

**PONTIFICIA UNIVERSIDAD CATÓLICA MADRE Y MAESTRA**

**FACULTAD DE CIENCIAS E INGENIERÍA**



**Sistemas Operativos II**

**ISC ISC365-101**

L8 – ncat (netcat) cuchilla de ejercito suizo.

**Presentado por:**

Junior Hernandez 2018-0999 10135069

**Entregado a:**

Juan Ramón Felipe Núñez Pérez

**Fecha de realización:** 4 de octubre del 2022

**Fecha de entrega:** 3 de noviembre del 2022

**Santiago de los caballeros; República Dominicana.**

## Introducción

Usando ncat

ncat es la cuchilla de ejercito suizo en computacion.

El objetivo de este trabajo es mostrar la versabilidad de este mandato.

Es conveniente realizar el trabajo en pareja.

Nueva vez, recomiendo consultas para que practiques con ejemplos variados.

Tales como:

- a.- Ejecutar una aplicación/mandato en una maquina remota.
- b.- Convertir maquina atacada en accesible por un puerto dado
- c.- Enviar archivo de una maquina a otra
- d.- "escanear" puertos de maquina atacada
- e.- Crear cliente y servidor
- f.- Comunicarse con un servidor: bajar una página web con

De ser posible con su compañero simularan un ataque fishing con el cual simularan algun dano en la maquina atacada.

## Comando Netcat

El comando nc, conocido como Netcat, es un comando propio de sistema Unix, que se usa para llevar a cabo diversas tareas de red. Funciona en sistemas Unix como Linux, BSD o macOS. Aunque el comando se usa abreviadamente como nc, su nombre completo es Netcat.

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 una Shell 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). Fue originalmente desarrollada por Hobbit en 1996 y liberada bajo una licencia de software libre permisiva (no copyleft, similar a BSD, MIT) para UNIX. Posteriormente fue portada a Windows y Mac OS X entre otras plataformas. Existen muchos forks de esta herramienta que añaden características nuevas como GNU Netcat o Cryptcat.

Algunos de sus parámetros mas utilizados son:

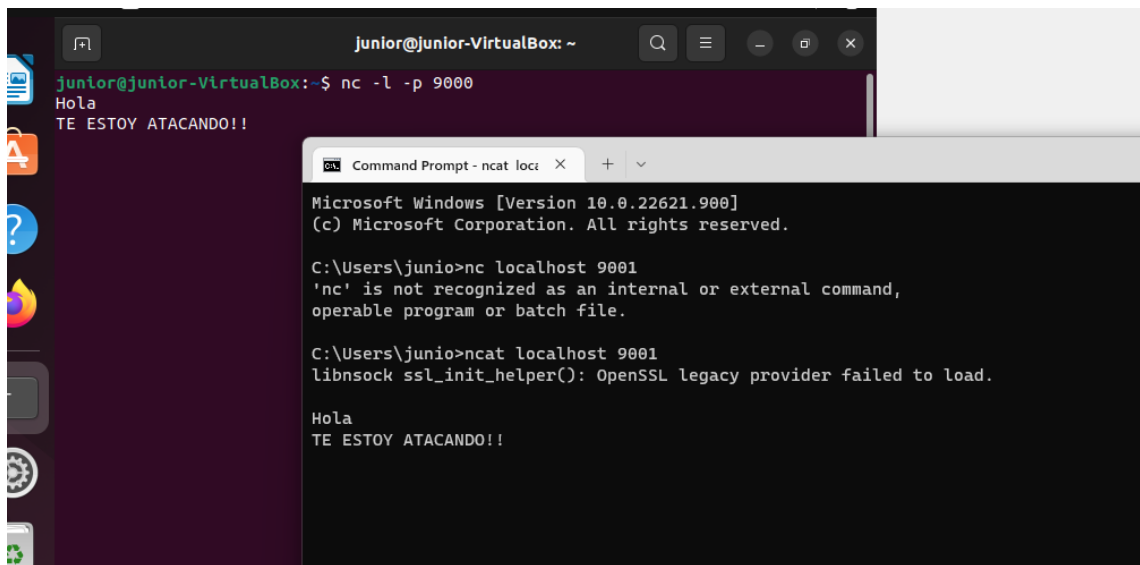
- -l: Indica que Netcat abre el puerto para Escucha (Listen): Acepta una única conexión de un Cliente y se cierra.
- -p: Especifica el puerto
- -k: Fuerza a que el puerto permanezca abierto tras haber recibido una Conexión. Se usa con el parámetro -l y permite infinitas Conexiones.
- -u: El puerto abierto se abre como UDP, en vez de TCP que es la opción por defecto.
- -v: Muestra información de la conexión.
- -t: Las respuestas son compatibles para sesiones de Telnet.
- -q segundos: Tras haber recibido el EOF de la Entrada de datos, espera los segundos indicados para enviarla.
- -i segundos: Especifica un delay (retraso) de tiempo para el envío o recepción de las líneas de texto.

