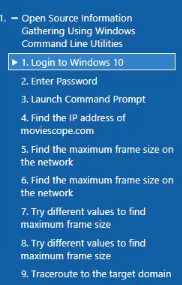
**[Footprinting and Reconnaissance](https://iclass.eccouncil.org/lessons/module-02-footprinting-reconnaissance/)**

Identify maximum frame size



Collect information about a website using Firebug

Mirroring using HTTPTrack website tracker

Adnvaced network route tracing using path analyser pro

Information gathering using Metasploit

Service postgresql start

Msfdb init

Service postgresql restart

Msfconsole

Db\_status

Nmap -Pn -sS -A -oX Test 10.10.10.0/24 – **ping sweep on the subnet**

Db\_import test

Hosts

Db\_nmap -sS -A 10.10.10.16 – Identify the **Services running**

Services – displays the services

**SMB scan**

Use scanner/smb/smb\_version

Show options

Set RHOSTS 10.10.8.16

Set THREADS 100

Run

Hosts

[**Scanning Networks**](https://iclass.eccouncil.org/lessons/module-03-scanning-networks/)

UDP and TCP packet cracking techniques using HPING3

Wireshark -> double ethernet adapter

Hping3 -c 3 10.10.10.10

**Scan parameter defines the port reange to scan -S represent -SYN flag set**

Hping3 –scan 1-3000 -S 10.10.10.10

**UDP scan**

Hping3 10.10.10.10 –udp –rand-source –data 500

TCP SYN request

Hping3 -S 10.10.10.10 -p 80 -c 5

Flooding request

Hping3 10.10.10.10 –flood

**Scanning the network using the coalsoft packet builder**

Select adapter

Add->ARP packet

Send->Send ALL tickt Burst Mode

Export\_>all packet .cap file save

Open it in wireshark

**MegaPing**

**Network scanning using NMap**

ZenMap -> IntenseScan

Command: nmap -O 10.10.10.\*

Trace all packets: nmap –packet-trace 10.10.10.10

Slow comprehensive scan:

Null Scan:

**Network scanning using NMap**

TCP scan:

Nmapt -sT -T3 -A 10.10.10.12

Xmas scan:

Turn on fire wall on windos macine

From Kali:

Nmap -sX -T4 10.10.10.12 – aggressive timing -T4 all 1000 ports open

Turn off fire wall

Nmap -sX -T4 10.10.10.12 – all ports closed.

ACK Scan:

Nmap -sA -v -T4 10.10.10.12

IDLE Scan

Nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12

Ping Seep

Nmap -sP 10.10.10.\* - show any live subsystem.

Scanning using NetScanTool Pro:

**Avoid scanning detection using Mulitiple decoy ip addresses**

Nmap -mtu 8 10.10.10.10

Decoying ip address

Nmap -D RND:10 10.10.10.10

**Drawing diagrams using network topology mapper**

**Checking live system using angry ip scanner**

**Identify target system OS with TTL and TCP window size using wireshark**

Launch wiresharp in the system

Login in windows 10

Comandprompt:

Ping 10.10.10.16

[**Enumeration**](https://iclass.eccouncil.org/lessons/module-04-enumeration/)

NetBIOS enumeration suing global netwok inventory

Enumerating resouces using advanced IP Scannner

Network enumeration using SuperScan

Enumeration of local macine suing Hyena