Assignment 7

Title: Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc.

Theory:

1. **whois**
    a. sudo apt install whois
    b. whois 172.16.182.54 or
       whois wikipedia.com
2. **Perform host discovery using Angry IP**
    a. Install Angry IP from here https://angryip.org/download/#linux (Package for *Ubuntu/Debian/Mint*)
    b. cd Downloads
    c. ls
    d. this should get displayed- ipscan_3.9.1_amd64.deb
    e. dpkg -i ipscan_3.9.1_amd64.deb
    f. Open Angry IP and click on start button by selecting the range of IPs

3. **Network Scanning**
    a. Scan a Target Network using Metasploit
        i. Open metasploit and type search portscan
        ii. use the auxiliary/scanner/portscan/syn
            set INTERFACE eth0
            set PORTS 80
            set RHOSTS 10.10.1.5-23
            set THREADS 50
        iii. run
            Now, we will perform a TCP scan for open ports on the target systems.

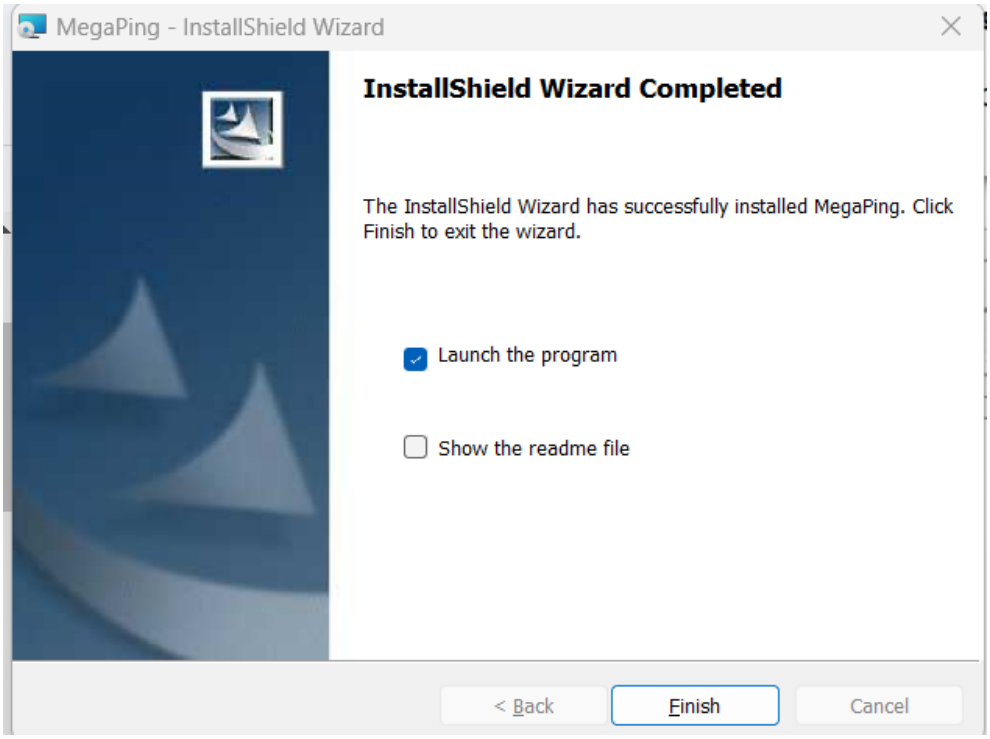
            To load the auxiliary/scanner/portscan/tcp module, type use auxiliary/scanner/portscan/tcp and press Enter.
        iv. set RHOSTS [Target IP Address (who's ports are open)]
        v. run
        vi. displaying all open TCP ports in the target IP address

