Introduction to Network Security
Lab 2 - NMap

1 Introduction: Nmap as an Offensive Network Security Tool

Nmap, short for Network Mapper, is a very versatile security tool that should be included in every professional's toolkit. Nmap is an open source utility for network exploration, security scanning and auditing. It comes with a very wide range of options that can make the utility more robust and can add or change features to your specifications.

Nmap was created by Gordon Lyon, a.k.a. Fyodor Vaskovich, and first published in 1997. Since the source code has been available the software has been expanded greatly and is currently at version 4.85. In addition to improvements in the functionality of the program, graphical user interfaces and support for numerous operating systems have been developed. Currently Nmap can run on Linux, Windows, OS X, FreeBSD, Solaris, Amiga, HP-UX, and others. GUI versions are also available on most of these systems along with the command line versions. There are also implementations that can take advantage of web browsing to allow for access to Nmap via a web browser.

Nmap is very popular among security professionals as well as black hat hackers because of its numerous uses. The most recent version of the program can be used to check for network host discovery, port scanning, version and OS detection, network inventory, ping sweeps, and detailing logging mechanisms. These various uses are all important, but what the most basic sections of the program deal with are host discovery and port scanning. Nmap can be used to check to see what other devices and machines are connected to the network. It can also be used to check which ports on these devices are open and closed. The results of these type scans can be saved to a log file which can be analyzed at a later time or saved for future comparison.

Nmap is a tool that can be used for good as well as for evil. In this lab we will focus on showing the practical uses for attack, defense, and forensic analysis. Complete documentation and download information can be found at http://nmap.org/ as well as much more information pertaining to the use of the product.

Nmap is often used in combination with other open source security tools such as *****, ****** and Wireshark to help secure networks from attacks. In combination with these other tools a powerful security suite can be established that can help to ensure protection of networks. Other important techniques to follow include frequently patching all systems, routine security audits, and enforcement of security policies.

In the following tasks, you will use the Nmap tool to perform several of the tasks listed above..

1.1 The target computer

Before starting this lab, a target computer has been set up for you. For demonstration purposes, a few ports have also been opened, but it will be your job to identify them. Your ultimate goal is to familiarize yourself with the computer and these programs sufficiently that you could begin an attack against this machine.

Your target computer has an IP of _____

1.2 Finding the target host(s)

Intruders have the ability to use Nmap to scan entire networks to look for potential targets. This can be done by "ping sweeping" with the –sp command. When using this command, Nmap sends in ICMP echo and a TCP ACK flag to each host that it scans. If Nmap receives a response, it notes that IP as being a running host and then continues its scanning process.

From the command line (START/RUN/cmd) you can scan for all hosts on the local network by typing in the following command:

nmap -sP 192.168.1.*

-sP stand for "sweep ping". Nmap will return with its scanning results after a short wait. Record the IP address, MAC address and type (Dell, NetGear, Xerox) of three different hosts in your report (at the end of this lab).

There is also another, more specific, way to ping your targeted computers. In some scenarios, a host may be blocking some sorts of traffic, so specifying a specific port for the scan may be necessary. You can try scanning on port 80 since that is normally open for http traffic. To specify a specific port, the –PT command is used.

From the command line, run:

nmap –sP –PT80 192.168.1.*

NOTE: For Nmap to determine if a host is running, the specified port (in this case 80) does not need to be open.

1.3 Task 1.4: OS Fingerprinting

It is usually important for an attacker to know what OS version is running on the target computer. This is done by using the –O command, which must be used in conjunction with a port scan (-sT or –sS which will be covered later).

From the command line run:

nmap -O -v *<IP address listed in part 1.1>*

Nmap will scan for specific ports, and then extrapolate the most likely target OS from the open port information. Record the resulting Nmap data in your report.

1.4 Task 1.3: Port Scanning

The most simple port scan is a TCP connect scan. This attempts to complete a normal 3-way handshake with the targeted computer. You can run this scan on a specific IP (ask your instructor what to use, or use the machine identified in 1.1) with the –sT command.

From the command line:

nmap –sT *<IP address listed in part 1.1>*

This will scan for open ports on that specific host. Record the results from this scan in your report.

