Security A(r)t Work

www.securityartwork.es
www.csirtcv.gva.es
www.s2grupo.es

S2 GRUPO

NMAP

José Luis Chica Uribe
Técnico en seguridad
CSIRT-cv

Índice

- Indroducción
- Descubrimiento de equipos y puertos
- Detectando la versión del SSOO y del servicio
- Detección y evasión de firewalls e IDS
- Nmap Scripting Engine
- Consejos de optimización del rendimiento
- Contramedidas contra Nmap

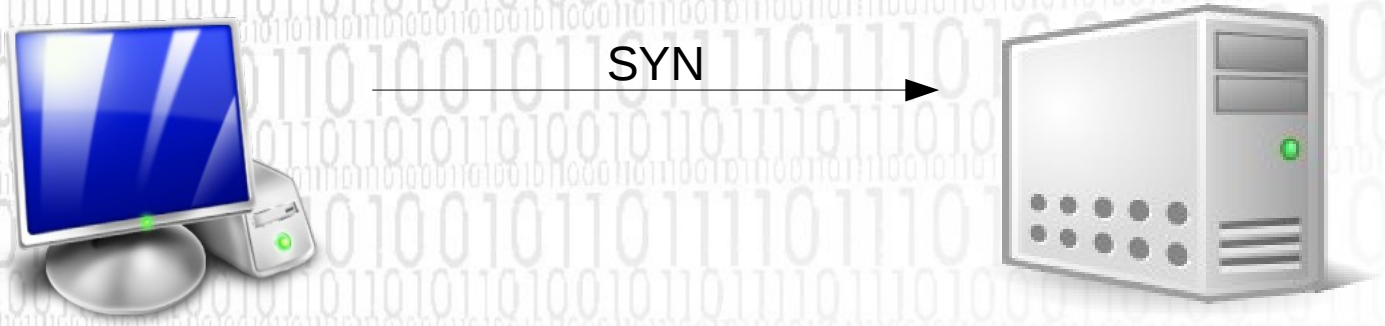
Introducción

- Herramienta de exploración y auditoría
- Escanea equipos y redes
- Primera versión 1997 por Fyodor
- Gratuita, abierta, GPL
- Multiplataforma
- Documentada
- Respaldada por una gran comunidad

Como funciona?

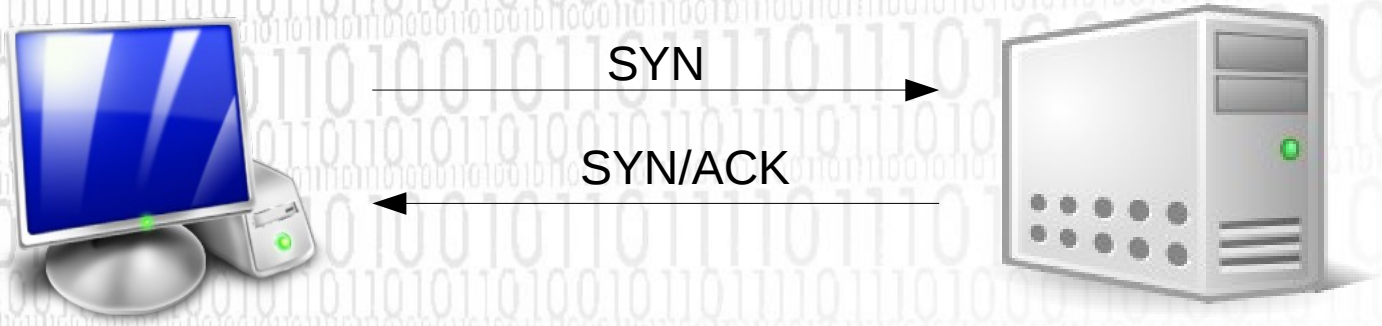
- Hace un barrido, enviando sondas
- En función de las respuestas, reconoce equipos y servicios activos.
- Aprovecha ambigüedades en protocolos de red para adivinar la versión del SSOO
- Necesario conocimientos básicos del protocolo TCP para entender y aprovechar al máximo el funcionamiento de Nmap

