nmap y Nessus

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez

Herramientas prevención

- Herramientas diseñadas para prevenir ataques computacionales
- Herramientas destinadas a dificultar el trabajo de penetración de personas ajenas al sistema.
- Encargadas de encontrar de forma automática vulnerabilidades de los sistemas
- Pequeño problema:
  - también las puede usar el intruso para ver cuales son las debilidades del sistema que desea atacar

Limites de las herramientas

- Las herramientas no son un sustituto para:
  - el sentido común.
  - La responsabilidad del usuario, operador o administrador.
- No son un corrector o reparador de los problemas que ha detectado.
  - es el administrador el que debe hacerlo
- No previenen/detectan ataques de ingenieria social

Lámina 3 Dr. Roberto Gómez

2006 Top 100 Security Tools

- Encuesta llevada a cabo por Fyodor
- Sección Security Tools de la página: www.insecure.org
  - también incluye una lista de listas de seguridad
- Herramientas comerciales y libres
- Historial
  - 50 herramientas: mayo/junio 200 encuesta 1,200 usuarios de Nmap de la lista de nmap-hackers
    - paticipantes podían sugerir hasta 5 herramientas
  - 75 herrramientas: mayo 2003, participantes podían sugerir hasta 8 herramientas (1,854 participantes)
  - 100 herramientas: 2006, 3,243 usuarios
    - incremento en inalámbricas y “exploitation frameworks”

Lámina 4 Dr. Roberto Gómez

Las 100 herramientas seguridad

1. Nessus ($)
2. Wireshark (Ethereal)
3. Snort ($)
4. Netcat
5. Metasploit Framework
6. Hping2
7. Kismet
8. TCPDump/WinDump
9. Cain & Abel
10. Johtn the Ripper
11. Ettercap
12. Nikto
13. Ping/traceroute/ping/telnet/whois/netstat
14. OpenSSH/ PuTTY / SSH
15. THC Hydra
16. Paros Proxy
17. Dsniff
18. NetStumbler
19. THC Amap
20. GFI LANguard ($)
21. Aircrack
22. Superscan
23. Netfilter
24. Sysinternals
25. Retina ($)
26. Perl / Python / Ruby
27. L0pthCrack ($)
28. Scapy
29. Sam Spade
30. GnuPG / PGP
31. AirSnort
32. BackTrack

Lámina 5 Dr. Roberto Gómez

Las 100 herrramientas (2)

33. P0f
34. Google
35. WebScarab
36. Ntop
37. Tripwire ($)
38. Ngrep
39. NbtScan
40. WebInspect ($)
41. OpenSSL
42. XProbe2
43. EtherApe
44. Core Impact ($)
45. IDA Pro ($)
46. SolarWinds ($)
47. Pwdump
48. LSoF
49. RainbowCrack
50. Firewalk
51. Angry IP Scanner
52. RKHunter
53. Ike-scan
54. Arpwatch
55. KisMAC
56. OSSEC HIDS
57. Openbsd PF
58. Nemesis
59. Tor
60. Knoppix
61. ISS Internet Scanner ($)
62. Fport
63. chkrootkit
64. SPIKE Proxy

Lámina 6 Dr. Roberto Gómez

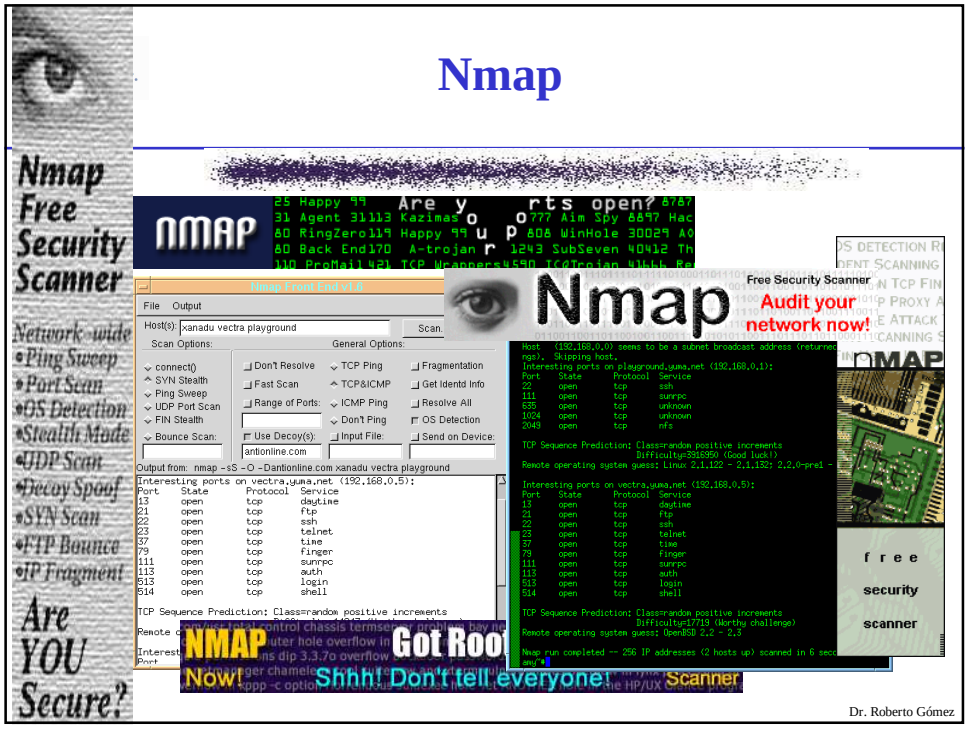
Las 100 herrramientas (3)

