**Gómez Miranda Leopoldo**

**Tarea NetCat**

Netcat es un pequeño programa creado para uso de los administradores de redes (y por supuesto para los Hackers) :), este programa fue creado originalmente por Hobbit y porteado a Win95 y NT por Weld Pond de L0pht.

Principalmente porque la estructura de sus comandos es poco familiar para el usuario medio. Netcat tiene infinidad de funciones, aunque se deja que sea el usuario quien las averigüe.

La especialidad de NetCat es el Protocolo tcp/ip, y le dá a la máquina de windows, cierto poder sobre este protocolo que solo tenía UNIX, trabaja con líneas de comandos desde MS-DOS (o desde el Shell de Linux), y según parece, puede hacer casi cualquier cosa sobre TCP/IP. El comando principal es nc con su respectiva variable u opción al mas puro estilo Unix.

Este es el resultado de el comando de ayuda de netcat en una máquina windows

c:>nc –h

connect to somewhere: nc [-options] hostname port [ports]

listen for inbound: nc -l -p port [options] [hostname] [port]

options:

-d detach from console, stealth mode

-e prog inbound program to exec [dangerous!!]

-g gateway source-routing hop point, 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

-L listen harder, re-listen on socket close

-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

-t answer TELNET negotiation

-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: m-n [inclusive]

Bien, un análisis rápido de estas variables nos da una idea del potencial de este pequeño programa y las infinitas posibilidades que nos ofrece el poder manejar conexiones de una manera tan básica y sencilla:

Opciones de Netcat

-d (Modo Stealth o encubierto)

Esta opción desvincula al Programa de la consola, haciéndolo trabajar en el BackGround.

-e<prog> (Ejecuta un programa cuando se conecta)

Puede ser utilizado para ejecutar incluso un Shell tanto en WinX como en UNIX.

-l (Escuchando conexiones) Deja a un puerto abierto en espera de una conexión

-L (lo mismo que anteriormente pero sigue escuchando aún cuando la conexión es cerrada)

-n (Dirección numérica especifica; no hace un DNS Lookup) Netcat tiene la facultad de resolver nombres de dominio mediante un DNS Lookup, con esta opción le especificamos que no lo haga, y use solamente direcciones IP.

-o<logfile> (obtiene un archivo log en Hex de la acción) Genera un Log de las actividades de netcat en código Hexadecimal.

-p<puerto> (Puerto para pegarse) Algunas veces debes especificarle con esta opción el puerto a realizar una acción.

-s<ip addr> (pegarse a un IP especifico) Netcat puede utilizar IP de una red como fuente local.

-t (Funciona como un pequeño demonio telnet) Con esta opción le especificas a netcat que debe realizar negociaciones telnet.

-u specify UDP (Utilizar Protocolo UDP) Con esta opción le dices a netcat que trabaje con protocolo UDP en vez de TCP.

-w <segundos> (Especifica un tiempo para terminar) Con esta opción le especificas un tiempo determinado para realizar conexiones .

-r (Genera un Patron Ramdom de puertos locales o remotos) Muy util para evitar patrones lógicos de Scanning.

-g <gateway> (especificar Gateways) Una de las opciones más interesantes de netcat, permite utilizar Routers como "puentes" de conexión.

-G <numero> (Especificar puntos de Routing), Con esta opción podemos crear una cadena aleatoria de hosts para crear un ruta perdida para tus paquetes

(Spoofing).

-i <segundos> Especifica un intervalo de segundos entre puertos Scaneados.

Utilizando Netcat.

Para ilustrar mejor como trabajamos con este programa, lo mejor es observar ejemplos prácticos y analizar su estructura para poder comprender mejor como funciona y así poder crear nuestras propias aplicaciones.

Obtener un Shell rapidamente en una máquina remota usando la opción -l (Listen) conjuntamente con la opción -e (ejecutar) , cuando el proggie corre con estas variables y la conexión es realizada, NetCat ejecuta el programa elegido y se conecta a stdin y stdout del programa en la conexión a la red.

nc -l -p 23 xxx.xxx.xxx.xx 23 -t -e cmd.exe

Este comando dejará a NetCat escuchando el Puerto 23 (telnet) , cuando es conectado a travéz del cliente, ejecutará un Shell (cmd.exe) la opción -t le dice a NetCat que maneje cualquier negociación que el cliente pueda esperar....

Si esta conexión es realizada desde una máquina NT, el Shell correrá los permisos del proceso que han generado a NetCat.