


TEC
DE MONTERREY
Campus Estado de México



Network
Security Scan

Escaneo de puertos y protección

nmap y portsentry

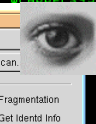
Lámina 1

Dr. Roberto Gómez Cárdenas

Nmap

Free Security Scanner

Audit your network now!



Nmap

Free Security Scanner

Audit your network now!

File Output

Host(s) xanadu vectra playground Scan

Scan Options: General Options:

☐ connect() ☐ SYN Stealth ☐ Ping Sweep ☐ UDP Port Scan ☐ FIN Stealth ☐ Bounce Scan

☐ Don't Resolve ☐ Fast Scan ☐ Range of Ports: ☐ Use Decoy(s)

☐ TCP Ping ☐ TCP&ICMP ☐ ICMP Ping ☐ Don't Ping ☐ OS Detection ☐ Input File

☐ Fragmentation ☐ Get Ident Info ☐ Resolve All ☐ OS Detection ☐ Send on Device

Output from: nmap -sS -O -d -i 192.168.0.1 -p 1-65535 -sS -O -d -i 192.168.0.1

Port	State	Protocol	Service
21	open	tcp	daytime
22	open	tcp	ssh
23	open	tcp	telnet
25	open	tcp	smtp
53	open	tcp	domain
79	open	tcp	finger
111	open	tcp	sunrpc
113	open	tcp	auth
513	open	tcp	login
514	open	tcp	shell

TCP Sequence Prediction: Class=windows positive increments
Diff=15793915990 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.152 2.2.0-mpd -

Nmap

Free Security Scanner

Audit your network now!

File Output

Host(s) xanadu vectra playground Scan

Scan Options: General Options:

☐ connect() ☐ SYN Stealth ☐ Ping Sweep ☐ UDP Port Scan ☐ FIN Stealth ☐ Bounce Scan

☐ Don't Resolve ☐ Fast Scan ☐ Range of Ports: ☐ Use Decoy(s)

☐ TCP Ping ☐ TCP&ICMP ☐ ICMP Ping ☐ Don't Ping ☐ OS Detection ☐ Input File

☐ Fragmentation ☐ Get Ident Info ☐ Resolve All ☐ OS Detection ☐ Send on Device

Output from: nmap -sS -O -d -i 192.168.0.1 -p 1-65535 -sS -O -d -i 192.168.0.1

Port	State	Protocol	Service
21	open	tcp	daytime
22	open	tcp	ssh
23	open	tcp	telnet
25	open	tcp	smtp
53	open	tcp	domain
79	open	tcp	finger
111	open	tcp	sunrpc
113	open	tcp	auth
513	open	tcp	login
514	open	tcp	shell

TCP Sequence Prediction: Class=windows positive increments
Diff=15793915990 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.152 2.2.0-mpd -

Nmap

Free Security Scanner

Audit your network now!

File Output

Host(s) xanadu vectra playground Scan

Scan Options: General Options:

☐ connect() ☐ SYN Stealth ☐ Ping Sweep ☐ UDP Port Scan ☐ FIN Stealth ☐ Bounce Scan

☐ Don't Resolve ☐ Fast Scan ☐ Range of Ports: ☐ Use Decoy(s)

☐ TCP Ping ☐ TCP&ICMP ☐ ICMP Ping ☐ Don't Ping ☐ OS Detection ☐ Input File

☐ Fragmentation ☐ Get Ident Info ☐ Resolve All ☐ OS Detection ☐ Send on Device

Output from: nmap -sS -O -d -i 192.168.0.1 -p 1-65535 -sS -O -d -i 192.168.0.1

Port	State	Protocol	Service
21	open	tcp	daytime
22	open	tcp	ssh
23	open	tcp	telnet
25	open	tcp	smtp
53	open	tcp	domain
79	open	tcp	finger
111	open	tcp	sunrpc
113	open	tcp	auth
513	open	tcp	login
514	open	tcp	shell

TCP Sequence Prediction: Class=windows positive increments
Diff=15793915990 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.152 2.2.0-mpd -

Nmap

Free Security Scanner

Audit your network now!

File Output

Host(s) xanadu vectra playground Scan

Scan Options: General Options:

☐ connect() ☐ SYN Stealth ☐ Ping Sweep ☐ UDP Port Scan ☐ FIN Stealth ☐ Bounce Scan



☐ Don't Resolve ☐ Fast Scan ☐ Range of Ports: ☐ Use Decoy(s)

☐ TCP Ping ☐ TCP&ICMP ☐ ICMP Ping ☐ Don't Ping ☐ OS Detection ☐ Input File

☐ Fragmentation ☐ Get Ident Info ☐ Resolve All ☐ OS Detection ☐ Send on Device

Output from: nmap -sS -O -d -i 192.168.0.1 -p 1-65535 -sS -O -d -i 192.168.0.1



Port	State	Protocol	Service
21	open	tcp	daytime
22	open	tcp	ssh
23	open	tcp	telnet



Características Nmap

- NMAP Network Security Scanner
- Herramienta auditoría red y escáner de seguridad.
 - realiza un “scaneo” de puertos
- Escaneo de puertos: método para descubrir canales de comunicación que se puedan explotar
 - la idea es de probar todos lo que este escuchando.
- Fue diseñada para escanear grandes redes, aunque funciona muy bien escaneando un simple host.
- Realiza 3 funciones:
 1. Escaneo de hosts (“alive”)
 2. Escaneo de puertos de dichos hosts
 3. Determina Sistema Operativo


Lámina 3Dr. Roberto Gómez Cárdenas




Obtención de nmap

- Nmap corre en sistemas Unix, Unix-like, windows.
- Se puede obtener en
 - <http://www.insecure.org>
- La versión para Windows NT se puede encontrar en
 - <http://www.eeye.com/html/Research/Tools/nmapnt.html>
- Nmap está disponible en dos versiones: versión de consola y gráfico.
- Nmap es software libre, disponible con código fuente, bajo la licencia GNU GPL.

Lámina 4Dr. Roberto Gómez Cárdenas



¿Qué puedo hacer con nmap?