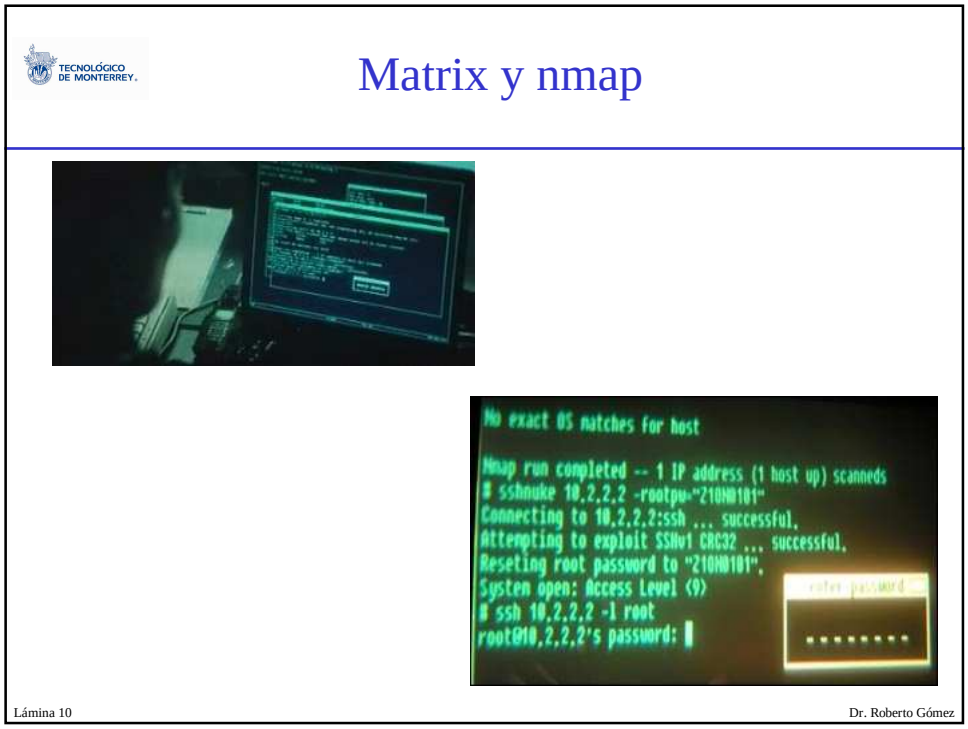
65. OpenBSD
66. Yersinia
67. Nagios
68. Fragroute/Fragrouter
69. X-scan
70. Whisker/libwhisker
71. Socat
72. Sara
73. QualysGuard ($)
74. ClamAV
75. cheops / cheops-ng
76. Burpsuite
77. Brutus
78. Unicornscan
79. Stunnel
80. Honeyd
81. Fping
82. BASE
83. Argus
84. Wikto
85. Sguil
86. Scanrand
87. IP Filter
88. Canvas ($)
89. VMWare ($)
90. Tcptraceroute
91. SAINT ($)
92. OpenVPN
93. OllyDbg
94. Helix
95. Bastille
96. Acunetix Web Vulnerability Scanner (S)
97. TrueCrypt
98. Watchfire AppScan ($)
99. N-Stealth ($)
100. MBSA

Lámina 7 Dr. Roberto Gómez

Visita George W. Bush a los cuarteles de la NSA

Lámina 8 Dr. Roberto Gómez


Nmap
Nmap Free Security Scanner
Network wide
Ping Sweep
Port Scan
OS Detection
Stealth Mode
UDP Scan
Decoy Spoof
SYN Scan
FTP Bounce
IP Fragment
Are YOU Secure?
NMAP
Nmap
Free Security Scanner
Audit your network now!
free security scanner
Got Root
Now!
Shhh... Don't tell everyone!
Dr. Roberto Gómez


TECNOLÓGICO DE MONTERREY
Matrix y nmap
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="210NB101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "210NB101".
System open: Access Level (9)
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
Lámina 10
Dr. Roberto Gómez

Características Nmap

- NMAP Network Security Scanner
- Herramienta para auditoría red y escáner de seguridad.
  - realiza un “escaneo” 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 4 funciones básicas:
  1. Escaneo de hosts (“alive”)
  2. Escaneo de puertos TCP/UDP de dichos hosts
  3. Determina Sistema Operativo
  4. Posible identificación de los servicios (aplicaciónes) responsables de los puertos abiertos identificados en 2.

Lámina 11 Dr. Roberto Gómez

Obtención de nmap

- Nmap corre en sistemas Unix, Unix-like y Windows.
- Se puede obtener en
  - http://www.insecure.org
- 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 12 Dr. Roberto Gómez

¿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 13 Dr. Roberto Gómez

Ejemplo salida nmap

```
amy.yuma.net
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=3916950 (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 14 Dr. Roberto Gómez

Modo gráfico

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

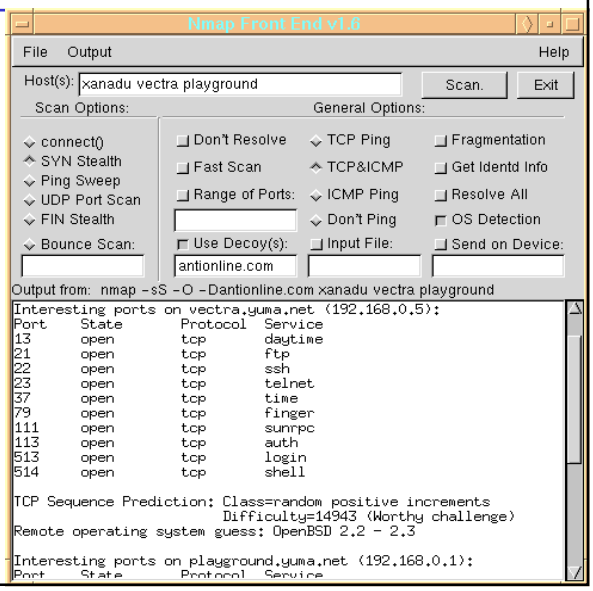


Lámina 15

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 = 2^{24} ip's

Lámina 16 Dr. Roberto Gómez

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 17 Dr. Roberto Gómez

ICMP 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 especficar un puerto (80 por default)

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

Lámina 18 Dr. Roberto Gómez

TCP SYN 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
```

