

# nixCraft

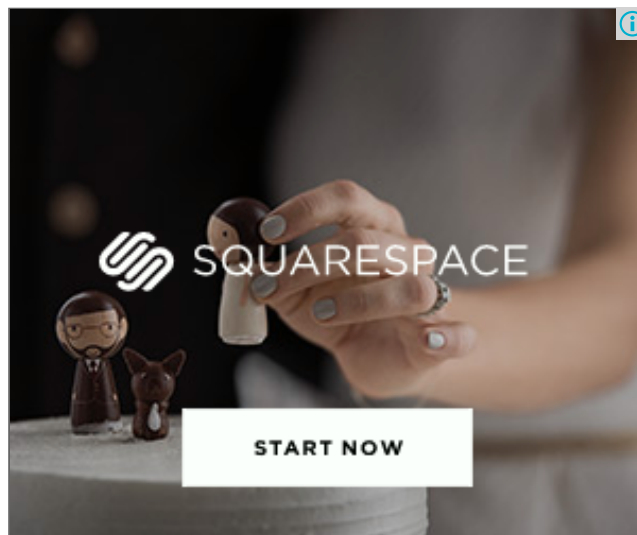
Linux Tips, Hacks, Tutorials, And Ideas In Blog

## Top 30 Nmap Command Examples For Sys/Network Admins

by VIVEK GITE on NOVEMBER 26, 2012 last updated DECEMBER 11, 2012

in [COMMAND LINE HACKS](#), [HOWTO](#), [NETWORKING](#), [SECURITY](#)

**N**map is short for Network Mapper. It is an open source security tool for network exploration, security scanning and auditing. However, nmap command comes with lots of options that can make the utility more robust and difficult to follow for new users.



The purpose of this post is to introduce a user to the nmap command line tool to scan a host and/or network, so to find out the possible vulnerable points in the hosts. You will also learn how to use Nmap for offensive and defensive purposes.

```

root@wks01:/home/vivek# nmap --top-ports 10 192.168.1.1

Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IST
Interesting ports on 192.168.1.1:
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds

```

nmap in action

## More about nmap

From the man page:

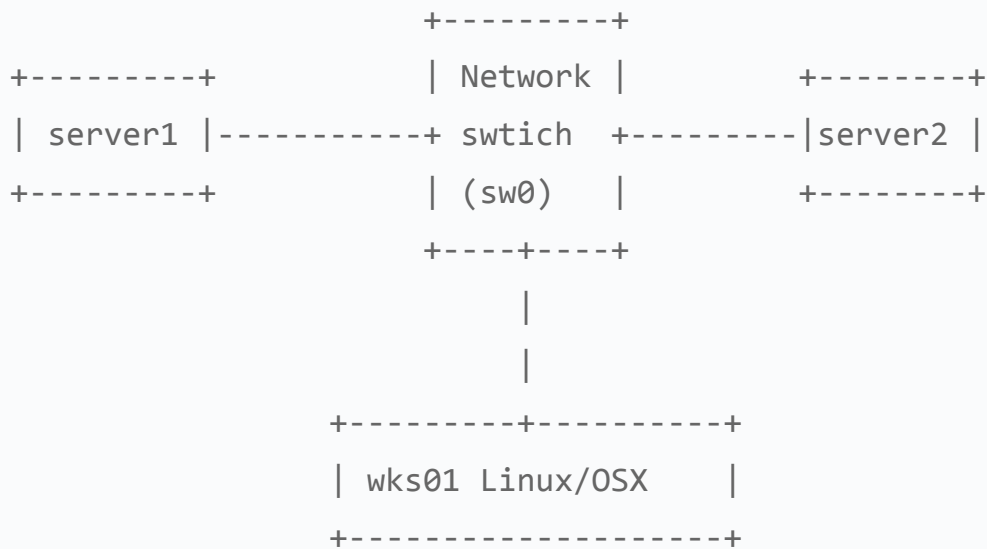
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

It was originally written by Gordon Lyon and it can answer the following questions easily:

1. What computers did you find running on the local network?
2. What IP addresses did you find running on the local network?
3. What is the operating system of your target machine?
4. Find out what ports are open on the machine that you just scanned?
5. Find out if the system is infected with malware or virus.
6. Search for unauthorized servers or network service on your network.
7. Find and remove computers which don't meet the organization's minimum level of security.

## Sample setup (LAB)

Port scanning may be illegal in some jurisdictions. So setup a lab as follows:



Where,

- wks01 is your computer either running Linux/OS X or Unix like operating system. It is used for scanning your local network. The nmap command must be installed on this computer.
- server1 can be powered by Linux / Unix / MS-Windows operating systems. This is an unpatched server. Feel free to install a few services such as a web-server, file server and so on.

