**Cyber and Infrastructure Defense, Fall 2021, Haadi Jafarian**

**Assignment 4 – Reconnaissance**

**Learning Objectives:**

* Learning about reconnaissance tools (Nmap, Wireshark, and Nessus/Rapid7 Vulnerability scanners).
* Learn how to discover what’s on your network and identify vulnerable services/hosts
* Learn about traffic analysis and TCP/IP protocols

Part of your responsibility for this assignment is to learn how to work with new security tools. This is an important exercise because as a cybersecurity specialist in any position you must be able to put your theoretical understanding of security, network, and system concepts to use in order to solve real-world problems. To do this, you must be able to learn how to work with new tools that are essentially built on the same theoretical concepts that you've learned.

**Submission Guidelines:** Please submit a PDF file that includes your detailed steps, results and answers to the following questions. Just a reminder that this is a group project.

**Rubric**

Part 1. Port scanning to map a network (30% total)

* Complete scanning including list of IP addresses of all machines in network, OS and version, open ports, services running on ports and versions, 30%
* Incomplete report, missing some of the information, max 15%

Part 2. Vulnerability Scanning (30^ total)

* Complete vulnerability scanning, including list of top 5 discovered vulnerabilities, and analysis of vulnerabilities (CVE information about each), 30%
* Incomplete report, missing discovered vulnerabilities, or analysis of vulnerabilities, max 15%

Part 3. Traffic Analysis with Wireshark (40% total)

* Complete analysis, including answers to all questions, 40%
* Incomplete analysis, missing answers to some of the questions, 5% deducted for each missing answer.

**Part 1. Port scanning to map a network (30 points)**

Use Nmap/Zenmap to scan your own home network. You can use ipconfig (windows) or ifconfig (Linux, MAC) to identify your address range based on your IP and subnet mask. For example, if your local IP address is 192.168.10.2 and your subnet mask is 255.255.255.0, then your network address range is 192.168.10.0/24.

Use **different Nmap options** to get as much information about targets (machines in your address range). List discovered machines, along with their open port numbers, running services and their versions, and OS type and version (anonymize IP/MAC addresses, especially if IP addresses are public).

Ethical practice: please do not scan somebody else’s network, this is unethical and could get you in trouble.

**Part 2. Vulnerability Scanning (30 points)**

Use **Nessus** or **Rapid7** Vulnerability scanners to scan one of these machines remotely (or locally, but remotely is preferred). Go through the generated report by the vulnerability scanner and list your top **5** vulnerabilities that you discovered.

For each vulnerability, use CVE database to discover more information about it. Write a short paragraph summarizing your finding of each vulnerability. You can use other resources if no CVE entry exists for the discovered weakness.

**Part 3. Traffic Analysis with Wireshark (40 Points)**

Run Wireshark and start capturing packets on your own main NIC. Then, open the browser and visit a website like Wikipedia.com. Wait for 30 seconds and stop the capture.

Then, use Wireshark filters to answer the following questions. Anonymize IP and MAC addresses in your responses (replace some letters from the middle with space).

3.1. Define a Display filter that finds the ARP queries and ARP responses.  
Narrow down the filter so that only those ARP packets are shown that were necessary for opening your chosen webpage (the rest of the captured ARP packets that were exchanged between the nodes of LAN, should be left out of the list).

3.2.   What is the transport layer protocol used in the DNS query packet? What is the decimal number in the network layer header that identifies this protocol?

3.3.   Define a display filter that finds the DNS queries and DNS responses.  
Narrow down the filter so that only those DNS packets are shown that were necessary for opening your chosen webpage (the captured DNS packets that were related to other applications/clients in your computer, should be left out of the list).

3.4.   Using the filters created in the previous steps, list all the ARP query/response pairs and DNS query/response pairs that were necessary for opening your chosen webpage.  
For each ARP query/response pair and DNS query/response pair, explain the following (you can group the queries and responses, to avoid repetitions in your explanations):

* What information was asked for (show the relevant information in the query)
* Who was it asked from (what was the MAC address and IP address of it),
* Who answered (what was the MAC address and IP address of it),
* What information was in the answer (show the relevant information in the response).
* Justify why was the query made.

**TCP connections**

3.5.   Define a display filter that finds the TCP packets.

3.6. Narrow down the filter even more, so that only these TCP packets are shown that were used to establish a TCP connection (the TCP packets that were following each connection establishment, should be left out of the list).

3.7.   Using the filter from the previous step, list all the TCP connections, that were necessary for opening your chosen webpage.  
For each TCP connection, explain the following (you can group the connections, to avoid repetitions in your explanations):

* local (client) TCP port number,
* remote (server) TCP port number,
* remote (server) IP address

3.8.   Using the same filter, explain the following:

3.8.1.   Outgoing packets:

* What is the destination MAC address of all the outgoing packets?
* Why are all the outgoing packets going to this particular MAC address?

3.8.2.   Incoming packets:

* What is the source MAC address of all the incoming packets?

**Some resources for the assignment**

**Link to software websites**

Nmap: <https://nmap.org/>

Wireshark: <https://www.wireshark.org/>

Rapid7: [https://www.rapid7.com/solutions/network-vulnerability-scanner/](https://www.rapid7.com/solutions/network-vulnerability-scanner/ )

Nessus Essentials: [https://www.tenable.com/products/nessus/nessus-essentials](https://www.tenable.com/products/nessus/nessus-essentials )

**Tutorials and Guidelines**

Tutorial on Wireshark Filters:

[https://www.wireshark.org/docs/wsug\_html\_chunked/ChWorkBuildDisplayFilterSection.html](https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html )

A nice cheatsheet on Nmap options: [https://www.stationx.net/nmap-cheat-sheet/](https://www.stationx.net/nmap-cheat-sheet/ )

Look at this nice report on what Nmap is able to do: [https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts](https://securitytrails.com/blog/top-15-nmap-commands-to-scan-remote-hosts )

CVE Database: <https://cve.mitre.org/>