Network Asset Discovery and Web Enumeration Report

1. Executive Summary

This report documents the process of network reconnaissance, service enumeration, and basic web analysis performed on a target machine in a controlled lab environment. The objective was to identify active hosts, discover open ports, analyze exposed services, and detect potential information disclosure vulnerabilities.

During the assessment, an exposed web service was discovered that allowed unauthorized access to sensitive information. This finding highlights the importance of secure configuration and proper access control mechanisms.

---

2. Scope

The assessment focused on the following activities:

- Host discovery
- Port scanning
- Service and version enumeration
- Web structure analysis
- Identification of information leakage

The testing was conducted in a safe and legal lab environment.

---

3. Methodology

The following methodology was applied:

3.1 Host Discovery

The first step was identifying active hosts on the network using network scanning techniques. This helped confirm that the target system was online and reachable.

3.2 Port Scanning and OS Detection

A full port scan was performed to detect open ports and potential services. Operating system fingerprinting was also conducted to gather additional system information.

3.3 Service Enumeration

After identifying open ports, service and version enumeration was performed to understand the technologies running on the system.

3.4 Web Enumeration

Directory and file brute-forcing techniques were used to discover hidden or unlisted web pages.

---

4. Tools Used

The following tools were used during the assessment:

- Nmap – Network scanning and service enumeration
- Gobuster – Web directory brute-force
- Curl – Web response analysis

---

5. Findings

5.1 Exposed Web Page

A hidden web page was discovered during directory enumeration.

This page contained sensitive information embedded in the HTML source code.

5.2 Information Disclosure Vulnerability

The analysis of the web response revealed a sensitive token exposed in the page source:

THM{SECRET_PAGE_38B9P6}

This represents an **information disclosure vulnerability**, as sensitive data was accessible without authentication.

---

6. Impact

The exposure of sensitive information can lead to:

- Unauthorized access to internal systems
- Credential or token leakage
- Increased risk of further exploitation
- Loss of confidentiality

Even in a simple lab environment, this scenario reflects real-world security risks.

---

7. Recommendations

The following security improvements are recommended:

- Remove sensitive data from client-side code
- Implement authentication and authorization controls
- Use secure coding practices
- Perform regular security assessments
- Monitor logs and suspicious activity
- Conduct periodic vulnerability scanning

---

8. Conclusion

This project demonstrates the importance of reconnaissance and web enumeration in identifying security weaknesses. Even basic testing techniques can uncover critical vulnerabilities such as information disclosure.

The results reinforce the need for secure system configuration, proper access control, and continuous monitoring to protect sensitive data.

---

9. Author

Caique – Cybersecurity Student
Focused on Blue Team, SOC, and Defensive Security