- server2 can be powered by Linux / Unix / MS-Windows operating systems. This is a fully patched server with firewall. Again, feel free to install few services such as a web-server, file server and so on.
- All three systems are connected via switch.

## How do I install nmap?

See:

1. [Debian / Ubuntu Linux: Install nmap Software For Scanning Network](#)
2. [CentOS / RHEL: Install nmap Network Security Scanner](#)
3. [OpenBSD: Install nmap Network Security Scanner](#)

## #1: Scan a single host or an IP address (IPv4)

```
### Scan a single ip address ###
```

```
nmap 192.168.1.1
```

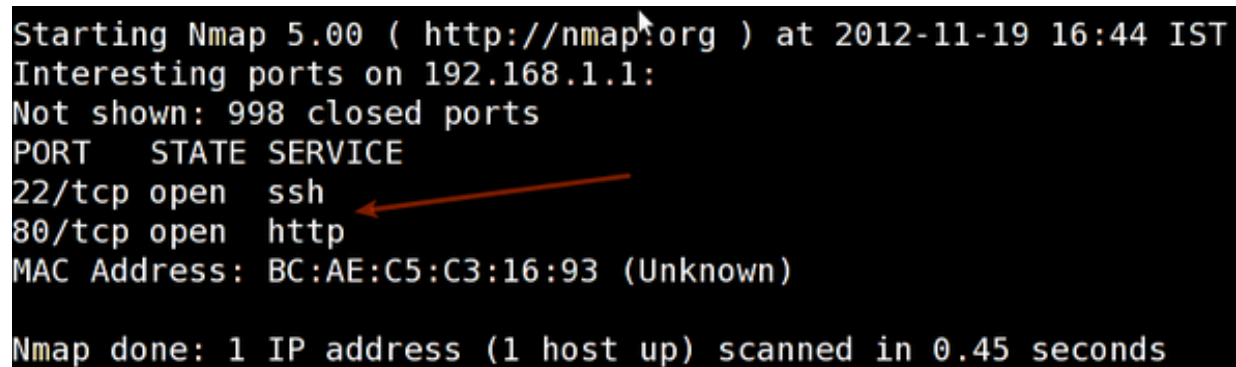
```
## Scan a host name ###
```

```
nmap server1.cyberciti.biz
```

```
## Scan a host name with more info###
```

```
nmap -v server1.cyberciti.biz
```

Sample outputs:



```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-19 16:44 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Fig.01: nmap output

## #2: Scan multiple IP address or subnet (IPv4)

```
nmap 192.168.1.1 192.168.1.2 192.168.1.3
## works with same subnet i.e. 192.168.1.0/24
nmap 192.168.1.1,2,3
```

You can scan a range of IP address too:

```
nmap 192.168.1.1-20
```

You can scan a range of IP address using a wildcard:

```
nmap 192.168.1.*
```

Finally, you scan an entire subnet:

```
nmap 192.168.1.0/24
```

## #3: Read list of hosts/networks from a file (IPv4)

The `-iL` option allows you to read the list of target systems using a text file. This is useful to scan a large number of hosts/networks. Create a text file as follows:

```
cat > /tmp/test.txt
```

Sample outputs:

```
server1.cyberciti.biz  
192.168.1.0/24  
192.168.1.1/24  
10.1.2.3  
localhost
```

The syntax is:

```
nmap -iL /tmp/test.txt
```

## #4: Excluding hosts/networks (IPv4)

When scanning a large number of hosts/networks you can exclude hosts from a scan:

```
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
```

OR exclude list from a file called `/tmp/exclude.txt`

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

## #5: Turn on OS and version detection scanning script (IPv4)

```
nmap -A 192.168.1.254  
nmap -v -A 192.168.1.1  
nmap -A -iL /tmp/scanlist.txt
```

## #6: Find out if a host/network is protected by a firewall

```
nmap -sA 192.168.1.254  
nmap -sA server1.cyberciti.biz
```

## #7: Scan a host when protected by the firewall

```
nmap -PN 192.168.1.1  
nmap -PN server1.cyberciti.biz
```

## #8: Scan an IPv6 host/address

The `-6` option enable IPv6 scanning. The syntax is:

```
nmap -6 IPv6-Address-Here  
nmap -6 server1.cyberciti.biz  
nmap -6 2607:f0d0:1002:51::4  
nmap -v A -6 2607:f0d0:1002:51::4
```

## #9: Scan a network and find out which servers and devices are up and running

This is known as host discovery or ping scan:

```
nmap -sP 192.168.1.0/24
```

### Sample outputs:

```
Host 192.168.1.1 is up (0.00035s latency).  
MAC Address: BC:AE:C5:C3:16:93 (Unknown)  
Host 192.168.1.2 is up (0.0038s latency).  
MAC Address: 74:44:01:40:57:FB (Unknown)  
Host 192.168.1.5 is up.  
Host nas03 (192.168.1.12) is up (0.0091s latency).  
MAC Address: 00:11:32:11:15:FC (Synology Incorporated)  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.80 second
```

### #10: How do I perform a fast scan?