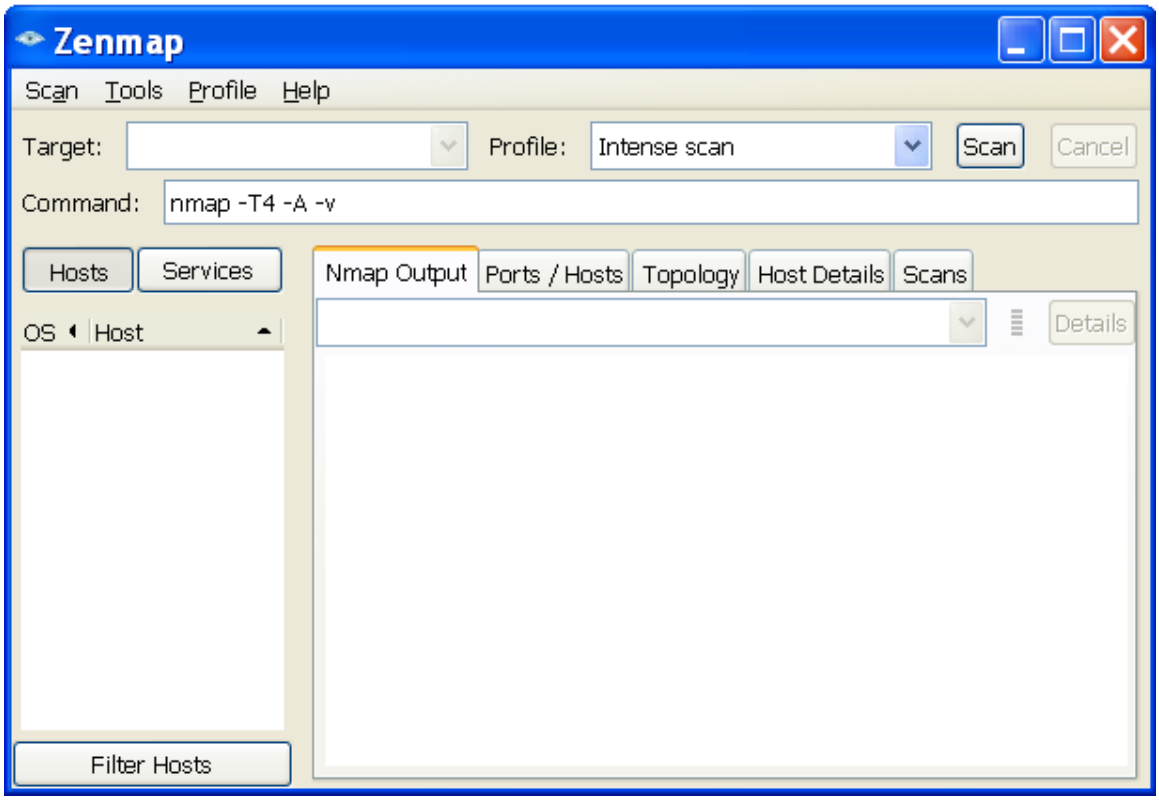
Note: This type of scan is very easy to detect since the target host will log the connection by the attacker. You can even check in the windows event logs of the target machine to see if a connection (scan) was attempted.

1.5 Stealth Scanning from the GUI

The basic deep scan (using the –sT command) can be detected easily, and there are alternatives to such brute force methods of scanning. Stealth port scanning is used to avoid logs being created of your scanning activity. The targeted computer doesn't log the connection because the 3-way TCP handshake never finishes. Instead of finishing the handshake, the attacker sends an RST (reset command) flag to disconnect the connection instead of acknowledging the connection.

Let's try the stealth port scan, but we will use the nmap GUI to make our task easier. Go to Start/nMap/nMap –ZenMap GUI.

You should see something that looks like this:



- In the target line, enter the IP address of your target machine.
- In the Profile line select "stealth scan" if it is available.
- IF STEALTH SCAN IS NOT AVAILABLE, type the following into the command line.

  nmap -sS -v *<IP address listed in part 1.1>*

- *NOTE: You can create your own scans and save them as "profiles"*
- When you are ready hit the SCAN button.

After you have run your scan, take a look at the other tabs. What information was disclosed by this scan?

Additional scanning techniques and their particular usage can be found at http://nmap.org.

REPORT

1.2 What computers did you find running on the local network? (IP Addresses)? Ex: 192.168.1.1 MAC Address: 00:24:B2:63:7F:85 (Netgear)	
1.3 What is the operating system of your target machine?	
1.4 What ports are open on the machine that you scanned?	