Nivel medio NMAP

PASCAL

¿Qué es?

Fue desarrollado como un escáner de puertos en el año 1997 por Gordon Lyon. Desde entonces su desarrollo ha crecido bastante.
El código de Nmap se utilizo para crear la primera versión de Nessus en 1998.
En el año 2006 se integra el Nmap Scripting Engine que permite hacer scripts a los usuarios para hacer tareas automatizadas en redes.
Para el futuro se espera que se integre un web scanner con spider más complejo y opciones como fuerza bruta por http.
Nmap: Es una herramienta que permite hacer un mapa de una red. Esta herramienta encuentra los dispositivos conectados en la red escaneada y detecta los servicios de puertos abiertos que corren cada uno de ellos.
Funciones:

- Detecta dispositivos en una red.
- Detecta puertos abiertos y sus servicios.
- Detecta Versiones de servicios.
- Detecta Sistemas Operativos y sus Versiones.
- Detecta Firewalls o Tipos de Paquetes Bloqueados.
- Evasión Firewalls.

¿Cómo detecta dispositivos activos?

Un escaneo básico de dispositivos utiliza una técnica llamada **sondeo ping**.
Esta técnica consiste en enviar un paquete de petición Echo ICMP y recibe mensajes de respuesta Echo cuando un Host esta vivo.

Listing 1: Código de ejemplo

```
ping 172.217.168.163
```

¿Cómo detecta los servicios en dispositivos?

Para detectar un servicio corriendo en un dispositivo de red Nmap realiza un intento de conexión a un puerto definido.
Esta conexión utiliza el método de conexión en 3 pasos.
Nmap utiliza una tabla de puertas comunes e intenta hacer esta conexión a cada uno de ellos en el rango de Ips especificados. Cuando se tiene éxito en la conexión se establece que el puerto se encuentra abierto.

¿Cómo detecta Firewall y como los evade?

Detectar un firewall es una tarea muy difícil ya que Nmap realiza su trabajo con normalidad y recibe una respuesta negativa de todos los puertos, esto quiere decir que están todos cerrados o bien están siendo bloqueados por un firewall.
Nmap tiene las siguientes opciones para evadir un firewall:

- Fragmentación de paquetes.
- Enviar un paquete utilizando un puerto que un firewall conocido acepta conexiones.
- Mac Spoofing correspondiente a un proveedor cisco.

¿Cómo detecta un sistema operativo?

Nmap realiza un envío de paquetes y analiza todos los bits de la respuesta con una base de datos de más de 1500 huellas y los compara. Al momento de dar una respuesta positiva con información de esta base de datos este presenta el sistema operativo que más concuerda con la base de datos.

Escaneo básico activo

Para llamar a Nmap utilizaremos el comando nmap para que nos aparezca todas las opciones posibles. Para realizar un escaneo básico escribiremos nmap seguido por una dirección IP o una dirección web. Se puede realizar un escaneo a más direcciones IP con un espacio entre ellas. Además podemos realizar un rango de escaneo de IPs con un guión entre ellas.
Por otro lado, podemos realizar otro tipo de escaneo colocando nmap -iL seguido del archivo .txt. Si le indicamos el comando ls podremos ver dónde está ubicado nuestro archivo. Se puede excluir una dirección IP con el comando -exclude seguido por la dirección IP.

Listing 2: Código de ejemplo

```
1 nmap -iL holamundo.txt -exclude 192.168.0.2
```

También se pueden excluir IPs a través de un archivo, utilizaremos el mismo comando anterior, pero en vez de -exclude utilizaremos el comando -excludefile.

Listing 3: Código de ejemplo

```
nmap -iL holamundo.txt -excludefile IPsexcluidas.txt
```

Además se puede escanear toda la subred escribiendo el comando nmap seguido por la dirección IP, y detrás de ella el comando /24.

Listing 4: Código de ejemplo

```
nmap  192.168.0.2/24
```

Seguidamente, se puede escanear un host random utilizando el comando -iR[número]. Si queremos que sea de IPv6 le añadiremos el comando -6.

Listing 5: Código de ejemplo

```
nmap  -iR[4]
```

Por último, para hacer un escaneo agresivo utilizaremos el comando nmap -A [objetivo].

