

# Ncat para Pentesting

**Alonso Eduardo Caballero Quezada**

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: <https://www.ReYDeS.com> :- e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 30 de Setiembre 2021

# Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

# Redes Sociales



<https://www.linkedin.com/in/alonsocaballeroquezada/>



[https://twitter.com/Alonso\\_ReYDeS](https://twitter.com/Alonso_ReYDeS)



<https://www.youtube.com/c/AlonsoCaballero>



<https://www.facebook.com/alonsoreydes/>



<https://www.reydes.com>



[reydes@gmail.com](mailto:reydes@gmail.com)



+51 949 304 030



# Ncat

Es una utilidad de red la cual lee y escribe datos a través de las redes desde la línea de comandos. Fue escrito para el proyecto Nmap, como una reimplementación muy mejorada del venerable Netcat.

Utiliza TCP y UDP para la comunicación, y está diseñada para ser una herramienta fiable, de tal manera instantáneamente proporcione conectividad de red hacia otras aplicaciones y usuarios. Ncat no únicamente trabaja con IPv4 e IPv6, también proporciona al usuario con un número virtualmente ilimitado de potenciales usos.

Entre la gran cantidad de funcionalidades está la capacidad de encadenar Ncats, redireccionar puertos TCP y UDP hacia otros sitios, soporte SSL, conexiones proxy vía SOCKS4 o HTTP proxies (Método CONNECT), etc.

\* <https://nmap.org/ncat/>

# Capacidades de Ncat

- Actúa como un cliente simple TCP/UDP/SCTP/SSL para interactuar con servidores web, servidores telnet, servidores de correo, y otros servicios de red TCP/IP
  - Actúa como un servidor simple TCP/UDP/SCTP/SSL para ofrecer servicios hacia clientes, o simplemente para entender aquello hecho por los clientes, capturando cada byte enviado
  - Redireccionar o “proxear” tráfico TCP/UDP/SCTP hacia otros puertos o hosts. Esto es hecho utilizando una simple redirección, o actuando como un SOCKS o proxy HTTP, así los clientes especifican sus propios destinos. En modo cliente Ncat puede conectarse hacia destinos a través de una cadena de proxys
- \* <https://nmap.org/ncat/guide/index.html>

# Capacidades de Ncat (Cont.)

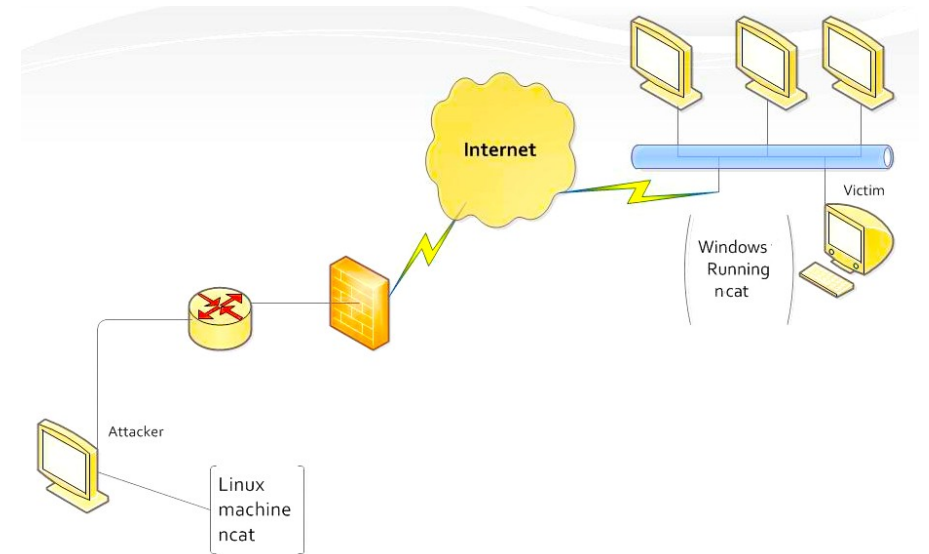
- Se ejecuta en los principales sistemas operativos. Windows, Linux, OS X.
- Encripta comunicaciones con SSL, y lo transporta sobre IPv4 e IPv6
- Actúa como una pasarela de red para la ejecución de comandos del sistema, con redirección de E/S hacia la red.
- Actúa como un agente de conexión, permitiendo dos o más clientes se conecten el uno con el otro a través de un tercer servidor. Esto permite múltiples máquinas se oculten detrás de pasarelas NAT para comunicarse el uno con el otro, y también permite el modo chat simple de Ncat.

