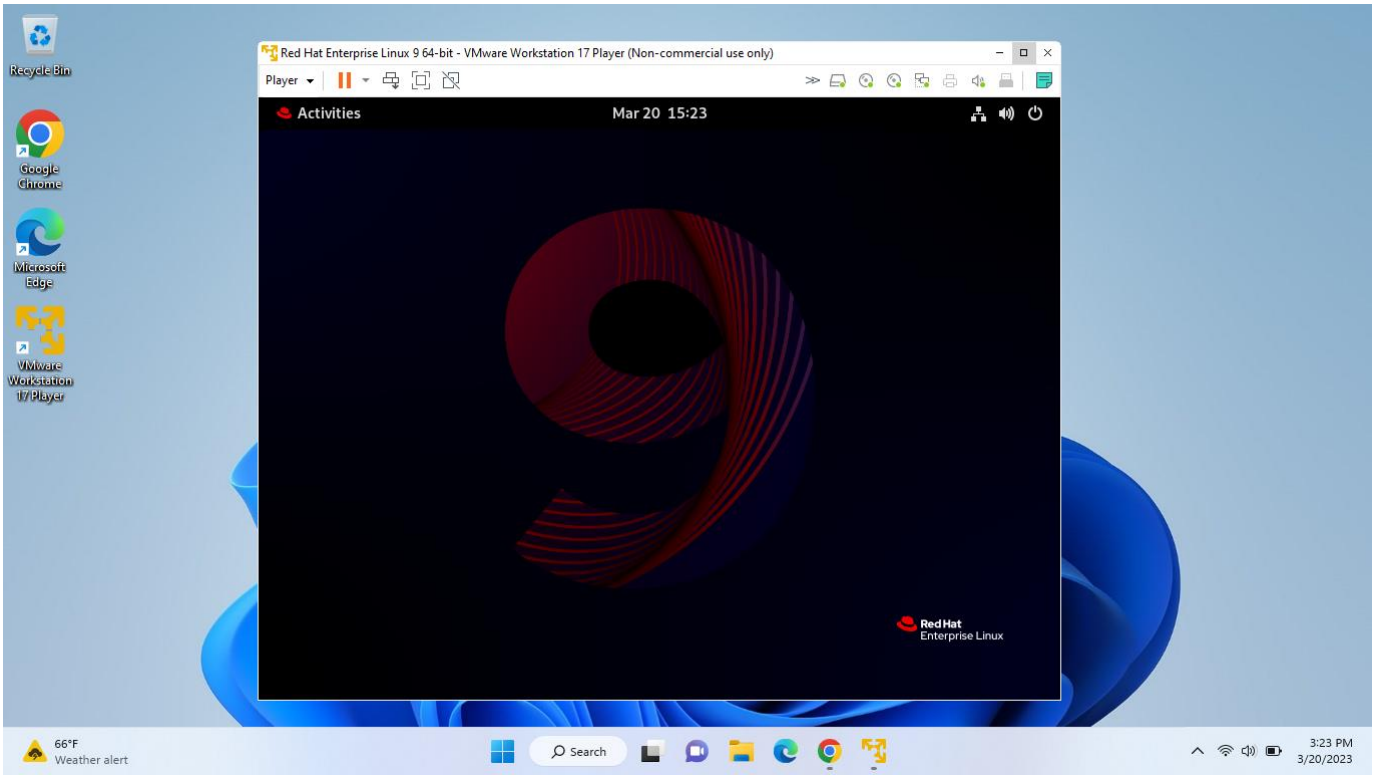
Question No. 3→ As a network administrator, briefly what techniques, tools and methodologies would follow to perform testing on the following (any software).

1. Network Devices Security
2. Physical Security

Solution→ As a network administrator, I am using “Red Hat Linux” as operating system for getting output like what techniques, tools and methodologies going to use for testing.

Firstly, I downloaded and installed Red Hat Linux



Network Devices Security→

1. Vulnerability scanning: Use open source vulnerability scanning tools like OpenVAS or Nessus to scan the network devices and identify any vulnerabilities.

