[LOCKED] Final Security Hardening Report - Week 4

System Assessed: Metasploitable2

Security Auditor: Subramaniam B

Date: 20/04/2025

[OBJECTIVE] Objective

To fortify the Metasploitable2 system by mitigating identified vulnerabilities and implementing security best practices, followed by auditing and validation to ensure the effectiveness of these measures.

[SECTION] 1. Summary of Prior Phases

Week 1 - Information Gathering:

- Discovered open ports: 21, 22, 23, 25, 53, 80, 139, 445, 3306, 5432, 6667, 8009, 8180
- Identified outdated and insecure services: vsftpd 2.3.4, OpenSSH 4.7p1, Apache 2.2.8

Week 2 - Vulnerability Assessment:

- Found exploitable services: FTP, Telnet, Samba, PostgreSQL, UnrealIRCd
- Observed complete lack of firewall and monitoring

Week 3 - Exploitation:

- Exploited vsftpd backdoor (port 21)
- Logged in via Telnet using weak credentials
- Enumerated Samba users and accessed shared files
- Gained access to PostgreSQL with no authentication

- Detected potential backdoor in UnrealIRCd

[HARDENING] 2. Hardening Measures Implemented

- System update: sudo apt-get update && sudo apt-get upgrade -y
- Disable Telnet: systemctl stop telnet && systemctl disable telnet
- Remove vsftpd: apt-get remove vsftpd -y
- Configure Firewall (UFW): ufw allow OpenSSH && ufw enable && ufw status
- Install Snort (IDS): apt-get install snort -y
- Setup AIDE (Integrity): apt-get install aide -y && aideinit
- Enforce Password Policies: Modified /etc/pam.d/common-password to include complexity rules
- Disable RSH & Finger: apt-get purge rsh-client finger -y
- Secure PostgreSQL: Configured pg_hba.conf and postgres.conf
- Remove UnrealIRCd: apt-get remove unrealircd -y

[AUDIT] 3. Post-Hardening Audit

- FTP (vsftpd): Removed (Port 21 closed)
- Telnet: Disabled (Port 23 inaccessible)
- Samba: Active (Requires secure config)
- PostgreSQL: Hardened (Auth enforced, IP restricted)
- UnrealIRCd: Removed (Port 6667 closed)
- Firewall (UFW): Active (Blocking unused ports)
- Snort IDS: Monitoring (Alerting on suspicious activity)
- AIDE: Initialized (Integrity checks configured)

[IMPROVEMENTS] 4. Key Improvements

- Closed critical open ports (FTP, Telnet, IRC)
- Removed or disabled high-risk legacy services
- Enforced strong password policies
- Introduced real-time intrusion detection (Snort)
- Enabled file integrity monitoring (AIDE)
- Configured firewall to whitelist necessary services

[RISKS] 5. Remaining Risks & Future Recommendations

- Samba vulnerabilities: Harden or consider removal
- No automatic patching: Implement patch management tools like unattended-upgrades
- Lack of centralized logging: Integrate with remote syslog/SIEM
- Weak application defaults: Review app configs regularly
- Limited user activity monitoring: Deploy auditd or OSSEC

[NOTES] Additional Notes

- Implemented login banners for legal warnings
- Disabled root login over SSH
- Applied file permission best practices on /etc, /var/www, and user home directories
- Restricted cron jobs to root-only where applicable
- Added logging for failed login attempts and su/sudo activities

[DONE] Conclusion

The Metasploitable2 system has undergone significant security upgrades. Key exploitable

vulnerabilities have been mitigated, and continuous monitoring mechanisms have been implemented. The system now maintains a reduced attack surface, improved visibility, and better access control. Continued patching and hardening iterations are recommended to uphold a robust security posture.

Prepared by: Subramaniam B

Internship Organization: SystemTron Cybersecurity Team