Su versatilidad y múltiples usos ha hecho que se merezca el nombre de la “navaja suiza de los hackers”, ya que con todas las funcionalidades de red que este provee, es posible hacer cosas que normalmente podrían ser consideradas maliciosas o que rompen contra la seguridad.

Probando netcat para romper la seguridad:

La siguiente prueba realizada fue la de crear un “cliente-servidor”, con la maquina virtual y windows, para esto se debe indicar en la maquina que será el servidor a través de que puerto debe escuchar, en este caso a través del puerto 9000.

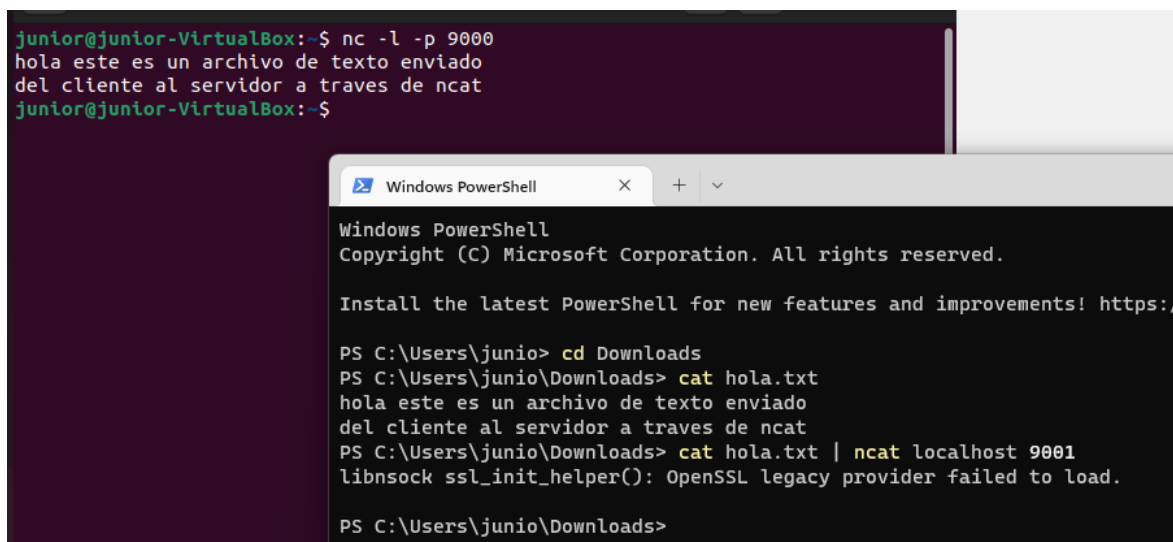
Posteriormente se debe establecer la conexión desde el cliente indicando en el en windows y el puerto a través del cual se conectará. (los mensajes “Hola...” y “TE ESTOY...” fueron enviados desde la maquina virtual)