```
nmap -F 192.168.1.1
```

### #11: Display the reason a port is in a particular state

```
nmap --reason 192.168.1.1  
nmap --reason server1.cyberciti.biz
```

### #12: Only show open (or possibly open) ports

```
nmap --open 192.168.1.1  
nmap --open server1.cyberciti.biz
```



## #13: Show all packets sent and received

```
nmap --packet-trace 192.168.1.1
nmap --packet-trace server1.cyberciti.biz
```

## 14#: Show host interfaces and routes

This is useful for debugging ([ip command](#) or [route command](#) or [netstat command](#) like output using nmap)

```
nmap --iflist
```

Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 02:01 IST
```

```
*****INTERFACES*****
```

DEV	(SHORT)	IP/MASK	TYPE	UP	MAC
lo	(lo)	127.0.0.1/8	loopback	up	
eth0	(eth0)	192.168.1.5/24	ethernet	up	B8:AC:6F:65:31:E5
vmnet1	(vmnet1)	192.168.121.1/24	ethernet	up	00:50:56:C0:00:01
vmnet8	(vmnet8)	192.168.179.1/24	ethernet	up	00:50:56:C0:00:08
ppp0	(ppp0)	10.1.19.69/32	point2point	up	

```
*****ROUTES*****
```

DST/MASK	DEV	GATEWAY
10.0.31.178/32	ppp0	
209.133.67.35/32	eth0	192.168.1.2
192.168.1.0/0	eth0	
192.168.121.0/0	vmnet1	
192.168.179.0/0	vmnet8	
169.254.0.0/0	eth0	

```
10.0.0.0/0      ppp0
0.0.0.0/0      eth0    192.168.1.2
```

## #15: How do I scan specific ports?

```
map -p [port] hostName
## Scan port 80
nmap -p 80 192.168.1.1

## Scan TCP port 80
nmap -p T:80 192.168.1.1

## Scan UDP port 53
nmap -p U:53 192.168.1.1

## Scan two ports ##
nmap -p 80,443 192.168.1.1

## Scan port ranges ##
nmap -p 80-200 192.168.1.1

## Combine all options ##
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
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 192.168.1.254

## Scan all ports with * wildcard ##
nmap -p "*" 192.168.1.1

## Scan top ports i.e. scan $number most common ports ##
nmap --top-ports 5 192.168.1.1
```

```
nmap --top-ports 10 192.168.1.1
```

### Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 01:23 IST
```

```
Interesting ports on 192.168.1.1:
```

PORT	STATE	SERVICE
------	-------	---------

21/tcp	closed	ftp
--------	--------	-----

22/tcp	open	ssh
--------	------	-----

23/tcp	closed	telnet
--------	--------	--------

25/tcp	closed	smtp
--------	--------	------

80/tcp	open	http
--------	------	------

110/tcp	closed	pop3
---------	--------	------

139/tcp	closed	netbios-ssn
---------	--------	-------------

443/tcp	closed	https
---------	--------	-------

445/tcp	closed	microsoft-ds
---------	--------	--------------

3389/tcp	closed	ms-term-serv
----------	--------	--------------

```
MAC Address: BC:AE:C5:C3:16:93 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

## #16: The fastest way to scan all your devices/computers for open ports ever

```
nmap -T5 192.168.1.0/24
```

## #17: How do I detect remote operating system?

You can identify a remote host apps and OS using the -O option:

```
nmap -O 192.168.1.1
nmap -O --osscan-guess 192.168.1.1
nmap -v -O --osscan-guess 192.168.1.1
```

Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 01:29 IST
NSE: Loaded 0 scripts for scanning.
Initiating ARP Ping Scan at 01:29
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 01:29, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:29
Completed Parallel DNS resolution of 1 host. at 01:29, 0.22s elapsed
Initiating SYN Stealth Scan at 01:29
Scanning 192.168.1.1 [1000 ports]
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Completed SYN Stealth Scan at 01:29, 0.16s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.1
Retrying OS detection (try #2) against 192.168.1.1
Retrying OS detection (try #3) against 192.168.1.1
Retrying OS detection (try #4) against 192.168.1.1
Retrying OS detection (try #5) against 192.168.1.1
Host 192.168.1.1 is up (0.00049s latency).
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Device type: WAP|general purpose|router|printer|broadband router

Running (JUST GUESSING) : 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%), Netgear Linux 2.4.X (89%)

Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (95%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (94%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (94%), Linux 2.4.21 - 2.4.31 (likely embedded) (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 exact OS matches for host (If you know what OS is running on it, see <http://nmap.org/submit/> ).

