Logo, company name

Description automatically generated

**COMP421: Information Security**

**Section: A**

**Semester: Fall 2021**

***Assignment-3.***

**Submitted to: Dr. Saad Bin Saleem.**

**AHMED IKRAM, 22-10019**

**Assignment description:**

**Nmap, which means the *Network Mapper,* is a tool which uses network packets to scan and identify the devices which are interconnected in local and remote networks. A simple example would be the examination of a website where Nmap can scan it and detect the IP address. After the retrieval of the address, it gets parsed, and the web domain associated to it is found out.**

**In our assignment, we must perform the following steps:**

* Install the “zenmap” tool.
* Run zenmap.
* Find the open ports in window machine.
* Temporarily block a port which you think is a liability to the system’s protection.
* This blocking is done by a rule which is defined by us in firewall section of Windows.

**Features and their practical functionality in *nmap:***

* A ‘fast’ scan is done using ***-F*** command. The connected devices and their relevant information are displayed.
* Port scanning is done using the scanning. This lets the attacker know of any actively running services or open ports.
* Outdated ports are more prone to vulnerabilities.
* A *custom profile* is made which is named as Search1 in this assignment.
* Search1 has a *custom command:* ***nmap -F -n -Pn***
* We must *target* a specific subnet to run the scan,
* This targeted subnet (my own laptop) is ***192.168.10.9***

|  |  |
| --- | --- |
| **Command** | **Functionality** |
| ***-F*** | Shows information of all the active hosts with their IP addresses in a network. Stands for “Fast” nmap scan. |
| *-n* | Treats the top 100 ID addresses as active online and instructs not to ping these IP’s. |
| ***-Pn*** | Instructs there to not be a reverse lookup. |
| ***-p*** | This command displays all the ports of the targeted IP address. |
| ***Information specification*** | Number of devices, device OS, device manufacturer, MAC address, service version |

* **The Visible ports:**

Graphical user interface, text, application, email

Description automatically generated

* **Filtered, open and closed ports:**

Graphical user interface, text, application

Description automatically generated

* **Advanced Firewall rules opened:**

Graphical user interface, text, application

Description automatically generated

* **Applying custom advanced Firewall rule to port 445:Graphical user interface, application

  Description automatically generated**
* **Port 445 is now blocked:**

Graphical user interface, text, application

Description automatically generated

* Applying the rule to specific profiles:

Graphical user interface, application, Teams

Description automatically generated

* **Now the following Custom Rule (COMP421 Assignment 3) rule appears as blocked:**

Graphical user interface, text, application

Description automatically generated

**References:**

1. <https://null-byte.wonderhowto.com/how-to/tactical-nmap-for-beginner-network-reconnaissance-0189856/>
2. <https://www.youtube.com/watch?v=ltEFbi_I2KY&t=10s>
3. <https://www.youtube.com/watch?v=Vbl_mj5z6U8>