
TOPICS

CERTIFICATIONS

EVENTS

CAREERS

CONTRIBUTORS

ABOUT INFOSEC

Nmap from Beginner [Updated 2019]

POSTED IN HACKING ON FEBRUARY 3, 2019



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[CONTRIBUTORS](#)[ABOUT INFOSEC](#)

Learn how to use Nmap

INFOSEC Skills

Gain practical experience and build your real-world pentesting skills. This [skills course](#) covers

- ⇒ Port and protocols
- ⇒ Advanced scanning
- ⇒ And more

Start your

Network Mapper (Nmap) is a network scanning tool used during several steps of penetration testing. Nmap provides information and enumeration, but it is also powerful as a host detector or a security scanner. So Nmap is a multiplatform utility that can be used to:

- Detect the live host on the network (host discovery)
- Detect the open ports on the host (port discovery)
- Detect the software and the version to the remote host
- Detect the operating system, hardware address
- Detect the vulnerability and security holes (Nmap Scripting Engine)

Nmap is a very common tool, and it is available in a graphical user interface. The objective of this article is to provide you with the necessary information about Nmap and its usage. In this piece I'll go over:

INFOSEC Skills

Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

-
- Introduction to operating system detection

TOPICS • [Nmap tutorial](#) CERTIFICATIONS EVENTS CAREERS CONTRIBUTORS

ABOUT INFOSEC

How to use Nmap? You might have heard this question many times before, but in my opinion, this is not the right question to ask. The best way to start off exploring Nmap is to ask: How can I use Nmap effectively? This article was written in an effort to answer that question.

Nmap uses different techniques to perform scanning including: TCP connect() scanning, TCP reverse ident scanning, FTP bounce scanning and so on. All these types of scanning have their own advantages and disadvantages, and we will discuss them as we go on.

How to Use Nmap Effectiv

The usage of Nmap depends on the target mac simple (basic) scanning and advance scanning. to bypass the firewall and intrusion detection/pr Below are the examples of some basic commar

If you want to scan a single system, then you ca

nmap target

nmap target.com

nmap 192.168.1.1

If you want to scan the entire subnet, then the c

nmap target/cdir

nmap 192.168.1.1/24

It is very easy to scan a multiple targets, all you space:

nmap target target1 target2

nmap 192.168.1.1 192.168.1.8

Let's suppose you want to scan a range of IP ar



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

TOPICS **# nmap 192.168.1.1/24** CERTIFICATIONS EVENTS CAREERS CONTRIBUTORS

ABOUT INFOSEC

Let suppose you have a list of a target machines. You can make Nmap scan for the entire list:

nmap -iL target.txt Make sure to put the file on the same directory

If you want to see the list of all the hosts that you are scanning, then use the command with an -sL parameter:

nmap -sL target/cdir

nmap -sL 192.168.1.1/24

In some cases we need to scan the entire subn might be dangerous for us. In this scenario, use parameter:

nmap 192.168.1.1/24 --exclude 192.168.1.1

If you have a file that contains the list of IP addr call the file in the exclude parameter:

nmap 192.168.1.1/24 --exclude file target.tx

If you want to scan a specific port on the target the HTTP, FTP, and Telnet port only on the targ command with the relevant parameter:

nmap -p80,21,23 192.168.1.1 It scan the tar

```
root@bt:~# nmap -p80,21,23 192.168.1.1
Starting Nmap 5.51 ( http://nmap.org )
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:22:93:CF:EB:6D

Nmap done: 1 IP address (1 host) scanned in 0.01 seconds
```



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

article, we need to explore more in depth.

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[CONTRIBUTORS](#)

Nmap Scanning Techniques

There are so many scanning techniques available on Nmap, including the TCP connect scanning method discussed earlier, so in this section, I will discuss the most popular scanning technique in detail.

TCP SYN Scan (-sS)

It is a basic scan, and it is also called half-open Nmap to get information from the remote host via Nmap sends SYN packets to the destination, but the target computer can't create any log of the IP making this feature an advantage of the TCP SYN scan.

If there is no scan type mentioned on the command default, but it requires the root/administrator privileges.

```
# nmap -sS 192.168.1.1
```

TCP connect() scan (-sT)

This is the default scanning technique used, if any because the SYN scan requires root privilege. It is a normal TCP three-way handshake process and a part of the operating system. Keep in mind that it scans the TCP ports, not the UDP ports.

```
# nmap -sT 192.168.1.1
```

UDP Scan (-sU)

As the name suggests, this technique is used to scan UDP ports.



