**Top 30 de Nmap ejemplos de comandos para SYS / Red Admins**

**# 1: Escanear un único host o una dirección IP (IPv4)**

# # # Escanear una única dirección IP # # #

nmap 192.168 0,1 0,1

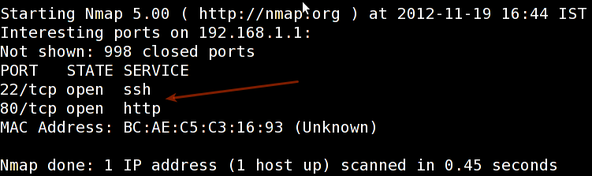
# # Escanear un nombre de host # # #

nmap server1.cyberciti.biz

# # Escanear un nombre de host con más info # # #

nmap-v server1.cyberciti.biz

Salidas de muestra:

[](http://translate.googleusercontent.com/translate_c?act=url&depth=1&hl=es&ie=UTF8&prev=_t&rurl=translate.google.es&sl=auto&tl=es&twu=1&u=http://www.cyberciti.biz/faq/howto-install-nmap-on-centos-rhel-redhat-enterprise-linux/&usg=ALkJrhhU9qH8cdDiLC19ZwAMSnAutkCL6A)Fig.01: salida de nmap

**# 2: Escanear varias direcciones IP o subred (IPv4)**

nmap 192.168.1.1 192.168.1.2 192.168.1.3

# # Trabaja con la misma subred 192.168.1.0/24 es decir,

nmap 192.168.1.1,2,3

Puede escanear un rango de direcciones IP también:

nmap 192.168.1.1-20

Puede escanear un rango de direcciones IP utilizando un comodín:

nmap 192.168.1. \*

Por último, permite escanear una subred completa:

192.168.1.0/24 nmap

**# 3: Lea la lista de hosts / redes desde un archivo (IPv4)**

La IL-opción le permite leer la lista de sistemas de destino mediante un archivo de texto. Esto es útil para analizar un gran número de hosts / redes. Cree un archivo de texto como sigue:  
cat > /tmp/test.txt  
Salidas de muestra:

server1.cyberciti.biz

192.168.1.0/24

192.168.1.1/24

10.1.2.3

localhost

La sintaxis es la siguiente:

nmap-iL / tmp / prueba.txt

**# 4: Exclusión de hosts / redes (IPv4)**

Al escanear un gran número de hosts / redes se pueden excluir los hosts de una exploración:

nmap 192.168.1.0/24 - exclude 192.168.1.5

nmap 192.168.1.0/24 - exclude 192.168.1.5,192.168.1.254

O Excluir lista desde un archivo llamado / tmp / exclude.txt

nmap-iL / tmp / scanlist.txt - excludefile / tmp / exclude.txt

**# 5: Encienda el script de sistema operativo y versión de escaneo de detección (IPv4)**

nmap-A 192.168.1.254

nmap-v-A 192.168.1.1

nmap-A-iL / tmp / scanlist.txt

**# 6: Para saber si un host / red están protegidos por un firewall**

nmap-sA 192.168.1.254

nmap-sA server1.cyberciti.biz

**# 7: Escanear un host si está protegido por el firewall**

nmap-PN 192.168.1.1

nmap-PN server1.cyberciti.biz

**# 8: Escanear un host de IPv6 / dirección**

La opción -6 habilitar el análisis de IPv6. La sintaxis es la siguiente:

nmap -6 IPv6-Address-aquí

nmap -6 server1.cyberciti.biz

nmap -6 2607: f0d0: 1002:51 :: 4

nmap-v A -6 2607: f0d0: 1002:51 :: 4

**# 9: Escanear una red y averiguar qué servidores y dispositivos están en marcha**

Esto se conoce como anfitrión descubrimiento o exploración de ping:

nmap-sP 192.168.1.0/24

Salidas de muestra:

Host 192.168.1.1 es hacia arriba (0.00035s latencia).

Dirección MAC: BC: AE: C5: C3: 16:93 (Desconocido)

Host 192.168.1.2 es hacia arriba (0.0038s latencia).

Dirección MAC: 74:44:01:40:57: FB (Desconocido)

Host 192.168.1.5 está arriba.

