Target: Metasploitable2 Linux VM (192.168.56.104)

Executive Summary

A full penetration test was conducted against the Metasploitable2 lab environment. The assessment began with service discovery and vulnerability scanning, which identified numerous exposed services. A critical remote code execution vulnerability was successfully exploited, leading to the complete compromise of the target and acquisition of root-level access. The system was found to be in a critically vulnerable state due to outdated software and malicious backdoors.

PTES Phase Log

Timestamp	Target IP	Vulnerability	PTES Phase
[Date]	192.168.56.104	Service Discovery	Intelligence Gathering
[Date]	192.168.56.104	UnrealIRCd Backdoor Exploitation	Exploitation

1. Intelligence Gathering & Vulnerability Analysis

Initial reconnaissance identified the target host and revealed a wide range of potentially vulnerable services, including FTP, Samba, IRC, and HTTP. The presence of the UnrealIRCd service on port 6667 was identified as a high-priority target due to a known backdoor vulnerability (CVE-2010-2075).

Evidence: `18_Nmap_Scan_Results.png`

2. Exploitation

The UnrealIRCd backdoor vulnerability was successfully exploited using the Metasploit Framework. This backdoor allowed unauthenticated command execution, providing immediate root-level access to the target system.

Evidence: `19_Exploit_Success.png`

3. Findings and Recommendations

Critical Vulnerability Summary

Finding ID	Vulnerability	CVSS Score	Remediation
F005	**UnrealIRCd 3.2.8.1 Backdoor**	**10.0 (Critical)**	**1. Immediately remove UnrealIRCd service 2. Verify software checksums before installation 3. Implement network segmentation**

Remediation Plan

1. Immediate Action: Remove the UnrealIRCd service from all affected systems
2. Software Assurance: Establish policy to only download software from official sources and verify checksums
3. Network Security: Implement firewall rules to restrict unnecessary service exposure
4. Patch Management: Establish regular vulnerability scanning and patch management procedures

4. Non-Technical Summary

Our security assessment revealed that the test server contained severely vulnerable software with a hidden backdoor. This vulnerability allowed complete takeover of the system within seconds, providing attackers with full access to all data and functionality. We recommend immediately removing the affected software and implementing stricter software verification processes to prevent similar issues in the future. This critical finding requires immediate attention to prevent certain system compromise.

Appendix: Screenshot Evidence

- `18_Nmap_Scan_Results.png`: Service discovery and vulnerability identification
- `19_Exploit_Success.png`: Successful exploitation and root access achieved

Distribution: Security Team, System Administrators, IT Management