Lámina 19 Dr. Roberto Gómez

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 20 Dr. Roberto Gómez

Opciones determinar host disponibles en modo gráfico

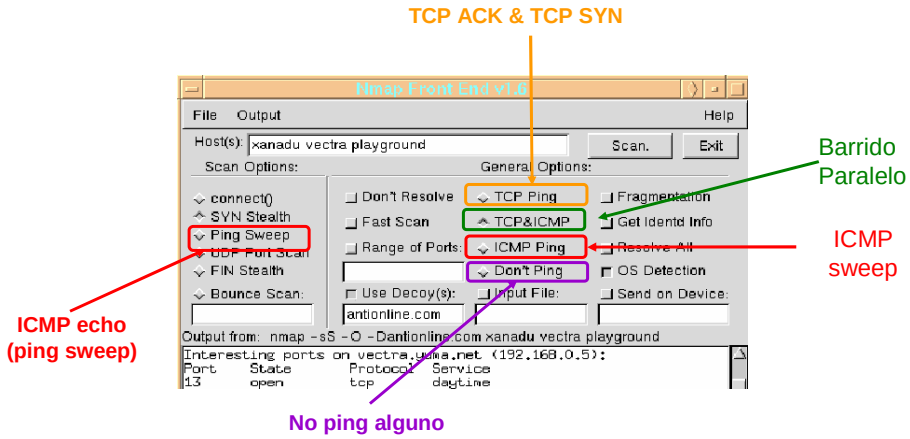


Lámina 21 Dr. Roberto Gómez

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

Lámina 22 Dr. Roberto Gómez

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

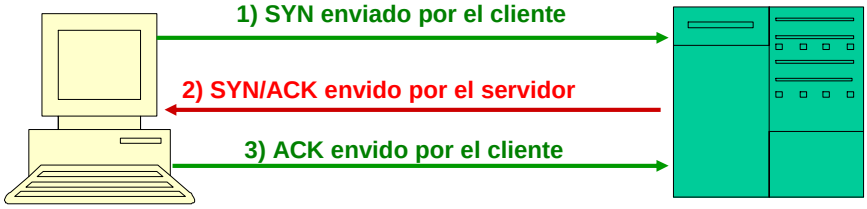
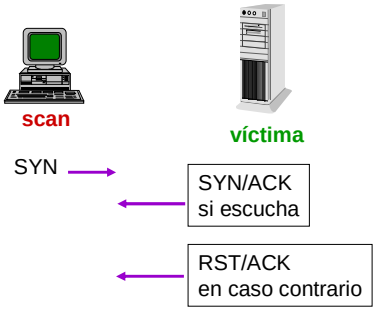


Lámina 23 Dr. Roberto Gómez

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

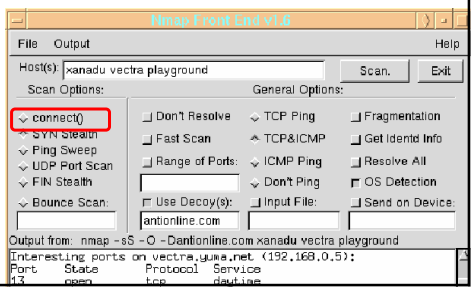
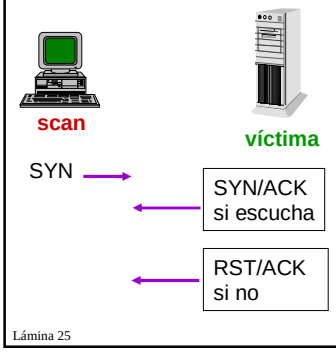


Lámina 24

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



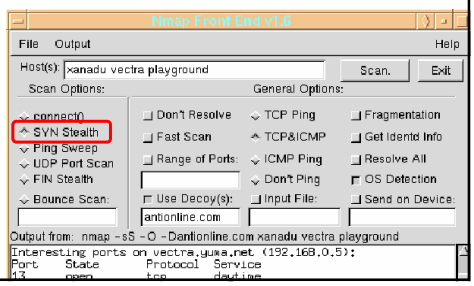
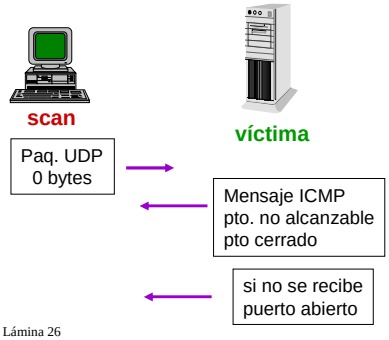


Lámina 25

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



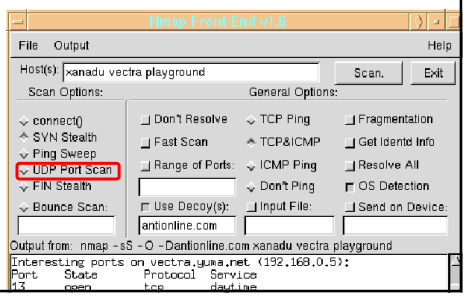


Lámina 26

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 27 Dr. Roberto Gómez

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 ruteadores de frontera que filtren paquetes TCP con la combinación de las banderas (FIN) y (ACK)