Open Source Website and Application Vulnerability Scanners:

i. OSV-Scanner – Best Open Source Code Scanner
ii. Wapiti – Best for SQLi Testing
iii. ZAP (OWASP Zed Attack Proxy) – Best for XSS Testing

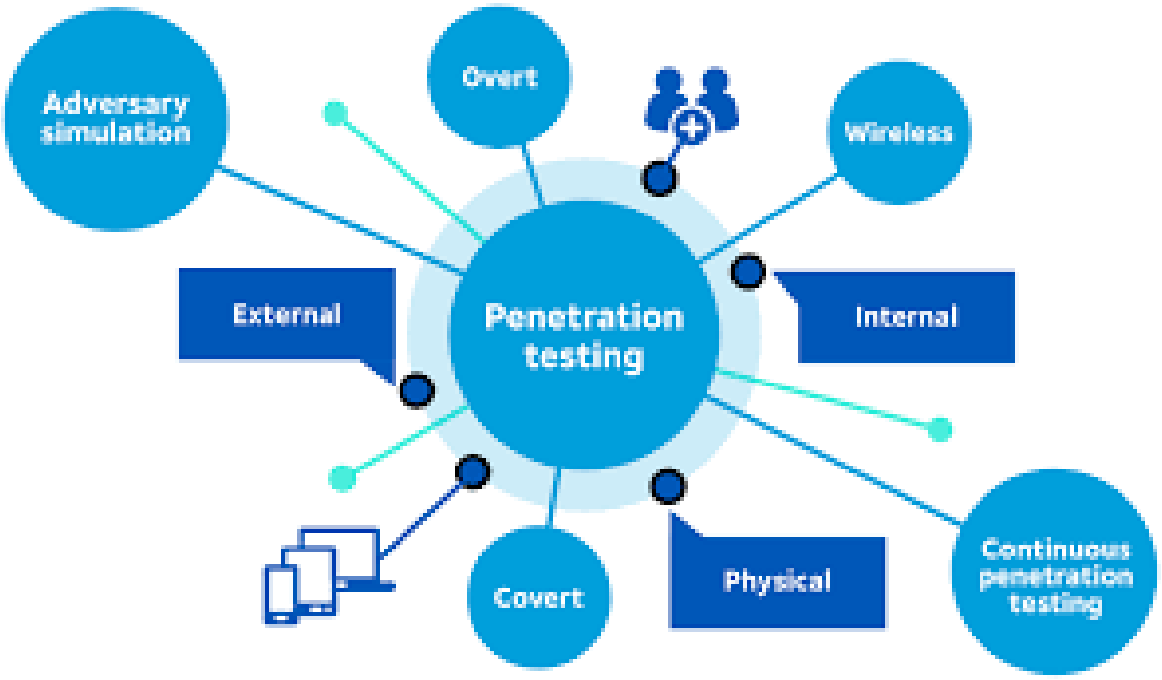
Open Source Infrastructure Vulnerability Scanners:

iv. CloudSploit – Best Cloud Resource Scanner
v. Firmwalker – Best for IoT Scanning
vi. Nikto2 – Best Web Server Scanner
vii. OpenSCAP – Best for Compliance-Focused Scanning
viii. OpenVAS – Best for Endpoint and Network Scanning
ix. Nmap – Best for Network and Port Scanning

