**Tutorial 4**

**Vulnerability Scanning – Assignment Workshop #1**

**Preparation:**

1. Kali Linux
2. Nessus (either installed in Kali Linux or Windows)
3. Windows Server 2008.vm

**Challenge:**

1. Find the specific vulnerabilities exists in the target machine.
2. Analyze the vulnerability.

**Vulnerability identification**

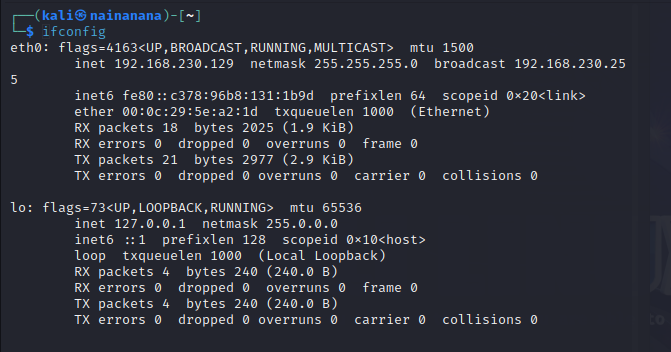
A **vulnerability assessment** often includes a penetration testing component to identify **vulnerabilities** in an organization's personnel, procedures or processes that might not be detectable with network or system **scans**. The process is sometimes referred to as **vulnerability assessment**/penetration testing, or VAPT.

You should consider critically evaluating the following tools:

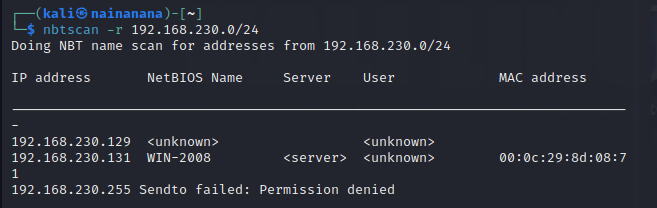
1. Nessus
2. Zenmap/Nmap
3. Retine
4. X-Scan
5. QualysGuard
6. OpenVAS

**Scanning with Nmap**

1. Turn on your virtual machines: Kali Linux and Windows Server 2008
2. In Kali Linux, open terminal, look for Kali Linux IP Address



1. Scan for other available machines

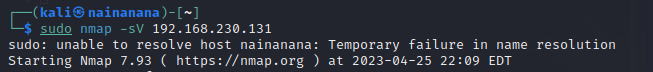


From here, we have identified the IP Address of the Windows Server 2008 which is 192.168.230.131

Nmap (Network Mapper) is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides several features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

1. Performing nmap scan on the target machine.

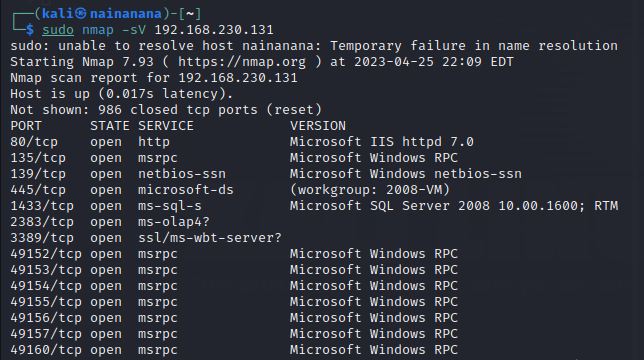


It might take a while to display results.

Question: What is **-sV** used for?

|  |
| --- |
| Answer: |

1. Results:



What can you tell from the results displayed?

|  |
| --- |
| Answer: |

1. Explore further nmap commands and investigate other types of information you can retrieved by using the commands.

Find out how to identify the **operating system version** using nmap?

|  |
| --- |
| Answer:  *Paste your screenshot here.* |

Tips: You can use nmap cheat sheet shared in class (*T4\_nmap cheat sheet.pdf*)

1. Visit any of the listed website to further analyze the identified vulnerability.

|  |
| --- |
| Answer:  *Paste your screenshot here.* |

**Scanning with Nessus**

As we have learnt from previous tutorial (T3\_Nessus Installation), kindly proceed to scan Windows Server 2008 using Nessus.

**What to submit?**

1. Screen Shots of Vulnerability scanning (step-by-step) including the result.
2. How many vulnerabilities did the scanner find?
3. How many open ports /which ones?
4. What services are highly vulnerable?
5. What type of attack is the selected service vulnerable to?
6. What versions of the service are affected by the vulnerability?
7. What security advisories are available for further research on the security bug?

**NOTE: Getting to know how to do vulnerability assessment is your challenge in this section. Kindly refer to the assignment question for what you have been asked to do.**