TCP



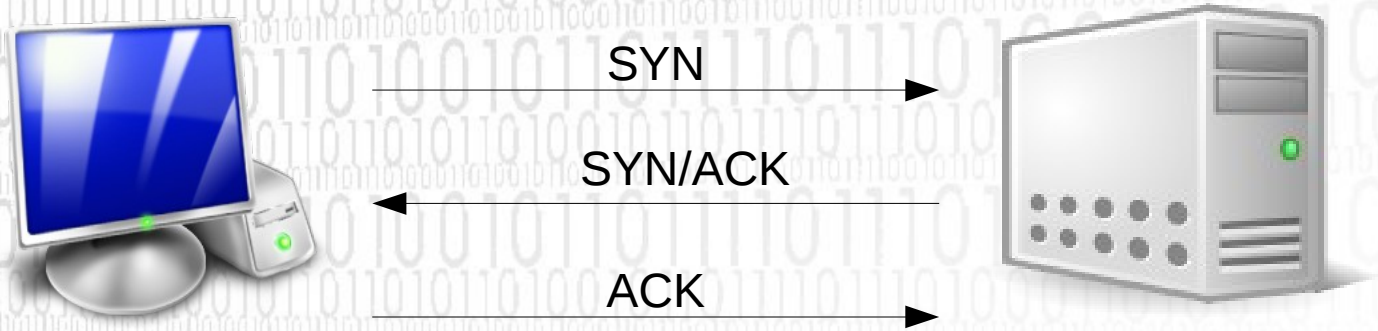
PETICIÓN DEL CLIENTE PARA CONECTARSE A UN

TCP



SI ESTÁ DISPONIBLE,
RESPUESTA AFIRMATIVA DEL SERVIDOR

TCP



CONFIRMACIÓN DEL CLIENTE, COMPLETANDO LA CONEXIÓN

TCP

Un paquete TCP entra a un bar y dice:

- *Quiero una cerveza.*

El camarero le contesta:

- *Una cerveza quieres?*

El paquete TCP responde:

- *Si, una cerveza.*

Un primer ejemplo

```
# nmap -T4 192.168.111.222

Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   closed ssh
25/tcp   open  smtp
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 12.69
seconds
```

Explicación estado puertos

- **ABIERTO**: el puerto es alcanzable y hay alguna aplicación a la escucha.
- **CERRADO**: el puerto es alcanzable, pero no hay ninguna aplicación a la escucha.
- **FILTRADO**: no hay respuesta. Seguramente hay un firewall en medio.

Enumeración de equipos

Barrido con pings

```
# nmap -sP 192.168.1.0/24
```

Si el tráfico ICMP está filtrado, se puede hacer barrido con ping TCP

```
# nmap -sP -PS80,21,22,25 192.168.1.0/24
```

Otros ejemplos

- Escaneo a puertos específicos -p <nums>

```
# nmap -T4 -p21,22,25,80,137,8080 192.168.1.0/24
```

- Escaneo rápido, 100 puertos más usuales -F

```
# nmap -T4 -F 192.168.1.0/24
```

Detección del SSOO

```
# nmap -T4 -O 10.10.10.30

Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 - SP2, Server 2008,
or Windows 7 Ultimate
```

Detección de versión

```
# nmap -T4 -sV 10.10.10.30

Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.2.16 (Debian)
3333/tcp open  ssh     OpenSSH 5.5p1 Debian
6+squeeze1 (protocol 2.0)
```

Todo en uno

```
# nmap -T4 -A 10.10.10.30
```

Modificador **-A**

- Detección de versión -sV
- Detección de SSOO -O
- Uso de scripts -sC
- Uso de traceroute --traceroute

Escaneo a UDP

```
# nmap -T4 -sU -F 10.10.10.20

Not shown: 997 closed ports
PORT      STATE         SERVICE
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
135/udp   open|filtered msrpc
```

- En UDP no podemos determinar si un puerto está abierto o filtrado (por eso tarda tanto)
- Interesante usar -sV para reconocer servicio y -F (hay pocos puertos comunes en UDP)

AUDITANDO FIREWALLS

- Nmap como herramienta de análisis de configuración de firewalls
- Detección de la política por defecto.
  - DEFAULT ACCEPT
  - DEFAULT DROP
- Detección del tipo de firewall
  - STATELESS
  - STATEFULL
- Evasión de firewalls e IDS

POLITICA POR DEFECTO

Basado en el estado de los puertos "no mostrados" en un escaneo

- **Cerrados**: accept by default
- **Filtrados**: deny by default

AUDITANDO FIREWALLS

FIREWALL ACCEPT POR DEFECTO

```
#nmap -T4 ejemplo.com
Not shown: 995 closed ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
```

