

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) REPORT

1. Executive Summary

A Vulnerability Assessment and Penetration Testing (VAPT) exercise was conducted on a target system within a controlled internal laboratory environment. The objective of this engagement was to identify security weaknesses, validate their exploitability, and assess the overall risk posed to the system if such vulnerabilities were exploited by a real-world attacker.

The assessment revealed the presence of multiple critical security flaws across exposed network services. Several of these vulnerabilities were successfully exploited, resulting in complete system compromise with root-level privileges. The ability to gain administrative access through multiple independent attack paths highlights a severe lack of security hardening and defense-in-depth controls.

The findings demonstrate that an attacker with basic technical knowledge could fully compromise the system, access sensitive information, and potentially pivot to other systems within the network. Immediate remediation is strongly recommended to mitigate the identified risks and improve the system's security posture.

2. Scope of Assessment

- **Target System:** Metasploitable2
- **Environment:** Internal laboratory setup
- **Assessment Type:** Network-based Vulnerability Assessment and Penetration Testing
- **Scope Included:**
 - Network service discovery
 - Service enumeration and version detection
 - Exploitation of identified vulnerabilities
 - Privilege validation and exploit chaining

- **Out of Scope:**
 - Denial-of-Service (DoS) testing
 - Physical security testing
 - Social engineering attacks

3. Methodology

The assessment followed a structured and systematic penetration testing methodology aligned with common industry practices. The process was divided into the following phases:

1. **Reconnaissance:** Identification of live hosts within the target network.
2. **Enumeration:** Detection of exposed services and identification of service versions.
3. **Vulnerability Identification:** Mapping discovered services to known weaknesses.
4. **Exploitation:** Validation of vulnerabilities through controlled exploitation.
5. **Exploit Chaining:** Verification of multiple attack paths leading to full compromise.
6. **Reporting:** Documentation of findings, impact, and remediation recommendations.

This methodology ensured that vulnerabilities were not only identified but also validated for real-world impact.

4. Attack Narrative

Network reconnaissance was conducted to identify active hosts and exposed services within the target environment. The target system was discovered to be running multiple insecure and outdated network services that significantly increased its attack surface. During service enumeration, an FTP service running an outdated version was identified as a high-risk entry point.

The vulnerable FTP service was successfully exploited, resulting in remote command execution on the target system. This exploitation immediately provided root-level access, indicating a critical failure in access controls and service hardening. After achieving initial compromise, further enumeration of the system revealed the presence of an exposed bind shell service running on the target host.

A direct connection to this bind shell allowed immediate root access without requiring any authentication. The existence of multiple independent attack paths confirmed that the system could be compromised in more than one way, demonstrating a complete breakdown of security controls. The attack chain resulted in full system compromise with unrestricted administrative privileges.

5. Technical Findings

Finding 1: Vulnerable FTP Service

- **Service:** FTP
- **Port:** 21/TCP

Description:

The target system was running an outdated and vulnerable FTP service. This service contained a known weakness that allowed remote attackers to execute arbitrary commands on the system.

Impact:

Successful exploitation resulted in immediate root-level access, allowing full control of the system.

Finding 2: Exposed Bind Shell

- **Service:** Bind Shell
- **Port:** 1524/TCP

Description:

An unauthenticated bind shell was exposed on the target system. This service allowed any remote user to connect directly and obtain a root shell without authentication.

Impact:

This vulnerability enabled instant administrative access and significantly increased the risk of unauthorized system takeover.

6. Impact Analysis

The successful exploitation of multiple vulnerabilities resulted in full compromise of the target system with root-level privileges. An attacker could gain unrestricted control over the operating system, access sensitive configuration files, extract credentials, and manipulate system processes. The presence of unauthenticated root shells allows immediate system takeover without requiring advanced skills or credentials.

Additionally, a compromised system could be used as a pivot point to attack other systems within the internal network. This increases the risk of lateral movement, data breaches, and long-term persistence. The overall impact of these vulnerabilities is classified as **Critical**, affecting confidentiality, integrity, and availability.

7. Remediation Recommendations

Immediate action is required to reduce the risk posed by the identified vulnerabilities. Vulnerable and unnecessary services should be disabled or removed from the system. The FTP service should be updated to a secure and supported version or replaced with a more secure alternative. All exposed bind shell services must be disabled to prevent unauthorized access.

Regular patch management processes should be implemented to ensure timely updates of operating systems and applications. Network-level security controls such as firewalls should be configured to restrict access to critical services. Applying the principle of least privilege, along with continuous monitoring and logging, will significantly improve the system's security posture.

8. Evidence Summary

Evidence ID	Description
E1	Network discovery identifying the target system
E2	Service enumeration results
E3	Successful exploitation of FTP service
E4	Root privilege confirmation
E5	Bind shell access
E6	Root privilege verification

9. Conclusion

The VAPT assessment identified multiple critical vulnerabilities that allowed complete system compromise through multiple attack paths. The lack of service hardening, outdated software, and exposed administrative access mechanisms represents a severe security risk. Without remediation, the system remains highly vulnerable to real-world attacks. Immediate corrective actions and continuous security improvements are strongly recommended.