



### **Integrantes:**

Kevin Francisco Lopez Reyes.

Rene Alexis Castro Hernandez.

Karla Daniela Rivera Rivera.

### **Asignatura:**

Ejecución de Pruebas de Seguridad.

### **Docente:**

Eduardo Chachagua Alfaro.

### **Temas:**

Control de Aplicaciones

Seguridad de las Aplicaciones.

Seguridad de dispositivos móviles.

### **Carrera:**

Técnico en Desarrollo de Aplicaciones Informáticas.

## **Definición de las soluciones de seguridad:**

**Control de Aplicaciones:** Se utiliza para gestionar la ejecución de aplicaciones en los equipos de los usuarios. Permite, con ello, implementar una política de seguridad corporativa que regule el uso de aplicaciones. Gracias a las restricciones de acceso, el componente también ayuda a reducir el riesgo de que los equipos se infecten.

**Seguridad de las Aplicaciones:** La seguridad de las aplicaciones se refiere al proceso de desarrollar, añadir y probar características de seguridad dentro de las aplicaciones para evitar vulnerabilidades de seguridad contra amenazas, tales como la modificación y el acceso no autorizados.

**Seguridad de Dispositivos Móviles:** Es un patrón de políticas, estrategias y herramientas establecidas para fortificar los dispositivos móviles frente a las amenazas de seguridad virtuales. Trata de proteger la información sensible almacenada o transportada por estos dispositivos contra la duplicación o el malware.

### **Marcas comerciales**

#### **Seguridad de dispositivos móviles:**

1. Apple
2. Samsung
3. Huawei
4. Xiaomi
5. Sony

#### **Seguridad de las aplicaciones:**

1. Netcat
2. Sqlmap
3. Aircrack
4. Snort
5. Metasploit

#### **Control de aplicaciones:**

1. Nikto
2. Nessus
3. DeskTime
4. Hours
5. Timecamp

## **Marca OpenSource:**

### **Seguridad de dispositivos móviles:**

1. Miradore.
2. IBM Maa 5360.
3. De Mobicontrol.
4. Suite de gestión de Beramendi.
5. Jamf pro.

### **Seguridad de las aplicaciones:**

1. Wireshark
2. BackTrack
3. Cain and Abel
4. Hub Staff
5. Harvest

### **Control de aplicaciones:**

1. Kali Linux
2. Metasploit
3. Wireshark
4. Netcat
5. Sqlmap

- **MARCA DEL PRODUCTO SELECCIONADO:**

NET CAT

- **QUE TIPO DE SEGURIDAD ABARCA**

Como sabemos NETCAT es una línea de comandos que sirve para escribir y leer datos en la red, esta herramienta se utiliza para diagnosticar errores y problemas que afectan a la funcionalidad y la seguridad de una red.

Abarca la seguridad en transferir archivos y sobre todo realiza auditorias de red trabaja directamente en TCP/IP en Windows y Linux; permite realizar escaneos de puertos, detecta agujeros en la seguridad, sirve para transferir archivos y crear un chat.

Es una gran utilidad de red que lee y escribe datos a través de las condiciones de red que se originan y escanea puertos; puede incluso conectarse a diferentes servicios de web que otros servicios ofrecen.

Entre sus múltiples aplicaciones, es frecuente la depuración de aplicaciones de red. También es utilizada a menudo para abrir puertas traseras en un sistema.

La forma más básica de operar de netcat consiste en:

- Crear un socket para conectarse a un servidor (o bien para hacer de servidor)
- Enviar todo lo que entre por la entrada estándar por el socket
- Sacar por la salida estándar todo lo recibido por el socket

A continuación, se listan algunos de los parámetros más usados con Netcat:

- Indica que Netcat abre el puerto para Escucha (Listen): Acepta una única conexión de un Cliente y se cierra.
- Especifica el puerto

- Fuerza a que el puerto permanezca abierto tras haber recibido una Conexión. Se usa con el parámetro `-l` y permite infinitas Conexiones.
- El puerto abierto se abre como [UDP](#), en vez de [TCP](#) que es la opción por defecto.
- Muestra información de la conexión.
- Las respuestas son compatibles para sesiones de [Telnet](#).
- Tras haber recibido el EOF de la Entrada de datos, espera los segundos indicados para enviarla.
- Especifica un delay (retraso) de tiempo para el envío o recepción de las líneas de texto.



