1. a) Illustrate **TWO (2)** penetration testing tools such as Packet Crafting Tools and Packet Sniffers. In addition, give an example for each of the penetration testing tool.

Password Crackers
- Password recovery tools
- use to crack or recover password
- Repeatedly make guesses to crack password
- Eg. John the Ripper, Rainbow Crack

Wireless Hacking Tools
- Used to hack into a wireless network to detect security vulnerabilities
- Eg. Aircrack-ng, Kismet

Network Scanning and Hacking Tools
- Used to probe network devices, servers and hosts for open TCP or UDP ports
- Eg. Nmap, SuperScan

Packet Crafting Tools
- Used to probe and test a firewall's robustness using specially crafted forged packets.
- Eg. Hping, Scapy, Socat

Packet Sniffers
- Used to capture and analyze packets within traditional Ethernet LANs or WLANs
- Eg. Wireshark, Ettercap

b) Differentiate Shoulder surfing and Dumpster diving in social engineering attacks.

Shoulder surfing
- Threat actor inconspicuously looks over someone's shoulder to steal their password or other information

Dumpster
- Threat actor rummages through trash bins to discover confidential documents

2. Differentiate Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA).

Cisco Email Security Appliance (ESA)

- Special device designed to monitor Simple Mail Transfer Protocol (STPM).
- Updated by real-time feeds from the Cisco Talos.
- Threat intelligence data is pulled by the Cisco ESA every three to five minutes

Cisco Web Security Appliance (WSA)

- Mitigation Technology for web-based threats.
- Combines advanced malware protection, application visibility and control, acceptable use policy controls and reporting.
- Eg, Provide complete control over how users access the internet.

3. Illustrate the techniques used in IP attacks.

ICMP Attacks

- Used ICMP echo packets to discover subnets and hosts on a protected network
- To generate DoS flood attacks and alter host routing tables.

Amplification and Reflection Attacks

- Attempt to prevent legitimate users from accessing information or services using DoS and DDoS attacks.

Address Spoofing Attacks

- Spoof the source IP address in an IP packet to perform blind spoofing or non-blind spoofing

Man-in-the-Middle Attack (MITM)

- Position between a source and destination to transparently monitor, capture and control the communication.

Session Hijacking

- Gain access to the physical network, and then use an MITM attack to hijack a session.

4. Explain **THREE (3)** different types of attack to an organization.

Data Modification Attack
- If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of sender or receiver.

IP Address Spoofing Attack
- Threat actors constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Sniffers
- An application or device that can read, monitor and capture network data exchanges and read network packets.
- If the organization's packets are not encrypted, a sniffer provides a full view of the data inside the packets.

5. Differentiate Adware, Spyware and Ransomware.

Adware
- Distributed by downloading online software
- Can display unsolicited advertising using pop-up web browser windows, new toolbars or unexpectedly redirect a webpage to a different website.

Spyware
- Similar with adware but used to gather information about the user and send to threat actors without the user 's consent.
- Can b e low threat, gathering browser data or high threat capturing personal and financial information.

Ransomware
- Denies a user access to their files by encrypting the files
- Then displaying a message demanding a ransom for the decryption key

6. Illustrate Reconnaissance Attacks, Access Attacks and DoS Attacks. In addition, give an example for each type of attack.

Reconnaissance Attacks

- Is information gathering
- Used to do unauthorised discovery and mapping of systems, services or vulnerabilities
- This attack precedes access attacks or DoS attacks.
- Eg. Run vulnerabilities scanner to identify ports to determine the type and version of the application and operating system.

Access Attacks

- Exploit known vulnerabilities in authentication services, FTP services and web services
- Purpose is to gain entry to web accounts, confidential databases and other sensitive information.
- Eg. Password Attacks which discover critical system passwords using various methods.

DoS Attacks

- Prevent normal use of a computer or network by valid users.
- Flood a computer or the entire network with traffic until a shutdown occurs because of overload.
- Eg. Overwhelming Quantity of traffic which sends an enormous quantity of data at a rate that the network, host or application cannot handle, causes transmission and response times to slow down.

7. Most organizations employ a defense-in-depth approach to security. It requires a combination of networking devices and services working together. Illustrate this approach.

- Require a combination of networking devices and services working together.
- Security devices and services implemented including VPN, ASA Firewall, IPS, ESA / WSA, AAA Server
- All network devices including the router and switches are hardened,
- Also secure data as it travels across various links or travel outside of the organization branch sites, telecommuter sites and partner sites.

8. a) Compare and contrast **TWO (2)** social engineering attacks. (4 marks)

Pretexing

- Threat actor pretends to need personal or financial data to confirm the identity of the recipient.

Phishing

- Threat actors sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.

b) Which of these two social engineering attacks is more commonly encountered among businesses? Include your reasons to support your answer. (4 marks)

- Phishing
- This is because businesses recently need to communicate with a lot of different organizations.
- This is an opportunity for threat actor to pretend to be a legitimate, or trusted source.

9. Network applications use TCP or UDP ports. Threat actors conduct port scans of targeted devices to discover the services they offer.
a) Illustrate TCP SYN Flood attack.

- Sends multiple SYN requests to a webserver.
- Web server replies with SYN-ACKs for each SYN request and waits to complete the three-way handshake.
- Threat actor does not respond to the SYN-ACKs and cause the valid user cannot access the web server because the server has too many half-opened TCP connections.

b) Explain UDP Flood attack.

- Uses tools like Unicorn or Low Orbit Ion Cannon.
- Send a flood of UDP packets, from a spoofed host to a server on the subnets.
- The program will sweep through all the known ports trying to find closed ports and cause the server to reply with an ICMP port unreachable message.

- The result is very similar to a DoS attack.