- Nmap utiliza paquetes tipo raw de para determinar:
 - Hosts disponibles en la red
 - Servicios (puertos)
 - Tipo de Sistema Operativo (versión del SO)
 - Tipos de filtros/firewalls que están en uso
- La sintáxis de nmap es


```
$ nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>
```


– donde:

 - **Scan Type(s)**
 - es el tipo(s) de scaneo
 - **Options**
 - opciones de scaneo
 - **<host or net #1 ... [#N]>**
 - host(s) a scanear

Lámina 5
Dr. Roberto Gómez Cárdenas



Ejemplo salida nmap



```

amy@#nmap -O -sS vectra/24
Starting nmap V. 2.2-BETA4 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host (192.168.0.0) seems to be a subnet broadcast address (returned 1 extra pi
ngs). Skipping host.
Interesting ports on playground.yuma.net (192.168.0.1):
Port      State      Protocol  Service
22        open       tcp       ssh
111       open       tcp       sunrpc
635       open       tcp       unknown
1024      open       tcp       unknown
2049      open       tcp       nfs


TCP Sequence Prediction: Class=random positive increments
Difficulty=3916960 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2

Interesting ports on vectra.yuma.net (192.168.0.5):
Port      State      Protocol  Service
13        open       tcp       daytime
21        open       tcp       ftp
22        open       tcp       ssh
23        open       tcp       telnet
37        open       tcp       time
79        open       tcp       finger
111       open       tcp       sunrpc
113       open       tcp       auth
513       open       tcp       login
514       open       tcp       shell


TCP Sequence Prediction: Class=random positive increments
Difficulty=17719 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Nmap run completed -- 256 IP addresses (2 hosts up) scanned in 6 seconds
amy@#
  
```

Lámina 6
Dr. Roberto Gómez Cárdenas



Modo gráfico



- Es posible definir las opciones/parámetros a partir de un GUI
- Opcional en ambientes Unix
- Salida por default en Windows

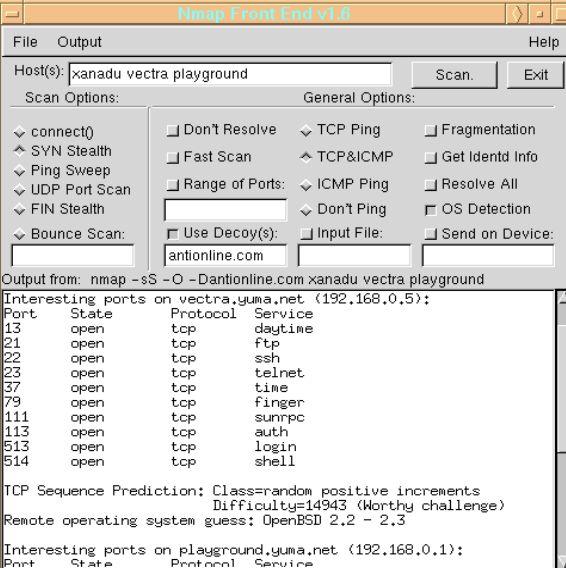




Lámina 7



Lo primero: definir el blanco





- Posible scanear una sola máquina o un conjunto de máquinas
- Por ejemplo un scaneo a una sola máquina:

```
$ nmap 10.14.23.57
```
- Para scanear una conjunto de redes se puede usar una máscara de subred con la opción **-i**
 - host/32 = 1 ip host/24 = 256 ip's
 - host/16 = 65536 host/8 = 2²⁴ ip's
- Por ejemplo:

```
$ nmap -i 192.168.2.0/24
```

 - escanea el rango [192.168.2.0 - 192.168.2.255]



Lámina 8



Determinando host disponibles en la red

- Antes de scanear un host es necesario determinar si el host esta activo.
- Se cuentan con varias técnicas para llevar a cabo lo anterior:
 - ICMP Echo (Ping sweep) Scan
 - TCP ACK sweep
 - TCP SYN sweep
 - ICMP sweep
 - Barrido paralelo
 - No ping alguno

Lámina 9 Dr. Roberto Gómez Cárdenas





ICMO Echo y TCP ACK

- ICMP Echo (Ping sweep) Scan
 - envía paquetes de tipo ICMP echo request (ICMP tipo 8) a cada dirección IP de la red que se especifica.

```
$ nmap -sP 192.45.56.0/24
```
- TCP ACK ping
 - se lanzan paquetes TCP ACK y luego se espera a que lleguen las respuestas
 - posibilidad de especificar un puerto (80 por default)

```
$ nmap -PT 53 192.45.56.0/24
```

Lámina 10 Dr. Roberto Gómez Cárdenas



TCP SYB y Barrido ICMP



- TCP SYN
 - usa un paquete ping (petición de eco ICMP) verdadero.
 - encuentra servidores que están activos y también busca direcciones de broadcast dirigidas a subredes en una red.

```
$ nmap -PS 192.45.56.0/24
```
- Barrido ICMP
 - usa un paquete ping (petición de eco ICMP) verdadero.
 - se trata de direcciones IP alcanzables desde el exterior que envían los paquetes IP entrantes a una subred de servidores.

```
$ nmap -PI 192.45.56.0/24
```

Riesgo detección direcciones broadcast: ataque smurf

Lámina 11 Dr. Roberto Gómez Cárdenas



Barrido paralelo y no-ping

- Barrido paralelo
 - este es el tipo de ping por defecto.
 - usa barridos ACK (**-PT**) e ICMP (**-PI**) en paralelo.
 - posible alcanzar firewalls que filtren uno de los dos (pero no ambos).

```
$ nmap -PB 192.45.56.0/24
```
- Opción no-ping
 - No intenta hacer ping a un host antes de escanearlo.
 - Permite el escaneo de redes que no permiten que pasen peticiones (o respuestas) de ecos ICMP por su firewall.

```
$ nmap -p0 192.45.56.0/24
```

Lámina 12 Dr. Roberto Gómez Cárdenas

Opciones determinar host disponibles en modo gráfico

TEC DE MONTERREY
Campus Estado de México

netwox security scanner

Output from: nmap -sS -O -Dantionline.com xanadu vectra playground
Interesting ports on vectra.uvma.net (192.168.0.5):
Port State Protocol Service
113 open tcp daytime

Lámina 13 Dr. Roberto Gómez Cárdenas


El escaneo de puertos

- Mayoría basadas en el handshake de TCP
- Tipos de scaneo
 - Sencillos
 - Vanilla TCP connect() scanning
 - UDP raw ICMP port unreachable scanning
 - Avanzados
 - TCP SYN (half open)
 - Stealth FIN
 - Stealth Xmas Tree
 - Stealth Null
 - envío paquetes fragmentados
 - Otros
 - TCP ftp proxy (bounce attack) scanning
 - TCP ACK and Window scanning


