Nmap from Beginner to Advanced

POSTED IN HACKING ON JULY 18, 2012

SHARE

Ethical Hacking Boot Camp

OUR MOST POPULAR COURSE!

CLICK HERE!

What's this?

Network Security Networking

Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac. Nmap is a very powerful utility that can be used to:

- Detect the live host on the network (host discovery)
- Detect the open ports on the host (port discovery or enumeration)
- Detect the software and the version to the respective port (service discovery)
- Detect the operating system, hardware address, and the software version
- Detect the vulnerability and security holes (Nmap scripts)

ETHICAL HACKING BOOT CAMP

threats to information assets; and discover where your organization is most vulnerable to black hat hackers. Some features of this course include:

- Dual Certification - CEH and CPT
- 5 days of Intensive Hands-On Labs
- CTF exercises in the evening

FIRST NAME *

LAST NAME *

COMPANY

EMAIL *

PHONE *

JOB TITLE *

WHO WILL FUND YOUR TRAINING? *

FIND PRICING FOR THIS COURSE

Nmap is a very common tool, and it is available for both the command line interface and the graphical user interface. The objective of this article is to create a handbook that contains all of the necessary information about Nmap and its usage. To provide an overview of the article, in this piece I'll go over:

- Introduction to Nmap
- What are the important parameters and techniques of scanning
- Introduction to operating system detection
- Nmap tutorial

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.

types of scanning have their own advantages and disadvantages, and we will discuss them as we go on.

How to Use Nmap Effectively

The usage of Nmap depends on the target machine because there is a difference between simple (basic) scanning and advance scanning. We need to use some advanced techniques to bypass the firewall and intrusion detection/preventative software to get the right result. Below are the examples of some basic commands and their usage:

If you want to scan a single system, then you can use a simple command

nmap target

 # nmap target.com

 # nmap 192.168.1.1

If you want to scan the entire subnet, then the command is

nmap target/cdir

 # nmap 192.168.1.1/24

It is very easy to scan a multiple targets, all you need to do is to separate each target via 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 addresses, but not the entire subnet. In this scenario, use this command:

nmap target-100

 # nmap 192.168.1.1-100

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

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 subnet but not a specific IP addresses because it might be dangerous for us. In this scenario, use the Nmap command with the excluding parameter:

 # nmap 192.168.1.1/24 – -exclude 192.168.1.1

If you have a file that contains the list of IP addresses that you want to exclude, then you can call the file in the exclude parameter:

 # nmap 192.168.1.1/24 –exclude file target.txt

If you want to scan a specific port on the target machines (for example, if you want to scan the HTTP, FTP, and Telnet port only on the target computer), then you can use the Nmap command with the relevant parameter:

 # nmap -p80,21,23 192.168.1.1 It scan the target for port number 80,21 and 23.

```
root@bt:~# nmap -p80,21,23 192.168.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-08 17:18 PKT
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 (ZTE)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

You now have a basic understanding of Nmap scanning techniques, but for the purposes of this article, we need to explore more in depth.

Nmap Scanning Techniques

popular scanning technique in detail.

TCP SYN Scan (-sS)

It is a basic scan, and it is also called half-open scanning because this technique allows Nmap to get information from the remote host without the complete TCP handshake process, Nmap sends SYN packets to the destination, but it does not create any sessions, As a result, the target computer can't create any log of the interaction because no session was initiated, making this feature an advantage of the TCP SYN scan.

If there is no scan type mentioned on the command, then avTCP SYN scan is used by default, but it requires the root/administrator privileged.

 # nmap -sS 192.168.1.1

TCP connect() scan (-sT)

This the default scanning technique used, if and only if the SYN scan is not an option, because the SYN scan requires root privilege. Unlike the TCP SYN scan, it completes the normal TCP three way handshake process and requires the system to call connect(), which is a part of the operating system. Keep in mind that this technique is only applicable to find out 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 find an open UDP port of the target machine. It does not require any SYN packet to be sent because it is targeting the UDP ports. But we can make the scanning more effective by using -sS along with –sU. UDP scans send the UDP packets to the target machine, and waits for a response—if an error message arrives saying the ICMP 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

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 with a FIN flag, so it is not required to complete the TCP handshaking.

root@bt:~# nmap -sF 192.168.1.8

Starting Nmap 5.51 (http://nmap.org) at 2012-07-08 19:21 PKT

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 of this scan (again, an advantage of FIN). Just like a FIN scan, we can perform an xmas scan (-sX) and Null scan (-sN). The idea is same but there is a difference between each type of scan. For example, the FIN scan sends the packets containing only the FIN flag, where as the Null scan does not send any bit on the packet, and the xmas sends FIN, PSH, and URG flags.

ETHICAL HACKING TRAINING

threats to information assets; and discover where your organization is most vulnerable to black hat hackers. Some features of this course include:

- Dual Certification - CEH and CPT
- 5 days of Intensive Hands-On Labs
- CTF exercises in the evening

FIRST NAME *

LAST NAME *

COMPANY

EMAIL *

PHONE *

JOB TITLE *

WHO WILL FUND YOUR TRAINING? *

Ping Scan (-sP)

Ping scanning is unlike the other scan techniques because it is only used to find out whether the host is alive or not, it is not used to discover open ports. Ping scans require root access s ICMP packets can be sent, but if the user does not have administrator privilege, then the ping scan uses connect() call.

 # 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 first step of this scan technique, version detection uses the TCP SYN scan to find out which ports are open.

 # nmap -sV 192.168.1.1

complete anonymity while scanning. In idle scan, Nmap doesn't send the packets from your real IP address—instead of generating the packets from the attacker machine, Nmap uses another host from the target network to send the packets. Let's consider an example to understand 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) is used to discover the open ports on 192.168.1.1 while it uses the zombie_host (192.168.1.6) to communicate with the target host. So this is an ideal technique to scan a target computer anonymously.

There are many other scanning techniques are available like FTP bounce, fragmentation scan, IP protocol scan. and so on; but we have discussed the most important scanning techniques (although all of the scanning techniques can important depending on the situation you are dealing with).

In the next section of this article, I will discuss Nmap's operating system (OS) detection and discovery techniques.

OS Detection Nmap

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]

Initiating OS detection (try #1) against localhost (127.0.0.1)

Retrying OS detection (try #2) against localhost (127.0.0.1)

The example above clearly demonstrates that the Nmap first discovers the open ports, then it sends the packets to discover the remote operating system. The OS detection parameter is *-O* (capital O).