Respuesta activa **RST** de 995 puertos

AUDITANDO FIREWALLS

FIREWALL DROP POR DEFECTO

```
#nmap -T4 asdf.com
Not shown: 996 filtered ports

PORT STATE SERVICE
22/tcp open ssh
25/tcp closed smtp
80/tcp open http
113/tcp closed auth
```

Sin respuesta de 996 puertos

AUDITANDO FIREWALLS

DETECCIÓN DEL TIPO DE FIREWALL

- Statefull: capaz de controlar las sesiones TCP
- Se lanza Nmap normal (SYN scan)
  - Se lanza otro escaneo “exótico”
    - ACK scan
    - Xmas scan
    - FIN scan
- Si el segundo scan no muestra resultado, es un firewall statefull

FIREWALL STATEFULL

```
#nmap -sA -T4 asdf.com
Not shown: 1000 filtered ports
```

Firewall detecta paquetes ACK sin establecer conexión previa y los dropea

AUDITANDO FIREWALLS

FIREWALL SIN ESTADO

```
#nmap -sA -T4 asdf.com
Not shown: 996 filtered ports

PORT STATE SERVICE
22/tcp unfiltered ssh
25/tcp unfiltered smtp
80/tcp unfiltered http
113/tcp unfiltered auth
```

Sondas ACK han burlado el firewall

Manipulación del puerto de origen

- Puertos que el equipo considera de “confianza”
- Permiten todo el tráfico entrante
- Aún teniendo reglas que lo bloqueen implícitamente!!!

Ej:

- W2K y XP permitía todo tráfico TCP y UDP desde el puerto 88 (Kerberos)
- OS X TIGER permitía tráfico desde el puerto 67 (DHCP) y 5353 (Zeroconf)

Escaneo IPv6

- Servicios que escuchan IPv6
- No se tienen en cuenta
- Electrónica que aún no soporta reglas de filtrado IPv6
- Posibilidad de llegar a servicios que están filtrados solo en IPv4

EVASIÓN DE FIREWALLS

```
#nmap -T4 asdf.com
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
80/tcp open http
113/tcp closed auth

#nmap -T4 -6 asdf.com
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
113/tcp closed auth
```

Fragmentación IP

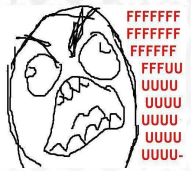
- Firewalls que no tratan paquetes fragmentados
- Podrían dejarlos pasar todos los fragmentos (o ignorarlos)
- Modificador -f <numbytes>
- Se puede usar también –mtu

BARRIDOS LEEEEENTOS

- Ralentizar los envíos de sondas
- Evitar detección por reglas de X paquetes en Y segundos.
- Modificador T0: envío de sonda por cada 300sg -_-zZzZzz
- Modificador T1: envío de sonda por cada 15sg

NMAP SCRIPTING ENGINE

- Herramienta muy potente y flexible
- Permite al usuario escribir scripts para automatizar tareas
- Basado en lenguaje LUA
- Permite:
  - Detección de vulnerabilidades
  - Explotación de vulnerabilidades
  - Etcetcetc……..



NMAP SCRIPTING ENGINE

```
# nmap -sC -p139 -T4 1.2.3.4

Starting Nmap ( http://nmap.org )
Nmap scan report for flog (1.2.3.4)
PORT     STATE SERVICE
139/tcp  open  netbios-ssn

Host script results:
| smb-os-discovery: Unix
| LAN Manager: Samba 3.0.31-0.fc8
|_Name: WORKGROUP

Nmap done: 1 IP address scanned in 0.33 seconds
```

NMAP SCRIPTING ENGINE

- Actualmente:
  - 284 scripts
  - 74 librerias
- Mantenidos activamente por comunidad en lista de correo nmap-dev
- Categorias:
  - Bruteforce, version, fuzzing, DoS

http://nmap.org/nsedoc/

NMAP SCRIPTING ENGINE

- uso de un script especifico

```
--script <nombre/categoria>
```

- si necesita algún argumento

```
--script-args
```

OPTIMIZACIÓN NMAP

- Capaz de escanear redes MUY extensas y heterogeneas
- No es lo mismo escanear una red lejana que una LAN
- Ni con firewalls que sin ellos
- Los tiempos de respuesta son diferentes

OPTIMIZACIÓN NMAP

- Necesidad de utilizar configuración personalizada
- Plantillas de tiempo: -T0...T5
  - T0,T1 MUY lento. Evasión de IDS
  - T2,T3, lento. Redes muy saturadas o inferiores a modems 56Kb
  - T4,T5 rápido, apaña para redes WAN o LAN
- (Por defecto T3)