Host nas03 (192.168.1.12) es más (0.0091s latencia).

Dirección MAC: 00:11:32:11:15: FC (Synology Incorporated)

Nmap hecho: 256 direcciones IP de hosts (4 más) escaneada en 2,80 segundos

**# 10: ¿Cómo puedo realizar un análisis rápido?**

nmap-F 192.168.1.1

**# 11: Muestra la razón, un puerto está en un estado particular**

nmap - razón 192.168.1.1

nmap - server1.cyberciti.biz razón

**Mostrar únicamente los puertos abiertos (o posiblemente abierto): # 12**

nmap - open 192.168.1.1

nmap - abierto server1.cyberciti.biz

**# 13: Muestra todos los paquetes enviados y recibidos**

nmap - packet-trace 192.168.1.1

nmap - packet-trace server1.cyberciti.biz

**14 #: show interfaces de host y rutas**

Esto es útil para la depuración ( comando ip o comando route o comando netstat como salida usando nmap)

nmap - iflist

Salidas de muestra:

Starting Nmap 5.00 (http://nmap.org) en 2012 -11 -27 02: 01 EST

INTERFACES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

DEV (SHORT) IP / máscara de tipo UP MAC

lo (lo) 127,0 0,0 0,1 / 8 hasta loopback

eth0 (eth0) 192.168 0,1 0,5 / 24 ethernet hasta B8: AC: 6F: 65: 31: E5

vmnet1 (vmnet1) 192.168 0.121 0,1 / 24 ethernet hasta 00: 50: 56: C0: 00: 01

vmnet8 (vmnet8) 192.168 0.179 0,1 / 24 Ethernet hasta 00: 50: 56: C0: 00: 08

ppp0 (ppp0) 10,1 0,19 0,69 / 32 hasta point2point

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* RUTAS \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*

DST / MASK DEV PASARELA

10,0 .31 .178 / 32 ppp0

209,133 .67 .35 / 32 eth0 192.168 0,1 0,2

192.168 0,1 0,0 / 0 eth0

192.168 0.121 0,0 / 0 vmnet1

192.168 0.179 0,0 / 0 vmnet8

169.254 0,0 0,0 / 0 eth0

10,0 0,0 0,0 / 0 ppp0

0,0 0,0 0,0 / 0 eth0 192.168 0,1 0,2

**# 15: ¿Cómo puedo escanear puertos específicos?**

mapa-p [puerto] hostName

# # Escanear el puerto 80

nmap-p 80 192.168 0,1 0,1

# # Escanear el puerto TCP 80

nmap-p T: 80 192.168 0,1 0,1

# # Scan UDP puerto 53

nmap-p U: 53 192.168 0,1 0,1

# # Escanear dos puertos # #

nmap-p 80, 443 192.168 0,1 0,1

# # Escanea rangos de puertos # #

nmap-p 80 -200 192.168 0,1 0,1

# # Combinar todas las opciones # #

nmap-p U: 53, 111, 137, T: 21 -25, 80, 139, 8080 192.168 0,1 0,1

nmap-p U: 53, 111, 137, T: 21 -25, 80, 139, 8080 server1.cyberciti.biz

nmap-v-sU-sT-p U: 53, 111, 137, T: 21 -25, 80, 139, 8080 192.168 0,1 0.254

# # Analizar todos los puertos con comodín \* # #

nmap-p "\*" 192.168 0,1 0,1

# # Escanear puertos principales, es decir $ escanear puertos numéricos más comunes # #

nmap - TOP-puertos 5 192.168 0,1 0,1

nmap - top-ports 10 192.168 0,1 0,1

Salidas de muestra:

Starting Nmap 5.00 (http://nmap.org) en 2012 -11 -27 01: 23 EST

Puertos de interés sobre 192.168 0,1 0,1:

PORT STATE SERVICE

21 / tcp cerrado ftp

22 / tcp abierto ssh

23 / tcp telnet cerrado

25 / tcp smtp cerrada

80 / tcp abiertos http

110 / tcp cerrado pop3

139 / tcp cerrado netbios-ssn

443 / tcp cerrado https

445 / tcp cerrado microsoft-ds

3389 / tcp cerrado ms plazo-serv

Dirección MAC: BC: AE: C5: C3: 16: 93 (Desconocido)

