



CEHv9 - Practice
Exam Questions



400+ Self-Practice Review
Questions with Answers

CLICK HERE

www.yeahhub.com



[Home](#)

[Tutorials](#) ▾

[CTF Challenges](#)

[Q&A](#) ▾

[Sitemap](#)

[Contact Us](#)



Search

TOP 10 NMAP COMMANDS

POWERED BY YEAHHUB.COM

RECENT ARTICLES

- » [10 Tips and Best Practices To Improve PHP Security](#)
- » [How to use Proxychains in Kali Linux OS](#)
- » [Tips to Hack Facebook without Hassle](#)

TECH ARTICLES

Top 10 NMAP Widely Used Commands

📅 June 11, 2019 👤 H4ck0 💬 Comment(0)

One may be curious to understand how the network intruder to know what ports are open on a computer? Or maybe how they detect which services are running in the system that too without any prior permission from the network administrator.

Well, anyone can do this stuff and even more than that with the help of Nmap tool which is one of the best Port Scanner used by many experts in network security, network researchers and administrators.

Suggested Read: [19 Useful NMAP Commands You Should Know](#)

There are plenty of scanning techniques that can be used in Nmap. This article is intended to provide a the basic overview on top 10 [Nmap scanning](#) techniques.

1. TCP Connect Scan (-sT)
2. TCP SYN Scan (-sS)
3. Version Detection (-sV)
4. UDP Scan (-sU)
5. OS Fingerprinting (-O)

- » [Bruteforce WordPress with XMLRPC Python Exploit](#)
- » [Top 10 Essential CTF Tools for Solving Reversing Challenges](#)
- » [How to turn on PowerShell Transcription Logging in Windows 10](#)
- » [Top 10 NMAP Widely Used Commands](#)
- » [Top 8 Basic Google Search Dorks \[Live Examples\]](#)
- » [Top 3 Open Source SSL Testing Tools](#)
- » [Overview of Mobile Learning Platforms](#)

**ADVANCED HACKING
TUTORIALS**

www.yeahhub.com

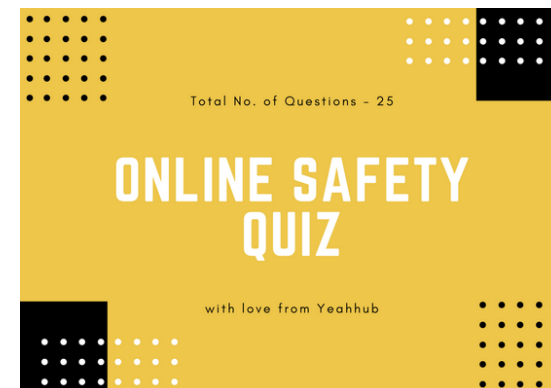
6. Scan OS Information (-A)
7. Scan Top Ports (-F)
8. Scan Targets from a File (-iL)
9. TCP ACK Scan (-sA)
10. Ping Scan (-sP)

[#1] – TCP Connect Port Scan

Syntax: nmap -sT <IP Address>

TCP connect scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks.

The TCP Connect Scan is a simple probe that attempts to directly connect to the remote system without using any stealth



is closed.

```
root@kali: ~  
File Edit View Search Terminal Help  
WEANNUB.COM  
root@kali:~# nmap -sS 10.228.13.224  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:21 IST  
Nmap scan report for 10.228.13.224  
Host is up (1.0s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql
```

[#3]- Version Scan

Syntax: nmap -sV <IP Address>

Version Detection collects information about the specific service running on an open port, including the product name and version number.

This information can be used in determining an entry point for an attack. The `-sV` option enables version detection, and the `-A` option enables both OS fingerprinting and version detection

```
root@kali: ~  
File Edit View Search Terminal Help  
Nmap  
root@kali:~# nmap -sV 10.228.13.224  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:22 IST  
Nmap scan report for 10.228.13.224  
Host is up (1.0s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rshcd  
513/tcp   open  login?  
514/tcp   open  shell        Netapp ONTAP rshd  
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)
```

[#4] – UDP Port Scan

Syntax: nmap -sU <IP Address>

UDP scan works by sending a UDP packet to the targeted port. If no response is received, then the port will be considered as Open | filtered.