```
root@bt:~# nmap -O 192.168.1.2

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15 10:25 PKT
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 between the target and attacker)

Suppose that the target machine has a firewall, IDS, and IPS all enabled. You can use the command ***-PN*** to ensure that you do not ping to find the remote operating system. The -PN tells Nmap not to ping the remote computer, since sometimes firewalls block the request.

 # nmap -O -PN 192.168.1.1/24

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:

```
root@bt:~# nmap -O 192.168.1.1
Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15 10:48 PKT
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 could not find at least 1 open and 1 closed port
```

This is an undesirable situation, and it is good to limit the operating system scans if Nmap is not sure about the OS. If Nmap is not sure about the OS, then there is no need to detect by using –***osscan_limit.***

```
root@bt:~# nmap -O --osscan_limit 192.168.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2012-07-15 10:48 PKT
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 at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.62 seconds
```

If it is very difficult for Nmap to detect the remote OS accurately, you have the option of using Nmap's guess feature:, ***–osscan-guess*** finds the nearest match of the target operating system.

 # nmap -O --osscan-guess 192.168.1.1

Conclusion

Nmap is a very powerful tool and it has ability to cover the very first aspects of penetration testing, which include information gathering and enumeration. This article was written in an effort to discuss Nmap from the beginner level to the advanced level. There are so many other things that you can do with the Nmap, and we will discuss them in the future articles.

INTERESTED IN LEARNING MORE? CHECK OUT OUR ETHICAL HACKING TRAINING

Instructions:

1. **Complete the form below** or call **Toll Free at 1-866-471-0059, Ext. 1.**
2. Click the "Click Here to Display Pricing Below" button, and view current course pricing **instantly** in your broswer!
3. Rest assured your contact information will **NEVER** be used for **spam** or **annoying high pressure sales pitches**

First Name

Sources & Citations:

http://darksidegeeks.com/everything-you-need-to-know-about-nmap/#more-672

165 Tweet 11 G+ Share 18 Share submit reddit 89 Like

AUTHOR
Irfan Shakeel

Irfan Shakeel is the founder & CEO of ehacking.net An engineer, penetration tester and a security researcher. He specializes in Network, VoIP Penetration testing and digital forensics. He is the author of the book title "Hacking from Scratch". He loves to provide training and consultancy services, and working as an independent security researcher.

FREE PRACTICE EXAMS

CCNA Practice Exam

Network + Practice Exam

CEH Practice Exam

CISSP Practice Exam

EDITORS CHOICE

Exploiting Corporate Printers

General HTML5 Security

Web Vulnerabilities Explained eBook

RELATED BOOT CAMPS

Information Security

CCNA

PMP

Microsoft

Incident Response

Information Assurance

8570

MORE POSTS BY AUTHOR

Introduction to Computer Forensics & Digital Investigation

MetaData and Information Security

Exploiting Corporate Printers

General HTML5 Security

Web Vulnerabilities Explained eBook

Crowdsourcing Cybersecurity: How to Raise Security...

Join the discussion…

Ciph3r00t • 4 months ago
We always suggest not to leave open ports unnecessarily.....
what if at the time of assessment we could find a random port (say, 9845) is open. what attacks can be performed on that port. what is the risk in leaving it open.
Reply • Share ›

Atif • a year ago
hi admin ,, hope u will be fine,,
i want to ask u something...
can we attack some ope ports of target pc through Nmap? if yes how nmap can help us in this case?
Reply • Share ›

DLS • a year ago
plz tell me command for this one
"enter the command below to conduct a TCP Connect Scan on 192.168.1.6"
Reply • Share ›

Marco Rovari • 3 years ago
Good Job Shakeel.
Congrats!
BRegards.

Rovari
Reply • Share ›

Irfan Shakeel • 3 years ago
@being john detroit: typos thanks for the correction.
Reply • Share ›

Irfan Shakeel • 3 years ago
Thank you very much for a such a valuable suggestions, the next article of this series will discuss about it.
Reply • Share ›

andrew new zealand • 3 years ago
Nice intuitive post - I agree with a, a filter evasion topic and a post dedicated to some of the other types of scans would be ideal.

INFOSEC INSTITUTE

TOPICS CONTRIBUTORS CONTENT ARCHIVES JOB BOARD CAREERS PHISH.IO

About InfoSec

InfoSec Institute is the best source for high quality information security training. We have been training Information Security and IT Professionals since 1998 with a diverse lineup of relevant training courses. In the past 16 years, over 50,000 individuals have trusted InfoSec Institute for their professional development needs!

Connect with us

Stay up to date with InfoSec Institute and Intense School - at info@infosecinstitute.com

Like 489

Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YOUR SUBSCRIBE

© INFOSEC RESOURCES 2015