## ● Netcat y cómo funciona?

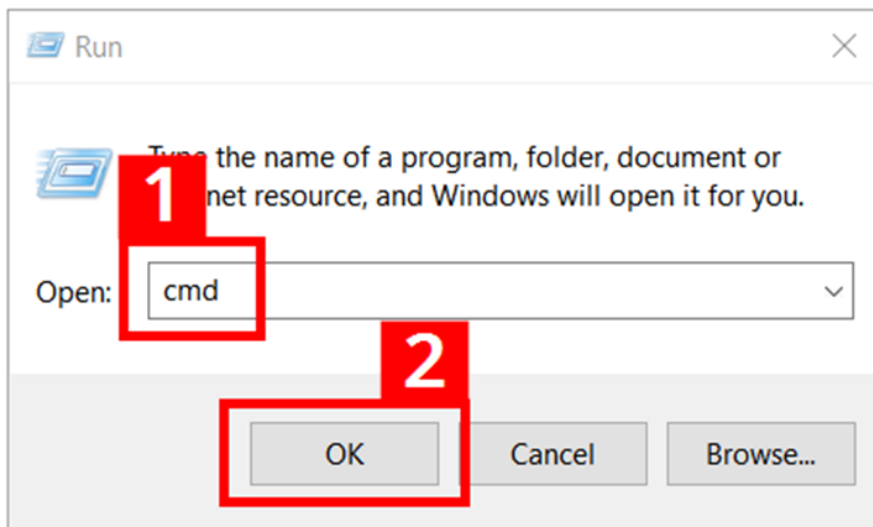
Netcat es una **herramienta de línea de comandos** que sirve para escribir y leer datos en la red. Para la transmisión de datos, Netcat usa los protocolos de red [TCP/IP](#) y [UDP](#). La herramienta proviene originalmente del [mundo de Unix](#); desde entonces, se ha **expandido a todas las plataformas**.

Gracias a su universalidad, a Netcat se la llama “la navaja suiza del TCP/IP”. Puede utilizarse, por ejemplo, para diagnosticar errores y problemas que afecten a la funcionalidad y la seguridad de una red. Netcat también puede escanear puertos, hacer *streaming* de datos o simplemente transferirlos. Además, permite configurar servidores de chat y de web e iniciar consultas por correo. Este software minimalista, desarrollado a mediados de los 90, puede operar en **modo servidor y cliente**.

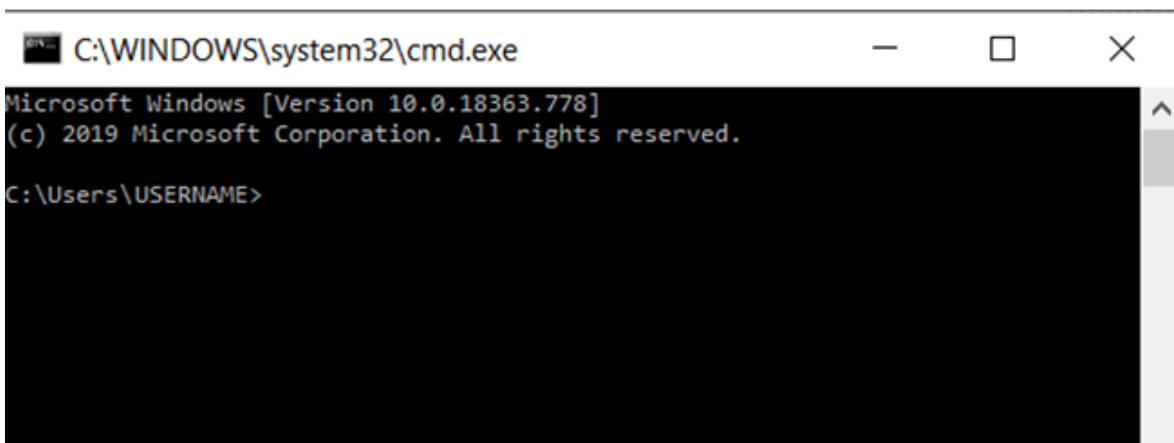
## ¿Cómo se utiliza Netcat?