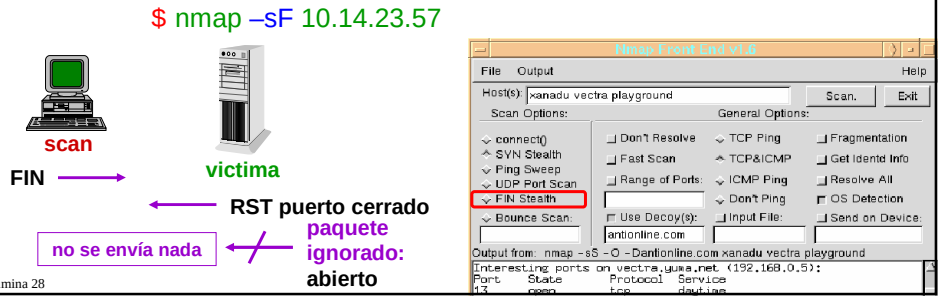


Lámina 28

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 ruteadores de frontera

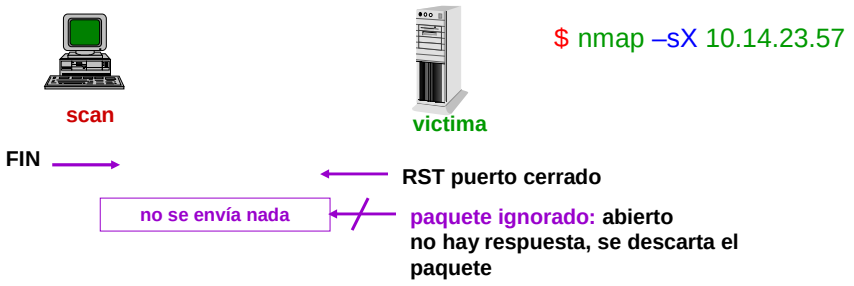


Lámina 29 Dr. Roberto Gómez

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 ruteadores intermedios y firewalls están prevenidos contra este tipo de intentos por lo que no es probable que obtengamos ninguna respuesta.

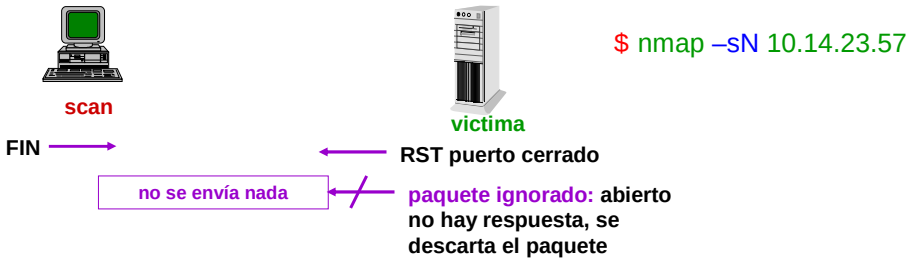


Lámina 30 Dr. Roberto Gómez

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

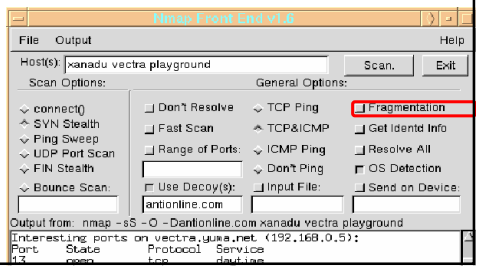


Lámina 31

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

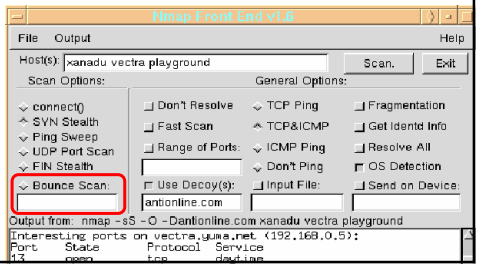


Lámina 32

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 interpetan de diferente manera los RFC's.
  - "Remote OS detection via TCP/IP Stack FingerPrinting", Fyodor

$ nmap –O 10.14.23.57

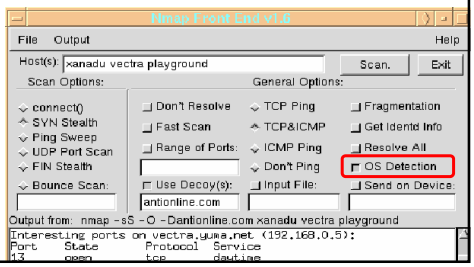


Lámina 33

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 34 Dr. Roberto Gómez

Combinando opciones

- Para hacer un escaneo estandard 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 21,22,23,25,80,110 warez.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 35 Dr. Roberto Gómez

Ejemplos combinación opciones

- Para encontrar hosts que esten arriba en la clase C 193.14.12, .13, .14, .15, ..., .30 .

  # nmap –sT '192.14.[12-30].*'

  – otra forma de hacer lo anterior es:

  # nmap -sT 193.14.23-30.0-254

- Escaneo de puertos entre 1 y 65000

  # nmap –p1-65000 victima.org/24

- La forma más común:

  # nmap –O –sS victima.org/24

Lámina 36 Dr. Roberto Gómez

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

$taRt|ng nmap V. 2.54B3T431 ( www.1n$ecur3.ORg/nmap/ )
|nt3r3sting pOrtz 0n 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     0pEn         smtp
80/tcp     0p3n         htTp
139/tcP    op3n         N3Tb1Oz-Ssn
143/tCP    0pen         imap2
515/tcp    f!lt3red     prinT3r
3128/tcp   Op3n         squ|d-HtTP
3306/tCp   Op3n         my$ql
6000/tcp   0p3n         x11

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


Dos complementos a nmap

lsoft y fport

Lsof

- Lsof – List Open Files
- Entrega la información sobre cada uno de los archivos que están abiertos por los procesos corriendo en el sistema.
- **TAMBIEN lista las comunicaciones abiertas por cada proceso.**
- **http://freshmeat.net/projects/lsof/**