Nmap hecho: 1 dirección IP (1 huésped up) escaneada en 0,51 segundos

**# 16: La forma más rápida para escanear todos los dispositivos / equipos para puertos abiertos a la vez**

nmap-T5 192.168.1.0/24

**# 17: ¿Cómo puedo detectar el sistema operativo remoto?**

Puede identificar algunas aplicaciones y el sistema operativo host remoto utilizando la opción-O :

nmap-O 192.168 0,1 0,1

nmap-O - osscan-Supongo 192.168 0,1 0,1

nmap-v-O - osscan-Supongo 192.168 0,1 0,1

Salidas de muestra:

Starting Nmap 5.00 (http://nmap.org) en 11/27/2012 01:29 IST

NSE: Cargado 0 secuencias de comandos para la exploración.

Inicio de ARP Ping Scan a las 01:29

Escaneo 192.168.1.1 [1 puerto]

Completado ARP Ping Scan a las 01:29, 0.01s transcurrido (1 hosts totales)

Iniciar paralelo resolución DNS de un host. a las 01:29

Completado resolución DNS en paralelo de un host. a las 01:29, 0.22s transcurrido

Iniciar SYN Scan sigilo a las 01:29

Escaneo de puertos 192.168.1.1 [1000]

Descubierto 80/tcp puerto abierto en 192.168.1.1

Descubierto 22/tcp puerto abierto en 192.168.1.1

Completado SYN Scan sigilo a las 01:29, 0.16s transcurrido (1000 puertos en total)

Inicio de detección de sistema operativo (prueba n º 1) en contra de 192.168.1.1

Intentando de nuevo OS detección (prueba # 2) contra 192.168.1.1

Intentando de nuevo OS detección (prueba n º 3) en contra de 192.168.1.1

Intentando de nuevo OS detección (prueba n º 4) contra 192.168.1.1

Intentando de nuevo OS detección (prueba n º 5) contra 192.168.1.1

Host 192.168.1.1 es hacia arriba (0.00049s latencia).

Puertos de interés sobre 192.168.1.1:

No se muestra: 998 puertos cerrados

PORT STATE SERVICE

Ssh 22/tcp abierto

80/tcp abierto http

Dirección MAC: BC: AE: C5: C3: 16:93 (Desconocido)

Tipo de dispositivo: WAP | Aplicaciones generales | Router | Imprimir | router de banda ancha

Funcionamiento (sólo una suposición): Linksys Linux 2.4.X (95%), Linux 2.4.X | 2.6.X (94%), Mikrotik RouterOS 3.x (92%), Lexmark Embedded (90%), Enterasys embedded (89 %), D-Link Linux 2.4.X (89%), Linux 2.4.X Netgear (89%)

Agresivo conjeturas SO: OpenWrt White Russian 0,9 (Linux 4.2.30) (95%), OpenWrt 0,9 a 7,09 (Linux 2.4.30 a 2.4.34) (94%), OpenWrt Kamikaze 7,09 (Linux 6.2.22) (94% ), Linux 2.4.21-2.4.31 (probablemente incrustado) (92%), Linux 2.6.15-2.6.23 (embedded) (92%), Linux 2.6.15-2.6.24 (92%), Mikrotik RouterOS 3.0beta5 (92%), Mikrotik RouterOS 3.17 (92%), Linux 2.6.24 (91%), Linux 2.6.22 (90%)

No hay coincidencias exactas para el host del sistema operativo (si usted sabe qué sistema operativo se está ejecutando en ella, ver http://nmap.org/submit/).

