dinámica de host, utilizado para asignar direcciones IP automáticamente.
68 (DHCP) – Usado por clientes DHCP para recibir respuestas del servidor.
69 (TFTP) – Trivial File Transfer Protocol (FTP simplificado y sin seguridad).
123 (NTP) – Protocolo de tiempo de red (para sincronización de tiempo).
137 (NetBIOS Name Service) – Servicio de nombres NetBIOS, utilizado para compartir archivos e impresoras en redes locales.
138 (NetBIOS Datagram Service) – Servicio de datagramas NetBIOS para compartir archivos.
139 (NetBIOS Session Service) – Protocolo de sesión NetBIOS para compartir archivos e impresoras.
161 (SNMP) – Protocolo simple de administración de red.
162 (SNMP Trap) – Usado para recibir notificaciones de eventos SNMP.
1812 (RADIUS) – Protocolo para autenticación remota, utilizado principalmente para acceso a redes VPN.
2000 (Cisco SCCP) – Usado para el protocolo de control de llamadas en dispositivos Cisco.
4500 (IPsec NAT-T) – Usado para la negociación de túneles IPsec en redes NAT.
500 (ISAKMP) – Protocolo de administración de claves para IPSec (usado en VPN).
514 (Syslog) – Protocolo para el envío de logs y mensajes de sistema.
5060 (SIP) – Protocolo de iniciación de sesión, utilizado para VoIP (llamadas de voz por Internet).
5061 (SIP TLS) – Protocolo de iniciación de sesión sobre TLS para comunicaciones seguras en VoIP.
1701 (L2TP) – Protocolo de túnel de capa 2, utilizado en conexiones VPN.

Técnicas Comunes de Evasión de Firewall con NMAP

1. Fragmentación de paquetes

Dividir datos en paquetes más pequeños puede confundir al firewall, dificultando la inspección completa del tráfico.

```
nmap -f (fragmentos) --mtu (MTU especificada) -p <puerto> <objetivo>
```

2. Puerto de origen

Un error de configuración común es confiar en el tráfico basándose únicamente en el número de puerto de origen. Las respuestas DNS provienen del puerto 53 y muchos administradores han caído en la trampa de simplemente permitir el tráfico entrante desde esos puertos.

```
nmap -g 53 -p <puerto> <objetivo>
```

3. Falsificación de direcciones MAC

Falsificar la dirección MAC ofrece otro método para eludir las restricciones del firewall. Este enfoque puede ser particularmente potente, en particular cuando un firewall emplea filtrado MAC para permitir la comunicación exclusivamente desde direcciones MAC designadas.

```
nmap -sT -PO -spoof-mac <mac> -p <puerto> <objetivo>
```

4. Escaneo con orden aleatorio / ofuscación

Los firewalls y sistemas IDS/IPS pueden detectar patrones de tráfico constante. Modificar el orden de los hosts y el tiempo de escaneo de puertos puede dificultar la detección. Además, alterar los datos de los paquetes para que no coincidan con los patrones esperados de tráfico puede ayudar a evadir.

```
nmap --data-length 100 --randomize-hosts -p <puerto> <objetivos>
```

5. Escaneo UDP (para evitar los filtros de puertos TCP comunes)

A veces los firewalls están configurados para bloquear puertos TCP comunes, pero no filtran adecuadamente el tráfico UDP.

```
nmap -sU -p <puerto> <objetivo>
```

6. Escaneo con Túneles ICMP (ICMP Echo Scan)

Este tipo de escaneo es útil cuando se sospecha que el firewall bloquea los puertos TCP y UDP, pero permite el tráfico ICMP. El comando ICMP puede usarse para enviar paquetes "ping" al objetivo.

```
nmap -PE -p <puerto> <objetivo>
```

7. Escaneo con Opciones de Spoofing de IP (Evitar Detección por IP de Origen):

Este tipo de escaneo hace que parezca que los paquetes vienen de una IP diferente, lo que puede eludir los filtros basados en direcciones IP. Sin embargo, para obtener respuestas útiles sobre los puertos abiertos en los objetivos, necesitarías emplear técnicas adicionales, como redirección de tráfico a través de un proxy o utilizar métodos.

```
nmap n -S <ip falsa> -p  <puerto> <objetivo>
```

8. Escaneo a Baja Velocidad (-T0, --scan-delay, --max-retries)

Al ajustar la demora entre los paquetes, puedes hacer que tu escaneo sea más difícil de detectar especificando un retraso más preciso.

```
nmap -T0 --scan-delay 1s  --max-retries 1 -p  <puerto> <objetivo>
```

9. Escanear empleado proxies

Esto puede ser útil cuando deseas realizar un escaneo sin exponer tu IP real, utilizando un servidor proxy como intermediario.

```
nmap --proxies  <proto://host:port > <puerto> <objetivos>
```

10. Enviar sumas de verificación incorrectas

Las sumas de verificación son fundamentales en el protocolo TCP/IP para garantizar la integridad de los datos durante la transmisión. Sin embargo, enviar deliberadamente paquetes con sumas de verificación incorrectas puede resultar ventajoso en determinados escenarios.

```
nmap --badsum <puerto> <objetivo>
```

11. Escaneo con señuelos (Decoy Scan)

Un escaneo con señuelos es una técnica de escaneo de puertos que hace parecer que los hosts especificados como señuelos están escaneando una red objetivo.

```
nmap -p <puerto>  <objetivo> -D <señuelos>
```

12. Escaneo Idle Scan empleando “zombis inactivos”

La técnica de escaneo de zombis inactivos es un método sofisticado que se emplea en las evaluaciones de seguridad de la red para realizar escaneos de puertos en los hosts de destino utilizando hosts inactivos dentro de la red. Su principal ventaja reside en su notable sigilo, ya que oculta el origen del escaneo al atribuir la dirección IP del host "zombi" inactivo en los archivos de registro del cortafuegos, ocultando así la identidad del escáner real.

Para garantizar resultados precisos, es imperativo identificar los hosts inactivos dentro de la red. Existen diversas herramientas para identificar un “zoombie”.

```
nmap -sl <zoombie> -p <puerto>  <objetivo>
```

Ejemplos empleando usuario con privilegios administrativos para emplear -sS (por defecto en nmap):

Escaneo básico con opciones avanzadas:

```
nmap -p 22,80,443 --scan-delay 1s --max-retries 1 --mtu 1280 --proxies http://proxy.example.com:8080 -f <objetivo>
```

Escaneo de alta evasión con decoys, retraso y suma incorrecta

```
nmap -T0 -p 22,80,443 --decoy 192.168.1.10,192.168.1.20,192.168.1.30 --badsum 192.168.1.0/24
```

Escaneo avanzado con spoofing, proxies y otras opciones de evasión

```
nmap -S 192.168.100.1 --data-length 100 --randomize-hosts -p 22,80,443 --scan-delay 1s --max-retries 1 --mtu 1280 --source-mac 00:11:22:33:44:55 --proxies http://proxy.example.com:8080 -f 192.168.1.0/24
```