TALLER DE NETCAT CON KALI – LINUX

Netcat es una herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP (útil por ejemplo para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos).

Sintaxis de comandos de netcat

nc [-argumentos] [host] [puerto | rango de puertos]
Argumentos: (Todos son opcionales)
-h = (Help) Ayuda
-n = (Numeric) Solo acepta IP numérico (si no ponemos esta opción hace resolución DNS)
-v = (Verbose) pone información adicional sobre la conexión Recomendable usarlo siempre
-v –v = (Very Verbose) información más detallada todavía No muy necesario, podría ser útil en diagnóstico de sistemas problemáticos
-w <segs> = (Wait) espera cierto tiempo a que se establezca la conexión (EJ: -w 3 espera 3 segundos para realizar la conexión y luego 3 más por las dudas, antes de darnos un time out)
-p <puerto> = (Port) puerto local a utilizar
-r = (Random) elección de puertos al azar (locales y remotos)
-l = (Listen) escuchar por conexiones del exterior.
-L = (Listen) escuchar por conexiones del exterior. Aún sigue escuchando cuando la conexión establecida se corta
-e <prog> = (Execute) correr un programa al establecerse una conexión.
-t = (Telnet) – Evita negociaciones iniciales con telnet. Útil, pero puede reducir confiabilidad en la transmisión de datos
-z = (Zero I/O) Rastreo eráa de puertos, evitando salida o entrada de datos.
-i <segs> = (Interval) Espera un intervalo de tiempo entre paquetes enviados
-g <eráa> (Gateway) Maquina que retransmitirá nuestros datos a otra máquina o al destino final.
-G <pointer> = (Gateway Pointer) Es lo que indica que eráa esta en uso en determinado momento. En ocasiones es útil mover este indicador nosotros mismos.
Definido en múltiplos de 4.
-o <logfile> = (obtiene un archivo log en Hex de la acción) Genera un Log de las actividades de netcat en código Hexadecimal.
-u = (UDP) Con esta opción le dices a netcat que trabaje con protocolo UDP en vez de TCP.
-d = (Modo Stealth o encubierto) Esta opción desvincula al Programa de la consola, haciéndolo trabajar en el Back Ground.

REQUERIMIENTOS PARA LA ACTIVIDAD DE NETCAT

VIRTUAL BOX, VIRTUALIZAR DOS SISTEMAS OPERATIVOS (Kali Linux o Backtrack 5)

Recomendaciones:

Verificar que las màquinas se encuentren en el mismo segmento de red, de no ser así no podrá ejecutar de forma exitosa los comandos para establecer comunicación con las dos màquinas.

Siga los siguientes pasos:

- 1. Señalar desde el virtual box la màquina Kali, luego clic a configuración y en la opción de red en el ítem que aparece conectado a, van a cambiar de NAT a ADAPTADOR PUENTE, operación que deberán hacerle también a la otra máquina kali o Backtrack.
- 2. Verificar las ip de ambas màquinas que se encuentren en el mismo segmento de red, ejemplo: si una de ellas es 10.0.2.15 la otra deberá ser 10.0.2.xx
- 3. Sino se encuentran en el mismo segmento, utilizar el comando: ifconfig eth0 10.0.2.16 netmask 255.255.255.0 . Con esto le asignará una IP fija a una de las máquinas.
- 4. Verificar si existe comunicación entre ellas haciéndoles un ping.

Luego de haber configurado sus máquinas realice:

Banner Grabbing

1. **nc –vv IP/HOSTNAME PUERTO**
   nc -v - n IP PUERTO

Este comando obtener información de un servidor web o un puerto especifico.

2. **nc -lvvp PUERTO**

Poner en escucha un puerto TCP/UDP.

3. **nc -vv ip PUERTO**

Conexión a un puerto.

4. Hacer un TELNET (Se requieren dos máquinas**)**

Servidor

Colocar un puerto en modo escucha **nc –lvv –p PUERTO**

Cliente

Establece conexión con **nc IP PUERTO**

5. **Transferencia de archivo.**

Máquina que envía **nc –vv IP PUERTO < NOMBRE DEL ARCHIVO.TXT**
Máquina que recibe **nc -lvp PUERTO > NOMBRE DEL ARCHIVO.txt**

6. Escaneo básico de puertos

nc –vv –z –w2 IP PUERTO

7. **Iniciar el Shell remoto en un puerto**

Una máquina **nc –lvvp PUERTO -e /bin/bash**

Conecte la otra máquina con **nc IP PUERTO**

8. Proponga 1 práctica con el comando NC usando máquinas Linux.