Network Scanning

Nmap and Netcat

Venkata SreeKrishna K. and Lavanya K. Galla

July 19th, 2016
Version 2.1

University of Idaho

CS 539: Applied Security Concepts

Executive Summary

Nmap is a tool which is used to create a map of the network by detecting the hosts and services running on a particular network. In this tutorial several options pertaining to scanning of a network will be discussed.

Netcat is used to read and write data across network connections using TCP or UDP protocol. Netcat was designed to be a back-end reliable tool that can be driven by other programs and scripts.

Prerequisites

Basic knowledge of networking, ports, and the bash command line.

Contents

1 Nmap Overview >

- Nmap
  - Used to discover hosts and services
  - First released on September 1, 1997.
  - Free and open source
  - Designed to rapidly scan large networks
  - Both console and graphical versions are available and supports all versions of Unix, Windows and Mac OS.

Nmap is a free software (GPLv2) network and port scanner. It is a command line tool that can identify hosts on a network, classify the status of ports on known hosts, and speculate what the operating system of a scanned host is. [1] The primary legitimate task it is used for is keeping track of network resources and uptime. However, it can be illegitimately used to scan someone else's network to identify vulnerabilities. For this reason, it is never a good idea to scan a network unless you have written permission from the appropriate authority. Using Nmap to scan a network without such permission strays into various levels of illegality, depending on the jurisdiction you reside in. It could get you sued or maybe even imprisoned. It goes without saying that it's good practice to always double-check the address you are about to scan with Nmap.

Nmap is useful because it has a massive variety of arguments that can be passed to it, can scan entire networks very quickly, is built for every major operating system (and in some cases can come packaged with a GUI), and can even be used to scan the ports of the local host.

2 Features <>

1. Port Scanning
2. Operating System Detection
3. Version Detection
4. Host Discovery
5. Scripting Interaction

1. Port scanning is used to create a list of all the open ports on target hosts. In general port scan is a process that sends client request to a range of server port addresses on a host with a goal of finding an active port.

2. One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses. If Nmap is unable to guess the OS of a machine, and conditions are good, Nmap will provide a URL you can use to submit the fingerprint if you know (for sure) the OS running on the machine. [2]

3. Using its Nmap-services database of about 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate—the vast majority of daemons listening on TCP port 25 are, in fact, mail servers.

4. Host discovery is a service which is used to identify hosts on a network. For example, listing the hosts that respond to TCP or ICMP request or have a particular port open.

5. Nmap scripting Engine allows users to write and share simple scripts using the Lua programming language to automate a wide variety of networking tasks. [2]

3 Legal Issues <>

- Unauthorized Port Scanning is a Crime
- Used to discover vulnerable hosts
- Unauthorized use of Nmap is illegal
- System Administrators have an advantage

There are many legal issues associated with using Nmap to scan a computer, network, or domain where you do not have explicit authorization to do so. In many jurisdictions, using Nmap to scan a random website or computer is illegal or leaves you with the possibility of getting sued or your internet service provider revoking your internet service. [1]

4 Related News <>

1. Nmap 7 brings faster scanning and improved IPv6 support [3]
2. SourceForge accused of hijacking Nmap project account [4]

1. Version 7 of Nmap moved a lot of code written in old, unsustainable C into the Nmap Scripting Engine (NSE), which has scripts written in Lua. This means that a lot of Nmap functionality is now coded into the NSE, where it is easier to maintain and modify for special purposes. Nmap 7 brings more IPv6 and SSL/TLS support. Also, it scans faster. [3]

2. The developer of Nmap, Gordon "Fyodor" Lyon, accused SourceForge of restricting his access to the Nmap code and installers hosted on the SourceForge website. He said that SourceForge moved the content to a new page that he has no control over. In the past, SourceForge has been caught committing other unethical acts in regards to free software, such as bundling adware with old versions of GIMP available for download from their website. [4]

5 How It Works <>

- DNS lookup
- Ping
- Different packets
- Firewalls

Initially when an IP address is selected for scanning, Nmap looks up the DNS server and resolves the IP. Then Nmap pings each of the ports by sending a zero byte packet. If the packets are not received back then it means that the port is closed and if the packets are received back then the port is said to be open. Nmap then sends different packets with different timing to determine whether the port is filtered or unfiltered. If firewalls are present on those systems they can interfere with the process.

