Penetration Testing for Beginners: Nmap

Anuraag Baishya Follow
Jun 27, 2016 · 5 min read

If you want to be a hacker or have interest in the field of Network Security, you might have come across the term 'Penetration Testing'. Broadly speaking penetration testing is one of the many specializations in the field of hacking.

What is Penetration Testing?

Penetration testing involves attacking your own or your client's network in the manner a hacker would. Also referred to as pen testing or security testing, Penetration Testing is primarily done to find security vulnerabilities in a network that may be exploited by hackers.

To be a penetration tester, it is very important to have a good understanding of networking protocols such as tcp, udp, etc., and their working

Penetration Testing is hacking. It is very important to ensure that you have the necessary permission to perform the testing. Else you would be labelled a cyber criminal and probably face legal actions.

. . .

To perform Penetration Testing, you'll need to know which ports are open and what services a system is running. You can always ask the system admin for this information but that's no fun. How do you get this information then?

Enter Nmap

Nmap is short for Network Mapper. Nmap is a veritable tool shed of functionality to perform network scans. It can be used for security scans, simply to identify what services a host is running, to "fingerprint" the operating system and applications on a host, the type of firewall a host is

using, or to do a quick inventory of a local network. It is, in short, a very good tool to know.

Nmap is available for all leading operating systems. However this guide is written from a Linux user's perspective (Ubuntu 14.04 in specific)

Installing Nmap

Nmap can be installed by a variety of different ways which are listed here. The traditional and best method is to build it yourself. To do this, open a command line and follow these steps:

```
svn co https://svn.nmap.org/nmap
cd nmap
./configure
make
sudo make install
make clean
```

Make sure you have subversion installed on your system. If you don't you can install it on debian/ubuntu using sudo apt-get install subversion

Alternately you can directly install nmap through apt-get on debian/ubuntu

```
sudo apt-get install nmap
```

. . .

The basic nmap syntax is nmap *scantype options target*. The simplest way to run nmap is to provide the target host address after nmap. Address can be supplied as an ip address or as a domain name. Addresses can also be supplied as a range of ip addresses (eg: 127.0.0.1–125)

```
nmap 127.0.0.1
```

The result this yields is as follows:

```
Starting Nmap 7.12SVN ( https://nmap.org ) at 2016-06-27 14:28 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
```

```
Not shown: 998 closed ports
PORT STATE SERVICE
631/tcp open ipp
5432/tcp open postgresql
```

Thus we can see that there are 2 ports open at the target host.

Nmap can also be used to determine the OS running on the target host. This can be done simply adding a -O flag to the previous command

```
nmap -O 127.0.0.1
```

This returns a more detailed result:

```
Starting Nmap 7.12SVN ( https://nmap.org ) at 2016-06-27 14:34 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
631/tcp open ipp
5432/tcp open postgresql
Device type: general purpose
Running: Linux 3.X|4.X
```

```
OS CPE: cpe:/o:linux:linux_kernel:3.19 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.19, Linux 3.8-4.4
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.14 seconds
```

The result now shows the OS running on the host.

The -v flag can be used to get verbose information about the scan. The -sV flag can be used to show the software versions running on the open ports.

```
nmap -v -sV hostname
```

This will return the following:

```
Starting Nmap 7.12SVN ( https://nmap.org ) at 2016-06-27 14:55 IST
NSE: Loaded 36 scripts for scanning.
Initiating Ping Scan at 14:55
Scanning 104.236.66.200 [4 ports]
Completed Ping Scan at 14:55, 0.62s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:55
Completed Parallel DNS resolution of 1 host. at 14:55, 3.90s elapsed
```

```
Initiating SYN Stealth Scan at 14:55
Scanning (104.236.66.200) [1000 ports]
Discovered open port 22/tcp on 104.236.66.200
Discovered open port 443/tcp on 104.236.66.200
Discovered open port 3000/tcp on 104.236.66.200
Completed SYN Stealth Scan at 14:57, 97.05s elapsed (1000 total
ports)
Initiating Service scan at 14:57
Scanning 4 services on (104.236.66.200)
Completed Service scan at 14:57, 16.07s elapsed (4 services on 1
host)
NSE: Script scanning 104.236.66.200.
Initiating NSE at 14:57
Completed NSE at 14:57, 4.00s elapsed
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Nmap scan report for (104.236.66.200)
Host is up (0.34s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux;
protocol 2.0)
80/tcp open http Apache httpd 2.4.7
443/tcp open ssl/http Apache httpd 2.4.7
3000/tcp open http Node.js Express framework
Service Info: Hosts: 104.236.66.200, localhost; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
Read data files from: /usr/local/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.40 seconds
Raw packets sent: 1795 (78.956KB) | Rcvd: 1118 (44.740KB)
```

This test shows the port number, the state of the port (open,closed), the service (ssh, ssl, http, etc) and the version of the service. Also this test shows more details about the nmap connection

A -p flag can be used to check if a particular port is open or closed. The -p flag can be used to check the port by port number or port name. (Ports can also be specified in range, eg: 1–40)

```
nmap -p ssh 127.0.0.1
```

This will return the state of the ssh port of the host. It returns the port number, state and the service

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000076s latency).
PORT STATE SERVICE
22/tcp closed ssh


Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

This test can also be run using the port number as nmap -p 22 127.0.0.1

A -sn flag is used to check if a host is alive or not. Running this on a range of addresses will show the following result:

```
nmap -sn 127.0.0.1-25

Starting Nmap 7.12SVN ( https://nmap.org ) at 2016-06-27 15:33 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000074s latency).
Nmap scan report for 127.0.0.2
Host is up (0.00015s latency).
Nmap scan report for 127.0.0.3
Host is up (0.000093s latency).
Nmap scan report for 127.0.0.4
Host is up (0.000079s latency).
Nmap scan report for 127.0.0.5
Host is up (0.000069s latency).
….
Nmap scan report for 127.0.0.24
Host is up (0.000095s latency).
Nmap scan report for 127.0.0.25
Host is up (0.000085s latency).
Nmap done: 25 IP addresses (25 hosts up) scanned in 0.00 seconds
```

Nmap allows multiple flags to be used together, i.e. a command such as

```
nmap -v -sV -O 127.0.0.1
```

is valid and so is the command

```
nmap -sV -p 1-65535 192.168.1.1/24
```

(Here /24 is the network mask)

Nmap comes with a GUI Zenmap for those who are not comfortable working with the command line

This guide barely scratches the surface of nmap. Nmap is an extensive tool with a lot of functionalities. Nmap is a widely used tool by itself and along with other softwares such as metasploit. It is also one of the simplest tools to begin the journey into penetration testing with. I myself am only getting started as a pentester. I will keep updating this blog with more guides as I explore more in this field. Till next time, this is Anuraag Baishya, signing out.

Tech | Penetration Testing | Information Security | Linux | Hacking

7 claps

WRITTEN BY

Anuraag Baishya

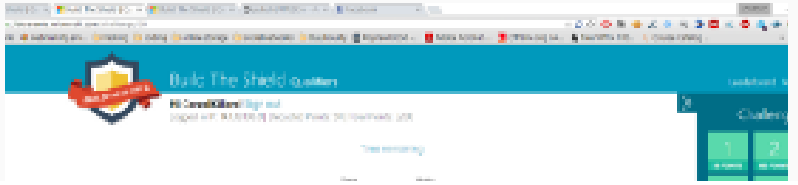
Follow

Digboi, Assam | New Delhi, NCR | Manipal, Karnataka
Photographer | Coder | Writer Progressive Trance | Classic Rock | Metal Snapchat @anuraagbaishya

See responses (1)

More From Medium

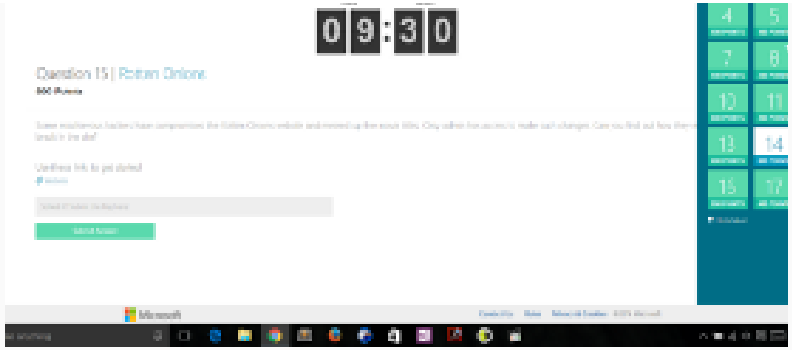
Related reads



From Microsoft “Build the Shield” to Microsoft “Hall of Fame”

Sai Krishna Kothapalli
May 18, 2018 · 7 min read

1.6K

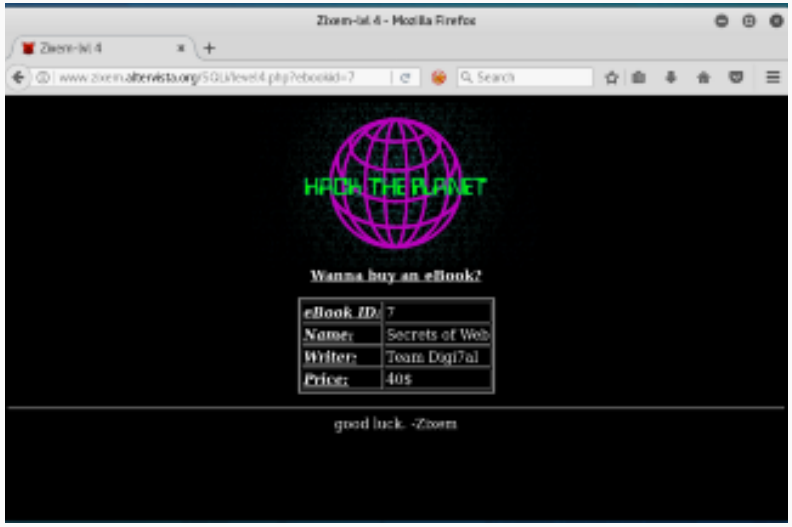


Related reads

Union SQLi Challenges (Zixem Write-up)

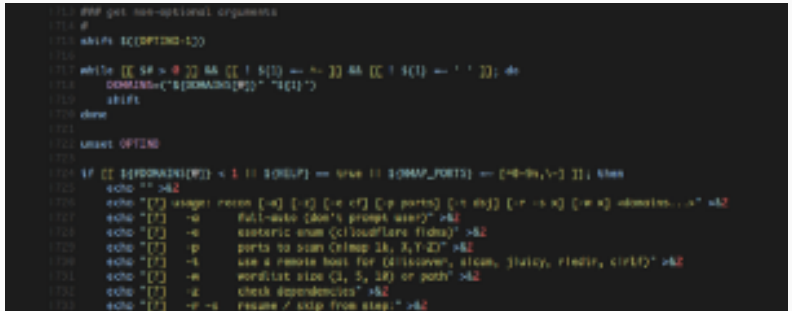
George O in CTF Writeups
Oct 21, 2018 · 9 min read

719



Related reads

Reconnaissance: a eulogy in three acts



europa

Feb 11, 2018 · 8 min read

1.5K