TCP/IP fingerprint:

OS:SCAN(V=5.00%D=11/27%OT=22%CT=1%CU=30609%PV=Y%DS=1%G=Y%M=BCAEC5%TM=5OS:4B%P=x86\_64-unknown-linux-gnu)SEQ(SP=C8%GCD=1%ISR=CB%TI=Z%CI=Z%II=1OS: )OPS(O1=M2300ST11NW2%O2=M2300ST11NW2%O3=M2300NNT11NW2%O4=M2300ST11NOS:=M2300ST11NW2%O6=M2300ST11)WIN(W1=45E8%W2=45E8%W3=45E8%W4=45E8%W5=4OS:6=45E8)ECN(R=Y%DF=Y%T=40%W=4600%O=M2300NNSNW2%CC=N%Q=)T1(R=Y%DF=Y%TOS:=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=FOS: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%TOS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=OS:=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 12.990 days (since Wed Nov 14 01:44:40 2012)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=200 (Good luck!)

IP ID Sequence Generation: All zeros

Read data files from: /usr/share/nmap

OS detection performed. Please report any incorrect results at <http://nmap.org>

Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds

Raw packets sent: 1126 (53.832KB) | Rcvd: 1066 (46.100KB)

See also: [Fingerprinting a web-server](#) and a [dns server](#) command line tools for more information.

## #18: How do I detect remote services (server / daemon) version numbers?

```
nmap -sV 192.168.1.1
```

Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 01:34 IST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      Dropbear sshd 0.52 (protocol 2.0)
80/tcp    open  http?
1 service unrecognized despite returning data.
```

## #19: Scan a host using TCP ACK (PA) and TCP Syn (PS) ping

If firewall is blocking standard ICMP pings, try the following host discovery methods:

```
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: Scan a host using IP protocol ping

```
nmap -PO 192.168.1.1
```

## #21: Scan a host using UDP ping

This scan bypasses firewalls and filters that only screen TCP:

```
nmap -PU 192.168.1.1  
nmap -PU 2000.2001 192.168.1.1
```

## #22: Find out the most commonly used TCP ports using TCP SYN Scan

*### Stealthy scan ###*

```
nmap -sS 192.168.1.1
```

*### Find out the most commonly used TCP ports using TCP connect scan (warning: no stealth scan)*

*### OS Fingerprinting ###*

```
nmap -sT 192.168.1.1
```

*### Find out the most commonly used TCP ports using TCP ACK scan*

```
nmap -sA 192.168.1.1
```

*### Find out the most commonly used TCP ports using TCP Window scan*

```
nmap -sW 192.168.1.1
```

*### Find out the most commonly used TCP ports using TCP Maimon scan*

```
nmap -sM 192.168.1.1
```

## #23: Scan a host for UDP services (UDP scan)

Most popular services on the Internet run over the TCP protocol. DNS, SNMP, and DHCP are three of the most common UDP services. Use the following syntax to find out UDP services:

```
nmap -sU nas03
nmap -sU 192.168.1.1
```

Sample outputs:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 00:52 IST
Stats: 0:05:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP S
can
UDP Scan Timing: About 32.49% done; ETC: 01:09 (0:11:26 remaining)
Interesting ports on nas03 (192.168.1.12):
Not shown: 995 closed ports
PORT      STATE      SERVICE
111/udp   open|filtered rpcbind
123/udp   open|filtered ntp
161/udp   open|filtered snmp
2049/udp  open|filtered nfs
5353/udp  open|filtered zeroconf
MAC Address: 00:11:32:11:15:FC (Synology Incorporated)

Nmap done: 1 IP address (1 host up) scanned in 1099.55 seconds
```

## #24: Scan for IP protocol

This type of scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.)



are supported by target machines:

```
nmap -sO 192.168.1.1
```

## #25: Scan a firewall for security weakness

The following scan types exploit a subtle loophole in the TCP and good for testing security of common attacks:

```
## TCP Null Scan to fool a firewall to generate a response ##
```

```
## Does not set any bits (TCP flag header is 0) ##
```

```
nmap -sN 192.168.1.254
```

```
## TCP Fin scan to check firewall ##
```

```
## Sets just the TCP FIN bit ##
```

```
nmap -sF 192.168.1.254
```

```
## TCP Xmas scan to check firewall ##
```

```
## Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree ##
```

```
nmap -sX 192.168.1.254
```

See [how to block Xmas packets, syn-floods and other conman attacks](#) with iptables.

## #26: Scan a firewall for packets fragments

The -f option causes the requested scan (including ping scans) to use tiny fragmented IP packets. The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and

other annoyances to detect what you are doing.