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

[Get started today](#)[No thanks](#)

UDP packets to the target machine, and waits for a response—if an error message arrives saying the port is unreachable, then it means that the port is closed, but if it gets an appropriate response, then it means that the port is open.

```
# nmap -sU 192.168.1.1
```

FIN Scan (-sF)

Sometimes a normal TCP SYN scan is not the best solution because of the firewall. IDS and IPS scans might be deployed on the target machine, but a firewall will usually block the SYN packets. A FIN scan sends the packet only set to complete the TCP handshaking.

```
root@bt:~# nmap -sF 192.168.1.8
```

Starting Nmap 5.51 (<http://nmap.org>) at 2012-11-01 11:00:00

Nmap scan report for 192.168.1.8

Host is up (0.000026s latency).

Not shown: 999 closed ports

PORT STATE SERVICE

111/tcp open|filtered rpcbind

The target computer is not able to create a log file. Like a FIN scan, we can perform an xmas scan (XMAS) but there is a difference between each type of scan. In a FIN scan, the packet contains only the FIN flag, whereas in an xmas scan, the packet contains the FIN, PSH, and URG flags.

Ping Scan (-sP)



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

ICMP packets can be sent, but if the user does not have administrator privilege, then the ping

TOPICS [Scan uses connect\(\) call](#)

[EVENTS](#)

[CAREERS](#)

[CONTRIBUTORS](#)

ABOUT INFOSEC

nmap -sP 192.168.1.1

Version Detection (-sV)

Version detection is the right technique that is used to find out what software version is running on the target computer and on the respective ports. It is unlike the other scanning techniques because it is not used to detect the open ports, but it requires the information from open ports to detect the software version. In the detection uses the TCP SYN scan to find out w

nmap -sV 192.168.1.1

Idle Scan (-sI)

Idle scan is one of my favorite techniques, and i anonymity while scanning. In idle scan, Nmap d address—instead of generating the packets for host from the target network to send the packet the concept of idle scan:

nmap -sI zombie_host target_host

nmap -sI 192.168.1.6 192.168.1.1

The idle scan technique (as mentioned above) i 192.168.1.1 while it uses the zombie_host (192 So this is an ideal technique to scan a target co

There are many other scanning techniques are scan, IP protocol scan. and so on; but we have techniques (although all of the scanning technic you are dealing with).

In the next section of this article, I will discuss N discovery techniques.



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

One of the most important feature that Nmap has is the ability to detect remote operating systems and software. It is very helpful during a penetration test to know about the operating system and the software used by the remote computer because you can easily predict the known vulnerabilities from this information.

Nmap has a database called *nmap-os-db*, the database contains information of more than 2,600 operating systems. Nmap sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The Nmap operating system discovery technique is slightly slower then the scanning techniques because OS detection involves the process of finding open ports.

Initiating SYN Stealth Scan at 10:21

Scanning localhost (127.0.0.1) [1000 ports]

Discovered open port 111/tcp on 127.0.0.1

Completed SYN Stealth Scan at 10:21, 0.08s el

Initiating OS detection (try #1) against localhost

Retrying OS detection (try #2) against localhost

The example above clearly demonstrates that tl sends the packets to discover the remote opera -O (capital O).

```
root@bt:~# nmap -O 192.168.1.2
Starting Nmap 5.51 ( http://nmap.
Nmap scan report for 192.168.1.2
Host is up (0.000073s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp    open  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 0 hops
```

Nmap OS fingerprinting technique discovers the

- Device type (router, work station, and so on)
- Running (running operating system)
- OS details (the name and the version of OS)
- Network distance (the distance in hops betw



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

tells Nmap not to ping the remote computer, since sometimes firewalls block the request.

TOPICS CERTIFICATIONS EVENTS CAREERS CONTRIBUTORS
nmap -O -PN 192.168.1.1/24

ABOUT INFOSEC

The command informs the sender every host on the network is alive so there is no need to send a ping request as well. In short, it bypasses the ping request and goes on to discover the operating system.