TCP / IP de huella digital:

OS: SCAN (V = 5,00 D = 11% / 27% = 22% OT CT = 1% CU = 30609% PV = Y% DS = 1% G = Y% m% = BCAEC5 TM = 50B3CA

OS:% P = 4B x86\_64-unknown-linux-gnu) SEC (SP = C8% GCD = 1% ISR = CB% TI = Z% CI = Z% II = I% TS = 7

OS :) OPS (O1 = M2300ST11NW2% O2 = O3 M2300ST11NW2% = M2300NNT11NW2% O4 O5 = M2300ST11NW2%

OS: = M2300ST11NW2% O6 = M2300ST11) WIN (W1 = 45E8% W2 = 45E8% W3 = 45E8% W4 W5 = 45E8% = 45E8% W

OS: 6 = 45E8) REC (R = Y% DF = Y% T = 40% W = 4600% O = CC = M2300NNSNW2% N% = Q) T1 (R = Y% DF = Y% T = 40% S

OS: =% S A = S + F% = EN% RD = 0% Q =) T2 (R = N) T3 (R = N) T4 (R = Y% DF = Y% T = 40% W = 0% S = A% A% = Z F = R% S% = R

OS: D = 0% Q =) T5 (R = Y% DF = Y% T = 40% W = 0% S = Z% A = S + F% = AR% O =% RD = 0% Q =) T6 (R = Y% DF = Y% T = 40% W =

OS: 0% S = A% A% = Z = F R% S% = RD = 0% = Q) T7 (R = N) U1 (R = Y% DF = N% T = 40% IPL = 164% UN = 0% =% RIPL G RID

OS: = G = G RIPCK%%% RUCK = G = G RUD) IE (R = Y% DFI = N% T = CD = 40% S)

Uptime conjetura: 12,990 días (desde mié 14 de noviembre 01:44:40 2012)

Distancia de red: 1 salto

Predicción de Secuencia TCP: Dificultad = 200 (Buena suerte!)

IP ID Generación de secuencia: Todo ceros

Leer archivos de datos de: / usr / share / nmap

OS detección realizada. Por favor reporte cualquier resultado incorrecto en http://nmap.org/submit/.

Nmap hecho: 1 dirección IP (1 huésped up) escaneada en 12,38 segundos

Paquetes enviados: Raw 1126 (53.832KB) | Rcvd: 1066 (46.100KB)

Véase también: Toma de huellas dactilares de un servidor web y un servidor DNS herramientas de línea de comandos para más información.

**# 18: ¿Cómo puedo detectar servicios remotos (servidor / daemon) números de versión?**

nmap-sV 192.168.1.1

Salidas de muestra:

Starting Nmap 5.00 (http://nmap.org) en 11/27/2012 01:34 IST

Puertos de interés sobre 192.168.1.1:

No se muestra: 998 puertos cerrados

ESTADO DEL PUERTO DE SERVICIO VERSION

22/tcp abierto ssh **sshd Dropbear 0,52 (protocolo 2.0)**

80/tcp abierto http?

Un servicio reconocido a pesar de los datos que regresan.

**# 19: Escanear un host que utiliza TCP ACK (PA) y TCP Syn (PS) de ping**

Si el firewall está bloqueando estándar pings ICMP, pruebe los métodos siguientes descubrimiento de acogida:

nmap-PS 192.168.1.1

nmap-PS 80,21,443 192.168.1.1

nmap-PA 192.168.1.1

nmap-PA 80,21,200-512 192.168.1.1

**# 20: Escanear un host con mesa de ping IP**

nmap-PO 192.168.1.1

**# 21: Escanear un host que utiliza UDP mesa de ping**

Este análisis no pasa por firewalls y filtros de pantalla que sólo TCP:

nmap-PU 192.168.1.1

nmap-PU 2000.2001 192.168.1.1

**# 22: Descubre los más utilizados los puertos TCP que utilizan TCP SYN Scan**

# # # Sigiloso escanear # # #

nmap-sS 192.168 0,1 0,1

# # # Conocé las más comunes que utilizan los puertos TCP TCP connect scan (aviso: no hay exploración sigilo)

# # # OS Fingerprinting # # #

nmap-sT 192.168 0,1 0,1

# # # Conocé las más comunes que utilizan los puertos TCP scan TCP ACK

nmap-sA 192.168 0,1 0,1

# # # Conocé las más comunes que utilizan los puertos TCP TCP Window scan

nmap-sW 192.168 0,1 0,1

# # # Conocé las más comunes que utilizan los puertos TCP TCP Maimon scan

nmap-sM 192.168 0,1 0,1

**# 23: Escanear un host para servicios UDP (UDP scan)**

Mayoría de los servicios populares de Internet se extienden sobre el protocolo TCP. DNS, SNMP y DHCP son tres de los servicios UDP más comunes. Utilice la sintaxis siguiente para averiguar los servicios UDP:

nmap-sU nas03

nmap-sU 192.168.1.1

Salidas de muestra:

Starting Nmap 5.00 (http://nmap.org) en 2012 -11 -27 00: 52 EST

Estadísticas: 0: 05: 29 transcurrido; 0 anfitriones completado (1 arriba), 1 experimentando UDP Scan

UDP Scan Tiempo: Acerca de 32,49% hecho, ETC: 01:09 (0:11:26 restante)

Puertos de interés sobre nas03 (192,168 .1 .12):

No se muestra: 995 puertos cerrados

PORT STATE SERVICE

111 / udp abierto | filtrado rpcbind

123 / udp abierto | filtrado ntp

161 / udp abierto | filtrado snmp

2049 / udp abierto | filtrado nfs

5353 / udp abierto | filtrado zeroconf

Dirección MAC: 00: 11: 32: 11: 15: FC (Synology Incorporated)

Nmap hecho: 1 dirección IP (1 huésped up) escaneada en 1099,55 segundos

**# 24: Analizar en busca de protocolo IP**

Este tipo de análisis permite determinar qué protocolos IP (TCP, ICMP, IGMP, etc) son compatibles con los equipos de destino:

nmap-sO 192.168.1.1

**# 25: Digitalizar un firewall para la debilidad en la seguridad**

Los siguientes tipos de exploración explotar una escapatoria sutil en el TCP y bueno para probar la seguridad de los ataques más comunes:

# # TCP Null Scan para engañar a un servidor de seguridad para generar una respuesta # #

# # No establece ningún bit (encabezado TCP bandera es 0) # #

nmap-sN 192.168 0,1 0.254

# # TCP Fin scan para comprobar firewall # #

# # Establece sólo el bit FIN TCP # #

nmap-sF 192.168 0,1 0.254

# # TCP Xmas escaneado para comprobar firewall # #

# # Establece el FIN, PSH, URG y banderas, encendiendo el paquete como un árbol de Navidad # #

nmap-sX 192.168 0,1 0.254

Vea cómo bloquear Navidad packkets, syn inundaciones y otros ataques conman con iptables.

**# 26: Digitalizar un servidor de seguridad de los fragmentos de paquetes**

La opción-f hace que la exploración solicitada (incluyendo las exploraciones ping) a utilizar pequeños paquetes IP fragmentados. La idea es dividir la cabecera TCP a través de  
varios paquetes para que sea más difícil para los filtros de paquetes, sistemas de detección de intrusos y otras molestias para detectar lo que está haciendo.

nmap-f 192.168.1.1

nmap-f fw2.nixcraft.net.in

nmap-f 15 fw2.nixcraft.net.in

# # Establece el tamaño de su propia compensación con la opción - mtu # #

nmap - mtu 32 192.168.1.1

**# 27: Capa de un análisis con señuelos**

La opción-D que aparecen al host remoto que el host (s) se especifica como señuelos a escanear la red de destino también . Así, sus IDS puede informar escaneos de puertos 5-10 de direcciones IP únicas, pero no sabrán qué IP se escanearlos y que eran señuelos inocentes:

nmap-n-Ddecoy-IP1, IP2-señuelo, su-propio-ip, señuelo-IP3, IP4-señuelo a distancia-host-ip

nmap-n-D192.168.1.5, 10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5

**# 28: Digitalizar un firewall para la falsificación de direcciones MAC**

# # # Spoof su dirección MAC # #

nmap - spoof-mac MAC-ADDRESS-HERE 192.168 0,1 0,1

# # # Añadir otra opción # # #

nmap-v-sT-PN - spoof-mac MAC-ADDRESS-HERE 192.168 0,1 0,1

# # # Usar una dirección MAC aleatoria # # #

# # # El número 0, significa nmap elige una dirección MAC completamente al azar # # #

nmap-v-sT-PN - spoof-mac 0 192.168 0,1 0,1

**# 29: ¿Cómo puedo guardar la salida en un archivo de texto?**

La sintaxis es la siguiente:

nmap 192.168.1.1> output.txt

nmap-oN / ruta / al / archivo 192.168.1.1

nmap-oN output.txt 192.168.1.1

**# 30: No es un ventilador de herramientas de línea de comandos?**

Trate Zenmap el asignador de red oficial de interfaz:

Zenmap es el oficial de Nmap Security Scanner GUI. Se trata de una plataforma multi-(Linux, Windows, Mac OS X, BSD, etc) la aplicación gratuita y de código abierto que tiene como objetivo hacer Nmap fácil de usar para principiantes al tiempo que proporciona funciones avanzadas para usuarios experimentados de Nmap. Exploraciones de uso más frecuente se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un creador de comando permite la creación interactiva de línea de comandos de Nmap. Los resultados del análisis se pueden guardar y ver más tarde. Resultados de análisis guardados se pueden comparar entre sí para ver qué se diferencian. Los resultados de los análisis recientes se guardan en una base de datos.

Puede instalar Zenmap usando el siguiente comando apt-get :  
$ sudo apt-get install zenmap  
Salidas de muestra:

Password [sudo] para vivek:

Leyendo lista de paquetes ... Hecho

Edificio árbol de dependencias

Leyendo la información de estado ... Hecho

Los siguientes paquetes NUEVOS serán instalados:

Zenmap

0 actualizados, 1 se instalarán, 0 para eliminar y 11 no actualizados.

Necesidad de obtener 616 kB de archivos.

Después de esta operación, 1.827 kB de espacio de disco adicional se utilizará.

Obtener: 1 chorrito http://debian.osuosl.org/debian/ / main Zenmap amd64 5.00-3 [616 kB]

Recuperados de 616 kB en 3s (199 kB / s)

Seleccionando previamente no seleccionado Zenmap paquete.

(Leyendo la base de datos ... 281105 ficheros y directorios instalados actualmente.)

Desembalaje Zenmap (de ... / zenmap\_5.00 3\_amd64.deb-) ...

Procesamiento de disparadores para desktop-file-utils ...

Procesamiento de disparadores para gnome-menus ...

Procesamiento de disparadores para man-db ...

Configuración de Zenmap (5.00-3) ...

Procesamiento de disparadores para python-central ...

Escriba el siguiente comando para iniciar Zenmap:  
$ sudo zenmap  
Salidas de muestra

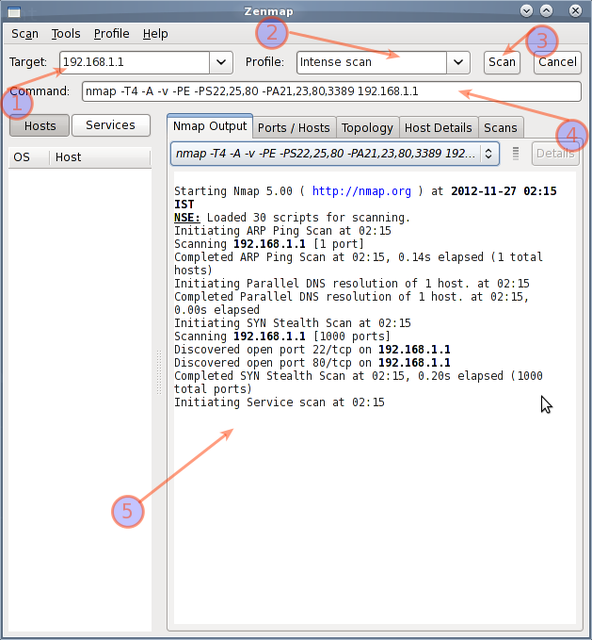
[](http://translate.googleusercontent.com/translate_c?act=url&depth=1&hl=es&ie=UTF8&prev=_t&rurl=translate.google.es&sl=auto&tl=es&twu=1&u=http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/attachment/nmap-usage-examples-output/&usg=ALkJrhjT5opq7qr_o6LcubiFgxEdHw0cOg)

Fig.02: Zenmap en acción