TEC DE MONTERREY
Campus Estado de México

netwox security scanner

Lámina 14 Dr. Roberto Gómez Cárdenas



El tree way handshake de TCP



1. Dispositivo 1 envía su número de secuencia y máximo valor del tamaño del segmento al dispositivo 2
2. Dispositivo 2 responde enviando su numero de secuencia y el máximo valor del tamaño del segmento al dispositivo 2
3. Dispositivo 1 confirma (ack) recepción del número de secuencia y de la información del tamaño de segmento

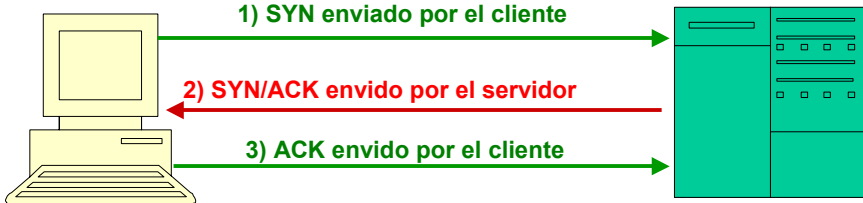




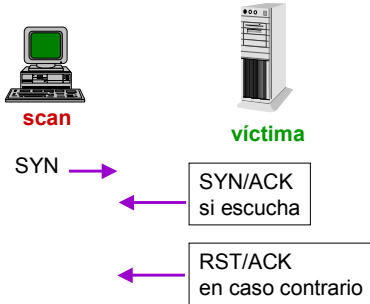
Lámina 15
Dr. Roberto Gómez Cárdenas



Vanilla TCP connect() scanning



- Identificar puertos TCP que esten escuchando.
- No requiere privilegios de root para ejecutarse
- Es la opción por default



```
$ nmap 10.14.23.57
$ nmap -sT 10.14.23.57
```

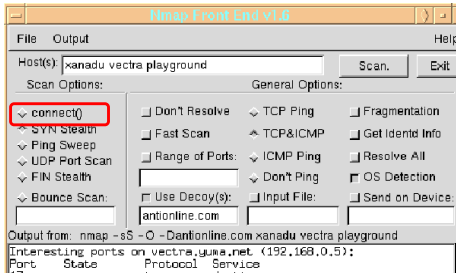




Lámina 16




TCP SYN (half open)




- A diferencia de Vanilla TCP Connect Scan, TCP Half-Open no incluye el paquete final del ACK
- Requiere privilegios de root para ejecutarse

\$ **nmap -sS** 10.14.23.57



scan



víctima

SYN →

SYN/ACK
si escucha

←

RST/ACK
si no

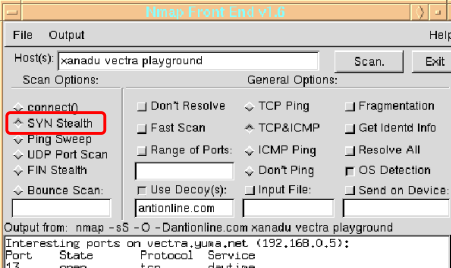




Lámina 17




Escaneo UDP raw ICMP port unreachable scanning




- Objetivo: puertos UDP abiertos
- A veces es tremendamente lento
- No se puede garantizar su llegada.
- Ejemplo:

\$ **nmap -sU** 10.14.23.57



scan



víctima

Paq. UDP
0 bytes

→

Mensaje ICMP
pto. no alcanzable
pto cerrado

←

si no se recibe
puerto abierto

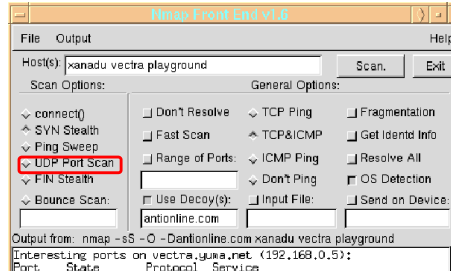




Lámina 18




Reconocimiento avanzado de puertos




- Escaneos anteriores suelen dejar huellas de su ejecución en los registros logs de las máquinas escaneadas
 - por ejemplo: en /var/log/messages
- Objetivo: cruzar barreras sin ser detectados.
- Nmap cuenta con modos de escaneos invisibles de forma que se evita finalizar la negociación TCP, evitando el registro en los archivos **logs**.
- Los puertos cerrados responden con un RST, los puertos abiertos deben ignorar los paquetes (RFC 794).
- Primer ejemplo: **TCP SYN (half open)**

Lámina 19


Dr. Roberto Gómez Cárdenas




TCP FIN Scan



- Utilizado para identificar los puertos TCP abiertos
 - basado en reacción petición cierre transacción puerto de TCP
 - utiliza un paquete fin vacío
- Puede pasar por desapercibido en firewalls básicos o por routers de frontera que filtren paquetes TCP con la combinación de las banderas (FIN) y (ACK)



scan



victima

FIN →

← RST puerto cerrado

← paquete ignorado: abierto

no se envía nada

\$ nmap -sF 10.14.23.57

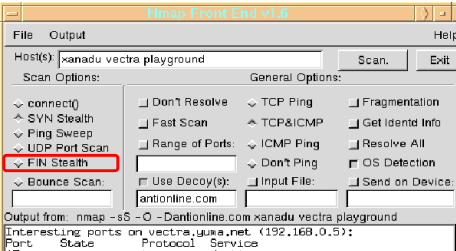





Lámina 20




TCP Xmas Scan



- Utiliza paquetes TCP extrañamente configurados
 - contienen un número de secuencia de 0 y las banderas Urgent(URG), Push(PSH) y FIN activadas
- Este tipo de escaneo puede pasar por desapercibido ante firewalls básicos o routers de frontera



scan



victima

\$ nmap -sX 10.14.23.57


FIN →

no se envía nada


← RST puerto cerrado

← ~~paquete ignorado: abierto~~
no hay respuesta, se descarta el paquete


Lámina 21
Dr. Roberto Gómez Cárdenas




TCP NULL Scan



- Este tipo de escaneo utiliza también una extraña configuración de paquetes TCP, con número de secuencia 0, y todas las banderas desactivadas
- La mayoría de los routers intermedios y firewalls están prevenidos contra este tipo de intentos por lo que no es probable que obtengamos ninguna respuesta.



scan



victima

\$ nmap -sN 10.14.23.57


FIN →

no se envía nada


← RST puerto cerrado

← ~~paquete ignorado: abierto~~
no hay respuesta, se descarta el paquete

Lámina 22
Dr. Roberto Gómez Cárdenas



TCP SYN/FIN With Fragments Scan



- Utilizado para poder pasar por un dispositivo de filtrado.
- Se fragmenta un paquete dentro del encabezado TCP.
 - dividir el encabezado del paquete TCP en varios paquetes para dificultar tarea filtros de paquetes, IDS y otras herramientas
 - si el dispositivo de filtrado no reensambla el paquete, no sabrá que es un paquete de tipo TCP SYN/FIN.

