**Cyber Security – Assessment # 3**

**Part 1: Conceptual**

**Q1**.- Define following terminologies: -

a. Socket

b. Port

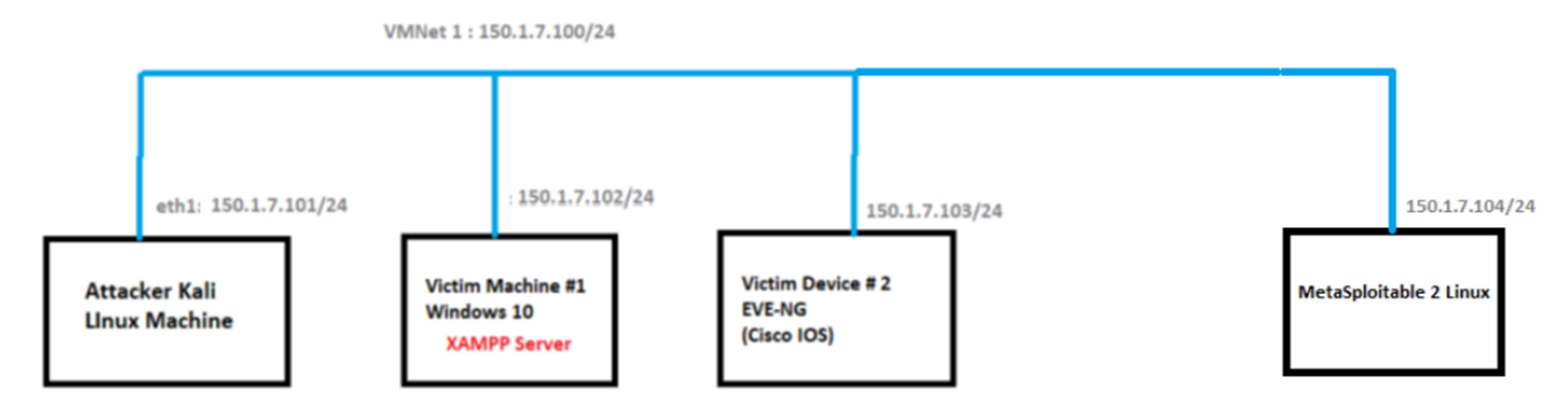
c. Protocol

**Q2.** Enumerate main objectives of Network scanning in CEH Hacking methodology.

**Part 2: Lab**

**Q3.** Perform host discovery using Nmap for 150.1.7.0/24 network. Ensure that port scan is disabled during this activity: -

* ARP Ping Scan
* UDP Ping Scan
* ICMP Echo Ping Scan / Sweep



**Q4**. Port scanning is a technique used to identify open ports and services available on a networked device. It helps network administrators assess security and detect potential vulnerabilities. Determine open ports on the Windows 10 and Metasploitable Linux in above topology. Ensure that host discovery should be disabled during this process.

**Conceptual Part**

**Answer 1:**

* **Socket:**
  + A socket is a combination of an IP address and a port number (Host + Port).
  + It acts as an endpoint for communication between devices on a network.
  + **Example:** A socket might look like 192.168.1.10:80 (where 192.168.1.10 is the IP, and 80 is the port).
* **Port**
  + A port is a logical number used to identify a specific application or service on a device.
  + It allows data to be sent to the right program (e.g., web servers usually use port 80 for HTTP or port 443 for HTTPS).
  + Example: Ports range from 0 to 65535, where some are reserved for standard services.
* **Protocol**
  + A **protocol** is a set of rules that define how data is transmitted and received in a network.
  + **Common protocols include:**
    - **HTTP** for web traffic.
    - **FTP** for file transfers.
    - **TCP/UDP** for communication between applications.

