Cyber Security Fundamentals

Assignment 1:

Question: Encrypt the message "HELLO" using a Caesar cipher with a shift of 4. Then, decrypt the ciphertext "Jg qh iwtg" using the reverse shift.

Assignment 2:

Question: Use the openssl command-line tool to generate an RSA key pair (public and private key). Export the keys and display them in PEM format.

Operating System Security

Assignment 1:

Question: Create two user accounts in Linux. Create a file and set its permissions so that only one user can read and write to the file, and the other user has no access.

Assignment 2:

Question: Disable SSH root login on a Linux system and restart the SSH service. Verify that root login is disabled by attempting to log in as root remotely.

Network Security & VPNs

Assignment 1:

Question: Set up OpenVPN on a Linux machine. Connect to the VPN and verify your IP address before and after connecting, using curl ifconfig.me.

Assignment 2:

Question: Use nmap to scan a target machine for open ports. Identify the services running on at least 3 open ports and explain what they are used for.

Web Application Security

Assignment 1:

Question: Perform a SQL injection attack on a vulnerable web application (such as DVWA or OWASP Juice Shop) and extract information from the database.

Assignment 2:

Question: Perform a Cross-Site Scripting (XSS) attack on a vulnerable web application by injecting a JavaScript alert (<script>alert('XSS');</script>) into a form field.

Ethical Hacking & Penetration Testing

Assignment 1:

Question: Use whois to gather information about a domain name of your choice. Perform a nslookup query on the same domain to obtain its IP address and DNS information.

Assignment 2:

Question: Use the Metasploit Framework to exploit a known vulnerability on a virtual machine (such as the MS08-067 vulnerability in Windows XP). Document the exploitation steps.

Malware Analysis & Reverse Engineering

Assignment 1:

Question: Use the strings command to extract readable text from a given malware sample. Identify any URLs, IP addresses, or commands in the output.

Assignment 2:

Question: Set up a sandbox environment and run a malware sample. Use Process Monitor or a similar tool to monitor its behavior, including file system, registry, and network activities. Document the suspicious behavior.

Incident Response & Digital Forensics

Assignment 1:

Question: Simulate a security breach by creating and executing a malicious script on a Linux system. Create an audit log and track the script's activity, including any file changes.

Assignment 2:

Question: Analyze a system log file (e.g., /var/log/auth.log) to identify suspicious login attempts. Provide a report that includes the timestamps and IP addresses of the suspicious activity.

Cloud & IoT Security

Assignment 1:

Question: Set up a virtual machine in AWS, Azure, or Google Cloud and configure the firewall (security group) to allow only HTTP and SSH access. Verify that other ports are blocked.

Assignment 2:

Question: Connect two IoT devices (e.g., Raspberry Pi or ESP32) to a Wi-Fi network. Use Wireshark to capture network traffic and identify any unsecured communications between the devices.