\$ nmap -sS -f 10.14.23.57

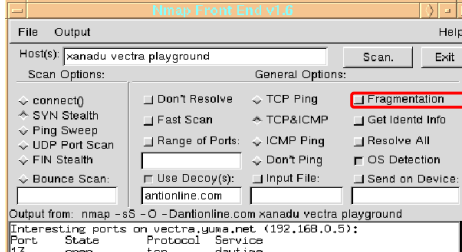




Lámina 23



Ataque de rebote FTP y nmap



- Posible escanear puertos TCP desde ftp server "proxy".
- Consecuencias:
 - posible conectarse a un servidor ftp tras una firewall, y escanear aquellos puertos que con más probabilidad se encuentren bloqueados (el 139 es uno bueno).
- No todos los hosts son vulnerables a este ataque

\$ nmap -b 10.14.23.57 192.45.2.12

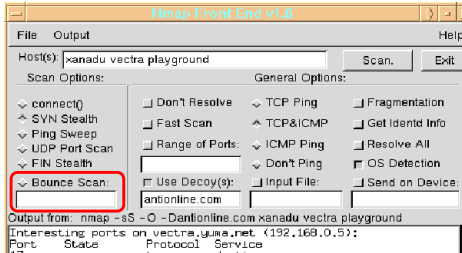




Lámina 24



Reconocimiento del sistema operativo



- “TCP/IP Fingerprinting”, de acuerdo a la implementación del stack de protocolos TCP/IP se puede reconocer el tipo de Sistema Operativo
 - prueba “estímulo/respuesta”.
 - desarrolladores interpretan de diferente manera los RFC’s.
 - “Remote OS detection via TCP/IP Stack FingerPrinting”, Fyodor

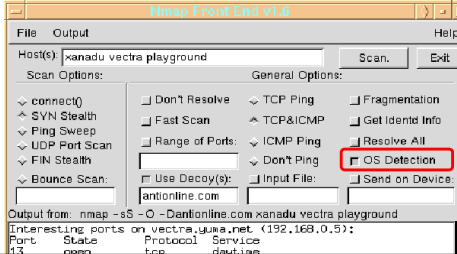


\$ nmap -O 10.14.23.57


Lámina 25





Opciones adicionales de nmap



Opción	Acción
-v	Verbose
-oN	Enviar la bitácora a un archivo
-iL	Tomar targets desde archivo
-p	Especificar rango de puertos
-g	Especifica el número de puerto de origen
-F	Solo escanear puertos especificados en /etc/services
-S	Spoofing de dirección IP, enmascara la dirección IP fuente, funciona bajo un mismo segmento Ethernet.



Lámina 26
Dr. Roberto Gómez Cárdenas



Combinando opciones

- Para hacer un escaneo estandar de tcp
`# nmap victima.org`
- Para checar la red clase C en la cual warez.com pone sus servicios (via fragmented SIN scan)
`# nmap -fsp 21,22,23,25,80,110warez.com/24`
- Para escanear la misma red por todos los servicios en su /etc/services via tcp (muy rápido)
`# nmap -F warez.com/24`
- Escanear secret.pathetic.net usando un ftp bounce attack off de ftp.pathe.net:
`# nmap -b ftp.pathe.net secret.pathe.net`


Lámina 27 Dr. Roberto Gómez Cárdenas




Ejemplos combinación opciones

- Para encontrar hosts que esten arriba en la clase C 193.14.12, .13, .14, .15, ..., .30 .
`# nmap -P '192.14.[12-30].*'`
– otra forma de hacer lo anterior es:
`# nmap -P 193.14.23-30.0-255`
- Escaneo de puertos entre 1 y 65000
`# nmap -p1-65000 victima.org/24`
- La forma más común:
`# nmap -O -Ss victima.org/24`

Lámina 28 Dr. Roberto Gómez Cárdenas



Una última opción




- Fyodor**, el desarrollador de esta herramienta, implementó la opción **-oS**, que muestra la salida del **Nmap** en un formato que les encantará a los **Script-kiddies**

nmap -oS - carlets


```

StaRtIng nmap V. 2.54B3T431 ( www.1n$ecur3.ORG/nmap/ )
Int3r3sting pOrtz On carletz.home.org (192.168.0.99):
(The 1545 Portz scannEd but nOT sh0wn bel0w ar3 In $tatE: cLOS3D)
Port    Stat3    S3rv1Ce
22/tcp  OpeN    $$H
25/Tcp  OpEn    smtp
80/tcp  Op3n    htTp
139/tcP  op3n    N3Tb1Oz-Ssn
143/tCP  Open    imap2
515/tcp  fl!t3red prinT3r
3128/tcp Op3n    sqljd-HtTP
3306/tCp Op3n    my$ql
6000/tcp Op3n    x11
  
