U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

NMAP

October 2023

cyberforcecompetition@anl.gov

Nmap 101

Introduction

Nmap ("Network Mapper") is a free and open-source network exploration and security auditing utility. It has become one of the preferred core tools many security professionals, network administrators, and ethical hackers use.

This tool uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to scan large networks rapidly but works fine against single-host scans.

Nmap can be a very powerful tool to use, but it is also very complex. There are over 100 command line options to use. With so many options, it can quickly become confusing for new users. This guide will help new users learn the basics of using Nmap.

Installing Nmap

Nmap can be installed on both Windows and Linux. However, it generally works best and faster on a Linux system. The installation steps in this guide will be focused on Debian based systems. Installing Nmap is straightforward to accomplish and only takes a few steps.

Open a new terminal window on your machine and run the following commands to install Nmap.

```
# sudo apt update && sudo apt upgrade

# sudo apt install nmap
```

After running the commands above, verify that Nmap has been successfully installed by running the command below.

```
# nmap --version
```

How to Use Nmap

The best way of learning how to use Nmap is by getting hands-on experience and using the tool yourself. To do this, we will review the most basic commands.

Basic syntax

The basic syntax of Nmap is as follows:

```
# nmap [Scan Type(s)] [Options] [Target(s)]
```

Here is a breakdown:
Scan Type(s) – This defines the type of scans you want to perform. See the **Basic Scan** section for more information.

Options – This is an additional parameter that will modify the behavior of your scan. Examples of these options are:

- -p: Specify a specific port you want to scan
- -A: Used to run an **Aggressive scan**. This will provide better information than a regular scan but is more likely to be detected.
- -oN <*filespec*>: This option chooses the output format. This option takes one argument: the filename in which results should be stored. Other examples: -oX, -oS, -oG

Target(s) – This is where you provide the target IP address, hostname, or IP address range you want to scan.

Basic Scan

Ping scan

```
# nmap -sp [Target(s)]
```

One of the first scans you will probably perform when mapping a network is a basic ping scan or ping sweep. This type of scan will discover any live hosts on a network by sending ICMP (Internet Control Message Protocol) echo requests to a specific IP address or a range of addresses.

Example:

```
# nmap -sp 192.168.1.1/24
```

TCP SYN Scan

```
#  nmap -sS [Target(s)]
```

A TCP SYN scan is specified using the -sS flag. It is used to identify open ports on a target without completing a full TCP handshake. The way it works is that a SYN packet will be sent to a target. If it responds with a SYN/ACK packet, then it means that the port is open. This type of scan is also called a 'stealth scan' because it never completes the TCP handshake.

TCP Connect Scan

```
#  nmap -sT [Target(s)]
```

A TCP connect scan is like a TCP SYN scan. The difference between the two is that a TCP connect scan will complete the TCP handshake with the target. This scan will yield more results than a TCP SYN scan at the expense of being slower and easier to detect.

UDP Scan

```
#  nmap -sU [Target(s)]
```

A UDP scan works similarly to a TCP scan, except it scans UDP ports. This is useful for finding DNS, SNMP, and DHCP services.

OS scanning

```
#  nmap -O [Target]
```

Operating System (OS) scanning is a powerful and valuable Nmap feature. Running this scan allows you to determine the OS and version of the target you're scanning. This scan sends TCP and UDP packets to a specific port and then analyzes the response. It compares this response to a database of 2600 operating systems and returns information on a host's OS (and version). It is important to note that you require one open and one closed port to use the –O command.

Version Detection Scan

```
#  nmap -sV [Target]
```

A version detection scan allows you to find what software version a computer is running. Keep in mind that this scan is not always 100% accurate.

CVE Detection

```
# nmap -sC [Target]     #load default scripts
```

or

```
# nmap --script \ filename|category|directory|expression,...   [Target]
```

Example:

```
# nmap --script vuln [Target]
```

A useful feature of Nmap is called the 'Nmap Scripting Engine' (NSE). This scripting engine allows users to use a pre-defined set of scripts or write their own using Lua programming language. NSE allows you to automate tasks, gather more detailed information, perform advanced network discovery, and even exploit vulnerabilities in a controlled manner. Nmap comes with a set of pre-build list of scripts. These scripts can be found in the Nmap installation directory under the script's subdirectory. For more information on this, visit the official documentation.

Tip

An easy way of remembering the command flags for different types of scans:
First, you want to remember that '-s' stands for 'scan.' Following this will be an upper-case letter representing what type of scan to perform. For example:

- **-sT** would signify a TCP connect scan
- **-sU** would signify a basic UDP scan
- **-sS** would signify a Stealth scan
- **-sA** would signify an ACK scan
- **-sF** would signify a FIN scan

Additional Resources

- https://www.tutorialspoint.com/nmap-cheat-sheet
- https://www.comparitech.com/net-admin/nmap-nessus-cheat-sheet/

Sources

- https://phoenixnap.com/kb/how-to-install-nmap-ubuntu
- https://nmap.org/book/toc.html
- https://www.codecademy.com/resources/docs/cybersecurity/nmap/aggressive-scan
- https://www.varonis.com/blog/nmap-commands
- https://www.edureka.co/blog/nmap-tutorial/
- https://nmap.org/book/nse.html
- https://www.comparitech.com/net-admin/the-definitive-guide-to-nmap/