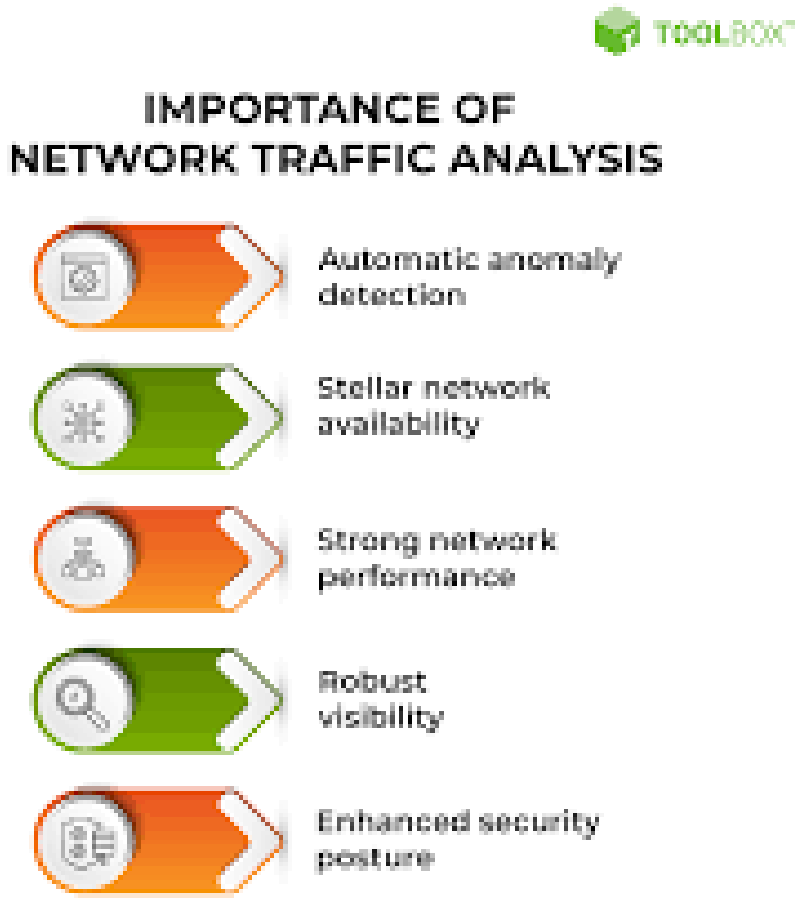
2. Penetration testing: Conduct penetration testing using open source tools such as Metasploit or Nmap to identify weaknesses in the network devices.

   Some tools name-

   i. Nmap
   ii. Wireshark
   iii. Jok3r
   iv. Zed Attack Proxy
   v. Nikto2
   vi. OpenSCAP
   vii. Scapy
   viii. CrackStation
   ix. Legion
   x. Aircrack-ng
   xi. Sqlmap

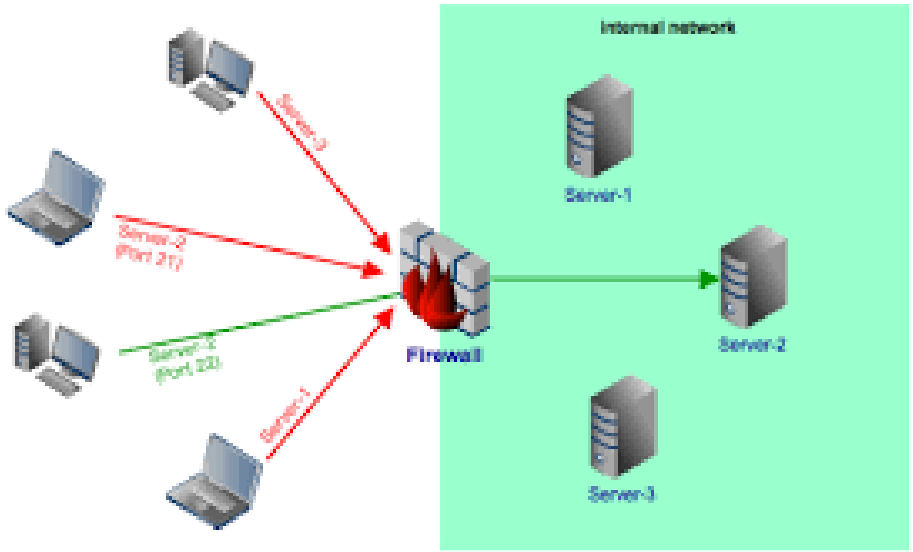


3. Network traffic analysis: Analyze network traffic using tools such as Wireshark to identify any malicious or suspicious activity.



