**EX NO: 4**

**DATE:**

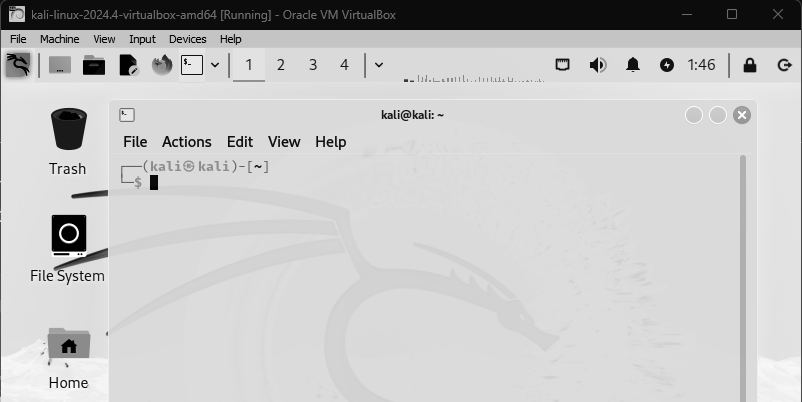
**UNDERSTAND THE NMAP COMMAND AND SCAN A TARGET USING NMAP.**

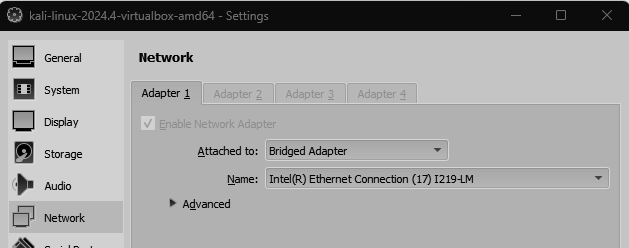
**AIM:**

To Understand the nmap command and Scan a target using nmap.

**PROCEDURE:**

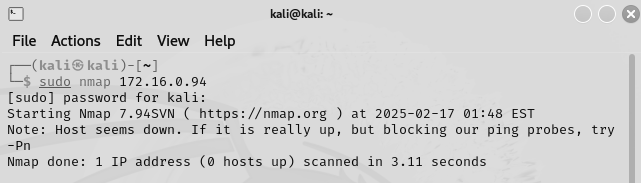
Step 1: The nmap command can be used in Kali Linux and Before using the nmap change the network adapter to bridged adapter.



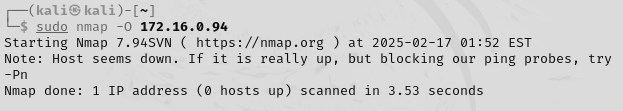


Step 2: The target can be Scanned using the following command:

**nmap <IP address> and sudo map <IP address>**

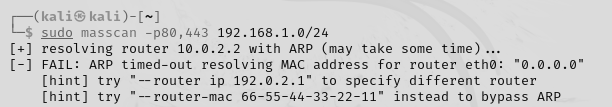


Step 3: This command will display all the posts which are open in that IP address and these are used to attack that system

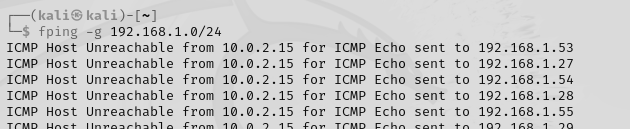


**Network Scanning and Reconnaissance Tools**

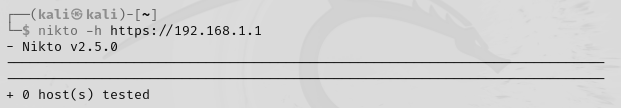
1. Masscan  
    **sudo masscan -p80,443 192.168.1.0/24**



1. Fping   
    **fping -g 192.168.1.0/24**

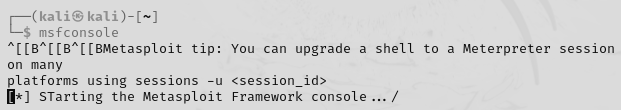


3. Nikto   
  **nikto -h** [**http://192.168.1.1**](http://192.168.1.1)



4. Metasploit (msfconsole)

**msfconsole**



**RESULT:**