**Lab 1: Practical Vulnerability Assessment for GRC Professionals**

**1. Introduction**

Welcome, GRC analysts. Your role transcends merely identifying technical flaws; it requires understanding their impact on organizational risk posture and compliance status. In this lab, you will act as an internal auditor conducting a technical assessment on a test system. Your primary deliverable will be a management-focused summary that translates technical findings into business risk and compliance terms.

**2. Scenario**

You have been tasked with performing a vulnerability assessment on a newly discovered test server (metasploitable) within the company's development environment. Your objective is to identify, classify, and report on vulnerabilities from a risk and compliance perspective, providing actionable insights for remediation.

**3. Objectives**

- Discover live hosts and identify open ports/services.
- Enumerate software versions and identify known vulnerabilities.
- Analyze findings and map them to common compliance frameworks (e.g., NIST, CIS, PCI DSS).
- Assess the risk level of each finding.
- Document your results in a structured, professional format, including visual reports.

**4. Lab Setup**

- **Your Machine:** Kali Linux (Attacker) - IP: 192.168.x.x
- **Target Machine:** Metasploitable (Victim) - IP: 192.168.x.y (Instructor will provide this)
- **Tools:** nmap, nikto, nuclei, xsltproc

**5. Step-by-Step Instructions**

**Phase 1: Discovery and Enumeration**

**Step 1: Network Discovery**

- **Task:** Confirm the target is alive and identify its IP address.
- **Command:**

ping -c 4 <TARGET_IP>

- **GRC Context:** This initial step is foundational for asset inventory management, a requirement in frameworks like **NIST CSF (ID.AM-1)** and **CIS Control 1**. You cannot protect or assess what you do not know exists.

**Step 2: Port and Service Enumeration with Nmap**

- **Task:** Perform a comprehensive scan to identify all open ports, services, and versions.

- **Command:**

nmap -sV -sC -O -p- <TARGET_IP>

  - -sV: Probe open ports to determine service/version info.
  - -sC: Run default Nmap scripts (safe for discovery).
  - -O: Enable OS detection.
  - -p-: Scan all 65,535 ports.

- **Action:**

1. **Save output in multiple formats** for comprehensive documentation and analysis:

nmap -sV -sC -O -p- -oA initial_scan <TARGET_IP>

This generates three files: initial_scan.nmap, initial_scan.gnmap, and initial_scan.xml.

2. **Generate an HTML report** for enhanced visualization and reporting:

xsltproc -o initial_scan_report.html /usr/share/nmap/nmap.xsl initial_scan.xml

Open initial_scan_report.html in your browser to review the formatted results.

- **GRC Question:** Why is knowing which ports are open (e.g., 21/FTP, 23/Telnet) a compliance issue? (Hint: Think about unnecessary services, attack surface reduction, and compliance with **CIS Control 9** and **NIST CSF PR.IP-1**).

**Phase 2: Vulnerability Identification**

**Step 3: Analyzing Nmap Output**

- **Task:** Review initial_scan.nmap and the HTML report. Identify:
  - Service versions (e.g., vsftpd 2.3.4).
  - Interesting script outputs (e.g., SSH host keys, HTTP headers).
  - Note every service and its version for further analysis.

**Step 4: Web Application Assessment**

- **Task:** Scan the web server for common vulnerabilities.
- **Command (Nikto):**

nikto -h http://<TARGET_IP> -o nikto_scan.txt

- **Action:**
  - Open http://<TARGET_IP> in Firefox and explore any applications (e.g., PHP, TWiki).
  - Manually inspect for obvious issues (e.g., default pages, verbose errors).

- **GRC Context:** Web applications are high-risk vectors. This aligns with **OWASP Top 10** and **PCI DSS Requirement 6**.

**Step 5: Focused Vulnerability Scanning**

- **Task:** Use Nuclei to scan for known vulnerabilities based on identified services.
- **Commands:**

# For web applications

nuclei -u http://<TARGET_IP> -o nuclei_web_scan.txt

# For all services

nuclei -target <TARGET_IP> -o nuclei_full_scan.txt

- **Review:** Nuclei output often includes CVE references and severity scores—crucial evidence for risk assessment.

**Phase 3: Analysis and Reporting (The Core GRC Task)**

**Step 6: Triage and Risk Assessment**
Create a risk assessment table summarizing key findings:

| Finding | Affected Service | CVE/Reference | Inherent Risk (L/M/H) | Compliance Violation | Business Impact |
|---|---|---|---|---|---|
| Weak Default Credentials | SSH, FTP | N/A | H | CIS 5.2, NIST CSF PR.AC-1 | Unauthorized access, data theft |
| vsFTPd 2.3.4 Backdoor | FTP | CVE-2011-2523 | H | CIS 7.1 (Patch Mgmt) | Full system compromise |
| Unencrypted Telnet Service | Telnet | N/A | H | NIST CSF PR.DS-2 | Credential sniffing, espionage |
| ... | ... | ... | ... | ... | ... |

- **Inherent Risk Criteria:**
  - ✓ **High (H):** Easy to exploit, leads to full system compromise.
  - ✓ **Medium (M):** Requires some skill, leads to data leakage.
  - ✓ **Low (L):** Information disclosure, low impact.

**Step 7: Drafting the Executive Summary**
Write a concise summary for management using non-technical language focused on risk and action:

**To:** IT Management
**From:** GRC Audit Team
**Date:** [Date]
**Subject:** High-Risk Findings on Development Server 'metasploitable'

**1. Executive Summary:**
A vulnerability assessment of the internal server revealed multiple critical security vulnerabilities that pose an immediate and high risk to the organization's information assets. The system is non-compliant with several key organizational policies based on the CIS Controls.

**2. Key Findings & Risks:**

- **Critical Risk - Remote System Compromise:** The FTP service contains a known backdoor (CVE-2011-2523) allowing attackers to gain full control without authentication. This violates our patch management policy (CIS Control 7.1).
- **High Risk - Data Interception:** Services (Telnet, FTP) transmit credentials in plaintext, violating data protection standards (NIST CSF PR.DS-2) and risking credential theft.
- **High Risk - Weak Authentication:** Default and weak passwords are in use, increasing the risk of unauthorized access (CIS 5.2).

**3. Recommended Actions:**

1. **Immediate Isolation:** Remove the server from the network until remediated.
2. **Remediate:** Apply security patches, especially for vsFTPd.
3. **Harden:** Disable unnecessary services (Telnet, Rlogin); enforce strong passwords.
4. **Process Review:** Reinforce procedures for deploying systems according to security baselines.

**6. Lab Conclusion**

You have successfully progressed from technical scanning to risk analysis a critical competency for GRC professionals. Remember, the value lies not in running tools but in interpreting results to drive business-focused risk decisions.

**7. Deliverables**

Submit the following:

1. Nmap output files (initial_scan.nmap, initial_scan.xml).
2. **Screenshot of the Nmap HTML report** (initial_scan_report.html).
3. Nikto and Nuclei scan outputs.
4. Completed Risk Assessment Table.
5. Executive Summary.