Lámina 39 Dr. Roberto Gómez

Lsof

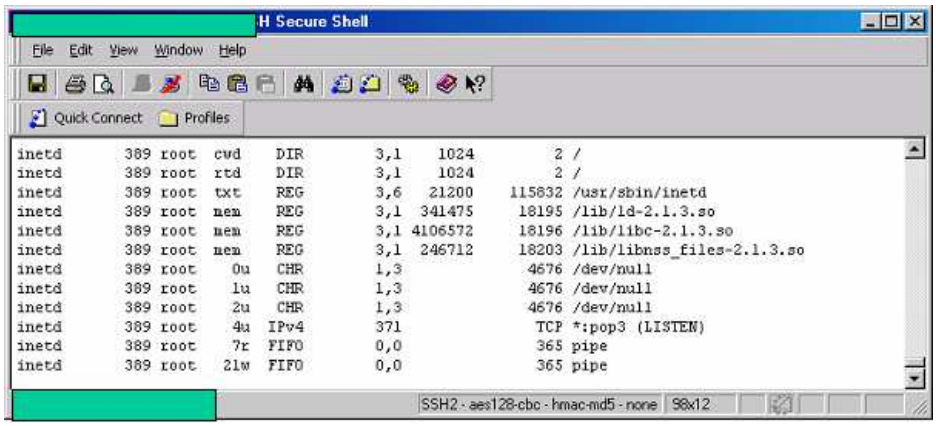


Lámina 40 Dr. Roberto Gómez

Fport - http://www.foundstone.com/

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

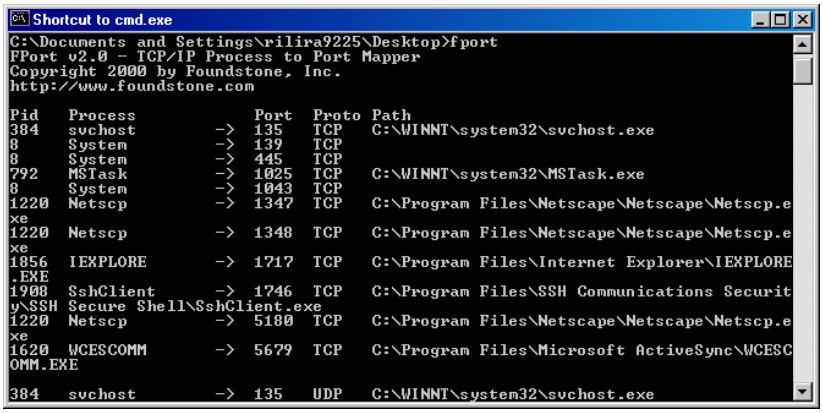


Lámina 41 Dr. Roberto Gómez

Defendiendose de nmap…

portsentry

Lámina 42 Dr. Roberto Gómez

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 “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.
  - se recomienda un análisis que contemple la posibilidad de un n ataque de negación de servicio en hosts legítimos. (ip spoofing).
- Disponible en:
  - http://www.psionic.com/abacus/portsentry/
  - acaba de ser comprado por Cisco Systems

Lámina 43 Dr. Roberto Gómez

Portsentry - instalación

- Descompactar y extraer los archivos de Portsentry.

```
$ gunzip portsentry-1.0.tar.gz
$ tar xvf portsentry-1.0.tar
```

- Compilar Portsentry
  - necesario elegir el sistema operativo de todos los soportados

```
$ make linux
```

- Ejecutar comando “make install” como root

```
# make install
```

- Portsentry queda instalado y listo para ser configurado en el directorio “/usr/local/psionic/portsentry”.

Lámina 44 Dr. Roberto Gómez

Portsentry

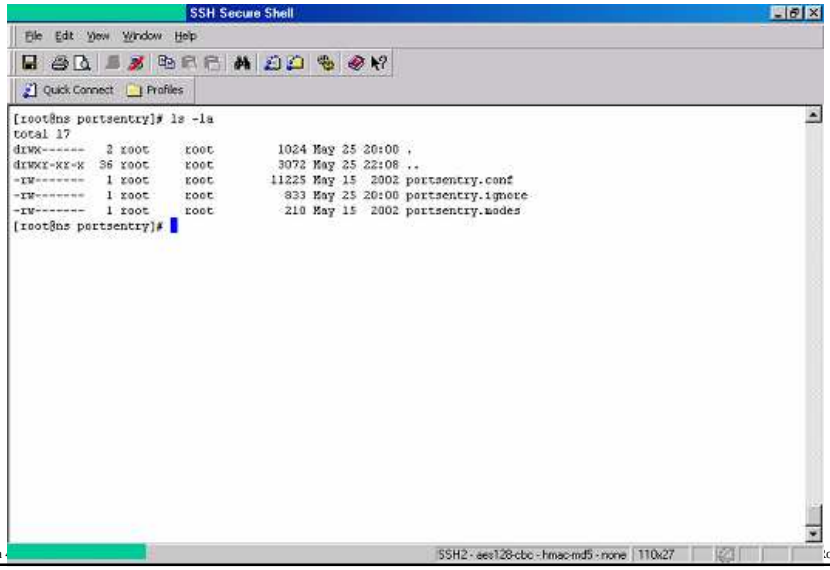


Lámina oberto Gómez

Portsentry

- Instalación genera básicamente 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 46 Dr. Roberto Gómez

Portsentry

- Depende de los archivos de configuración.
  - el archivo más importante es portsentry.conf.
  - aquí se define como reaccionará portsentry
- Portsentry modos más comunes:
  - **tcp**
    - modo básico.
    - se asocia a puertos TCP encontrados en el archivo portsentry.conf
    - posible asociar hasta 64 puertos.
  - **udp**
    - hace lo mismo que la anterior para los puertos UDP.