Filtered because some firewalls won't respond to the blocked UDP ports. If the port is closed, then an ICMP response (ICMP port unreachable error type 3, code 3) will be sent by the target device.

```
root@kali: ~  
File Edit View Search Terminal Help  
WEATHER.COM  
root@kali:~# nmap -sU 10.228.13.224  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:22 IST  
Nmap scan report for 10.228.13.224  
Host is up (0.00049s latency).  
Not shown: 996 open|filtered ports  
PORT      STATE SERVICE  
53/udp    open  domain  
111/udp   open  rpcbind  
137/udp   open  netbios-ns  
2049/udp  open  nfs  
  
Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds  
root@kali:~#
```

[#5] – OS Fingerprinting

Syntax: nmap -O <IP Address>

With -O (Capital O) or --osscan-guess, you can easily detect the target Operating System behind it using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines the responses. After performing dozens of tests, Nmap compares the results to its database and prints out the OS details if there is a match.

[#6] – Scan OS Information

Syntax: nmap -A <IP Address>

With Nmap, you can detect which OS and version is running on the remote host. To enable OS & version detection, script scanning and traceroute, you can use “-A” option with NMAP.

This type of scan uses the ACK flags. Unlike other scans, ACK scan is not used to determine whether the port is Open or Closed.

It is used to map out firewall rule-sets, determining whether they are stateful or not and which ports are filtered. Stateful Firewalls, will respond with a RST packet as the sequence is not in order.


```
root@kali: ~  
File Edit View Search Terminal Help  
WEAIB.COM  
root@kali:~# nmap -F 10.228.13.224  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:28 IST  
Nmap scan report for 10.228.13.224  
Host is up (1.0s latency).  
Not shown: 82 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
513/tcp   open  login  
514/tcp   open  shell  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
8009/tcp  open  ajp13  
Nmap done: 1 IP address (1 host up) scanned in 3.30 seconds
```

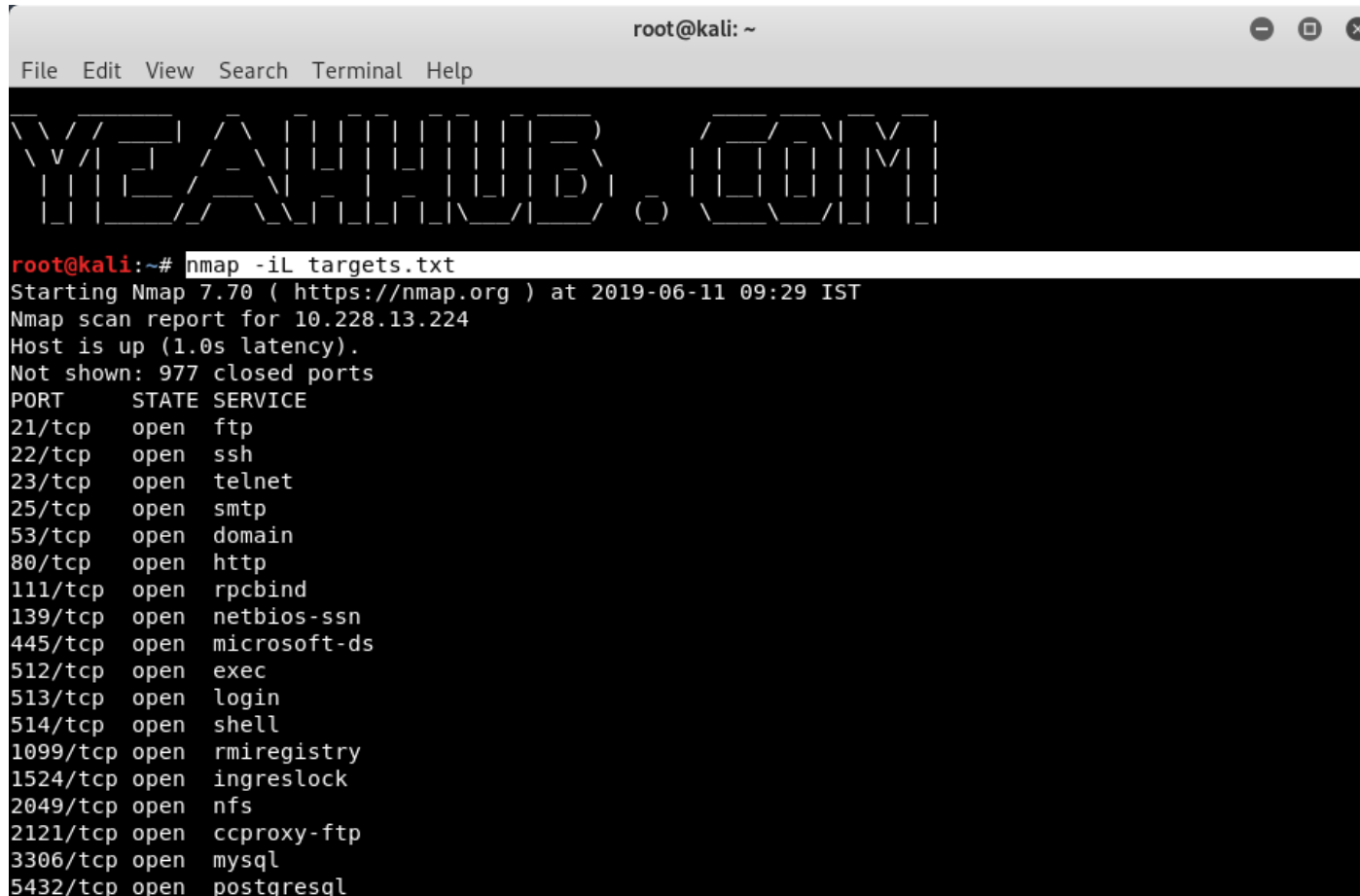
Using “**–top-ports**” parameter along with a specific number also lets you scan the top X most common ports for that host.