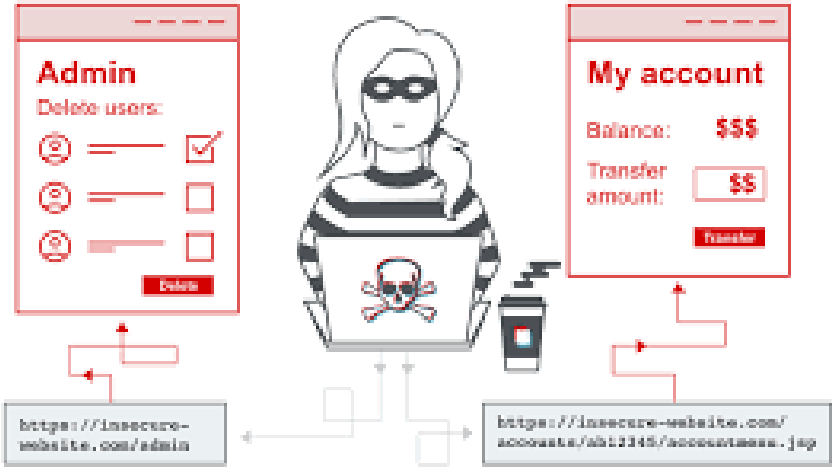
4. Configuration analysis: Use tools such as CIS-CAT to analyze the configuration of network devices against established security benchmarks. The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cyber security experts globally to help you protect your systems against threats more confidently.

5. Firewall testing: Test the firewall rules and policies using tools such as Firewall Test and Audit Script (Fwtest) to identify any gaps or misconfigurations.



Physical security testing→

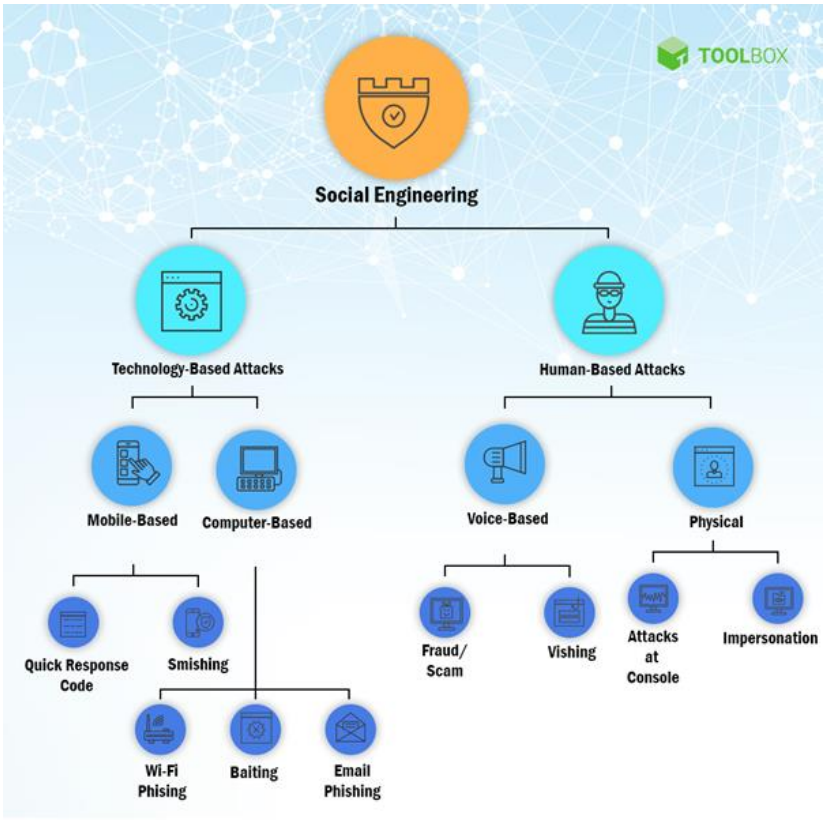
1. Access control testing: Conduct access control testing by attempting to gain unauthorized access to restricted areas and equipment.



2. CCTV testing: Test the coverage and quality of CCTV cameras using open source tools such as ZoneMinder.

3. Lock picking: Test the physical security of locks and doors by attempting to pick locks and bypass doors.

4. Social engineering: Conduct social engineering tests to see if employees can be tricked into revealing sensitive information or granting unauthorized access.



5. Physical intrusion detection testing: Test the effectiveness of intrusion detection systems such as alarms and motion sensors by attempting to bypass or trigger them.