\* <https://nmap.org/ncat/guide/index.html>

# Resumen de Opciones

Ncat incluye las siguientes opciones:

- Opciones para el protocolo
- Opciones para el modo de conexión
- Opciones para el modo de atención
- Opciones para SSL
- Opciones para Proxy
- Opciones para la ejecución de comandos
- Opciones para el control de acceso
- Opciones sobre el tiempo
- Opciones de salida
- Opciones misceláneas



\* <https://nmap.org/book/ncat-man.html>

## Curso Virtual Hacking Kali Linux 2021

Domingos 3, 10, 17 y 24 de Octubre del 2021. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



### Presentación

Kali Linux es una distribución basada en el sistema operativo GNU/Linux Debian, diseñada específicamente para realizar auditorías de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a las más diversas tareas en seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux incluye más de 600 herramientas para pruebas de penetración, es libre, tiene un árbol GIT open source, cumple con FHS, tiene un amplio soporte para dispositivos inalámbricos, incluye un kernel parchado para inyección, es desarrollado en un entorno seguro, sus repositorios y paquetes están firmados con GPG, tiene soporte para múltiples lenguajes, incluye soporte para ARMEL, y ARMHF, además de ser completamente personalizable.



**Alonso Eduardo Caballero Quezada** es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of

Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor

Más Información: [https://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_con\\_Kali\\_Linux](https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux)

✉ e-mail: [reydes@gmail.com](mailto:reydes@gmail.com)

🌐 Sitio Web: <https://www.reydes.com>

Alonso Eduardo Caballero Quezada :- Sitio web: <https://www.reydes.com> :- e-mail: [reydes@gmail.com](mailto:reydes@gmail.com)



# Demostraciones

The image shows a Kali Linux desktop environment. On the left, a terminal window displays the following content:

```
File Actions Edit View Help

--chat Start a simple Ncat chat server
--proxy <addr[:port]> Specify address of host to proxy t
--proxy-type <type> Specify proxy type ("http", "socks
--proxy-auth <auth> Authenticate with HTTP or SOCKS pr
--proxy-dns <type> Specify where to resolve proxy des
--ssl Connect or listen with SSL
--ssl-cert Specify SSL certificate file (PEM)
--ssl-key Specify SSL private key (PEM) for
--ssl-verify Verify trust and domain name of ce
--ssl-trustfile PEM file containing trusted SSL ce
--ssl-ciphers Cipherlist containing SSL ciphers
--ssl-servername Request distinct server name (SNI)
--ssl-alpn ALPN protocol list to use
--version Display Ncat's version information

See the ncat(1) manpage for full options, descriptions and usag
kali@kali:~$
kali@kali:~$ cat response_server.html
<title>
<head>
<title>Servidor NCAT</title></head>
<body>
<h3>Este es un servidor ejecutando NCAT</h3>
</body>
</title>
kali@kali:~$
kali@kali:~$ ncat -l -v 80 -c "echo 'HTTP/1.0 200 OK\r\n\r\n'; cat response_server.html"
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 192.168.0.98.
Ncat: Connection from 192.168.0.98:57462.
kali@kali:~$
```

On the right, a Firefox browser window is open to the URL `192.168.0.98`. The page content is:

```
<head> <title>Servidor NCAT - Mozilla Firefox
<head> <title>Servidor NCA x +
192.168.0.98
Este es un servidor ejecutando NCAT
```