```

Lámina 29 Nmap rUn c0mpl3ted -- 1 !P aDdr3Sz (1 hOst uP) scANnEd !n 3 \$ec

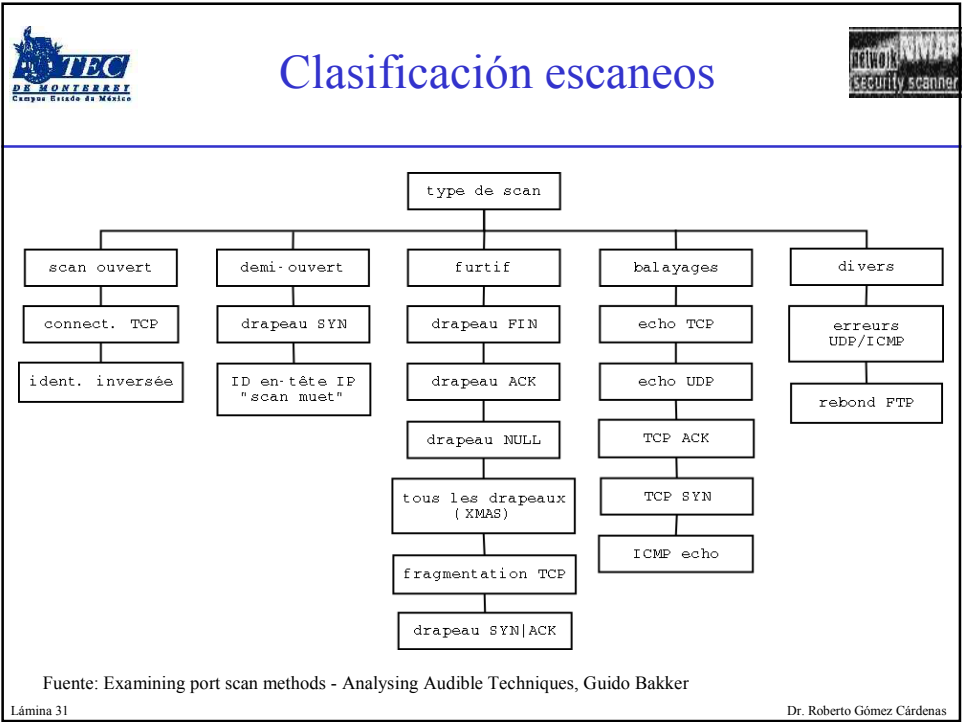


¿Es nmap lo único?



- Posible construir herramienta
 - manejo de sockets tipo raw
- Otras herramientas
 - ISIS (IP Stack Integrity Checker)
 - hping: construcción paquetes, no soporta varios paquetes ICMP
 - más usado hping2
 - sing
 - icmppush

Lámina 30 Dr. Roberto Gómez Cárdenas





¿Y cómo me defiendo?

PortSentry

Lámina 32



Dr. Roberto Gómez Cárdenas



Psionic PortSentry

- Tercer componente de la suite Abacus
 - logcheck y hostsentry son los otros dos
- Detecta y guarda un log de los escaneos de puertos,
 - incluyen escaneos clandestinos (stealth)
 - básicamente debería ser capaz de detectar cualquier cosa que sea posible hacer con Nmap
- Posible configurar para que bloquee la máquina atacante haciendo difícil el completar un escaneo de puertos.
 - no se recomienda ya que se podría utilizar para generar un ataque de denegación de servicio en hosts legítimos
- Disponible en:
 - <http://www.psionic.com/abacus/portsentry/>



Lámina 33 Dr. Roberto Gómez Cárdenas



Archivos generados

- Básicamente se usan los siguientes archivos:
 - **portsentry** Programa binario de Portsentry.
 - **portsentry.conf** Archivo de configuración de Portsentry.
 - **portsentry.ignore** Archivo donde se declaran los hosts que serán ignorados por Portsentry.
- Después de correr por primera vez Portsentry, se crearán los siguientes archivos con información de las actividades que se han llevado a cabo:
 - **portsentry.history**
 - **portsentry.blocked.***



Lámina 34 Dr. Roberto Gómez Cárdenas



¿Cómo funciona?

- Depende de los archivos de configuración.
 - el más importante es el fichero portsentry.conf.
 - aquí se define como reaccionará portsentry frente a la adversidad.
- Necesario los diferentes modos operativos y lo que hacen.
- Portsentry puede usar seis modos diferentes, según la opción elegida al arrancar.



Lámina 35 Dr. Roberto Gómez Cárdenas



Modos

- **tcp**
 - es el modo básico.
 - se atan los puertos TCP encontrados en el fichero de config en la parte "portconfiguration".
 - posible atar hasta el limite de 64 puertos.
- **udp**
 - hace lo mismo que la anterior para los puertos UDP.
- **stcp**
 - la "s" significando "stealth" (furtivo).
 - esta opción y las siguientes son disponibles solamente bajo Linux.
 - usa un socket para vigilar los paquetes llegando, es decir los puertos no se atan a nada.



Lámina 36 Dr. Roberto Gómez Cárdenas



Modos

- **sudp**
 - hace lo mismo que la anterior para los puertos UDP.
- **atcp y audp**
 - son las opciones más eficaces
 - "a" significa "advanced"
 - hace una lista de los puertos TCP y UDP escuchando,
 - si seleccionan ambos es posible bloquea el host tratando de conectar con estos puertos, a menos que el dicho host sea presente en el fichero portsentry.ignore.

Lámina 37 Dr. Roberto Gómez Cárdenas



¿Y que hace?

- Puede crear logs.
 - posible usar logcheck al lado de portsentry.
- Mandar un correo para informar de una tentativa de intrusión.
- Puede escribir el "target host" en el fichero /etc/hosts.deny, para aprovechar TCPWrappers.
- El host local puede cambiar la ruta del tráfico de la red hacia un host muerte (drooping route)
- El host local puede "echar" los paquetes vía la herramienta local de filtraje de paquete.

Lámina 38 Dr. Roberto Gómez Cárdenas



Archivo portsentry.conf



- La primera sección concierne los puertos a monitorear

```
TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111, . . . , 40425,49724,54320"
UDP_PORTS="1,7,9,66,67,68,69,111,137,138, . . . ,32774,31337,54321"
```
- La segunda son las opciones de Advanced Stealth Scan
 - numero puertos se desea que PortSentry monitore en modo avanzado
 - todo puerto abajo de este sera monitoreado, a excepción de los excluidos

```
ADVANCED_PORTS_TCP="1024"
ADVANCED_PORTS_UDP="1024"
ADVANCED_EXCLUDE_TCP="113,139"
ADVANCED_EXCLUDE_UDP="520,138,137,67"
```
- La tercera: archivos de configuración

```
IGNORE_FILE="/usr/local/psionic/portsentry/portsentry.ignore"
HISTORY_FILE="/usr/local/psionic/portsentry/portsentry.history"
BLOCKED_FILE="/usr/local/psionic/portsentry/portsentry.blocked"
```

Lámina 39 Dr. Roberto Gómez Cárdenas




Secciones 4 y 5 de configuración


- Cuarta: Misc. Configuration Options
 - DNS: 1-> DNS lookups para los host atacantes

```
RESOLVE_HOST = "1"
```
- Quinta: Opciones de respuesta
 - opciones de reacción ante un ataque
 - acción será ejecutada si un ataque es detectado
 - \$TARGET\$ = host atacante, \$PORT\$ puerto atacante
 - posibles acciones
 - ignorar
 - dropping routes
 - tcp Wrappers
 - external command