```
nmap -f 192.168.1.1
nmap -f fw2.nixcraft.net.in
nmap -f 15 fw2.nixcraft.net.in
## Set your own offset size with the --mtu option ##
nmap --mtu 32 192.168.1.1
```

## #27: Cloak a scan with decoys

The `-D` option it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus their IDS might report 5-10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys:

```
nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-h
nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
```

## #28: Scan a firewall for MAC address spoofing

*### Spoof your MAC address ##*

```
nmap --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
```

*### Add other options ###*

```
nmap -v -sT -PN --spoof-mac MAC-ADDRESS-HERE 192.168.1.1
```

*### Use a random MAC address ###*

*### The number 0, means **nmap** chooses a completely random MAC address*

```
###
```

```
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

## #29: How do I save output to a text file?

The syntax is:

```
nmap 192.168.1.1 > output.txt  
nmap -oN /path/to/filename 192.168.1.1  
nmap -oN output.txt 192.168.1.1
```

## #30: Not a fan of command line tools?

Try [zenmap the official network mapper](#) front end:


Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

You can install zenmap using the following [apt-get command](#):

```
$ sudo apt-get install zenmap
```

Sample outputs:

```
[sudo] password for vivek:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zenmap
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.
Need to get 616 kB of archives.
After this operation, 1,827 kB of additional disk space will be used.
Get:1 http://debian.osuosl.org/debian/ squeeze/main zenmap amd64 5.00-
Fetched 616 kB in 3s (199 kB/s)
Selecting previously deselected package zenmap.
(Reading database ... 281105 files and directories currently installed)
Unpacking zenmap (from ../zenmap_5.00-3_amd64.deb) ...
Processing triggers for desktop-file-utils ...
Processing triggers for gnome-menus ...
Processing triggers for man-db ...
Setting up zenmap (5.00-3) ...
Processing triggers for python-central ...
```