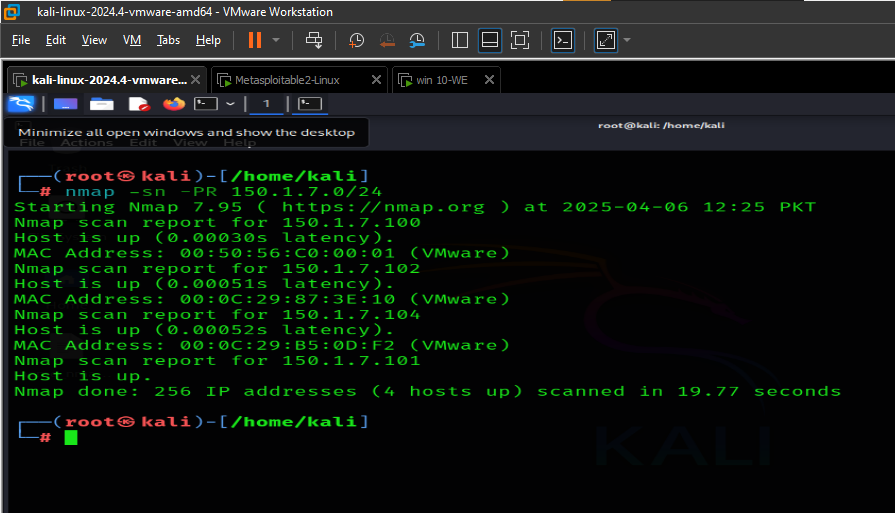
**Answer 2**

Main Objectives of Network Scanning in CEH:

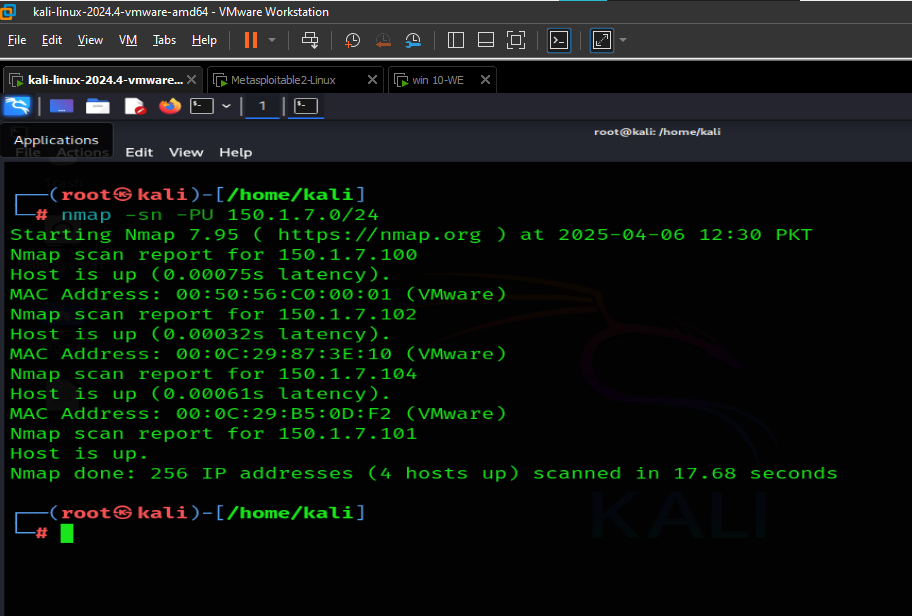
1. **Discover Live Hosts:** Identify active devices or systems within a network.
2. **Detect Open Ports:** Find open or active ports on the target systems.
3. **Identify Services:** Determine the services or applications running on the open ports.
4. **Operating System Detection:** Gather information about the operating system and system architecture (OS fingerprinting).
5. **Vulnerability Identification:** Detect potential vulnerabilities in live hosts for further exploitation.
6. **Network Mapping:** Create a map of the network topology, including devices and their connections.