6 Nmap Port States <>

1. Open
2. Closed
3. Filtered
4. Unfiltered
5. Open | Filtered
6. Closed | Filtered

1. An open port actively responds to an incoming connection. It shows the available services on the port. [5]
2. A closed port is a port on a target that actively responds to a probe but does not have any service running on the port. Closed ports are commonly found on systems where no firewall is in place to filter incoming traffic. [5]
3. Filtered ports are those which are typically protected by a firewall of some sort that prevents Nmap from determining whether or not the port is open or closed. [5]
4. An unfiltered port is a port that Nmap can access but is unable to determine whether it is open or closed. [5]
5. An open|filtered port is a port which Nmap believes to be open or filtered but cannot determine which exact state the port is actually in. [5]
6. A closed|filtered port is a port that Nmap believes to be closed or filtered but cannot determine which respective state the port is actually in. [5]

7 Basic Nmap Commands <>

1. Single target: **$ Nmap [target]**
2. Mutliple targets: **$ Nmap [target1 target2]**
3. Range of IP address: **$ Nmap [range of ip addresses]**
4. Exclude Targets from a Scan: **$ Nmap [targets] –exclude [targets]**
5. Aggressive Scan: **$ Nmap –A [target]**
6. IPv6 Target: **$ Nmap –6 [target]**

1. Executing Nmap with no command line options will perform a basic scan on the specified target. A target can be specified as an IP address or host name. A default Nmap scan will check for the 1000 most commonly used TCP/IP ports. [5]

   Ex: **$ Nmap 192.168.10.1**

2. Nmap can be used to scan multiple hosts at the same time. The easiest way to do this is to string together the target IP addresses or host names on the command line. [5]

   Ex: **$ Nmap 192.168.10.1 192.168.10.100 192.168.10.101**

3. A range of IP addresses can be used for target specification. [5]

   Ex: **$ Nmap 192.168.10.1-100**

4. The –exclude option is used with Nmap to exclude hosts from a scan. [5]

   Ex: **$ Nmap 192.168.10.0/24 –exclude 192.168.10.100**

5. The -A parameter instructs Nmap to perform an aggressive scan. The aggressive scan selects some of the most commonly used options within Nmap and is provided as a simple alternative to typing a long string of command line arguments. [5]

   Ex: **$ Nmap –A 10.10.1.51**

6. The -6 parameter is used to perform a scan of an IP version 6 target.Most Nmap options support IPv6 with the exception of multiple target scanning using ranges. [5]

   Ex: **$ Nmap –6 fe80::29aa:9db9:4164:d80e**

8 Discovery Options <>

1. Ping Only Scan: **$ Nmap -sP [target]**
2. Don't Ping: **$ Nmap -PN [target]**
3. Operating System Detect: **$ Nmap -O [target]**
4. TCP ACK Ping: **$ Nmap -PA [target]**
5. Traceroute: **$ Nmap -traceroute [target]**
6. Verbose: **$ Nmap -v [target]**

1. The -sP option is used to perform a simple ping of the specified host. This option is useful when you want to perform a quick search of the target network to see which hosts are online without actually scanning the target(s) for open ports. [5]

   Ex: **$ Nmap -sP 192.168.10.2/24**

2. Nmap attempts to scan a system for open ports it will first ping the target to see if it is online. This feature helps save time when scanning as it causes targets that do not respond to be skipped. the specified target is not scanned as it does not respond to Nmap's pings. The -PN option instructs Nmap to skip the default discovery check and perform a complete port scan on the target. This is useful when scanning hosts that are protected by a firewall that blocks ping probes. [6]

   Ex: **$ Nmap -PN 10.10.5.11**

3. In order to detect the operating system the target is running we use the -O command. [6]

   Ex: **$ Nmap -O 10.10.5.11**

4. The -PA performs a TCP ACK ping on the specified target. The -PA option causes Nmap to send TCP ACK packets to the specified hosts. This method attempts to discover hosts by responding to TCP connections that are nonexistent in an attempt to solicit a response from the target. [6]

   Ex: **$ Nmap -PA 192.168.1.254**

5. The –traceroute parameter can be use to trace the network path to the specified host. [6]

   Ex: **$ Nmap -traceroute scanme.insecure.org**

9 Scanning Options <>

1. TCP SYN Scan: **$ Nmap -sS [target]**
2. Fast Scan: **$ Nmap -F [target]**
3. Scan Specific Ports: **$ Nmap -p [port] [target]**
4. Scan Ports by Name: **$ Nmap -p [port name(s)] [target]**
5. Scan All Ports: **$ Nmap -p "*" [target]**
6. Top ports: **$ Nmap -top-ports 10 [target]**