Netcat puede usarse en todas las plataformas a través de la **línea de comandos**. En Linux y macOS, esta herramienta de línea de comandos suele estar preinstalada. En cambio, los usuarios de Windows deben descargar el programa de internet. Para ello, no se requiere una instalación especial: basta con descargar el instalador (*nc.exe*). Así, podrás usar Netcat para varias tareas de red usando el **símbolo del sistema** (*cmd.exe*). Abre el símbolo del sistema de la siguiente manera:

1. Pulsa la combinación de teclas [Windows] + [R]
2. Escribe "cmd" en el campo de entrada (1)
3. Pulsa el botón "Aceptar" (2)



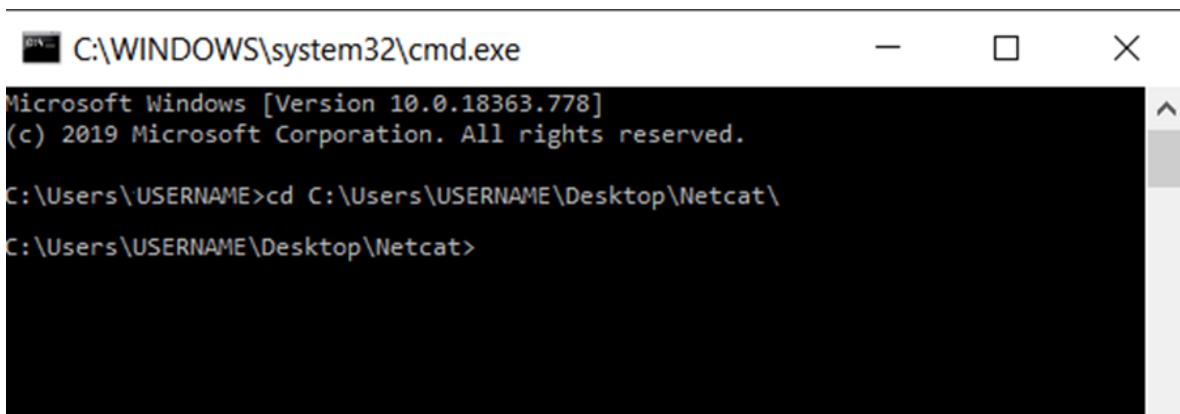
Se abrirá *cmd.exe*. La interfaz tiene el siguiente aspecto:



Pantalla de inicio del símbolo del sistema. "NOMBRE DE USUARIO" es un marcador de posición que indica el nombre de la cuenta de usuario activa.

Para iniciar el archivo de programa (*nc.exe*), debes **cambiar la ubicación de almacenamiento**. Si guardas el *nc.exe* en la carpeta “netcat” en el escritorio de Windows, la sintaxis es la siguiente:

El comando “**cd**” (**change directory o cambiar directorio**) efectúa el cambio, y la ruta de programa a continuación indica la dirección de la carpeta de almacenamiento de *nc.exe*. En la línea de comandos, el cambio tiene este aspecto:



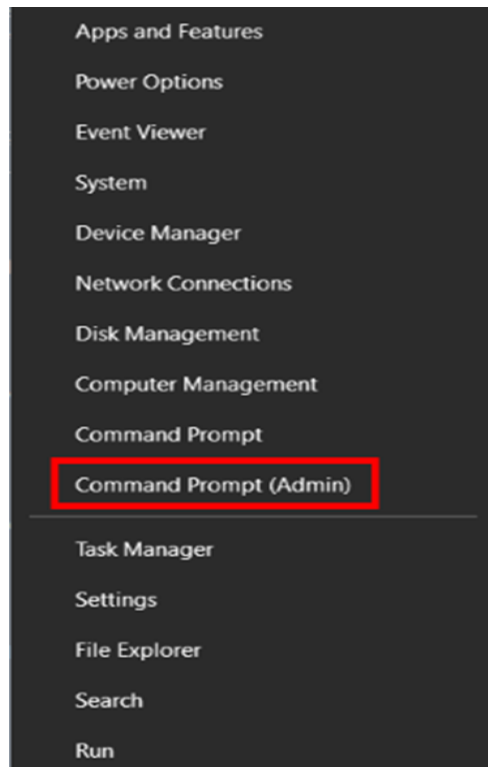
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\USERNAME>cd C:\Users\USERNAME\Desktop\Netcat\
C:\Users\USERNAME\Desktop\Netcat>
```

Cambia el directorio del programa Netcat introduciendo el comando “cd” en el símbolo del sistema.

Netcat requiere **derechos de acceso ampliados** para algunas operaciones. En Windows 10, se puede iniciar el símbolo del sistema con derechos de administrador:

1. Haz clic con el botón derecho del ratón en el icono de Windows, a la izquierda de la barra de tareas, o pulsa la combinación de teclas [Windows] + [X].
2. Selecciona la entrada "Windows PowerShell (Administrador)" del menú contextual.



Inicio del símbolo del sistema con derechos de administrador a través del menú contextual de la barra de tareas de Windows

Nota

El uso de Netcat implica ciertos riesgos de seguridad. Por lo tanto, esta herramienta solo deben utilizarla usuarios expertos y administradores de sistemas, especialmente en el modo con derechos de administrador.

### **Sintaxis de Netcat: ¿qué comandos y opciones están disponibles?**

La sintaxis de Netcat consiste en dos componentes fundamentales: el comando básico “**nc**”, siempre idéntico, seguido por varias “**opciones**”. El comando básico direcciona al archivo de programa *nc.exe*, mientras que las opciones determinan el rango concreto de funciones de la versión de Netcat, por lo que varían dependiendo del sistema operativo y de la versión de Netcat utilizada.

La siguiente tabla se limita a recoger las **opciones más importantes** disponibles en la mayoría de las versiones para Linux, macOS y Windows. También se



enumeran otras opciones útiles, en particular las extensiones de la **versión GNU Netcat**, ampliamente utilizada en Linux, Unix y macOS:

Opciones	Descripción
-4	Fuerza el uso de IPv4 (GNU Netcat)
-6	Fuerza el uso de IPv6 (GNU Netcat)
-d	Elimina Netcat de la consola (operación en segundo plano; disponible en Windows y en las versiones actuales de GNU Netcat)
-D	Habilita la opción de depurar los <i>sockets</i> (GNU Netcat)
-h (display help)	Muestra la ayuda (comandos/opciones con una breve descripción)
-i (secs)	Retardo en segundos para las líneas enviadas o los puertos escaneados
-k	Netcat espera una nueva conexión después de que termine la anterior (solo en GNU Netcat y en combinación con “-l”)
-l (listen mode)	Modo de escucha/ <i>listen</i> y servidor para las solicitudes de conexión entrantes (sobre el puerto especificado)
-L (listen harder)	Hace que Netcat funcione en modo de escucha incluso después de las desconexiones del lado del cliente (usando los mismos parámetros en todo momento; solo en la versión de Windows)

-n (numeric-only)	Solo números IP, sin nombres DNS
-o (file)	Se realiza un volcado hexadecimal del tráfico (el contenido de los archivos se muestra en vista hexadecimal); se utiliza para la depuración ( <i>debugging</i> de aplicaciones de red); permite el registro de la comunicación ( <i>sniffing</i> ) para paquetes salientes y entrantes
-p (port)	Especifica el puerto de origen local que Netcat debe utilizar para las conexiones salientes
-r	Usa valores de puerto aleatorios al escanear (para puertos locales y remotos)
-s (adress)	Especifica la dirección de la fuente local (dirección o nombre IP)
-t	Modo Telnet (por ejemplo, permite el direccionamiento del servidor a través de Telnet); requiere una compilación especial de Netcat; de lo contrario, la opción no está disponible
-u	Uso del modo UDP (en lugar de TCP)
-U (gateway)	Netcat utiliza <i>sockets</i> de dominio Unix (GNU Netcat)
-v	Salida detallada (por ejemplo, para la visualización y el alcance de los mensajes de error mostrados)
-w (secs)	Define los tiempos muertos: para establecer y cerrar una conexión (unidad: segundos)

-z	Modo de escáner de puerto (modo de I/O 0); solo escaneo para servicios de escucha (no envío de datos)
----	---

Un ejemplo simple de la utilización de la sintaxis de Netcat es acceder a la ayuda con el parámetro “-h”:

```
1 | C:\Usuarios\NOMBRE DE USUARIO\Escritorio\netcat>nc -h
```

```

C:\WINDOWS\system32\cmd.exe
C:\Users\USERNAME\Desktop\Netcat>nc -h
[v1.11 NT www.rodneybeede.com/]
connect to somewhere:  nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [options] [hostname] [port]
options:
  -d                detach from console, background mode