Type the following command to start zenmap:

```
$ sudo zenmap
```

Sample outputs

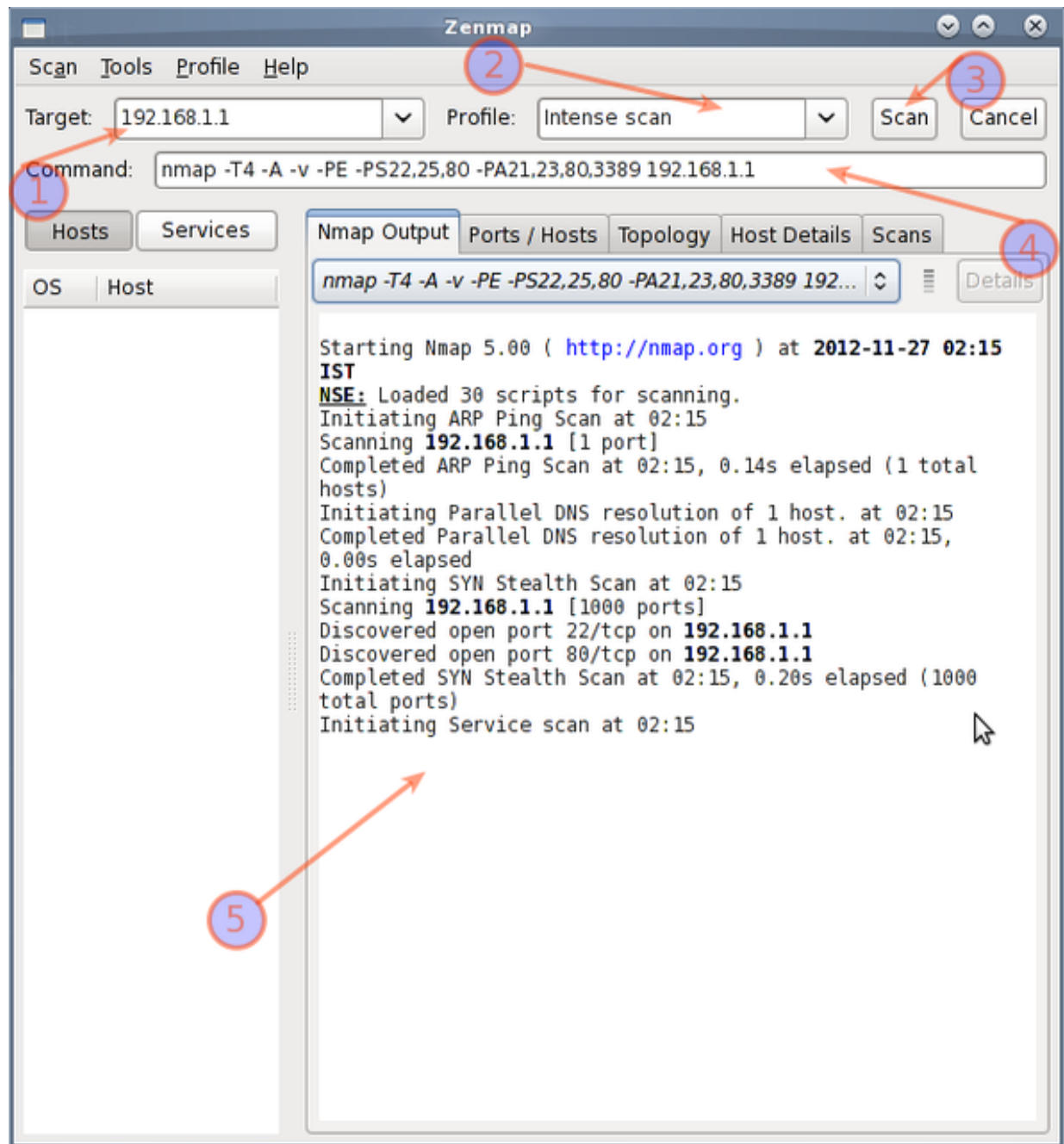


Fig.02: zenmap in action

## How do I detect and block port scanning?

Try the following resources:

1. [How to use psad tool to detect and block port scan attacks in real time.](#)
2. [Debian / Ubuntu Linux: Install and Configure Shoreline Firewall \(Shorewall\).](#)
3. [CentOS / Redhat Iptables Firewall Configuration Tutorial.](#)

4. [Linux: 20 Iptables Examples For New SysAdmins.](#)
5. [20 Linux Server Hardening Security Tips.](#)

#### References:

- [The official Nmap project guide to network discovery and security Scanning.](#)
- [The official Nmap project home page.](#)

*The nmap command has many more options, please go through man page or the documentation for more information. What are some of your favorite nmap command-line tricks? Share your favorite tips, tricks, and advice in the comments below.*

[Twitter](#)[Facebook](#)[Google+](#)[Download PDF version](#)[Found an error/typo on this page?](#)

#### More like this:

- [15 Greatest Open Source Terminal Applications Of 2012](#)
- [Linux ifdata Command: See Network Interface Info Without Parsing ifconfig...](#)
- [5 Linux / Unix Commands For Connecting To The Serial Console](#)
- [agedu: Unix / Linux Command For Tracking Down Wasted Disk Space](#)
- [Goldendict: A Feature-rich Dictionary Lookup Linux Program](#)
- [HowTo: Connect Two Wireless Router Wirelessly \( Bridge \) With Open Source...](#)
- [Collecting Ubuntu Linux System Information](#)
- [30 Cool Open Source Software I Discovered in 2013](#)
- [Amazon AWS Route 53 GEO DNS Configurations](#)
- [Testing HTTP Status: 206 Partial Content and Range Requests](#)





Tagged as: [Apple](#), [Debian Linux](#), [FreeBSD](#), [Linux](#), [Ubuntu](#), [Unix](#)

Comments on this entry are closed.

20 Comments

nixCraft Blog

1 Login ▾

♥ Recommend 81

🔗 Share

Sort by Best ▾



Join the discussion...

**Andrew** · 3 years ago

One of the uses for nmap, as stated above, is to "find out if the system is infected with malware or virus." How is this accomplished? Are you referring to using the script, http-malware-host?

15 ^ | ▾ · Reply · Share ›

**A white hatter** · 3 years ago

Several places mentioned the -PN switch, but this is depreciated, use -Pn instead. -Pn (No ping) .

This option skips the Nmap discovery stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host discovery with -Pn causes Nmap to attempt the requested scanning functions against every target IP address specified. So if a class B target address space (/16) is specified on the command line, all 65,536 IP addresses are scanned. Proper host discovery is skipped as with the list scan, but instead of stopping and printing the target list, Nmap continues to perform requested functions as if each target IP is active. To skip ping scan and port scan, while still allowing NSE to run, use the two options -Pn -sn together.

For machines on a local ethernet network, ARP scanning will still be performed (unless --send-ip is specified) because Nmap needs MAC addresses to further scan target hosts. In previous versions of Nmap, -Pn was -P0. and -PN..