Listing 6: Código de ejemplo

```
nmap  -A[192.168.0.2]
```

Comandos de salida

La primera opción de salida son los archivos de texto, para guardarlo en un archivo de texto utilizaremos el comando nmap -oN [texto.txt][Objetivo].

Listing 7: Código de ejemplo

```
nmap  -oN[ejemplo.txt][192.168.0.2]
```

Seguidamente, para darle una salida en xml utilizaremos el comando nmap -oX[texto.xml][Objetivo].

Listing 8: Código de ejemplo

```
nmap  -oX[ejemplo.xml][192.168.0.2]
```

Posteriormente, podemos utilizar la salida grep. Para ello utilizaremos el comando nmap -oG[texto.txt][Objetivo].

Listing 9: Código de ejemplo

```
nmap  -oG[texto.txt][192.168.0.2]
```

A continuación para la salida en todos los tipos de archivo utilizaremos el comando nmap -oA[Ruta/Archivo][Objetivo].

Listing 10: Código de ejemplo

```
nmap -oA[Escritorio/texto.txt][192.168.0.2]
```

Seguidamente, para mostrar periódicamente todas las estadísticas utilizaremos el comando nmap -stats-every[tiempo][Objetivo].

Listing 11: Código de ejemplo

```
nmap -stats-every[15s][192.168.0.2]
```

Posteriormente, para la salida 133t utilizaremos el comando nmap -oS[texto.txt][Objetivo].

Listing 12: Código de ejemplo

```
nmap -oS[texto.txt][192.168.0.2]
```

Y finalmente, para unos resultados detallados utilizaremos el comando nmap -v[Objetivo].

Listing 13: Código de ejemplo

```
nmap -v[192.168.0.2]
```

Escaneo de puertos

Para realizar un análisis rápido utilizaremos el comando nmap -F[Objetivo].

Listing 14: Código de ejemplo

```
nmap -F[192.168.0.2]
```

Seguidamente, para realizar un escaneo de puertos específico utilizaremos el comando nmap -p[Puertos][Objetivo].

Listing 15: Código de ejemplo

```
nmap -p[2][192.168.0.2]
```

Por otro lado, si lo queremos realizar por nombre utilizaremos el comando nmap -p [nombre del puerto][Objetivo].

Listing 16: Código de ejemplo

```
nmap -p[Puerto1][192.168.0.2]
```

Seguidamente, para escanear los puertos del protocolo utilizaremos el comando nmap -sU-sT-p U:[Puertos], T:[puertos][Objetivo].

Listing 17: Código de ejemplo

```
nmap -sU-sT-p U:[0.2], T:[0.2][192.168.0.2]
```

Posteriormente, para analizar todos los puertos utilizaremos el comando nmap -p¨*¨[Objetivo].

Listing 18: Código de ejemplo

```
nmap -p * [192.168.0.2]
```

A continuación, para escanear los puertos principales utilizaremos el comando nmap -top-ports[número][Objetivo].

Listing 19: Código de ejemplo

```
nmap -top-ports[2][192.168.0.2]
```

Y finalmente, si queremos realizar un escaneo de puertos secuencial utilizaremos el comando nmap -r[Objetivo].

Listing 20: Código de ejemplo

```
nmap -r[192.168.0.2]
```

Opciones avanzadas de escaneo

Primero, para realizar un escaneo TCP SYN utilizaremos el comando nmap -sS[Objetivo].

Listing 21: Código de ejemplo

```
nmap -sS[192.168.0.2]
```

Segundo, para realizar un escaneo de conexión tipo TCP utilizaremos el comando nmap -sT[Objetivo].

Listing 22: Código de ejemplo

```
nmap -sT[192.168.0.2]
```

Tercero, para realizar un escaneo tipo UDP utilizaremos el comando nmap -sU[Objetivo].

Listing 23: Código de ejemplo

```
nmap -sU[192.168.0.2]
```

Cuarto, para realizar un escaneo tipo TCP Null utilizaremos el comando nmap -sN[Objetivo].
Y por otro lado, si lo queremos realizar tipo Fin utilizaremos el comando nmap -sF[Objetivo].

Listing 24: Código de ejemplo

```
nmap -sN[192.168.0.2]
nmap -sF[192.168.0.2]
```

Seguidamente, si queremos realizar un escaneo tipo Xmas utilizaremos el comando nmap -sX[Objetivo].

