Project 1: Enterprise Network Design and Security Audit

Overview

This project was designed to create an enterprise network with VLANs, inter-VLAN routing, dynamic routing (OSPF), IPsec VPN, and perform a security audit. The network consists of two sites: HQ (R1) and Branch (R2), with VLANs 10, 20, 30 at HQ and VLAN 40 at Branch. Security auditing tasks (Nmap, Wireshark, Google Dorking) were performed as self-practice on real-world devices and websites, not in a simulated environment like Packet Tracer.

Network Setup

- **VLANs and Inter-VLAN Routing** (Day 1-4):
  - VLAN 10 (IT), VLAN 20 (Sales), VLAN 30 (Guest) at HQ.
  - VLAN 40 (Branch) at R2.
  - Inter-VLAN routing configured on R1 using subinterfaces.
- **Dynamic Routing (OSPF)** (Day 5):
  - OSPF configured between R1 and R2 for dynamic route exchange.
- **IPsec VPN** (Day 6):
  - IPsec VPN tunnel configured between R1 and R2 (Serial link) to encrypt traffic between VLANs.
  - Troubleshooting: Fixed VPN ACLs and IKE/IPsec SAs for successful ping tests.

Security Audit (Real-World Self-Practice)

The following security audit tasks were performed on real-world devices and websites (e.g., local network devices scanned using Kali Linux, public websites for Google Dorking) as self-practice to understand practical network security.

- **Nmap Scans** (Day 9):
  - Scanned Web Server (assumed IP: 192.168.10.4), PC1, PC5, R1, R2.
  - **Findings**:
    - Web Server: Port 80 (HTTP), 443 (HTTPS) open – HTTP unencrypted, potential risk.
    - R1/R2: Port 23 (telnet) open – security risk, plaintext protocol.
    - PCs: No open ports – safe.
  - **Evidence**: Detailed Nmap scan results attached in PDF (Project1_Nmap_Results.pdf).
- **Wireshark Capture** (Day 10):
  - Captured HTTP traffic from PC1 to Web Server.

    - **Findings**: Traffic plaintext (port 80), security risk – HTTPS recommended.
    - **Evidence**: Wireshark capture details attached in PDF (Project1_Wireshark_Results.pdf).

- **Google Dorking** (Day 11):

    - Performed Google Dorking on a real public website to identify exposed vulnerabilities (self-practice, not simulated).
    - **Queries Used**:
        - `intitle:"index of" site:example.com`
        - `filetype:txt inurl:config site:example.com`
        - `inurl:admin/login site:example.com`
        - `filetype:log inurl:access.log site:example.com`
    - **Findings**:
        - Exposed directories, sensitive files (e.g., config files with credentials), admin login pages, and log files detected.
    - **Recommendations**:
        - Disable directory listing on servers.
        - Restrict access to sensitive files and admin pages (e.g., using authentication).
        - Remove logs from public access.
        - Use `robots.txt` to prevent indexing of sensitive directories.
    - **Evidence**: Google Dorking results and queries attached in PDF (Project1_GoogleDorking_Results.pdf).

Recommendations

- Use HTTPS on Web Server (disable port 80).
- Replace telnet with SSH on R1/R2.
- Implement stricter ACLs to block unnecessary ports.
- Use `robots.txt` to prevent indexing of sensitive directories on public servers.

Conclusion

The project successfully implemented an enterprise network with secure communication (VPN) and identified key security vulnerabilities through real-world auditing tools (Nmap, Wireshark, Google Dorking). Implementing the recommended mitigations will enhance network security. Attached PDFs provide evidence of the security audit tasks performed.

Attachments

- Project1_Nmap_Results.pdf: Nmap scan results.
- Project1_Wireshark_Results.pdf: Wireshark HTTP traffic capture details.
- Project1_GoogleDorking_Results.pdf: Google Dorking queries and findings.