**Hugo González**

**@hugo_glez**

**http://atit.upslp.edu.mx/~hugo/**

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

# TCPDUMP, Netcat y otras herramientas de red

Hugo Francisco González Robledo
hugo.gonzalez@itslp.edu.mx
Centro de Telecomunicaciones
Instituto Tecnológico de San Luis Potosí

GULEV 2004
25 de Noviembre 2004

# Objetivos

- Aprender sobre netcat, y utilizarlo para monitoreo, detección de intrusos, curiosidad ...
- Utilizar tcpdump para análisis de tráfico en la red, para monitoreo, detección de intrusos, curiosidad ...
- Mencionar otras herramientas

# Agenda

- Netcat
- Repaso de TCP/IP
  - Encabezados
- TCPDUMP
- Otras herramientas
- P y R
- Conclusiones

# Netcat

- La navaja suiza de las redes.
- Puede abrir conexiones TCP, mandar paquetes UDP
- Puede también escuchar por peticiones
- Puede servir para realizar escaneos de puertos
- Puede convertir una aplicación simple en una aplicación para red ...

# Algunos usos más sofisticados

- Proxies TCP simples
- Clientes y servidores HTTP con scripts de shells
- Verificación de servicios en la red
- Depuración de programas
- Honeypots
- Y mucho, mucho más ...

# Corriendo netcat

```
[hugo@movies hugo]$ nc -h
  [v1.10]
  connect to somewhere:   nc [-options] hostname port[s] [ports] ...
  listen for inbound:     nc -l -p port [-options] [hostname] [port]
  options:
   -g gateway             source-routing hop point[s], up to 8
   -G num                 source-routing pointer: 4, 8, 12, ...
   -h                     this cruft
   -i secs                delay interval for lines sent, ports scanned
   -l                     listen mode, for inbound connects
   -n                     numeric-only IP addresses, no DNS
   -o file                hex dump of traffic
   -p port                local port number
   -r                     randomize local and remote ports
   -s addr                local source address
   -u                     UDP mode
   -v                     verbose [use twice to be more verbose]
   -w secs                timeout for connects and final net reads
   -z                     zero-I/O mode [used for scanning]
  port numbers can be individual or ranges: lo-hi [inclusive]
```

# Abriendo cualquier programa

- El ejecutar nc -e
- podemos ejecutar cualquier programa, siendo stdin la entrada de la red y stdout y stderr la salida hacia la red.
- Solo funciona si esta compilado con la bandera GAPING_SECURITY_HOLE,por defecto en algunas distros no está.

# Utilizarlo para escuchar

- Con la opción de -l lo puedes poner a escuchar en un puerto, para esto hay que definir el puerto con -p

- nc -l -p 1090 (Fedora)
- nc -l maquina1 1090 (OpenBSD)

- lo que reciba en el puerto

# Guardando lo que pasa

- para guardar en hexadecimal la información que recibe y envía netcat se utiliza el parametro

  **-o nombrearchivo**

- nc -l -p 1090 -o registro1

# Para generar UDP

- para generar tráfico UDP solo es necesario utilizar el parámetro

  **-u**

- nc -u maquina1 80

# Siendo más explicito

- Para ver mas detalles de la conexión se utilizan

  **-v** ó **-vv** ó **-vvv**

- Entre más v's tenga es más explicito o “chismoso”

# Opciones para escanear

- Para escanear puede ser posible utilizar el parametro

**-i s** que especifica s segundos de espera

**-z** que significa no mandar información.

- nc -i 1 -z -v maquina1 10-50

- Un ejemplo muy sencillo de como transmitir información puede ser el siguiente:
- [hugo@movies hugo]$ nc -l -p 2020 -o /tmp/conexion
- [hugo@movies hugo]$ echo "Ejemplo" | nc -nv 192.168.2.20 2020
- (UNKNOWN) [192.168.2.20] 2020 (?) open
- Ejemplo

# Ejemplo mas complejo

- Existen escripts para ciertas tareas, como buscadores, cliente web minimalista, proxyweb, etc
- generalmente se instalan en /usr/share/doc/nc-1../scripts/

# Como usarlo como honeypot

- Pues si tengo los servicios apagados, en el inetd puedo ejecutar un nc -l -p xx > log
- de esta forma cuando quieran tener acceso a este puerto lo manda a un log ...

# Usarlo como proxy, o redireccionador

- Una forma muy interesante es usar netcat como redireccionador ...
- utilizando un backpipe
- mknod backpipe p
- nc -s localhost -l -p 1220 <backpipe | nc sig 1222 1>backpipe

# Encabezados IP

# Encabezados TCP

# Internet, Servicios

- Los servicios son programas (generalmente orientados a la red) que se asocian con un números de puerto para tener acceso a ellos ...
- puedes verlos en /etc/services
- algunos clásicos son el web (80), pop3 (110), smtp (25) ....

# TCP /IP

- En los encabezados viene casi todo lo que nos interesa
- Podemos ver también el contenido de los paquetes

# TCPDUMP

- Sirve para volcar la información del trafico en la red a pantalla o a archivo
- También sirve para leer información volcada con anterioridad, ya sea con tcpdump, snort, firewalls (pf) u otros.
- En un bridge, podemos examinar todo el tráfico de la red
- Podemos ver la información que circula

# Corriendo tcpdump

```
[root@movies root]# tcpdump -h
tcpdump version 3.8
libpcap version 0.8.3
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c
count] [ -C file_size ] [ -E algo:secret ]
[ -F file ] [ -i interface ] [ -M secret ]
[ -r file ] [ -s snaplen ] [ -T type ]
[ -w file ] [ -W filecount ]
[ -y datalinktype ] [ -Z user ]
[ expression ]
```

# Uso principal

- El uso principal que se le puede dar a tcpdump es para monitorear la red ...
- ¿Y por que no otros, como ethereal?
- tcpdump se puede utilizar en tiempo real, y a través de una consola ...
- por la red la puedo checar ...

# Otros usos

- TcpDUMP también puede ser utilizado para leer archivos de eventos ...
- por ejemplo ...
- de firewalls
- de capturas

# Vamos a analizar algún tráfico

# Otras cosas que se pueden hacer

- identificar problemas en la red ...
- detectar virus que se propagan en la red
- ver conexiones no autorizadas ...
- mmm, leer el correo y las paginas que estan viendo otras personas ...

# Existen otras herramientas complementarias

- tcpshow
- tcpdump para samba
- ethereal
- dsniff
- kismet

# Contacto

Hugo Francisco González Robledo
hugo.gonzalez@itslp.edu.mx
Centro de Telecomunicaciones
Instituto Tecnológico de San Luis Potosí