The Nmap OS detection technique works on the basis of an open and closed port. If Nmap fails to discover the open and closed port, then it gives the error:

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

```
root@bt:~# nmap -O 192.168.1.1
Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:22:93:CF:EB:6D (ZTE)
Warning: OSScan results may be unreliable because we
```

This is an undesirable situation, and it is good to not be sure about the OS. If Nmap is not sure about the OS, it gives the warning using **--osscan_limit**.

```
root@bt:~# nmap -O --osscan_limit 192.168.1.1
Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15
Nmap scan report for 192.168.1.1
Host is up (0.00072s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:22:93:CF:EB:6D (ZTE)
OS detection performed. Please report any incorrect results.
Nmap done: 1 IP address (1 host up) scanned in 5.00s
```

If it is very difficult for Nmap to detect the remote OS, then Nmap's guess feature, **--osscan-guess** finds the OS of the remote system.

nmap -O --osscan-guess 192.168.1.1



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[CONTRIBUTORS](#)[ABOUT INFOSEC](#)

Earn your CEH, guaranteed!

Complete the form below to receive course pricing.

*

*

*

*

[VIEW SPECIAL OFFER](#)

Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Conclusion

Nmap is a very powerful tool and it has ability to do a lot of things, which include information gathering and reconnaissance, and effort to discuss Nmap from the beginner level to the advanced level and other things that you can do with the Nmap, and

[Get started today](#)[No thanks](#)

TOPICS Want more? Check out this article about Nmap. CERTIFICATIONS EVENTS CAREERS CONTRIBUTORS

ABOUT INFOSEC

[Nmap Evade Firewall & Scripting \[Updated 2018\]](#)

Tweet



AUTHOR

Irfan
Shakeel

Irfan Shak
engineer,
specialize
forensics.
Scratch". I
and workii



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[CONTRIBUTORS](#)
Keeping your cybersecurity skills
relevant in 2019[ABOUT INFOSEC](#)[Top 50 Network Administrator
Interview Questions \[Updated for
2019\]](#)[CISSP Certification – The Ultimate
Guide](#)[AWS Security Monitoring Checklist
\[Updated 2019\]](#)

Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

[Get started today](#)[No thanks](#)

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[Information Security
CONTRIBUTORS](#)[Security Awareness](#)[DoD 8140](#)[Ethical Hacking](#)[Hacker Training Online](#)[Security+](#)[Computer Forensics](#)[ABOUT INFOSEC](#)

Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

[Get started today](#)[No thanks](#)

[TOPICS](#)[CERTIFICATIONS](#)[EVENTS](#)[CAREERS](#)[CONTRIBUTORS](#)[ABOUT INFOSEC](#)

AWS Security Monitoring Checklist [Updated 2019]



Anonymization and pseudonymization of personal data



Cybersecurity engineer resume tips



9 responses to "Nmap from Beginner to Advanc



a says:

[July 18, 2012 at 3:52 pm](#)

something about filter evasion?

[Reply](#)



[being john detroit](#) says:

[July 19, 2012 at 1:36 am](#)

It's "cldr", not "cdlr".

[Reply](#)



andrew new zealand says:

[July 21, 2012 at 9:13 pm](#)

Nice intuitive post – I agree with a, a filter evasic types of scans would be ideal.

[Reply](#)



[Irfan Shakeel](#) says:

[July 23, 2012 at 12:26 pm](#)

Thank you very much for a such a valuable sug; about it.

[Reply](#)



[Irfan Shakeel](#) says:

[July 23, 2012 at 12:26 pm](#)



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks

marco rovari says:

[August 2, 2012 at 11:58 pm](#)

[Congrats!](#)

[Records](#)

[ABOUT INFOSEC](#)

[Reply](#)



DLS says:

[March 25, 2014 at 4:13 am](#)

plz tell me command for this one

"enter the command below to conduct a TCP Connect Scan on 192.168.1.6"

[Reply](#)



Atif says:

[May 7, 2014 at 2:16 pm](#)

hi admin ,, hope u will be fine,,

i want to ask u something...

can we attack some ope ports of target pc throu

case?

[Reply](#)



MohdAqeelasif says:

[June 2, 2015 at 7:40 am](#)

We always suggest not to leave open ports unno

what if at the time of assessment we could find :

can be performed on that port. what is the risk in

[Reply](#)

Leave a Reply

Your email address will not be published. Requ

Comment

Name *

Email *

Website

Save my name, email, and website in this brow

seven ×



=



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

[Get started today](#)

[No thanks](#)

[About Infosec](#)

[Connec](#)

fight against cybercrime. We

provide the best certification and

skills development training for IT

and security professionals, as well

as employee security awareness

training and phishing simulations.

Learn more at

infosecinstitute.com.

Follow @infosecedu

CAREERS

CONTRIBUTORS ENTER YOUR

SUBS

✕ 9



Free Infosec Skills subscription

- 400+ courses
- 50+ learning paths
- 100+ hands-on labs
- Certification practice exams

Get started today

No thanks