Capstone Project 3 Pitch Template

Capstone Project 3 Pitch
Target System: Metasploitable 3
Date: [07/29/2025]
Prepared By: [Alexander Focsha]

---

1. Business Problem Scenario

The organization is facing significant cybersecurity risks stemming from outdated software and unpatched vulnerabilities within their IT infrastructure. These vulnerabilities expose the organization to potential data breaches, unauthorized access, and service disruptions. For example, if a SQL injection vulnerability remains undiscovered, attackers could exploit it to access sensitive customer information, leading to significant compliance violations and legal repercussions, as well as loss of customer trust and financial damage.

The primary goal of my penetration test is to uncover vulnerabilities, test the efficacy of existing defenses, and assess the overall risk exposure of the organization's systems. The organization needs a penetration test to ensure that their systems are fortified against emerging threats and to validate the effectiveness of their security measures. The biggest risks we are concerned with include SQL injection vulnerabilities, cross-site scripting (XSS), and weak authentication protocols. Addressing these risks is crucial to maintaining operational integrity and protecting sensitive data.

2. Problem-Solving Process

My process will follow these main stages:

1. **Reconnaissance**: Conducting passive and active information gathering about the target system, including network structure, services, and potential entry points.
2. **Enumeration and Scanning**: Identifying open ports, services, and potential vulnerabilities using automated scanning tools to map the attack surface.
3. **Exploitation/Post-exploitation**: Attempting to exploit identified vulnerabilities to gain unauthorized access, assessing the impact, and determining the persistence of access.

Tools Planned:

- **Nmap**: For detailed network mapping and port scanning.
- **Metasploit**: For exploiting discovered vulnerabilities and post-exploitation analysis.
- **Burp Suite**: For web application testing and vulnerability discovery.

- **Custom Scripts**: To automate repetitive tasks such as port scanning and vulnerability detection.

How Custom Scripts Will Be Used: My custom port scanner will streamline the detection of open ports and services, providing quick feedback on the target's security posture. The web scanner will assist in identifying common web vulnerabilities like XSS and SQL injection, integrating seamlessly into my workflow to enhance efficiency and accuracy.

3. Timeline and Scope

Phase	Estimated Time	Notes
Reconnaissance	3 days	Initial testing and information gathering.
Scanning & Enumeration	5 days	Detailed scanning for vulnerabilities.
Exploitation	4 days	Attempting to exploit discovered vulnerabilities.
Script Development	3 days	Developing and testing custom automation scripts.
Report Writing	4 days	Drafting the penetration testing report, detailing findings and recommendations.
Critique and Updates	2 days	Incorporating peer feedback and making necessary updates.
Final Submission Prep	3 days	Polishing the final report and preparing the presentation.

I expect the first **3 days** to be focused on **Reconnaissance**, then move into **Scanning & Enumeration** for the next **5 days**. After the critique, I will update **vulnerabilities and findings** and finalize everything within the above time frames.

4. Deliverable Quality and Success Metrics

- **Port Scanner Success Metric 1:** The port scanner will be considered complete when it reliably detects open ports within the specified range without false negatives. **Port Scanner Success Metric 2:** It will handle unreachable hosts or timeouts gracefully, providing clear error messages.

- **Web Scanner Success Metric 1:** The web scanner will be deemed successful if it accurately detects reflected XSS payloads without returning false positives. **Web Scanner Success Metric 2:** It will identify SQL injection vulnerabilities accurately, ensuring that the output is actionable for remediation.
- **Penetration Test Report Success Metric 1:** The report will feature a Clear Findings Table, with an Executive Summary tailored for non-technical stakeholders, presenting the information in an accessible format. **Penetration Test Report Success Metric 2:** The report will have a logical structure, complete with actionable remediation recommendations for each identified vulnerability.
- **Overall Project Quality Goal:** All deliverables will be free of major errors, logically organized, and professionally formatted to meet industry standards, ensuring clarity and effectiveness in communication.