Lámina 40 Dr. Roberto Gómez Cárdenas



Acciones PortSentry




- Ignorar
 - habilitar respuestas para UDP/TCP
 - 0 = Do not block UDP/TCP scans.
 - 1 = Block UDP/TCP scans.
 - 2 = Run external command only (KILL_RUN_CMD)

```
BLOCK_UDP="1"
BLOCK_TCP="1"
```


- Dropping routes
 - usado para tirar la ruta del paquete o añadir el host a una tabla de filtrado local

```
KILL_ROUTE="/sbin/route add -host $TARGET$ reject
KILL_ROUTE="/usr/local/bin/iptables -I INPUT -s $TARGET$ -j DROP
```

Lámina 41
Dr. Roberto Gómez Cárdenas



Dos últimos tipos de acciones



- TCP Wrappers
 - Añadir hosts al archivo hosts.deny para uso de wrappers, dos formatos



```
KILL_HOSTS_DENY="ALL: $TARGET$"
```

→
estilo viejo

```
KILL_HOSTS_DENY="ALL: $TARGET$ : DENY"
```


→
estilo nuevo
- External Command
 - comando que se ejecuta cuando un host se conecta
 - puede ser lo que uno desea
 - puede ejecutar comando antes (1) de que la “ruta” sea tirada o después (0) dependiendo de la opción KILL_RUN_CMD_FIRST

```
KILL_RUN_CMD_FIRST = "0"
KILL_RUN_CMD="/usr/local/etc/notify"
```




```
#!/bin/sh
echo "My computer has been attacked" | \
mail -s "Strobe Attack on My System" you@your-email.com
```

Lámina 42
Dr. Roberto Gómez Cárdenas




Una última recomendación




- Para evitar alarmas falsas y enorme "logging", se recomienda usar el archivo portsentry.ignore.
- Posible añadir la dirección de la red local con los bits del netmask, o la dirección IP de algunas maquinas.
- Ejemplo:


```
$ cat portsentry.ignore
127.0.0.1/32
0.0.0.0
192.168.2.0/24
192.168.0.0/16
192.168.2.1/32
$
```

Lámina 43
Dr. Roberto Gómez Cárdenas




Ejemplo bitácora portsentry




```
Active System Attack Alerts
=====
Jul 23 08:59:42 asterix portsentry[575]: attackalert: Connect from
host: dia25021.toto.cachafas.mx/184.241.25.21 to UDP port: 161
Jul 23 08:59:42 asterix portsentry[575]: attackalert: Host:
184.241.25.21 is already blocked. Ignoring
Jul 23 12:07:24 asterix portsentry[575]: attackalert: Connect from
host: eye.alguien.cachafas.mx/122.254.7.182 to UDP port: 161
Jul 23 12:07:24 asterix portsentry[575]: attackalert: Host:
122.254.7.182 is already blocked. Ignoring
Jul 23 12:07:26 asterix portsentry[575]: attackalert: Connect from
host: eye.alguien.cachafas.mx/122.254.7.182 to UDP port: 161
Jul 23 12:07:26 asterix portsentry[575]: attackalert: Host:
122.254.7.182 is already blocked. Ignoring
Jul 23 12:07:27 asterix portsentry[575]: attackalert: Connect from
host: eye.alguien.cachafas.mx/122.254.7.182 to UDP port: 161
```

Lámina 44
Dr. Roberto Gómez Cárdenas




Puertos más probados y atacados




- Login services
 - telnet (23/tcp)
 - SSH (22/tcp)
 - FTP (21/tcp)
 - NetBIOS (139/tcp)
 - rlogin et al (512-514)
- RPC and NFS
 - Portmap/rpcbind (111/tcp and 111/udp)
 - NFS (2049/tcp and 2049/udp)
 - lockd (4045/tcp and 4045/udp)

- NetBios en Windows NT y 2000
 - 135 (tcp y udp), 147
 - 138
 - Windows 2000
- X Windows
 - 6000/tcp hasta 6255/tcp
- Naming services
 - DNS (53/udp) máquinas no servidores DNS
 - DNS zone transfers (53/tcp)
 - LDAP (389/tcp and 389/udp)

Lámina 45
Dr. Roberto Gómez Cárdenas





Puertos más probados y atacados



- Mail
 - SMTP puerto 25
 - pop 109/tcp y 110/tcp
 - imap 143/tcp
- Web
 - puerto 80 HTTP
 - puerto 443 SSL
 - High-order HTTP 8000/tcp, 8080/tcp, 8888/tcp
- Small Services
 - ports below 20/tcp y 20/udp, time (37/tcp y 37/udp)

- Miscelaneo
 - TFTP: 69/udp
 - finger 79/tcp
 - NNTP 119/tcp
 - NTP 123/tcp
 - LPD 515/tcp
 - syslog 514/udp
 - SNMP 161/tcp y 161/udp
 - BGP 179/tcp
 - SOCKS 1080/tcp

Lámina 46
Dr. Roberto Gómez Cárdenas





Cerrando puertos

Sistemas Operativos *nix

Lámina 47

Dr. Roberto Gómez Cárdenas





Los servicios de red

- Servicio:
 - puerto, protocolo y proceso
- Todo a cargo del proceso inetd, el cual sabe que proceso invocar ya que puede determinar la relación entre puertos y servicios.
- Para poder realizar la petición apropiada de acuerdo a los solicitado tiene que:
 - consultar el archivo /etc/services
 - consultar archivo configuración inted.conf

Lámina 48

Dr. Roberto Gómez Cárdenas



Ejemplo /etc/services

Networks services, Internet style

tcpmux 1/tcp

echo 7/tcp

ftp 21/tcp

telnet 23/tcp

smtp 25/tcp mail

time 37/tcp timeserver

time 37/udp timeserver

Host specific functions

tftp 69/udp

rje 77/tcp

finger 79/tcp

link 87/tcp ttylink

Unix specific services

these are not officially assigned

exec 512/tcp

login 513/tcp

shell 514/tcp cmd # no passwd used

printer 515/tcp spooler # line printer spooler

courier 530/tcp rpc # experimental

uucp 540/tcp uucpd # uucp daemon

biff 512/udp comsat

who 513/udp whod

talk 517/udp

kerberos 750/udp kdc # Kerberos by server

kerberos 750/tcp kdc # Kerberos by server



lockd 4045/udp # NFS lock daemon

lockd 4045/tcp

fs 7100/tcp # Font server

Lámina 49

Dr. Roberto Gómez Cárdenas



Atención petición servicio

Ejemplo petición de una sesión Telnet

Niveles más altos

in.telnetd

↑

inetd (super server)

