CSCE 5585: Secure Network Design and Implementation project

Project Objectives and Project Structures, Technologies, and Tools

The main aim of this project is to design, implement, and evaluate a SECURE NETWORK using industry-based network security tools that encompasses security of the communications pathways of the network and the security of network devices and devices attached to the network, to create a secure network with firewalls, VPNs and IDS/IPS, to ensure both internal and external threats are mitigated. This project will be included pen-testing to assess the robustness of the design.

Technologies:

- **Network Design**
- **Firewall**
- **VPN**
- **IDS/IPS**
- **Testing Tools**: Nmap, Metasploit, Nessus, Wireshark

Expected Deliverables:

- Final network topology diagrams.
- Firewall, VPN, and IDS/IPS configurations.
- Penetration testing report.
- Complete documentation and presentation.

1. Set Up the Network Environment

Virtualized Lab (Recommended)

- **Tools**: VirtualBox, VMware, GNS3, or EVE-NG for network device virtualization.
- **Setup**:
    - Use virtualization tools to create virtual instances of routers, switches, firewalls (e.g., pfSense), and servers.
    - Simulate network segmentation using VLANs and virtual networks.
    - Create separate virtual machines (VMs) to act as internal servers (e.g., web, mail, database) and client devices.
    - Install virtualized security appliances (e.g., pfSense, Snort) to act as firewalls and intrusion detection systems.

2. Network Design and Segmentation

Step-by-Step:

1. **Create the Network Topology**:
   - Start by designing the logical network architecture.
   - Include essential components like internet access, internal network, DMZ, VPN access, and external connections.
   - Divide the network into segments:
     - **VLANs** for internal departments (e.g., Sales, HR, R&D).
     - **DMZ** for hosting public-facing services like web servers.
     - **Internal network** for sensitive systems such as databases.
2. **Configure VLANs**:
   - Implement VLANs on routers or Layer 3 switches.
   - Assign devices to specific VLANs to create segmentation (e.g., VLAN 10 for HR, VLAN 20 for Finance).
   - Ensure communication between VLANs is controlled via a router or Layer 3 switch.
3. **Update the Network Diagram**:
   - Document your design choices and show how each part of the network is segmented.

3. Configure the Firewall

Step-by-Step:

1. **Install the Firewall (e.g., pfSense)**:
   - Install pfSense as a virtual machine (VM) or on a dedicated device.
   - Assign interfaces (WAN, LAN, and DMZ) to the firewall.
2. **Create Firewall Rules**:
   - Define access control lists (ACLs) to control traffic flow between network segments.
     - Allow only required traffic (e.g., HTTP/HTTPS from DMZ to the internet, internal traffic between departments).
     - Block unnecessary or malicious traffic.
   - Enable logging for rule violations and suspicious traffic.
3. **Test the Firewall**:
   - Perform basic connectivity tests to ensure traffic is allowed or blocked as per the rules.
   - Use tools like **Nmap** to scan the firewall and test whether open ports are properly protected.

4. Implement VPN for Remote Access

Step-by-Step:

1. **Install a VPN Solution (e.g., OpenVPN)**:
   - Install OpenVPN on a dedicated server or integrate it into the firewall.
   - Configure server settings (e.g., certificates, encryption, and authentication).
2. **Set Up Client Access**:
   - Create VPN profiles for remote users and distribute configuration files.
   - Test client-to-site VPN connections to ensure remote users can securely access internal resources.
3. **Test the VPN**:
   - Ensure that VPN users can access internal network resources securely.
   - Check encryption protocols and verify that all data transmitted over the VPN is encrypted.

5. Configure IDS/IPS

Step-by-Step:

1. **Install IDS/IPS (e.g., Snort or Suricata)**:
   - Install the IDS/IPS on a dedicated VM or integrate it into the firewall (pfSense supports Snort as a plugin).
   - Configure network interfaces to monitor traffic.
2. **Set Detection Rules**:
   - Implement predefined rules to detect common attacks (e.g., DDoS, SQL injection, port scanning).
   - Customize rules based on the network’s specific needs (e.g., blocking unauthorized SSH access).
3. **Test IDS/IPS Functionality**:
   - Simulate attacks (e.g., using Metasploit or custom scripts) to test if the IDS/IPS detects and logs the threats.
   - Tune the system to reduce false positives and ensure accurate threat detection.

6. Testing and Security Assessment

Step-by-Step:

1. **Penetration Testing**:
   - Use tools like **Nmap** and **Metasploit** to scan for open ports, services, and vulnerabilities.
   - Test different attack vectors, such as cross-segment attacks or external threats.
2. **Security Validation**:
   - Verify that the firewall blocks unauthorized traffic.
   - Test VPN encryption by inspecting network traffic (e.g., using **Wireshark**).
   - Review IDS/IPS logs to ensure they correctly capture malicious activity.
3. **Risk Assessment**:
   - Identify any weaknesses in the network.
   - Propose mitigation strategies for discovered vulnerabilities.

7. Documentation and Final Presentation

Step-by-Step:

1. **Document the Network Setup**:
   - Write detailed documentation on the topology, configuration steps, and security controls.
   - Include diagrams and screenshots of configurations (e.g., firewall rules, IDS/IPS settings).
2. **Prepare a Presentation**:
   - Summarize the network design and security measures.
   - Present test results, including successful VPN connections, firewall logs, and detected threats by IDS/IPS.