**1.Install Nmap from official website.**

I use kali linux, where nmap is a built-in one and effective.

**2. Find your local IP range (e.g., 192.168.1.0/24).**

My IP address is 10.0.2.15

A computer screen shot of a program

AI-generated content may be incorrect.

**3. Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.**

Sleath scan or half tcp scan is used to find the open ports which are vulnerable to the exploitation.

Nmap -sS 192.168.0.1/24

A screenshot of a computer program

AI-generated content may be incorrect.

**4.Note down IP addresses and open ports found**

IP ADDRESS: 192.168.1.0/24

22/tcp ssh

23/tcp telnet

53/tcp domain

80/tcp http

**5.Optionaly analyze packet capture with Wireshark.**

A screenshot of a computer

AI-generated content may be incorrect.

**6.Research common services running on those ports.**

A computer screen with white text

AI-generated content may be incorrect.

A computer screen shot of a number

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

**7.Identify potential security risks from open ports.**

Port 22, commonly used for SSH ----- brute-force attacks, man-in-the-middle attacks, and potential compromise of sensitive data

Port 23, commonly used by telnet ---- security risks due to its use of unencrypted communication.

Port 53, used by DNS----DNS hijacking, spoofing, tunneling, and DDoS attacks

Port 80, used by HTTP------data interception, man-in-the-middle attacks, and other exploits where attackers can eavesdrop on or manipulate data in transit.