OPTIMIZACIÓN NMAP

Pero a veces no es suficiente

- Perfiles demasiado genéricos
- Se puede exprimir más!
- Uso de modificadores para configuración avanzada de tiempo

OPTIMIZACIÓN NMAP

`--min-hostgroup, --max-hostgroup`

- Agrupa las IPs y las escanea en paralelo
- Interesante usarlo en escaneos UDP o con pocos puertos por host

OPTIMIZACIÓN NMAP

--max-rtt-timeout,--initial-rtt-timeout

- Ajusta el tiempo de rtt (round trip time)
- Se puede aproximar con ping/hping3

```
5 packets transmitted, 5 received, time 4005ms
rtt min/avg/max/mdev=210.736/215.089/221.475/4.063
```

OPTIMIZACIÓN NMAP

`--min-parallelism, --max-paralleism`

- Número de sondas pendientes de respuesta que es capaz de manejar.
- Nmap calcula este valor de forma dinámica
- Si se están perdiendo paquetes, ralentiza el envío de sondas y reduce el número de respuestas pendientes, para no perder precisión

OPTIMIZACIÓN NMAP

TABLA DE TIEMPOS

	T0	T1	T2	T3	T4	T5
min-rtt-timeout	100	100	100	100	100	50
max-rtt-timeout	300,000	15,000	10,000	10,000	1,250	300
Initialrtt-timeout	300,000	15,000	1,000	1,000	500	250
max-retries	10	10	10	10	6	2
host-timeout	0	0	0	0	0	900,000
min-parallelism			Dinámico			
max-parallelism	1	1	1		Dinámico	
min-hostgroup			Dinámico			
max-hostgroup			Dinámico			

OPTIMIZACIÓN NMAP

- **nmap -T4 1.2.3.0/24**

```
# Nmap done at Tue Nov 29 14:45:36 2011 -- 256 IP
addresses (229 hosts up) scanned in 3475.76 seconds
```

- **nmap -T4 --initial-rtt-timeout 250 --max-rtt-timeout 500 --max-retries 2 --min-parallelism 70 1.2.3.0/24**

```
# Nmap done at Wed Nov 30 11:30:57 2011 -- 256 IP
addresses (229 hosts up) scanned in 1052.46 seconds
```

OPTIMIZACIÓN NMAP

SCAN MLP EDITION

- **nmap -T4 217.124.152.0/22**

```
# Nmap done at Wed Dec  7 12:50:22 2011 -- 1024 IP
addresses (339 hosts up) scanned in 2227.96 seconds
```

- **nmap -T4 --initial-rtt-timeout 2 --max-rtt-timeout 5 --max-retries 2 --min-parallelism 70 217.124.152.0/22**

```
# Nmap done at Wed Dec  7 13:33:08 2011 -- 1024 IP
addresses (395 hosts up) scanned in 875.07 second
```

DEFENSA CONTRA NMAP

UN BUEN ATAQUE!

- Escanea tu red
- Cierra puertos innecesarios
- Busca vulnerabilidades y arréglalas!
- Interesante programar escaneos periódicos y comparar resultados con Ndiff

DEFENSA CONTRA NMAP

DETECTAR ESCANEOS

- Firewalls o IDS son capaces de detectar
- Es habitual ignorar la detección, debido a que casi siempre son inofensivos
- Pero a veces es precursor a una intrusión
- Interesante correlar esta información
  - Escaneo y acceso SSH
  - Escaneo y caida de servicio

DEFENSA CONTRA NMAP

"OCULTAR" PUERTOS

- Nmap escanea 1000 puertos usuales
- Interesante bindear un servicio a un puerto poco conocido
- Obligas a hacer un barrido completo
- Valorar seguridad vs usabilidad
  - Poco util servidor web puerto 23981

DEFENSA CONTRA NMAP

OTROS

- OS Spoofing
  - Operating System: MS Mapache 2011
- Port Knoking
  - "Llamar" a una secuencia de puertos
- Honeypots
  - Falsos servicios abiertos y golosos para entretener al atacante

GRACIAS

www.neuronasdigitales.com
Twitter: @spankito

S2 GRUPO

Ramiro de Maeztu, 7
46022 Valencia
Tel. (+34) 963 110 300
Fax (+34) 963 106 086

Orense, 85. Ed.Lexington
28020 Madrid
T. (+34) 915 678 488
F. (+34) 915 714 244

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es