11 ^ | ▾ · Reply · Share ›

**S Mohamed** · 3 years ago

My favorite nmap to scan for OS of a range of IPs, with output as a XML file:

```
nmap -A -T3 -oX MyFile.xml 192.168.56.101-120
```

(A: OS detection, version detection, script scanning, traceroute T3: Speed medium)

6 ^ | ▾ · Reply · Share ›

**Murphy Mason** · 2 years ago

very interreting

1 ^ | ▾ · Reply · Share ›



**Roy** · 3 years ago

I love namp. Great post Sir.

1 ^ | v · Reply · Share ›

**Felipe** · 3 years ago

Wow ! Pretty good and easy. Thank you so much for the great topic, I'm a huge fan of nmap/zenmap

1 ^ | v · Reply · Share ›

**P4** · a month ago

for blocking a portscan give portsentry a try :)

<https://plus.google.com/+Remik...>

^ | v · Reply · Share ›

**Bob Cynic** · a year ago

Beautifully formatted man page...thanks! ;)

^ | v · Reply · Share ›

**far** · a year ago

what does nmap -sn -PI 192.168.1.0/24 do?

^ | v · Reply · Share ›

**Scott** · a year ago

Anyone got any examples of using nmap to generate a RARP message?

^ | v · Reply · Share ›

**HD** · 2 years agoThe question is how to monitor people who use/run NMAP and create a report about it ...  
Thanks

^ | v · Reply · Share ›

**benhuan** · 2 years ago

Love it , Thanks for sharing

^ | v · Reply · Share ›

**s33d3r** · 2 years ago

Very Useful and Thanks for the information

^ | v · Reply · Share ›

**Ksdyathish** · 3 years ago

Very very useful and simple commands! Thank you.

^ | v · Reply · Share ›

^ | v · Reply · Share ›



**DUNGNA** · 3 years ago

Thanks you for sharing...!

^ | v · Reply · Share ›



**Chris** · 3 years ago

Thanks for this very usefull post!!

^ | v · Reply · Share ›



**Jalal Hajigholamali** · 3 years ago

Hi,

Very nice and useful article

Thanks again

^ | v · Reply · Share ›



**cycop** · 3 years ago

Nice Info,,,

^ | v · Reply · Share ›



**Nully man** → cycop · a year ago

hello pleas i have download nmap and install , but idnt know wher to even run it

^ | v · Reply · Share ›



**HoppingBunny** → Nully man · 9 months ago

If you are on a linux or similar system, it should be available on the command line like this:

```
sudo nmap -F www.gmail.com <== type this on the command line
```

you will get the output below:

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-05-13 23:18 EDT
```

```
Nmap scan report for www.gmail.com (216.58.219.197)
```

```
Host is up (0.010s latency).
```

```
rDNS record for 216.58.219.197: lga25s40-in-f5.1e100.net
```

```
Not shown: 98 filtered ports
```

```
PORT STATE SERVICE
```

```
80/tcp open http
```

```
443/tcp open https
```

^ | v · Reply · Share ›

## ALSO ON NIXCRAFT BLOG

## WHAT'S THIS?

## Learning bash scripting for beginners

9 comments • 8 months ago

**Dan okellz** — bookmarked.. i am always looking for sites that enable me to get this linux coding business in order

## How to paste password easily when pasting into password input fields

1 comment • 16 days ago

**soul\_rebel** — I have this script saved as pastekeypresses and bound to Ctrl-Shift-V:  
`#!/bin/sh sleep 2 exec xte "str $(xclip -o)" ...`

## 5 Awesome Open Source Cloning Software

17 comments • a year ago

**Tyler** — Cloning in the sense this article uses would exclude rsync; rsync doesn't clone a hard drive; rather, it copies filesystem ...

## Secure Your Linux Desktop and SSH Login Using Two Factor Google Authenticator

13 comments • a year ago

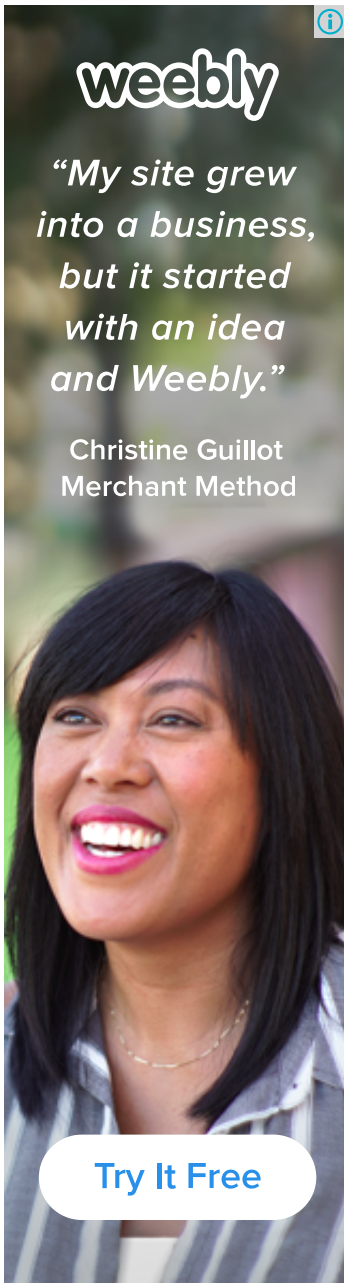
**Arkitech** — Awesome.

Next post: [Download Samba 4: Active Directory Compatible Server](#)

Previous post: [diff Command: Colorize Output On The Unix / Linux Command Line](#)



To search, type and hit enter

A vertical advertisement for Weebly. At the top is the Weebly logo in a white, rounded, lowercase font. Below it is a quote in a white, italicized serif font: "My site grew into a business, but it started with an idea and Weebly." Under the quote is the name "Christine Guillot" and her title "Merchant Method" in a white sans-serif font. The background of the ad is a photograph of Christine Guillot, a woman with dark hair and a bright smile, wearing a striped shirt. At the bottom of the ad is a white rounded rectangle with the text "Try It Free" in a blue sans-serif font. A small blue information icon is in the top right corner of the ad.

**weebly**

*"My site grew into a business, but it started with an idea and Weebly."*

Christine Guillot  
Merchant Method

**Try It Free**

## FEATURED ARTICLES:

30 Cool Open Source Software I Discovered in 2013

30 Handy Bash Shell Aliases For Linux / Unix / Mac OS X

Top 30 Nmap Command Examples For Sys/Network Admins

25 PHP Security Best Practices For Sys Admins

20 Linux System Monitoring Tools Every SysAdmin Should Know

20 Linux Server Hardening Security Tips

Linux: 20 Iptables Examples For New SysAdmins

## Top 20 Nginx WebServer Best Security Practices

## 15 Greatest Open Source Terminal Applications Of 2012

## My 10 UNIX Command Line Mistakes

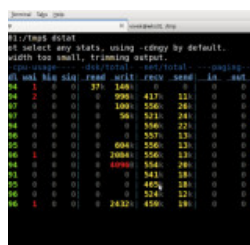
## Top 10 Open Source Web-Based Project Management Software

## Top 5 Email Client For Linux, Mac OS X, and Windows Users

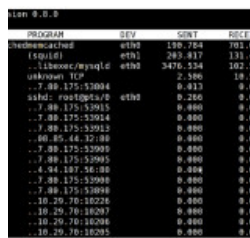
# The Novice Guide To Buying A Linux Laptop



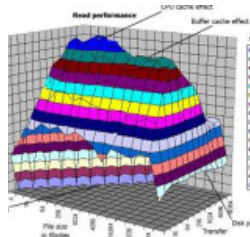
## ss: Display Linux TCP / UDP Network and Socket ...



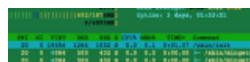
## dstat: Monitoring Linux Systems Performance ...



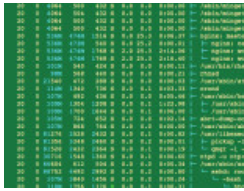
## Linux: See Bandwidth Usage Per Process With ...



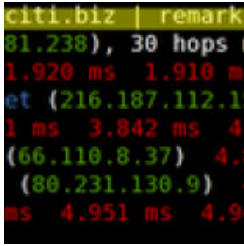
## How To Measure Linux Filesystem I/O



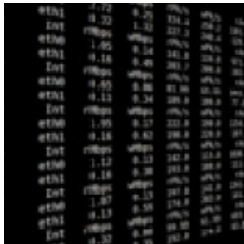
## How do I find out Linux Resource



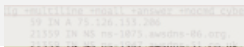
## Linux Resource utilization ...



## Linux / Unix: Highlight / colour traceroute ...



## Linux and Unix nload App: Monitor Network ...



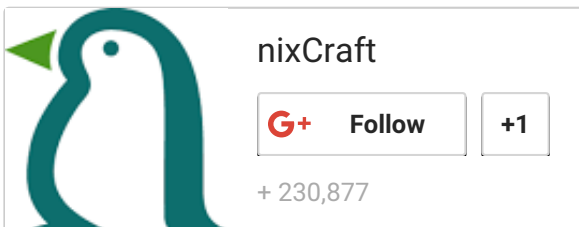
## Find the network

## DON'T MISS ANY LINUX TIPS

Get nixCraft in your inbox. It's free:



## FOLLOW US





---

©2000-2016 nixCraft. All rights reserved. [Privacy Policy](#) - [Terms of Service](#) - [Questions or Comments](#)  
The content is copyrighted to nixCraft and may not be reproduced on other websites.