Lámina 47 Dr. Roberto Gómez

Portsentry

- atcp
  - Cualquier conexión a un puerto TCP debajo del puerto señalado en ADVANCED_PORTS_TCP="X" provocará que se bloquee la dirección IP fuente. Ej: X=1024
- audp
  - Cualquier conexión a un puerto UDP debajo del puerto señalado en ADVANCED_PORTS_UDP="X" provocará que se bloquee la dirección IP fuente. Ej: X=1024

Existe un archivo portsentry.ignore donde se colocan las direcciones ip que serán excluidas y dentro de portsentry.conf para excluir puertos: ADVANCED_EXCLUDE_TCP

Lámina 48 Dr. Roberto Gómez

Portsentry

- Además existen los modos stcp y sudp, igual que tcp y udp solo que detecta escaneos stealth y fin además de poder bloquear las dirección IP fuente.

Lámina 49 Dr. Roberto Gómez

¿Y que puede hacer?

- 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 50 Dr. Roberto Gómez

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 desa 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 51 Dr. Roberto Gómez

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 52 Dr. Roberto Gómez

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 53 Dr. Roberto Gómez

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 cuento 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 54 Dr. Roberto Gómez

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 55 Dr. Roberto Gómez

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 56 Dr. Roberto Gómez

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)

Fuente: The SANS Top 20 Internet Security Vulnerabilities (http://www.sans.org/top20/)

Lámina 57 Dr. Roberto Gómez

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/tcp 162
  - BGP 179/tcp
  - SOCKS 1080/tcp

Fuente: The SANS Top 20 Internet Security Vulnerabilities (http://www.sans.org/top20/)

Lámina 58 Dr. Roberto Gómez

Nessus

Escáner de vulnerabilidades

Lámina 59 Dr. Roberto Gómez

NESSUS

- Escáner remoto de vulnerabilidades y debilidades de sistemas.
- Escrito por Renaud Deraison (a los 18 años, París)
  - Comenta que conoció Linux a los 16 años y desde entonces se ha dedicado a cuestiones de seguridad de sistemas (específicamente hacking).
- Se puede obtener de
  - http://www.nessus.org

Lámina 60 Dr. Roberto Gómez

Puntos significativos Nessus

- Actualizado
- Incorpora ataques basados en Web
- Gratis (existen opciones del comerciales del propio desarrollador)
  - distribuido bajo la licencia GNU, Free Software Foundation
- Open Source (únicamente hasta la versión 2)
  - elimina el riesgo de que ejecute código malicioso.
- Cuenta con su propio lenguaje de programación
  - NASL, Nessus Atack Scripting Language
  - optimizado para pruebas de seguridad
- **Fácil instalación y uso**

Lámina 61 Dr. Roberto Gómez

Puntos significativos Nessus

- Arquitectura de “plug-ins”
  - cada plug-in es una prueba de seguridad
- Arquitectura cliente/servidor.
  - Nessus está compuesto por un servidor (nessusd) el cual realiza las pruebas y un cliente (nessus) el cual es el entorno gráfico donde se presentan los resultados.
  - Al día de hoy, existen versiones tanto para Windows como Linux-Unix.
- Puede probar varios hosts a la vez, depende de la fortaleza del equipo donde se ejecuta el demonio y la velocidad de la red.

Lámina 62 Dr. Roberto Gómez

Puntos significativos Nessus

- Reconocimiento inteligente de servicios
  - Smart service recognition
  - no se da por hecho que el target-host sigue la norma de puertos IANA (Internet Assigned Number Authority).
  - Nessus identificará un ftp-server en el puerto XXXX, o un web-server en el puerto YYYY.
  - *"Never trust the version number, never trust that a given service is listenning on the good port"*
- Genera reportes en diferentes formatos de salida

Lámina 63 Dr. Roberto Gómez

Plugins de Nessus

Más de 13,000 plug-ins en la base de datos.
http://cgi.nessus.org/plugins/
Algunas categorías:

- Backdoors
- CGI abuses
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Misc.
- NIS
- Port Scanners
- Remote file access
- RPC
- SMTP problems
- SNMP
- Useless services
- Windows

Lámina 64 Dr. Roberto Gómez

Nessus y NASL

- NASL (Nessus Attack Scripting Language)
- Permite que cualquiera escriba sus propias pruebas de seguridad
- Permite que dichas pruebas sean compartidas sin importar el sistema operativo
- Garantiza que solo se hará la prueba al target-host, a ningún otro

Lámina 65 Dr. Roberto Gómez

Ejemplo NASL

```
#
# Check for ssh
#
if(description)
{
 script_name(english:"Ensure the presence of ssh");
 script_description(english:"This script makes sure that ssh is running");
 script_summary(english:"connects on remote tcp port 22");
 script_category(ACT_GATHER_INFO);
 script_family(english:"Administration toolbox");
 script_copyright(english:"This script was written by Joe U.");
 script_dependencies("find_service.nes");
 exit(0);
}
```

Lámina 66 Dr. Roberto Gómez

Ejemplo NASL

```
#
# First, ssh may run on another port.
# That's why we rely on the plugin
#'find_service'

port = get_kb_item("Services/ssh");
if(!port)port = 22;

}
```

Lámina 67 Dr. Roberto Gómez

Ejemplo NASL

```
#declare that ssh is not installed yet
ok = 0;
if(get_port_state(port))
{
   soc = open_sock_tcp(port);
   if(soc)
   {
        #Check that ssh is not tcpwrapped. And that it's really  SSH
      data = recv(socket:soc, length:200);
      if("SSH" >< data)ok = 1;
   }
   close(soc);
}
```

Lámina 68 Dr. Roberto Gómez

Ejemplo NASL

```
#
#Only warn the user that SSH is NOT
#installed
#

if(!ok)
{
  report = "SSH is not running on this host !";
  security_warning(port:22, data:report);
```

Lámina 69 Dr. Roberto Gómez

Usando Nessus (Linux-Unix)

- Instalarlo
- Crear cuenta nessusd
- Configurar demonio
- Actualizar plugins
- Activar servidor
- Lanzar cliente
- Configurar scaneo
- Verificar resultados