Example: `nmap –top-ports 20 10.228.13.224`

[#8] – Scan Targets from a File

Syntax: `nmap -iL targets.txt`

In this case, Nmap is also useful to read files that contain hosts and IP addresses inside.



```
root@kali: ~
File Edit View Search Terminal Help

WYGAHUB.COM

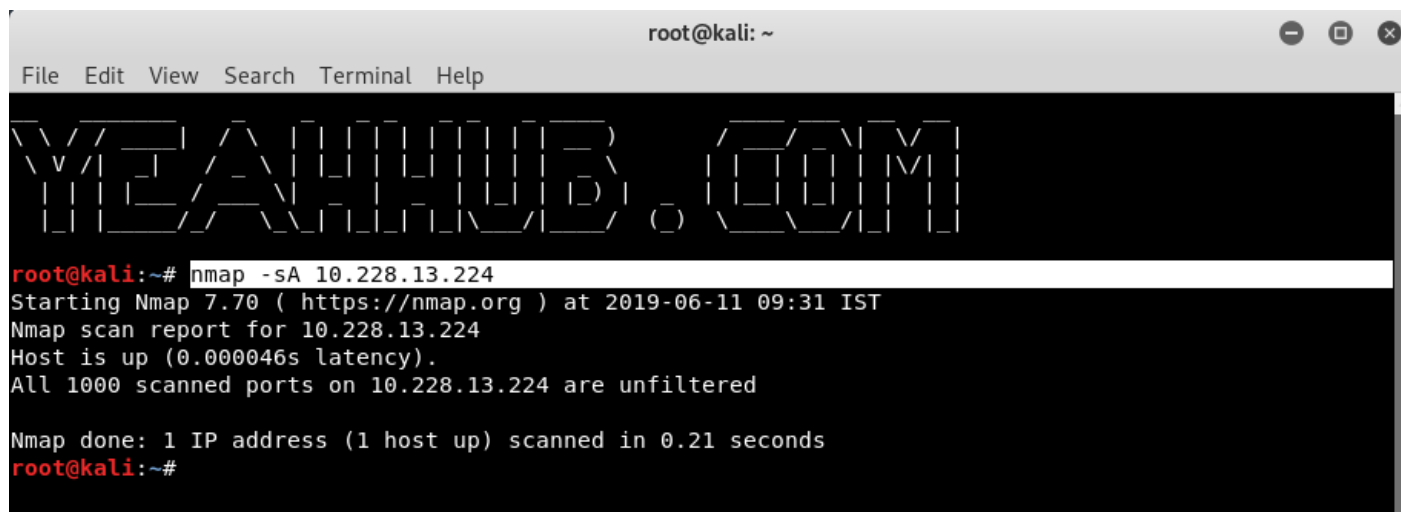
root@kali:~# nmap -iL targets.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:29 IST
Nmap scan report for 10.228.13.224
Host is up (1.0s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

[#9] – TCP ACK Port Scan

Syntax: nmap -sA <IP Address>

This type of scan uses the ACK flags. Unlike other scans, ACK scan is not used to determine whether the port is Open or Closed.

It is used to map out firewall rule-sets, determining whether they are stateful or not and which ports are filtered. Stateful Firewalls, will respond with a RST packet as the sequence is not in order.

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'nmap -sA 10.228.13.224' being executed. The output indicates that the host is up and all 1000 scanned ports are unfiltered. The terminal also displays a large ASCII art logo for 'VEANIMUS.COM' at the top.