1. The -sS option performs a TCP SYN scan. The TCP SYN scan is the default option for privileged users. The default TCP SYN scan attempts to identify the 1000 most commonly used TCP ports by sending a SYN packet to the target and listening for a response. This type of scan is said to be stealthy because it does not attempt to open a full-fledged connection to the remote host. This prevents many systems from logging a connection attempt from your scan. [5]

   Ex: **$ Nmap -sS 10.10.1.48**

2. The -F option instructs Nmap to perform a scan of only the 100 most commonly used ports. Nmap scans the top 1000 commonly used ports by default. The -F option reduces that number to 100. [5]

   Ex: **$ Nmap -F 10.10.1.44**

3. The -p option is used to instruct Nmap to scan the specified port(s). In addition to scanning a single port, you can scan multiple individual ports or a range of ports. [5]

   Ex: **$ Nmap -p 80 10.10.1.44**, **$ Nmap -p 25,53,80-200 10.10.1.44**

4. One can search for open SMTP and HTTP ports by name using the -p option. The name(s) specified must match a service in the Nmap-services file. [5]

   Ex: **$ Nmap -p smtp,http 10.10.1.44**

5. The -p "*" option is a wildcard used to scan all 65,535 TCP/IP ports on the specified target. [5]

   Ex: **$ Nmap -p "*" 10.10.1.41**

6. One can search only the top ports running by using the top ports command. [5]
   Ex: **`$ Nmap -top-ports 10 192.123.1.1`**

10 Questions <>

1. Which option is used to TCP SYN stealth port scan?
2. What is the port status if it does not allow entry or access to a service?
3. How can port scanning lead to vulnerabilities?

Answers are in the appendix.

11 Questions Contd.. <>

4. Which of the following does Nmap require for OS identification?

   (a) one open and one closed port

   (b) two open ports and one filtered port

   (c) one closed port

   (d) one open port

12 Challenge 1 <>

- For this challenge use Nmap to discover all the services that are running on the network. Remember that there are a few hidden servers for this challenge. Give the IP address for all the servers along with the OS running on them.

13 Challenge 2 <>

- A secret service is being hidden in one of the servers. Find the IP address of the server along with the port number of the service. Also name the service and the server on which the service is running?

  PS: The service is moved to a new random port.

14 Netcat Overview <>

- Networking program used to write and read data across TCP and UDP network connections.
- Released in 1996
- Network debugging and investigation tool.

Netcat has often been referred to as "Swiss Army Knife". Netcats functionality is helpful as both a standalone program and a backend tool in a wide range of application. It provides a basic TCP/UDP networking subsystem that allows users to interact manually or via script with network applications and services on the application layer. It lets us see raw TCP and UDP data before it gets wrapped in the next highest layer like FTP, SMTP or HTTP. [7]

15 Features <>

- Oubound or inbound connections, TCP or UDP, to or from any ports.
- Ability to use any local source port and any source address
- Built-in port scanning capabilities.
- Hex dump of transmitted and received data.

Some of the other features include

- Reading command line arguments from standard input
- Featured tunneling mode which permits user defined tunneling.
- Optional ability to let other program service establish connections. [7]

16 Uses of Netcat <>

1. Port Scanning
2. Banner grabbing
3. Port Listening and redirection
4. File transfers
5. Backdoor

1. Though Netcat has port scanning capabilities it is not preferred because it contains only basic functions or options.
2. Banner grabbing is used to determine the version, operating system or other relevant information about a particular service. It is important if one is looking for a vulnerability associated with a particular version of some service.
3. This is used to redirect both ports and traffic. This is particularly useful if you want to obscure the source of an attack. This technique can also be used to hide netcat traffic on more common ports, or change ports of applications whose normal ports might be blocked by a firewall.
4. It has the ability to both pull and push files. All the netcat file transfers are unencrypted.
5. Netcat can be used as back-door where different files and scripts can be executed. [8]

17 Port Scanning with Netcat <>

- Port scanning with netcat occurs in client mode.
  `$ nc -[options] hostname [ports]`
- Options:
  - -z : Speed up your scan
  - -i : Sets a delay interval between ports scanned
  - -r : Scans port randomly
  - -v : Runs netcat in verbose mode which redirects the output to a file

Netcat is not only limited to transfer data between machines but also performs a port scan on a machine against a range of ports. Port scanning can be used by system administrators or hackers to gain insight of a network infrastructure.

Few other options include

- -n : Instructs necat to bypass name resolution.
- -w 1 : Instructs netcat to wait one second between each scanned port.
- -ip address: To scan against that address
- -port : To scan a single or a range of ports.