Lámina 70 Dr. Roberto Gómez

1er. paso: instalación

- Requisitos:
  - GTK (gimp toolkit) ftp://ftp.gimp.org/pub/gtk
  - nmap http://www.insecure.org/nmap
- La forma más fácil y menos peligrosa
  - Nessus está disponible como un paquete de autoinstalación.
  - Para usarlo se baja el escript nessus-installer.sh bajo el directorios nessus-installer/ y se teclea el siguiente comando

```
#sh nessus-installer.sh
```

  - No se necesita ningún otro paquete que el instalador

Lámina 71 Dr. Roberto Gómez

Otra forma de instalación

- La forma más común
  - Bajar y compilar los siguientes paquetes en el órden indicado (./configure, make, make install).

nessus-libraries-x.x.tar.gz
libnasl-x.x.tar.gz
nessus-core.x.x.tar.gz
nessus-plugins.x.x.tar.gz

Lámina 72 Dr. Roberto Gómez

2do. paso: crear cuenta

- El servidor nessusd tiene propia base de datos de usuarios, donde cada usuario cuenta con un conjunto de restricciones
- Lo anterior permite compartir un servidor nessusd para toda una red con diferentes administradores que probaran su parte de la red
- Se puede usar la utilería *nessus-adduser* para crear una nueva cuenta

Lámina 73 Dr. Roberto Gómez

Ejemplo uso nessus-adduser

```
toto@maquina:34> nessus-adduser
        Addition of a new nessusd user
        ------------------------------
        Login : renaud
        Password : secret
        Authentification type (cipher or plaintext) [cipher] : cipher
        Now enter the rules for this user, and hit ctrl-D once you are done :
        (the user can have an empty rule set)
        ^D
        Login          : renaud
        Pssword        : secret
        Authentification : cipher
        Rules          :

        Is that ok (y/n) ? [y] y

        user added.
toto@maquina:35>
```

Lámina 74 Dr. Roberto Gómez

Continuando ...

- Tercer paso: configurar el demonio nessus
  - en el archivo /usr/local/etc/nessus/nessusd.conf, se pueden definir diferentes opciones para nessusd
  - se le puede indicar a nessus que use un determinado idioma
  - el archivo configuración estándar tiene inglés como idioma
- Cuarto paso: actualizar los plug-ins (/usr/local/sbin)

```
toto@maquina:35> nessusd -update
```

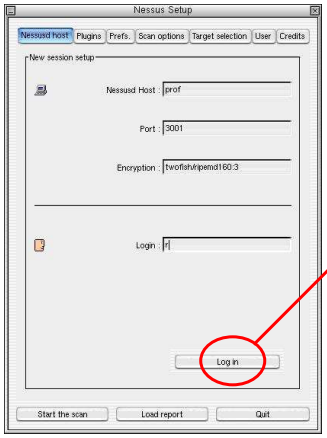
- Quinto paso: arrancar nessusd
  - una vez realizado lo anterior, es posible arrancar el servidor nessusd (se requieren permisos de root):

```
toto@maquina:36> nessusd -D
```

Lámina 75 Dr. Roberto Gómez

Configurando el cliente

- Lo anterior se hizo como root, ahora se conecta como usuario normal y se lanza nessus



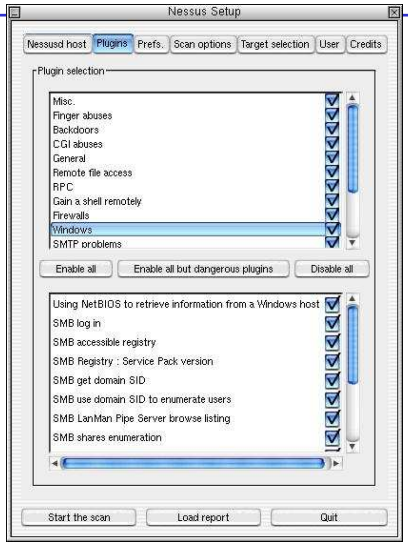
primera vez, por lo que solicita login y password, la próxima vez solo con la llave pública será suficiente

una vez conectado, boton Log in cambia a Log out y aparece etiqueta Connected

Lámina 76 Dr. Roberto Gómez

TECNOLÓGICO DE MONTERREY

Configuración del chequeo a realizar



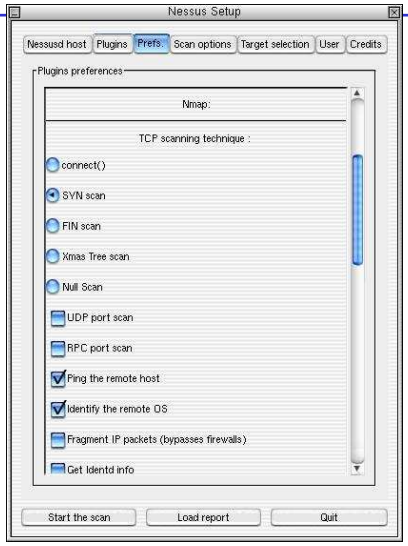
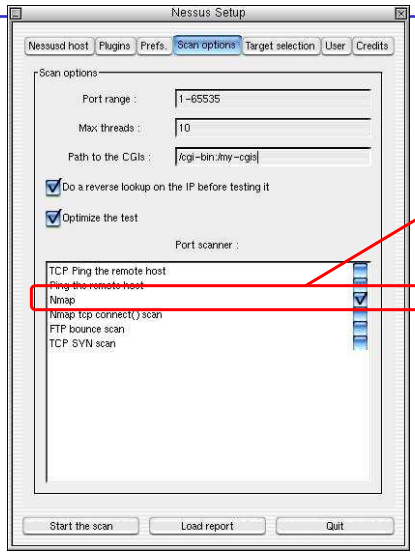