The image shows two terminal windows. The top window is a Linux terminal with the prompt 'junior@junior-VirtualBox: ~'. It shows the command 'nc -l -p 9000' being executed, followed by the received messages 'Hola' and 'TE ESTOY ATACANDO!!'. The bottom window is a Windows Command Prompt titled 'Command Prompt - ncat loc...'. It shows the command 'C:\Users\junio>nc localhost 9001' which fails with the message "'nc' is not recognized as an internal or external command, operable program or batch file.". Then, the command 'C:\Users\junio>ncat localhost 9001' is executed, showing the message 'libnsock ssl\_init\_helper(): OpenSSL legacy provider failed to load.', followed by the received messages 'Hola' and 'TE ESTOY ATACANDO!!'.

```
junior@junior-VirtualBox: ~  
junior@junior-VirtualBox:~$ nc -l -p 9000  
Hola  
TE ESTOY ATACANDO!!  
  
Command Prompt - ncat loc...  
Microsoft Windows [Version 10.0.22621.900]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\junio>nc localhost 9001  
'nc' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\junio>ncat localhost 9001  
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.  
  
Hola  
TE ESTOY ATACANDO!!
```

Otra de las pruebas a realizar era pasar un archivo de una maquina a otra. Para esto se debe hacer cat al archivo que se quiere pasar del cliente al servidor a través de un piping



The image shows two terminal windows. The top window is a Linux terminal with the prompt 'junior@junior-VirtualBox: ~'. It shows the command 'nc -l -p 9000' being executed, followed by the received message 'hola este es un archivo de texto enviado del cliente al servidor a traves de ncat'. The bottom window is a Windows PowerShell window titled 'Windows PowerShell'. It shows the command 'PS C:\Users\junio> cd Downloads' being executed, followed by 'PS C:\Users\junio\Downloads> cat hola.txt' which outputs 'hola este es un archivo de texto enviado del cliente al servidor a traves de ncat'. Then, the command 'PS C:\Users\junio\Downloads> cat hola.txt | ncat localhost 9001' is executed, showing the message 'libnsock ssl\_init\_helper(): OpenSSL legacy provider failed to load.', followed by the received message 'hola este es un archivo de texto enviado del cliente al servidor a traves de ncat'.

```
junior@junior-VirtualBox:~$ nc -l -p 9000  
hola este es un archivo de texto enviado  
del cliente al servidor a traves de ncat  
junior@junior-VirtualBox:~$  
  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Install the latest PowerShell for new features and improvements! https://  
  
PS C:\Users\junio> cd Downloads  
PS C:\Users\junio\Downloads> cat hola.txt  
hola este es un archivo de texto enviado  
del cliente al servidor a traves de ncat  
PS C:\Users\junio\Downloads> cat hola.txt | ncat localhost 9001  
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.  
  
PS C:\Users\junio\Downloads>
```

Probablemente un uso más convencional para ncat sea la ejecución de comando de manera remota, para esto se debe crear un servidor, indicando que se usará el Shell. Posteriormente se hace la conexión desde el cliente y a partir de esto se pueden ejecutar comandos sin ningún problema.

```
junior@junior-VirtualBox:~$ ncat -lkv 9000 -c "sh"
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.0.2.2.
Ncat: Connection from 10.0.2.2:65094.
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PowerShellLatest

PS C:\Users\junio> ncat -v localhost 9001
Ncat: Version 7.93 ( https://nmap.org/ncat )
libnsock ssl_init_helper(): OpenSSL legacy provider failed

Ncat: Connection to ::1 failed: No connection could be made
Ncat: Trying next address...
Ncat: Connected to 127.0.0.1:9001.
ls
a.out
Descargas
Documentos
Escritorio
hola.txt
Imágenes
Música
Plantillas
Público
snap
Videos
```