  -g gateway        source-routing hop point[s], up to 8
  -G num            source-routinDesktop\netcat>nc -h ...
  -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
  -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]

```

Al acceder a la ayuda en el símbolo del sistema de Windows, aparece una lista de las opciones disponibles de Netcat

Si, por ejemplo, quieres definir un servidor o un cliente para la transferencia de datos en la red, debes observar la siguiente sintaxis:

Modo cliente (connect to somewhere):

**nc [opciones] [dirección IP/nombre del host] [puerto]**

Modo de servidor (listen for inbound):

**nc -l -p port [opciones] [nombre del host] [puerto]**

El esquema básico para ejecutar un escaneo de puertos tiene el siguiente aspecto:

nc [opciones] [host] [puerto]

### Copiar archivos con Netcat

Una característica muy popular de Netcat es la copia de archivos, que puede usarse para transferir grandes cantidades de datos, así como para clonar particiones individuales o discos duros enteros. En nuestro ejemplo, el archivo *test.txt* debe copiarse del ordenador A (cliente) al ordenador B (servidor) a través del puerto 6790. Es necesario seguir estos pasos:

1. Determinar la dirección IP del ordenador B (PC de destino).
2. Crear el archivo de prueba *test.txt* en el directorio Netcat del ordenador A. En este ejemplo, el archivo de prueba se encuentra en el directorio de Netcat del cliente. En el ordenador de destino B, el archivo copiado termina también en la carpeta de Netcat (se deben cambiar las otras rutas de archivo en consecuencia).
3. Introducir la sintaxis de Netcat en la línea de comandos.

Ordenador B (actúa como servidor receptor):

```
nc -l -p 6790 > test.txt
```

INTRO

Ordenador A (actúa como cliente que envía):

```
nc [dirección IP del ordenador B] 6790 < test.txt
```

INTRO

El éxito de la transferencia no se confirma en el símbolo del sistema. Puedes comprobar si el archivo se ha transferido correctamente buscándolo en la carpeta de destino.

### Escanear puertos

Puedes ejecutar un escaneo y encontrar puertos abiertos, por ejemplo, para detectar errores y problemas de seguridad. En el siguiente ejemplo, el ordenador tiene la dirección IP 192.168.11.1. Después de la dirección IP, se puede especificar si se desean escanear puertos individuales (por ejemplo, 1), varios puertos (1, 2, 3, etc.) o un rango completo (1-1024):

```
nc -w 2 -z 192.168.10.1 1-1024
```

La opción “-w” determina la duración de un tiempo muerto (en este ejemplo, “Intentar conectarse a los puertos durante dos segundos”). La opción “-z” indica a Netcat que busque solo servicios de escucha y que no envíe ningún dato.

La opción “-v” sirve para obtener información más detallada sobre el escaneo:

```
nc -v -w 2 -z 192.168.11.1 1-1024
```

Netcat confirma entonces un puerto abierto que ha encontrado con el mensaje “succeeded!”.

```
Connection to 192.168.11.1 25 port [tcp/smtp] succeeded!
```

En los puertos escaneados 1-1024, se ejecutan los servicios más conocidos, como correo electrónico, FTP o SSH. En este ejemplo, Netcat ha encontrado el puerto SMTP abierto de un cliente de correo electrónico.

## Netcat como programa de chat simple

Netcat puede establecer una conexión TCP o UDP simple entre dos ordenadores y luego abrir un canal de comunicación. En el siguiente ejemplo, el receptor se instala primero en el sistema remoto y se pone en modo de listening (escucha). De este modo, actúa como la parte de “escucha” y utiliza el puerto 1605 para recibir mensajes, a los que se puede acceder a través de la dirección IP 192.168.11.1:

```
nc -l -p 1605
```

INTRO

A continuación, el ordenador local (PC emisor) establece una conexión con el destinatario del mensaje mediante el siguiente comando:

```
nc 192.168.11.1 1605
```

INTRO

Si la conexión se establece correctamente, los mensajes pueden intercambiarse en ambas direcciones.

## Configurar un servidor web simple

Netcat también sirve para configurar un servidor web simple. Si, por ejemplo, no se puede acceder al servidor original debido a problemas técnicos, se puede al menos responder a las solicitudes con un mensaje de error predeterminado (en forma de archivo .html) con información sobre el error:

```
nc -l -v -p 85 -w10 -L &lt; mensaje de error.html
```

Netcat espera a las solicitudes en el puerto 85 y responde a ellas con el archivo mensaje de error.html. La opción “-L” asegura que Netcat mantenga este procedimiento más allá de una sola solicitud. El parámetro “-w” termina la conexión después de 10 segundos (tiempo muerto). El parámetro “-v” proporciona al operador del servidor información sobre las solicitudes y documentos, como el sistema operativo y el tipo de navegador del ordenador cliente solicitante mediante mensajes de estado.

**Link del video:**

[https://drive.google.com/file/d/1MN7SfopW-FpCdz56NVOVelrB8wu-\\_n5x/view?usp=drivesdk](https://drive.google.com/file/d/1MN7SfopW-FpCdz56NVOVelrB8wu-_n5x/view?usp=drivesdk)