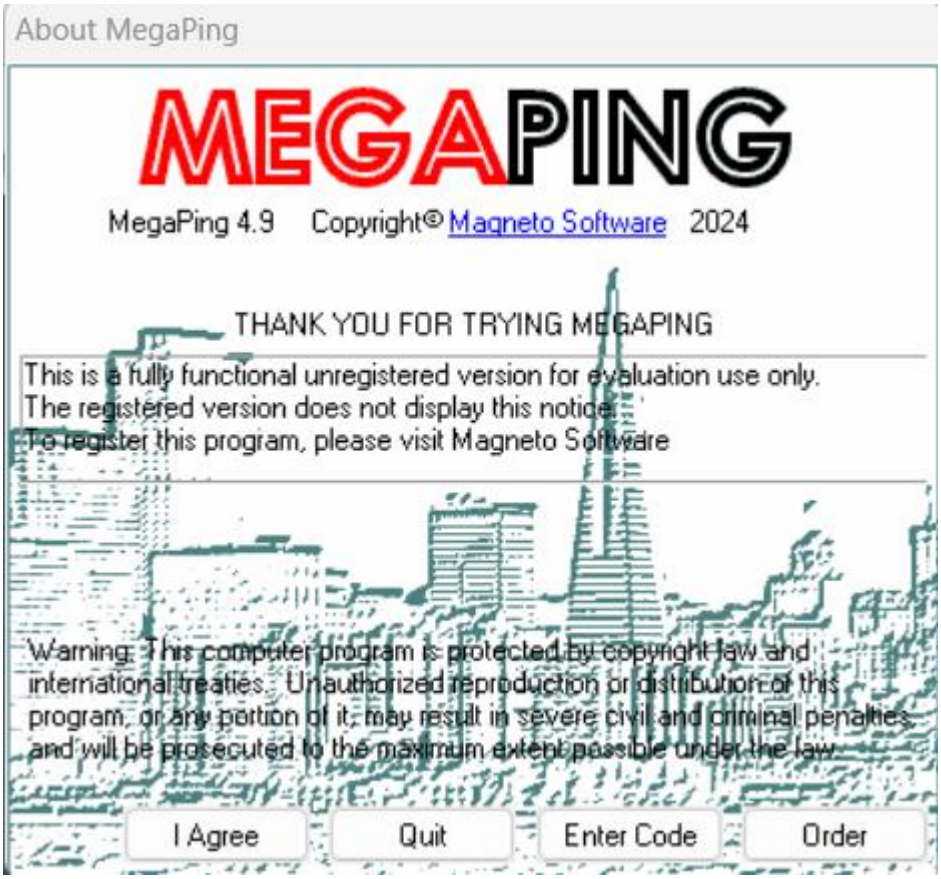
4. **Port scanning**

    a. Perform port and service discovery using MegaPing

i. download the setup for **windows** from https://megaping.informer.com/download/#downloading

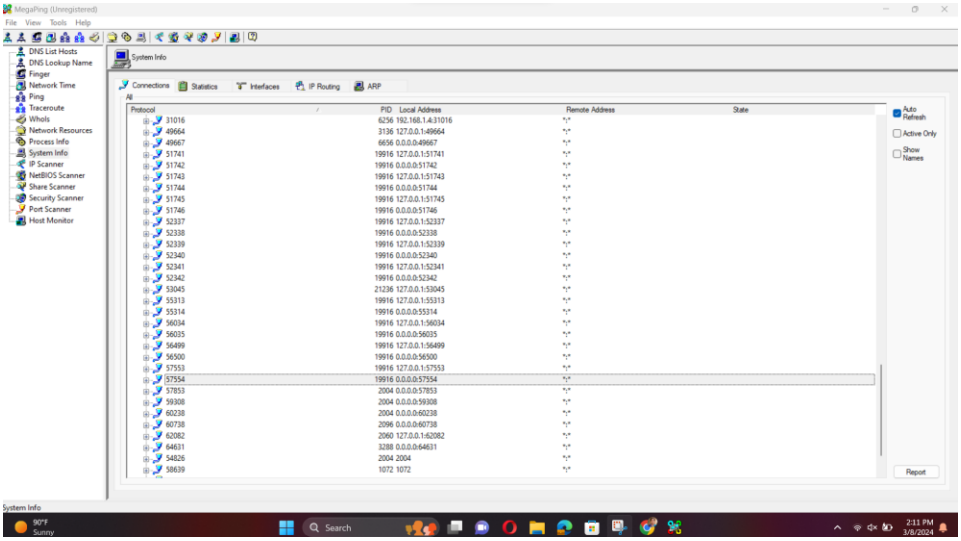
ii.





iii. select I Agree

iv. The MegaPing (Unregistered) GUI appears displaying the System Info, as shown in the screenshot.



v. Select the IP Scanner option from the left pane. In the IP Scanner tab in the right-hand pane, enter the IP range in the From and To fields; in this lab, the IP range is 172.16.182.1 TO 172.16.182.25; then, click Start

vi. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot

vii. . Select the Port Scanner option from the left-hand pane. In the Port Scanner tab in the right-hand pane, enter the IP address of the (172.16.182.54) machine into the Destination Address List field and click Add.

viii. Select the 172.16.182.54 checkbox and click the Start button to start listening to the traffic on 172.16.182.54.

viii. MegaPing lists the ports associated (172.16.182.54), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot. Using this information attackers can penetrate the target network and compromise it, to launch attacks.

b. Perform port and service discovery using NetScanTools Pro

i. download the setup for **windows nstp11demo.exe (http://e.informer.com/netscantools.com/nstpromain.html)**

ii. complete the setup and start demo version, click the **Start NetScanTools Pro Demo...** button.

iii.under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option,

iv. select **Ping Scanner and Use Default System DNS. enter start IP and end IP**

iv. select I accept. and check the result on browser

Conclusion:

FAQs

1. **What is an angry IP scanner?**
2. **What is dpkg? explain the purpose of it.**
3. **ENlist the various Port scanning tools.**

4. **What are the various modules provided by metasploit?**