20 23 25 53 119

Nivel TCP



Nivel IP

↑

Petición de red

Lámina 50



Dr. Roberto Gómez Cárdenas



Archivo inetd.conf

- Demonio inetd lee archivo inetd.conf para sus acciones
- En sistema V
 - /etc/inet/inetd.conf
- En BSD
 - /etc/inetd.conf
- Si es modificado lo mejor es bootear
 - en algunos sistemas es posible modificarlo en tiempo real

Lámina 51 Dr. Roberto Gómez Cárdenas



Estructura archivo inted.conf

- Esta compuesto por líneas,
 - cada una se indica el nombre del servicio que atenderá y su programa a ejecutar.
- Las líneas que comienzan con un '#' son ignoradas
- Campos líneas:
 - Nombre del servicio, (ftp, telnet, etc)
 - Tipo de socket. (stream, dgram, etc)
 - Protocolo. (tcp, udp)
 - wait/nowait
 - usuario con el que se ejecutara el servicio. (root, nobody, etc)
 - programa que brindara el servicio. (/usr/sbin/tcpd /usr/sbin/in.telnetd)



Lámina 52 Dr. Roberto Gómez Cárdenas



Ejemplo archivo /etc/inetd.conf

```
#:STANDARD: These are standard services.  
  
ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.ftpd  
telnet stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetd  
  
#:BSD: Shell, login, exec and talk are BSD protocols.  
shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd  
login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind  
exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd  
  
#:INFO: Info services  
  
finger stream tcp nowait nobody /usr/sbin/tcpd /usr/sbin/in.fingerd  
ident stream tcp nowait nobody /usr/sbin/identd identd -i  
  
#:BOOT: Tftp service is provided primarily for booting. Most sites  
# run this only on machines acting as "boot servers."  
#tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /boot  
#bootps dgram udp wait root /usr/sbin/bootpd bootpd -i -t 120
```



Lámina 53 Dr. Roberto Gómez Cárdenas



El demonio tcpd

- TCP-Wrappers
- Se invoca dentro del último campo del archivo `inetd.conf` como `/usr/sbin/tcpd`
- Cuando `inetd` recibe un pedido por un servicio, en vez de ejecutar el programa servidor correspondiente, ejecuta el `tcpd` y le pasa como parámetro el nombre del servidor correspondiente.
- El `tcpd` decide si permite el acceso o no al servicio, dependiendo de unas reglas de acceso y la dirección del cliente que lo solicita.
 - dichas reglas se encuentran en los archivos `hosts.allow` y `hosts.deny` en el directorio `/etc`



Lámina 54 Dr. Roberto Gómez Cárdenas



tcpd y archivos host.*

- Pasos que realiza el tcpd con los archivos hosts.allow y hosts.deny:
 1. Lee el archivo hosts.allow y verifica si la dirección o nombre del host que trata de conectarse, tiene acceso al servicio. Si es así, ejecuta el servicio correspondiente y le da el control de la conexión, no lee el archivo hosts.deny.
 2. Si en el paso anterior, no encontró el host, lee el archivo hosts.deny y busca la dirección o nombre del host. Si lo encuentra, rechaza la conexión.
 3. Si en ninguno de los dos archivos encontró el nombre o dirección de host, le permite el acceso.

Lámina 55 Dr. Roberto Gómez Cárdenas



Ejemplos archivos host.*



Archivo host.deny:

```
ALL:ALL
```

Archivo host.allow:

```
ipop3d: ALL: ALLOW
in.telnetd: .myschool.edu : ALLO
# allow connections from my local network
ALL: ALL@127.0.0.1 : ALLOW
# allow all connections from computers on my network
ALL: ALL@192.168.124.1 : ALLOW
ALL: ALL@192.168.124.10 : ALLOW
ALL: ALL@192.168.124.11 : ALLOW
ALL: ALL@192.168.124.20 : ALLOW
```



Lámina 56 Dr. Roberto Gómez Cárdenas



xinetd

- Ofrece capacidades de control de acceso similares a las proporcionadas por tcp_wrapper.
- Aspectos particulares
 - control de acceso para los servicios TCP, UDP y RPC
 - control de acceso basado en intervalos de tiempo
 - prevención contra ataques del tipo Negación de Servicios (DoS)
 - limitación del número de servidores del mismo tipo ejecutándose en forma simultánea.
 - limitación del número total de servidores
 - limitación del tamaño de los archivos log.
 - puede oficiar de proxy para otros sistemas lo cual resulta muy práctico en el caso de usar (NAT)

Lámina 57Dr. Roberto Gómez Cárdenas





Ejemplo archivo xinetd.conf

```
service ftp
{
    socket_type = stream
    wait        = no
    user        = root
    server       = /usr/sbin/in.ftpd
    server_args = -l
    instances   = 4
    access_times = 7:00-12:30 13:30-21:00
    nice        = 10
    only_from   = 192.168.1.0/24
}

service ntalk
{
    socket_type = dgram
    wait        = yes
    user        = nobody
    server       = /usr/sbin/in.ntalkd
    only_from   = 192.168.1.0/24
}
```

Lámina 58Dr. Roberto Gómez Cárdenas





Bajando servicios a “tiempo real”

- Es posible matar el proceso inetd (kill)
- Otra opción es “parar” el servicio:

```
# cd /etc/rc.d/init.d  
# ./servicioX stop
```
- Para “levantar” el servicio:

```
# cd /etc/rc.d/init.d  
# ./servicioX start
```



Lámina 59 Dr. Roberto Gómez Cárdenas



Cerrando puertos

Sistema Operativo Windows ****



Lámina 60 Dr. Roberto Gómez Cárdenas



Los puertos en Windows

- Algunos de los puertos y servicios sin importar si están bloqueados son levantados de forma automática por el servicio que dejas permitido
- Las llamadas a RCP utilizan una asignación de puertos dinámica
- Windows 2000 utiliza al menos 10 puertos no definidos por la IANA
- Es relativamente fácil bloquear servicios TCP con W2K,
 - es mejor filtrar tanto TCP como UDP en los equipos de conectividad (switch's o ruteadores), recomendado por los expertos del área.

