Task 6 Report: Full VAPT Engagement

Target: Metasploitable2 Linux VM (192.168.56.104)

Executive Summary

A full-scale penetration test was conducted against the Metasploitable2 lab environment. The assessment revealed multiple critical vulnerabilities, with the most immediate being a backdoor in the UnrealIRCd service (version 3.2.8.1). This vulnerability was successfully exploited to gain unauthorized root access to the system within minutes of initial reconnaissance. The target environment exhibited numerous security failures including outdated software, default credentials, and insufficient network hardening.

PTES Phase Log

Target IP	Vulnerability	PTES Phase
192.168.56.104	UnrealIRCd 3.2.8.1 Backdoor	Exploitation
192.168.56.104	Privilege Escalation	Post-Exploitation

Technical Findings

1. Reconnaissance Results

Network scanning revealed numerous exposed services including FTP, SSH, Samba, and UnrealIRCd running on outdated versions with known vulnerabilities.
Evidence: `14_Nmap_Scan_Results.png` showing service enumeration.

2. Vulnerability Analysis

The UnrealIRCd service (port 6667) was identified as running version 3.2.8.1, which contains a documented backdoor (CVE-2010-2075) allowing unauthenticated remote command execution.

3. Exploitation

The Metasploit Framework was used to exploit the UnrealIRCd backdoor vulnerability, resulting in immediate root-level access to the target system.
Evidence: `15_UnrealIRCd_Backdoor_Success.png` showing successful exploitation and root shell access.

4. Post-Exploitation

With root access obtained, comprehensive system reconnaissance was conducted, revealing multiple additional security misconfigurations including world-writable directories, SUID misconfigurations, and stored plaintext credentials.

Attack Timeline

1. Information Gathering: Nmap scanning identified vulnerable services
2. Vulnerability Mapping: UnrealIRCd backdoor selected as primary attack vector
3. Weaponization: Metasploit exploit configured for target environment
4. Exploitation: Backdoor exploited granting immediate root access
5. Post-Exploitation: System reconnaissance and data collection
6. Reporting: Documentation of findings and remediation recommendations

Remediation Plan

1. Immediate Action: Remove and reinstall all compromised software from verified sources
2. Patch Management: Establish regular security updates for all system software
3. Service Hardening: Disable unnecessary services and implement proper service configuration
4. Network Segmentation: Isolate lab systems from production networks
5. Access Controls: Implement principle of least privilege for all system accounts
6. Monitoring: Deploy intrusion detection systems to identify exploitation attempts

Non-Technical Summary

Our security assessment revealed that the test system contained severely vulnerable software that allowed complete compromise within minutes. The most critical issue was a hidden backdoor in the chat service that provided attackers with full administrative control. We recommend immediately removing the affected software and replacing it with trusted versions. Additionally, we advise implementing network segmentation to prevent lateral movement and establishing regular security updates to address vulnerabilities promptly. These measures are essential to prevent actual attackers from gaining unauthorized access to sensitive systems and data.