```
root@kali: ~  
File Edit View Search Terminal Help  
VEANIMUS.COM  
root@kali:~# nmap -sA 10.228.13.224  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:31 IST  
Nmap scan report for 10.228.13.224  
Host is up (0.000046s latency).  
All 1000 scanned ports on 10.228.13.224 are unfiltered  
  
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds  
root@kali:~#
```

[#10] – Ping Scan

Syntax: nmap -sP <IP Address>

This types of scan is used to detect which computers or devices are online, rather than which ports are open.

In this, Nmap sends an ICMP ECHO REQUEST packet to the destination system. If an ICMP ECHO REPLY is received, the system is considered as up, and ICMP packets are not blocked.

If there is no response to the ICMP ping request, Nmap will try a "TCP Ping", to determine whether ICMP is blocked, or if the host is really not online.

```
root@kali: ~
File Edit View Search Terminal Help

WEAHHUB.COM

root@kali:~# nmap -sP 10.228.13.224
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-11 09:31 IST
Nmap scan report for 10.228.13.224
Host is up (0.00046s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
root@kali:~#
```



Have something to say about this article? Comment below or share it with us on [Facebook](#) or [Twitter](#).

Tagged Best Nmap Books, Commands Nmap, Nmap All Commands, Nmap Amazon Books, Nmap Articles, Nmap Basic Commands, Nmap books, Nmap Bugbounty, Nmap Command Examples, Nmap Commands, Nmap Commands 2019, Nmap Commands Useful, Nmap download, Nmap Download Books, Nmap Examples, Nmap Fingerprinting, Nmap Free Books, Nmap Hacking, Nmap Host Commands, Nmap Host Discovery, Nmap Kali Linux, Nmap Pentesting, Nmap Port Scanner, Nmap Port Scanning, Nmap Security, Nmap Service Scan, Nmap Tutorial, Nmap Useful Commands, Nmap Version Detection, nmap widely used commands, Nmap yeahhub, Top Nmap Books, Top Nmap Commands



H4ck0

Step by step hacking tutorials about wireless cracking, kali linux, metasploit, ethical hacking, seo tips and tricks, malware analysis and scanning.

<https://www.yeahhub.com/>

WHERE SHOULD WE SEND ?

HACKING TUTORIALS & INFOSEC NEWS?

Subscribe to Our Newsletter and Get Instant Delivered to Your Email Inbox.

Enter your first name

Enter your email here

Subscribe Now

We respect your privacy and take protecting it seriously.

RELATED ARTICLES



TECH ARTICLES

5 Most Commonly Used Nmap Commands

September 19, 2018 H4ck0

◀ Top 8 Basic Google S...



TECH ARTICLES

Nmap gets a new look and feel with NMapGUI

October 23, 2017 H4ck0



TECH ARTICLES

Top 30 Basic NMAP Commands for Beginners

November 6, 2018 H4ck0

How to turn on Power...

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Please enter an
answer in digits:

19 + sixteen =

Post Comment

DISCLAIMER

Yeahhub.com does not represent or endorse the accuracy or reliability of any information's, content or advertisements contained on,

RECENT COMMENTS

LATEST ARTICLES

- » 10 Tips and Best Practices To Improve PHP Security
July 17, 2019

distributed through, or linked, downloaded or accessed from any of the services contained on this website, nor the quality of any products, information's or any other material displayed, purchased, or obtained by you as a result of an advertisement or any other information's or offer in or in connection with the services herein.

💬 Cortez on [Persistent Backdoor in Android using Kali Linux with a Shell script](#)

💬 yr ho on [How to Download Wistia Videos without any Tool](#)

💬 Jimmy Johns Jarner on [How to Download Wistia Videos without any Tool](#)

💬 Wangolo Joel on [Subdomain Enumeration Tools – 2019 Update](#)

» [How to use Proxychains in Kali Linux OS](#)
July 9, 2019

» [Tips to Hack Facebook without Hassle](#)
June 25, 2019

» [Bruteforce WordPress with XMLRPC Python Exploit](#)
June 17, 2019

» [Top 10 Essential CTF Tools for Solving Reversing Challenges](#)
June 16, 2019

Copyright © 2019 | Developed & Maintained by [Mohali VA/PT Team](#)

[Write for us](#) | [Advertise](#) | [Privacy Policy](#) | [Terms of use](#) | [Cookie Policy](#) | [Disclaimer](#) | [Report a bug](#)