# Cursos Virtuales Disponibles en Video

## Curso Virtual de Hacking Ético

[https://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](https://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

## Curso Virtual de Hacking Aplicaciones Web

[https://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)

## Curso Virtual de Informática Forense

[https://www.reydes.com/d/?q=Curso\\_de\\_Informatica\\_Forense](https://www.reydes.com/d/?q=Curso_de_Informatica_Forense)

## Curso Virtual Hacking con Kali Linux

[https://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_con\\_Kali\\_Linux](https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux)

## Curso Virtual OSINT - Open Source Intelligence

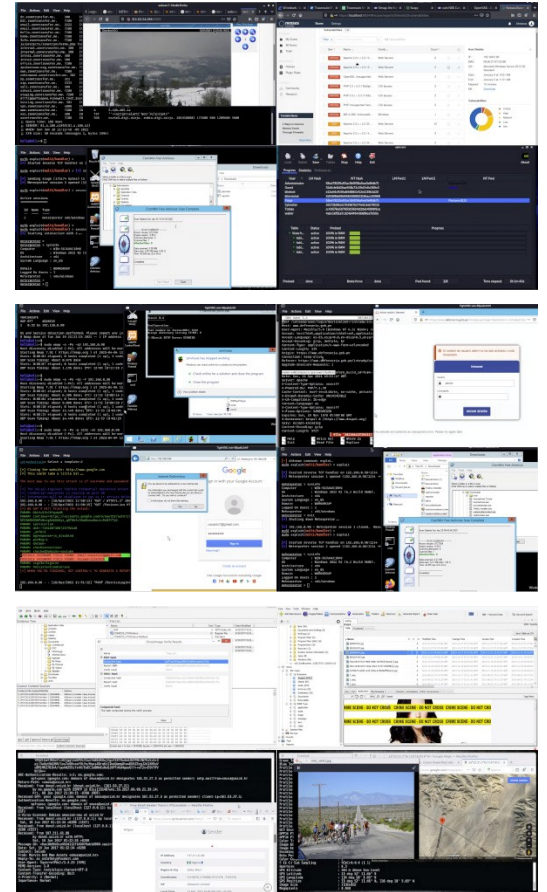
[https://www.reydes.com/d/?q=Curso\\_de\\_OSINT](https://www.reydes.com/d/?q=Curso_de_OSINT)

## Curso Virtual Forense de Redes

[https://www.reydes.com/d/?q=Curso\\_Forense\\_de\\_Red](https://www.reydes.com/d/?q=Curso_Forense_de_Red)

## Y todos los cursos virtuales:

<https://www.reydes.com/d/?q=cursos>



# Más Contenidos

## Videos de 70 webinars gratuitos

<https://www.reydes.com/d/?q=videos>

## Diapositivas de los webinars gratuitos


<https://www.reydes.com/d/?q=eventos>

## Artículos y documentos publicados

<https://www.reydes.com/d/?q=documentos>


## Blog sobre temas de mi interés

<https://www.reydes.com/d/?q=blog/1>




**ALONSO CABALLERO / REYDES** Cursos Videos Blog Eventos Contacto

**Presentación**

 **Alonso Eduardo Caballero Quezada** es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el **OWASP LATAM Tour** Lima, Perú del año 2014, expositor en el **0x11 OWASP Perú Chapter Meeting 2016** y **OWASP LATAM at Home 2020**, además de Conferencista en **PERUHACK 2014**, instructor en **PERUHACK2016NOT**, y conferencista en **8.8 Lucky Perú 2017**. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad **RareGazZ** y al grupo peruano de seguridad **PeruSEC**. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com) y su página personal está en: <https://www.ReYDeS.com>.

[Read more](#)



**Cursos**

- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de OSINT Open Source Intelligence
- Curso Forense de Autopsy
- Curso Maltego
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de WireShark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso de Hacking Windows
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux

**Servicios**

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

# Ncat para Pentesting

**Alonso Eduardo Caballero Quezada**

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: <https://www.ReYDeS.com> :- e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 30 de Setiembre 2021