Listing 25: Código de ejemplo

```
nmap -sX[192.168.0.2]
```

Posteriormente, si queremos realizar un escaneo TCP ACK utilizaremos el comando nmap -sA[Objetivo].

Listing 26: Código de ejemplo

```
nmap -sA[192.168.0.2]
```

A continuación, si queremos realizar un escaneo customizado TCP utilizaremos el comando nmap -scanflags[flags][Objetivo].

Listing 27: Código de ejemplo

```
nmap -scanflags[0.3][192.168.0.2]
```

Seguidamente, si queremos realizar una exploración del protocolo IP utilizaremos el comando nmap -sO[Objetivo].

Listing 28: Código de ejemplo

```
nmap -sO[192.168.0.2]
```

Por otro lado, si queremos enviar paquetes Ethernet utilizaremos el comando nmap -send-eth[Objetivo].

Listing 29: Código de ejemplo

```
nmap -send-eth[192.168.0.2]
```

Y finalmente, se podrán enviar paquetes IP mediante el comando nmap -send-ip[Objetivo].

Listing 30: Código de ejemplo

```
nmap -send-ip[192.168.0.2]
```

Detección de versiones

Primero, para la detección del sistema operativo utilizaremos el comando nmap -O[Objetivo].

Listing 31: Código de ejemplo

```
nmap -O[192.168.0.2]
```

Para poder enviar las fingerprints TCP/IP se utilizará la dirección www.nmap.org/submit/. Posteriormente, para tratar de adivinar un IP desconocido utilizaremos el comando nmap -osscan-guess[Objetivo].

Listing 32: Código de ejemplo

```
nmap -osscan-guess[192.168.0.2]
```

Seguidamente, para el servicio de detección de versión utilizaremos el comando nmap -sV[Objetivo].

Listing 33: Código de ejemplo

```
nmap -sV[192.168.0.2]
```

Posteriormente, para la solución de problemas de las exploraciones versión utilizaremos el comando nmap -sV-version-trace[Objetivo].

Listing 34: Código de ejemplo

```
nmap -sV-version-trace[192.168.0.2]
```

Finalmente, si queremos realizar un análisis RCP utilizaremos el comando nmap -sR[Objetivo].

Listing 35: Código de ejemplo

```
nmap -sR[192.168.0.2]
```

Opciones de descubrimiento

Para realizar un escaneo tipo ping rápido sin pasar por todos los puertos utilizaremos el comando nmap -sP

Listing 36: Código de ejemplo

```
nmap -sR 192.168.0.2/24
```

Por otro lado, para realizar otro tipo de escaneo para determinar los puertos de la direcciones IP utilizaremos el comando nmap -P0[Objetivo].

Listing 37: Código de ejemplo

```
nmap -P0 192.168.1.70
```

Seguidamente, para un escaneo tipo con la bandera SYN activada utilizaremos el comando nmap -PS SYN [Objetivo].

Listing 38: Código de ejemplo

```
nmap -PS SYN 192.168.1.70
```

Se pueden activar otras banderas, como la ACK, para ello utilizaremos el comando nmap -PA[Objetivo].

Listing 39: Código de ejemplo

```
nmap -PA 192.168.1.70
```

Evasión de Firewalls

La fragmentación de paquetes nos permite dividir un paquete en distintos fragmentos y confundir los firewall. Para ello, utilizaremos el comando nmap -f[Objetivo].

Listing 40: Código de ejemplo

```
nmap -f 192.168.1.70
```

Windows está muy limitado en la fragmentación, por lo que se recomienda realizarlo en un sistema opertivo basado en UNIX.
Posteriormente, para falsificar la dirección MAC utilizaremos el comando nmap –spoof-mac[Dirección MAC][Objetivo]

Listing 41: Código de ejemplo

```
nmap --spoof-mac 00:AB:CD:EF:07:15 192.168.1.70
```

Seguidamente, cambiaremos el puerto de origen mediante el comando nmap –source-port[Nuevo puerto][Objetivo].

Listing 42: Código de ejemplo

```
nmap --source-port 21 192.168.1.70
```

Otra de las técnicas para evadir el firewall es el checksum inválido para ello utilizaremos el comando nmap –badsum[Objetivo].

Listing 43: Código de ejemplo

```
nmap --badsum  192.168.1.70
```