By default netcat performs port scan with TCP packets. To perform with UDP we need to append -u flag to the command. [7]

18 Banner Grabbing <>

- Allows individual to gather information about running services/versions from a machine.
- Run netcat in client mode.
- Command:
  `$ nc -v [ip address port]`

Once you have established a connection with the machine, by issuing the get command the return information gives us the web version software and version number. Depending upon which port to be used in banner grabbing their respective information will be displayed like ssh version for port 22 and the HTTP version information for port 80. [7]

19 Questions <>

5. If you would like to establish a UDP connection between a client and server using netcat which command would you use?
6. How to know if netcat is running in client or server mode?

20 Challenge 3 <>

- For this challenge you need to create a chat relay. In order to do that use both the VM machines in which one will be a client and the other will be a server.

21 Challenge 4 <>

- In this challenge you need to transfer a file from one VM to the other. The file is a 'cpp' program where you need to transfer it from the Windows VM to the Kali VM and run it in-order to know what it is.

22 Conclusion <

- Nmap can be installed on Windows, Linux or Mac OS X.
- Additional parameters give Nmap the power to control parallel scanning of a certain number of IP addresses.
- Netcat has two modes of operation : Client and Server.
- The -e option which allows netcat to execute programs is what it makes netcat so powerful.

23 Appendix: Setting Up the VM, Answers, and Changelog <

- Setting Up the VM
- Answers
- Changelog

Setting Up the VM

1. Start a virtual machine based on Ubuntu 16.04 LTS
2. Install Nmap and Netcat with the following commands in a bash terminal:
   ```
   $ sudo apt-get update
   $ sudo apt-get install nmap=6.47-3
   $ sudo apt-get install netcat=1.10-41
   ```
   For this tutorial to be guaranteed to work, use only the operating system and software versions listed above. The packages may behave differently than documented in this tutorial if you use a different version released in a future update.

Answers:

1. -sS
2. Closed
3. Could find exposures by OS/services that should not be there.
4. The answer is (a): Nmaps requires one open and one closed port to perform OS identification.
5. Append a -u flag before you initiate the client and server.
6. The -l flag denotes listening , or server mode. the absence of it indicates a client mode.

   Netcat originates on port 12345, yet the attacker would see the attack coming from port 54321. The piped data is a one way connection, therefore the source cannot receive

any response from target. A second relay from target to source must be established to receive a response from the target computer.

Challenge Hints:

1. For this challenge start searching ports which are not common. Try to search a range of ports

2. In order to find all the IP addresses in a network scan the entire subnet which will give the complete result. For finding the Operating system running use the ' -O ' option along with scan.

3. Use the commands -l for the server to listen and on the client side use the IP address. Don't forget to add the port on which you want to listen.

4. In order to do this challenge use the concept of the previous challenge where on the source the IP address must be presentand destination must be able to listen to the port number which you assign. Remember in this challenge you will have to use the symbols " $<$, $>$ " in order to specify the file name. Figure out which symbol must be present on source and which one on the destination.

Changelog:

Network Scanning: Nmap and Netcat			
Ver.	Date	Authors	Changes
v1	Feb. 10th 2016	Venkata SreeKrishna K. and Lavanya K. Galla	First draft of tutorial.
v2	Jun. 1st 2016	Adam Odell	Moderate content addition and fixed grammar mistakes.
v2.1	Jul. 19th 2016	Adam Odell	Added appendix and other minor enhancements.

References

[1] *Nmap*. Nmap Security Scanner.
https://Nmap.org/

[2] Lyon, G. Nmap Network Scanning, Nmap Project, The Internet, 2009.

[3] *Nmap 7 Brings Faster Scanning and Improved IPv6 Support*. 23 November 2015.
http://www.infoworld.com/article/3007301/network-security/nmap-7-brings-faster-scanning-and-improved-ipv6-support.html

[4] *SourceForge Accused of Hijacking Nmap Project Account*. 3 June 2015.
http://www.digitaltrends.com/computing/sourceforge-accused-of-hijacking-n

[5] Marsh, Nicholas. Nmap Cookbook: The Fat-free Guide to Network Scanning. CreateSpace, 2010.

[6] *Introducing Nmap*
http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Nmap.pdf

[7] *Introduction to Netcat*
http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introduction-to-Netcat.pdf

[8] Gregg, Michael. Certified ethical hacker (CEH) cert guide. Pearson IT Certification, 2013.