**Week 6:  Capstone Network Security Project**

**Objective:**  Simulate a secure network environment with monitoring and defense.

**Task#05:** **Prepare and submit a final report: network configuration, test results, screenshots, and lessons learned.**

**Network Security Internship Module - Final Report**

**Name:** Muhammad Azhan Hassan  
**Duration:** 6 Weeks  
**Program:** Network Security Internship Module

**Week 1: Introduction to Networking & Network Security**

**Objective:** Understand basic network components, models, and security principles.

**Tasks Performed:**

* Defined key networking concepts including IP address, DNS, Subnetting, Router, Switch, Firewall.
* Summarized OSI and TCP/IP models with all layers and their functions.
* Executed ipconfig (Windows) or ifconfig (Linux) to view device configurations.
* Installed and used Wireshark to capture and analyze HTTP request traffic.
* Listed common network attacks such as DoS, ARP Spoofing, Phishing, MITM.

**Tools Used:** Wireshark, Terminal/Command Prompt

**Key Learnings:**

* Gained foundational understanding of network architecture.
* Understood the layered models and their practical significance.
* Learned about traffic monitoring using packet analyzers.

**Week 2: Network Commands & Tools**

**Objective:** Learn essential networking commands and tools.

**Tasks Performed:**

* Used ping, tracert/traceroute, netstat, nslookup for network diagnostics.
* Set up a basic LAN using virtual machines.
* Performed a port scan using Nmap and identified open ports.
* Researched and documented differences between stateful and stateless firewalls.

**Tools Used:** CMD/Terminal, Nmap, VMs

**Key Learnings:**

* Understood how to test network paths and troubleshoot using CLI tools.
* Identified open services and ports, and their relevance to security.
* Differentiated between firewall architectures.

**Week 3: Encryption, VPNs & Security Protocols**

**Objective:** Study encryption standards and secure communication protocols.

**Tasks Performed:**

* Explained symmetric vs asymmetric encryption with examples (AES & RSA).
* Installed and tested OpenVPN connection.
* Researched HTTPS, SSL/TLS, SSH, IPSec and their roles.
* Remotely connected to Linux server via SSH.
* Created and decoded encrypted messages using online tools.

**Tools Used:** OpenVPN, SSH, Web Tools

**Key Learnings:**

* Learned the importance of encryption for secure data transmission.
* Understood secure tunneling through VPNs and remote access.
* Applied encryption/decryption practically.

**Week 4: Firewalls, IDS, and IPS**

**Objective:** Set up and manage network defense mechanisms.

**Tasks Performed:**

* Created iptables rule to block specific ports on Linux VM.
* Installed and configured pfSense firewall.
* Set up and tested Snort IDS for alert capturing.
* Compared IDS/IPS tools and their advantages.
* Explained proxy vs reverse proxy with real-world examples.

**Tools Used:** iptables, pfSense, Snort

**Key Learnings:**

* Practically applied network perimeter security mechanisms.
* Differentiated roles of firewalls, IDS, and IPS.
* Understood traffic inspection and alerting processes.

**Week 5: Ethical Hacking Fundamentals**

**Objective:** Perform safe, simulated penetration tests.

**Tasks Performed:**

* Explored Kali Linux tools including Metasploit, Hydra, Nmap.
* Conducted a safe DoS simulation using Ping of Death.
* Performed SSH brute-force attempt using Hydra (lab-only).
* Ran Nikto to scan local web server for vulnerabilities.
* Documented legal and ethical guidelines in penetration testing.

**Tools Used:** Kali Linux, Metasploit, Hydra, Nikto

**Key Learnings:**

* Understood ethical boundaries in security testing.
* Gained hands-on with offensive tools for vulnerability scanning.
* Validated responsible testing techniques in controlled labs.

**Week 6: Capstone Network Security Project**

**Objective:** Simulate a secure network environment with monitoring and defense.

**Tasks Performed:**

* Designed a secure network topology using VLANs, IDS, VPN, firewall.
* Performed MITM attack simulation using Ettercap in isolated VM.
* Set up Syslog-ng for log monitoring.
* Wrote a full network security policy for a mock organization.

**Tools Used:** Ettercap, Syslog-ng, Diagramming Tools

**Key Learnings:**

* Understood real-world implementation of defense-in-depth.
* Validated log monitoring as key to incident response.
* Applied all concepts in an integrated network design.

**Screenshots:**