Lámina 61 Dr. Roberto Gómez Cárdenas



Desvinculación de servicios en Windows 95/98/Me

- El camino es: Mi Pc->Panel de control->Red.
- En la solapa de Configuración seleccione TCP/IP, y pulsar en Propiedades.
- Tras Aceptar el mensaje que aparece,
 - seleccionar Enlaces donde debe desmarcar todos excepto Cliente para Redes Microsoft ó Inicio de sesión en Microsoft Family.
- Luego pulsar en Aceptar tantas veces sea necesario, para a continuación reiniciar el equipo.

Lámina 62 Dr. Roberto Gómez Cárdenas

Bloqueo puertos Windows 2000 (1/2)

Propiedades de Conexión de área local

General | Recurso compartido

Conectar usando:
Intel(R) PRO/100 VE Network Connection

Configurar

Esta conexión utiliza los componentes seleccionados:
☒ Cliente para redes Microsoft
☒ Compartir impresoras y archivos para redes Microsoft
☒ Protocolo Internet (TCP/IP)

Instalar... Desinstalar Propiedades

Descripción:
Protocolo TCP/IP. El protocolo de red de área extendida predeterminado que permite la comunicación a través de redes diversas interconectadas.

☒ Mostrar icono en la barra de tareas al conectar

Aceptar Cancelar

Propiedades de Protocolo Internet (TCP/IP)

General

Puede hacer que la configuración IP se asigne automáticamente si su red es compatible con este recurso. De lo contrario, necesita consultar con el administrador de la red cuál es la configuración IP apropiada.

☒ Obtener una dirección IP automáticamente

☐ Usar la siguiente dirección IP:
Dirección IP:
Máscara de subred:
Puerta de enlace predeterminada:

☒ Obtener la dirección del servidor DNS automáticamente

☐ Usar las siguientes direcciones de servidor DNS:
Servidor DNS predilecto:
Servidor DNS alternativo:

Avanzada...

Aceptar Cancelar

Configuración avanzada de TCP/IP

Configuración de IP | DNS | WINS | Opciones

Opciones

Direcciones IP:
Dirección IP:
Máscara de subred:
DHCP habilitado

Agregar... Modificar... Quitar

Puertas de enlace predeterminadas:
Puerta de enlace:
Métrica:

Agregar... Modificar... Quitar

Métrica de la interfaz: 1

Aceptar Cancelar

Lámina 63

Bloqueo puertos Windows 2000 (2/2)

Configuración avanzada de TCP/IP

Configuración de IP | DNS | WINS | Opciones

Opciones

Configuración opcional:
Servidor IP:
Filtro TCP/IP

Propiedades

Descripción:
El filtro TCP/IP le permite controlar el tipo de tráfico de red TCP/IP que llega a su equipo de Windows.

Aceptar Cancelar

Filtro TCP/IP

☒ Habilitar filtro TCP/IP (todos los adaptadores)

☒ Permitir todos
☐ Permitir sólo
Puertos TCP:
Agregar... Quitar

☒ Permitir todos
☐ Permitir sólo
Puertos UDP:
Agregar... Quitar

☒ Permitir todos
☐ Permitir sólo
Protocolos IP:
Agregar... Quitar

Aceptar Cancelar

Agregar filtro

Puerto TCP:
Aceptar Cancelar

Agregar filtro

Puerto UDP:
Aceptar Cancelar

Agregar filtro


Protocolo IP:
Aceptar Cancelar

Lámina 64

Dr. Roberto Gómez Cárdenas




Algunos utilerías utiles




- netstat
- fport

Lámina 65
Dr. Roberto Gómez Cárdenas



netstat



- Comando para Windows y Unix
- Ejecutar desde modo comando

C:\>netstat -an

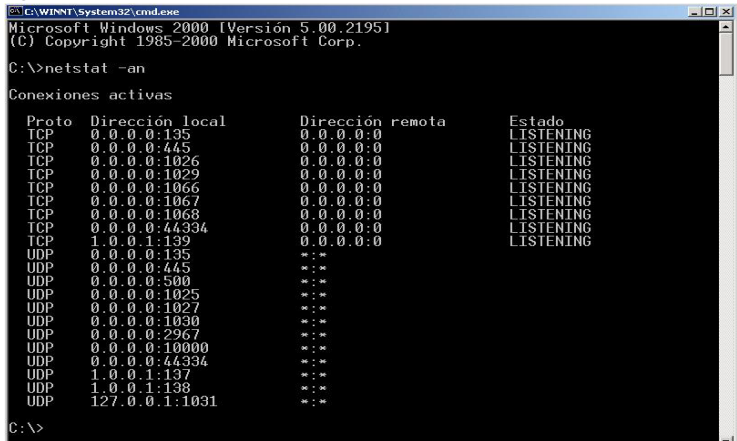


Lámina 66
Roberto Gómez Cárdenas



Fport -

<http://www.foundstone.com/>



- Fport reporta todos los puertos TCP y UDP abiertos y la aplicación dueña de dichos puertos.




```

C:\Documents and Settings\rilira9225\Desktop>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com


Pid  Process          Port  Proto  Path
---  -
384  svchost             -> 135   TCP    C:\WINNT\system32\svchost.exe
8    System              -> 139   TCP
8    System              -> 445   TCP
792  MSTask              -> 1025  TCP    C:\WINNT\system32\MSTask.exe
8    System              -> 1043  TCP
1220 Netscp              -> 1347  TCP    C:\Program Files\Netscape\Netscape\Netscp.exe
1220 Netscp              -> 1348  TCP    C:\Program Files\Netscape\Netscape\Netscp.exe
1856 IEEXPLORE          -> 1717  TCP    C:\Program Files\Internet Explorer\IEEXPLORE
1908 SchClient         -> 1746  TCP    C:\Program Files\SSH Communications Security\SSH
1220 Netscp              -> 5180  TCP    C:\Program Files\Netscape\Netscape\Netscp.exe
1620 WCESCOMM           -> 5679  TCP    C:\Program Files\Microsoft ActiveSync\WCESCOMM.EXE
384  svchost             -> 135   UDP    C:\WINNT\system32\svchost.exe

```

Lámina 67
Dr. Roberto Gómez Cárdenas



Referencias



- <http://www.linuxsecurity.com>
- <http://www.sans.org>
- <http://www.infosyssec.org>
- <http://www.securityfocus.com>
- <http://www.cs.purdue.edu/coast/hotlist/>
- Página de dominios/nombres
 - <http://www.allwhois.com>
- Página para puertos/servicios
 - <http://www.iana.org/numbers.html>
 - <http://www.portsdb.org/>

Lámina 68
Dr. Roberto Gómez Cárdenas