**LAB PART**

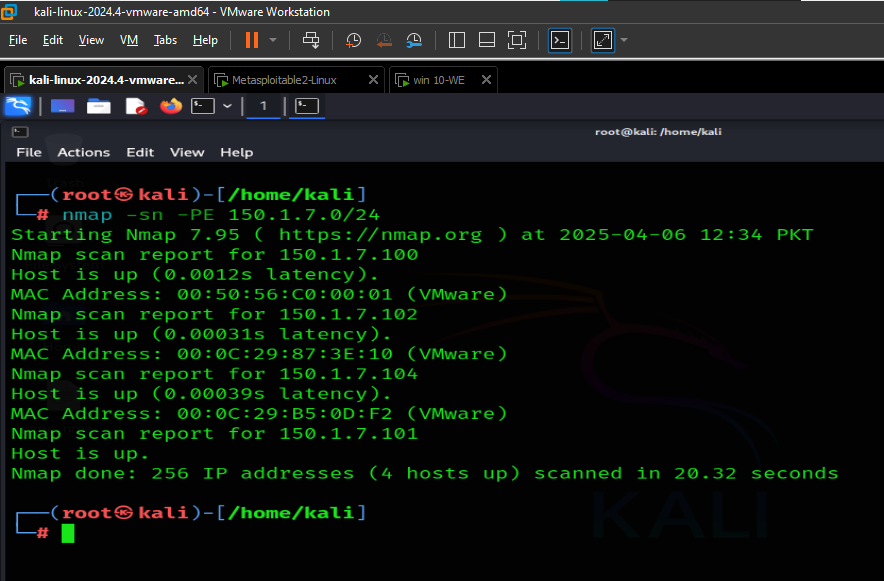
***ARP Ping Scan:***



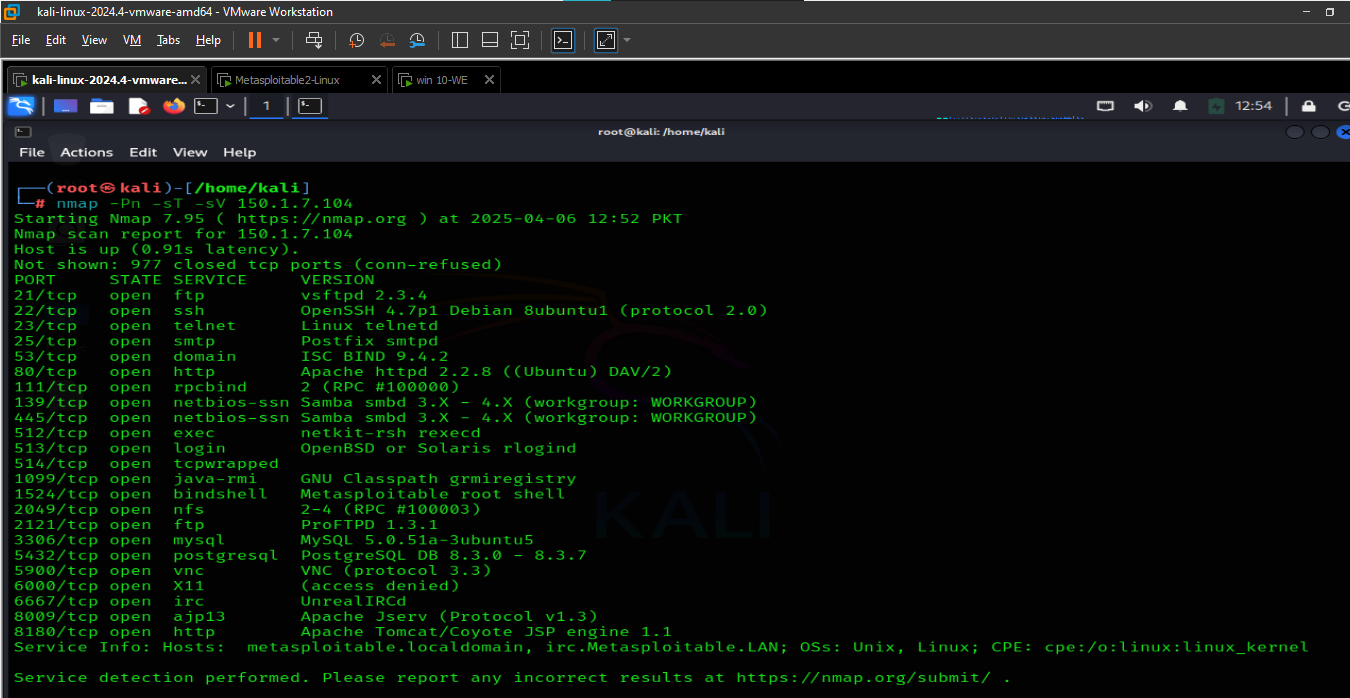
***UDP Ping Scan:***



***ICMP Echo Ping Scan / Sweep:***



***Port + Version scanning (Metasploitable Linux):***

****

***Port + Version scanning (Windows 10):***