Lámina 77 Dr. Roberto Gómez

TECNOLÓGICO DE MONTERREY

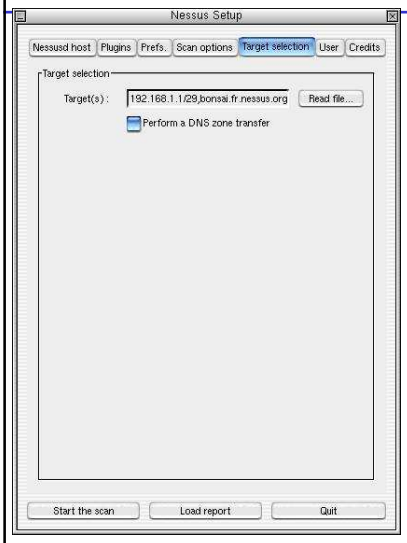
Opciones de scaneo



se elige nmap como herramienta de scaneo de puertos, ya que es rápido

Lámina 78 Dr. Roberto Gómez

Definiendo el objetivo



Posible usar cualquiera siguientes opciones:

192.168.1.1
una sola dirección IP

192.168.1.1-7
un rango de direcciones IP

192.168.2.1-192.168.2.50
otro rango de direcciones IP
Another range of IP addresses.

192.168.1.1/29
otro rango de direcciones IP (not. CIDR)

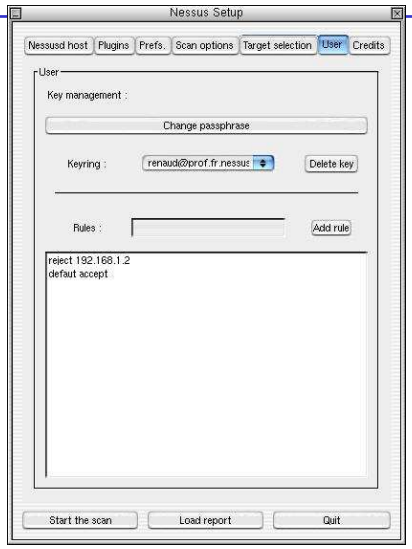
prof.fr.nessus.org
un hostname (Full Qualifie Domain Name).

prof
un hostname (si puede "resolverlo" el servidor)

prof, 192.168.1.1/29, ...
cualquier combinación separada por una coma

Lámina 79 Dr. Roberto Gómez

La sección de reglas



Se desea probar
192.168.1.0/29,
excepto 192.168.1.2

Lámina 80 Dr. Roberto Gómez

TECNOLÓGICO DE MONTERREY

Empieza el scanneo

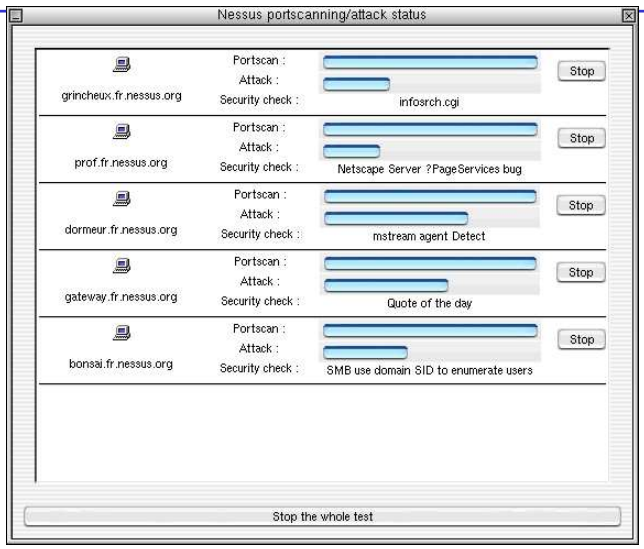


Lámina 81 Dr. Roberto Gómez

TECNOLÓGICO DE MONTERREY

El reporte otorgado

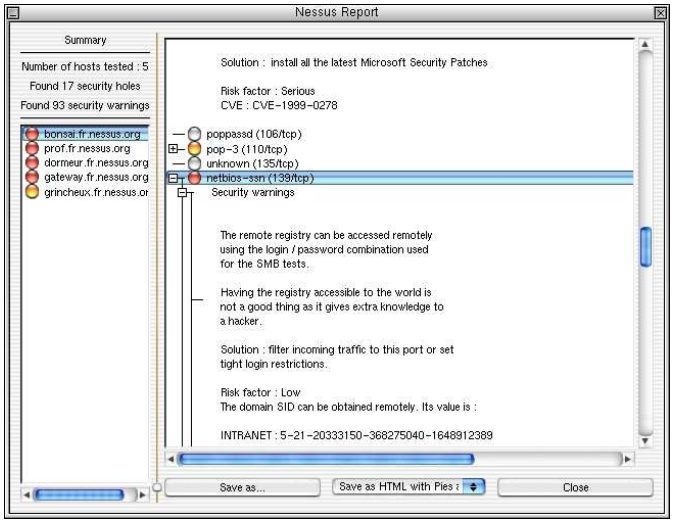


Lámina 82 Dr. Roberto Gómez

Opciones reporte

- Posible obtener reporte en diferentes formatos
  - en formato .NSR, que puede ser leído por el cliente unix y NessusJ
  - en formato spiffy HTML, con gráficas y pasteles
  - en formato HTML
  - en formato texto
  - en formato LaTex

Lámina 83 Dr. Roberto Gómez

Otros escáners de vulnerabilidades

- SAINT
  - SAINT® network vulnerability assessment scanner
  - http://www.wwdsi.com/saint
- SARA
  - Security Auditor's Research Assistant
  - http://www-arc.com/sara/
- SATAN
  - Security Administrator Tool for Analyzing Networks
  - http://www.fish.com/satan/

Lámina 84 Dr. Roberto Gómez