|  |
| --- |
|  |
| Capstone Experience IST 894  Carl Laneave |
| Lab 4 Report |

Table of Contents

[1.0 Nmap and Hping 3](#_Toc147092687)

[1.1 Lab Results – Nmap and Hping 4](#_Toc147092688)

[2.0 References: 15](#_Toc147092689)

[3.0 Activity Log 16](#_Toc147092690)

# Nmap and Hping

During the execution of this lab, an evaluation was done to show different flags that both Nmap as well as Hping3 can execute. This type of Nmap scans all users to focus directly on individual ports, and a range of ports, as well as saving the executed results as multiple different format types, such as XML. Furthermore, technology was used in execution to scan key networking ports for open accessibility using networking types such as UDP, TCP, SYN, ACK, and more. These networking capabilities are critical functions to both individual and enterprise-level networking. Through using the technology of Nmap, results were captured of scans of key ports into files such as XML as well as greppable files, which will allow security engineers to quickly analyze the results of open ports. Beyond even scanning open ports, Nmap provides the ability to analyze scans to capture important information such as software versioning and OS usage for the host. This information provides critical insight into a host and their network and instance design.

Using the CLI Hping3, analyses can be done even further on Network information, such as TCP/IP. This analysis can provide deep dives into scan results on a network level as well as provide important information on the diagnosed scans.

By having a strong understanding of Nmap and its flags, attackers as well as security analysts can quickly assess the network vulnerabilities of their enterprises. Even more important, it's important to understand what attackers can do with these scans, such as using Nmap's ability to do automated vulnerability scanning while doing the network scans. Through this gained knowledge, security engineers can do their own internal scans and quickly see any potential vulnerabilities and address them prior to any attackers executing their attacks.

# Lab Results – Nmap and Hping

A computer screen shot of a computer

Description automatically generated

Figure 1.0 – Execute Nmap on the localhost lab machine.

A computer screen shot of a computer

Description automatically generated

Figure 1.1 – Scan the lab using Nmap.

A computer screen shot of a program

Description automatically generated

Figure 1.2 – Output the scan results into a file and cat out the results from the created file.

A screenshot of a computer screen

Description automatically generated

Figure 1.3 – Create and xml file of Nmap results and cat the created XML file itself.

A computer screen shot of a computer

Description automatically generated

Figure 1.4 – Create a greppable file of the Nmap results.

A screenshot of a computer

Description automatically generated

Figure 1.5 – Scan to see OS of a host using Nmap.

A screenshot of a computer screen

Description automatically generated

Figure 1.6 – Complete an OS scan using SNMPs full scan and save the results to an XML file.

A screenshot of a computer program

Description automatically generated

Figure 1.7 – Scan the OS using TCP/IP stack fingerprinting and save results to xml file.

A computer screen shot of a program

Description automatically generated

Figure 1.8 – Scan using Nmap’s scripting engine for automated networking tasks and vulnerability detections.

A screenshot of a computer

Description automatically generated

Figure 1.9 – Run Nmap scan to detect software and service versions.

A screen shot of a computer

Description automatically generated

Figure 1.10 – Scan against ports 100-200 using an UDP scan.

A computer screen shot of a program

Description automatically generated

Figure 1.11 – Scan ports 22 and 80 using Nmap flags.

A computer screen shot of a computer

Description automatically generated

Figure 1.12 – Scan port ranges 20-100 as well as scan all ports and output to xml file.

A screenshot of a computer screen

Description automatically generated

Figure 1.13 – Attempt to run Nmap as a non-root user, the request fails.

A computer screen with white text

Description automatically generated

Figure 1.14 – Default scan type when a user doesn’t have any raw packet privileges.

A computer screen with white text

Description automatically generated

Figure 1.15 – Execute a null scan to not include any information in the header but still see if there is any open ports.

A screen shot of a computer

Description automatically generated

Figure 1.16 – Execute a pingless can against the host.

A screen shot of a computer

Description automatically generated

Figure 1.17 – Execute a default normal time template, then change to a t5 to do an even faster scan template.



Figure 1.18 – Start the Hping CLI used to analyze TCP/IP packets.

A screen shot of a computer

Description automatically generated

Figure 1.19 – Run the Hping tool to scan port 80 using SYN packet analysis.

Screens screenshot of a computer screen

Description automatically generated

Figure 1.20 – Start a tcpdump to listen on port 80; execute hping3 on port 80 and see the results in the saved sys scan file

A screenshot of a computer program

Description automatically generated

Figure 1.21 – Use the -8 flag to do a combination scan of ranged ports.

A screenshot of a computer screen

Description automatically generated

Figure 1.22 – listen on port 22 for ACK scans, execute a scan of port 22 using ACK on Hping and see the captured results.

# 2.0 References:

[1] hping3 | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/hping3/

[2] hping3 - Linux man page. (2010). Die.net. https://linux.die.net/man/8/hping3

[3] Kacherginsky, P. (2020, December 18). Hping Tips and Tricks. Medium. https://iphelix.medium.com/hping-tips-and-tricks-85698751179f

‌

[4] Command-line Flags | Nmap Network Scanning. (n.d.). Nmap.org. https://nmap.org/book/port-scanning-options.html

‌

‌

# 3.0 Activity Log

| **Member Name** | **Task Date** | **Task Details** |
| --- | --- | --- |
| Carl Laneave | 9/30/2023 | Created Template, executed all labs, took screenshots, and completed report |
|  |  |  |
|  |  |  |