Project description:

I am a Security Analyst who needs to utilize nmap to perform authorized, non-malicious scanning to identify potential vulnerabilities on a network: active hosts, ports and services and the operating system on a target.

Nmap is a safe, yet powerful tool to use for this purpose.

## Objective 1 – Install and Verify Nmap Installation

I used terminal to verify the installation and version of Nmap installed on our system. The whole exercise gave familiarity with which commands to use.

Command: nmap --version

Having verified that Nmap have been successfully installed, and which version, it was clear that it was ready for use.

See also: Verification of installed version of nmap.png

## Objective 2 – Access the Help Feature and Man Page for Nmap

**I utilized a public RADIUS server and submitted a username and a password. The RADIUS will**

**Reference additional scanning details available for nmap using the help feature and man page (man stands for manual)**

**Command to access help**: nmap --help

**As can be seen in the attached file, it shows scan types, options, and descriptions that are available to you when scanning a target. These are important things to know because you might have to troubleshoot scanning errors for instance..**

**See also: Nmap help command.png**

**To access the manual – command**: man nmap **which is very useful when you need to recall information to use when scanning.**

**See also: Nmap man command.png**

## Objective 3 – Run a Basic Nmap Scan on a Target

**I performed a basic ping scan on scanme.nmap.org. A ping scan detects if a target is active, and what ports are open and which services are running.**

**In the terminal then, several things are shown.**

* **Nmap version**
* **The time and date the scan started**
* **Whether the host was up and reachable at the time of the scan**
* **Port information**
* **Number of IP addresses scanned**
* **The duration the scan took to complete**

**See also: Nmap basic ping scan.png**

**Next, I performed another basic scan on subnet on the network.**

**Command:** nmap scanme.nmap.org/30

**The number 30 specifies the size of our IP address subnet. It states that our network part of the address are 30 bits long, leaving 2 bits for the host. The are 4 IP addresses in our subnet, so this command scanned all 4 IP address in our subnet.**

**See also: Nmap basic ping scan subnet.png**

**There are a lot of open ports, and if these ports are not properly secured, they can potentially be vulnerabilities and pose a security risk.**

## Objective 4 - – Run a Basic Nmap Scan On My Host

I performed a scan on my Rhyme host IP address using Nmap, and noted open ports and running services on my host. The command ifconfig located the IP address of my host, which were 172.18.0.53

The command nmap 172.18.0.53 then initialized the ping scan.

As can be seen ports 5901 and 6901 are open, for the services vnc-1 and jetstream respectively.

See also: Nmap basic scan own host.png

## Objective 5 – Run an Nmap Scan using Options

I ran a nmap scan using options to further assess the network. This can lead to faster scans, more accurate results and customized output. I need to know the operating system, the service version of the authorized target, in addition to open ports and running services.

The command nmap -A -T4 scanme.nmap.org where:

* A is parameter that instructs Nmap to enable OS detection, version detection, script scanning and traceroute
* T is parameter that instructs Nmap the speed – or more correctly put the intensity- of the scan. 4 is an aggressive scan which advisable in this situation but needs to be handled with care since that generate a lot of network traffic and may also affect accuracy negatively.

The result of the scan shows that port 22 corresponding to the service OpenSSH. SSH is used to establish secure remote access and administration of a system. While SSH is generally secure the presence of this open port can expose the system to attacks, such as brute force or the exploitation of open SSH is there are known vulnerabilities for that version.

Disabling route login and enabling strong authentication methods can help mitigate risk.

Port 80 is also open (HTTP), and that can be indication that a webserver is running on the target system and potentially expose the server to various attacks such as SQL injection or cross-site-scripting or remote code execution. That depends on the web apps hosted and needs further investigation.

Port 9929 on TCP is also open. The Nping echo service is used to test and troubleshoot networks. An attacker can use this port to flood the target with echo request causing a DOS attack, or DDOS attack, or expose the system to potential information disclosure . A better way to mitigate risk would be restrict access to trusted host or better yet disabling the Nping echo service if it is not in use.

Port 31337 on TCP is open, and that is TCPwrapped. TCP wrapper is a security tool that monitors and filers incoming requests to network services and adds an extra layer of security. That could still be bypassed of course and should be added to the firewall rules to monitor that port for suspicious activity.

See also: Nmap scan Using Options.png

## Objective 6 – Output Nmap Scan Results to a File

I performed a scan on a target on the network and output the scan results to a file. What is interesting for me as a security analyst could be the integrity of the webserver, it’s configurations and running services.

With this method the outputs are also saved as a txt file for later review.

Command: nmap -p 80 -A -oN scan.txt scanme.nmap.org/30 where

* p80 specifies scan only port 80
* A is a parameter that instructs Nmap to enable OS detection, version detection, script scanning and traceroute
* oN is a parameter that instructs Nmap to output the results into a file, in our case called scan.txt
* The scanme.nmap.org/30 was used already before.

Port 80 is marked as filtered, meaning that Nmap is unable to determine whether it is open or closed. That could be because of a firewall, an IPS or other security related software that is blocking or even filtering the packet sent by Nmap.

There is another service Nginx, that uses port 80 and for which port 80 is open.

Nginx is often used as webserver, a proxy server or a load balancer, and having it listen on port allows it serve applications to clients using HTTP connections. It should be OK as long as Nginx is updated.

See also: Scan result port 80.png.

## Objective 7 – Output Nmap Scan Results for ports 22 to 80 to a File

The command nmap -p 22-80 -A -T3 -oN scanme.nmap.org

will execute an aggressive scan on ports 22 to 80, speed 3 and save the results to a txt file called Output.txt.

See also: Scan result port 22 – 80.png

Upon checking the file Output.txt does exist and it has the same content as what is shown on the terminal.

See also: Output.png

These images are just excerpt in many cases.

Summery:

In this project I went through both basic ping scan as well as more aggressive variants to extract more information of the target system. These results could be saved into a txt file, and there would not be too complicated to compliment this with a python automation script to facilitate the analysis for a coming hardening process. That would to no small degree enhance the organizations security posture.