02-ABSENT

For Windows-GUI

Zenmap GUI

For Linux

nmap
---
netdiscover
--> List of IP address and Mac address in my network.

What is Nmap?
--> Network Mapper

When to Use NMAP?
--> All the Services Server/Mobile/PC/Swtich/Router

--> Versions of Services

--> OS Information

--> Audit Security (NSE)

--> GUI-Zenmap

Basic Commands for testing scanme.nmap.org
1. Scan for Single Host

==> nmap xavier.ac.in (ICMP Packets)

2. Version of Services

==> nmap -sV xavier.ac.in

3. Stealth Scan

==> nmap -sS xavier.ac.in (SYN packet)

4. Aggressive Scan

==> nmap -A scanme.nmap.org

5. Multiple Host

==> nmap 192.168.0.1/24
==> nmap 192.168.0.1 192.168.0.12 192.168.0.15
==> nmap -iL /root/Desktop/ip.txt

6. Port Scanning

==> nmap -p portno xavier.ac.in

==> nmap -p 75-225 xavier.ac.in

==> nmap -p T:225,85 xavier.ac.in

7. Zenmap GUI Commands

==> nmap -Pn --script vuln xavier.ac.in