Cybersecurity Project Report

# Executive Summary

This report outlines the results of a security assessment performed on the target system (Metasploitable 2) using Parrot OS as the attacking machine. The project included vulnerability scanning, network testing, and initial exploitation, revealing critical misconfigurations and exploitable services. A root shell was successfully achieved using a known FTP backdoor exploit, and service enumeration revealed multiple attack surfaces. Remediation recommendations are provided based on the findings.

# Scope & Methodology

The scope of this assessment was limited to a local lab setup including:  
- Attacker: Parrot Security OS  
- Target: Metasploitable 2 (IP: 10.138.16.109)  
  
Tools used:  
- Nmap (port and vulnerability scanning)  
- Nikto (web server scanning)  
- Hydra (password attacks)  
- Wireshark (traffic analysis)  
- Metasploit Framework (exploitation)  
  
Approach:  
1. Identify open ports and services  
2. Scan for known vulnerabilities  
3. Test discovered services for misconfigurations or exploits  
4. Capture traffic and analyze service behavior  
5. Exploit using Metasploit and password brute-force (Hydra)

# Vulnerability Assessment Findings

Automated scans using Nmap and Nikto revealed several vulnerabilities:  
  
- Anonymous FTP access (High Risk)  
- Outdated Apache Web Server 2.2.8 (High Risk)  
- SSL POODLE Vulnerability (CVE-2014-3566) (High Risk)  
- SSL CCS Injection (CVE-2014-0224) (High Risk)  
- RMI Remote Code Execution (High Risk)  
- Slowloris DoS (Medium Risk)  
  
Fix Suggestions:  
- Disable anonymous FTP  
- Update Apache and OpenSSL packages  
- Disable SSLv3 support  
- Harden RMI service and restrict access

# Network Testing Results

Protocol Testing:  
- Identified open ports: FTP, SSH, HTTP, Telnet  
  
Network Map:  
See visual diagram showing attacker, target, and discovered services (attached in appendix).  
  
Service Enumeration:  
- enum4linux revealed NetBIOS info and user shares  
  
Traffic Analysis:  
- Wireshark confirmed ICMP echo traffic  
- Verified live host, unencrypted traffic  
  
Access Points:  
- FTP: Vulnerable to anonymous login  
- Telnet: Insecure protocol (plaintext auth)  
- Apache: Directory indexing, phpinfo, outdated

# Exploitation Proofs

Tool Used: Metasploit Framework  
Target: vsFTPd 2.3.4 (Port 21)  
Exploit: unix/ftp/vsftpd\_234\_backdoor  
Result: Successful shell session opened as root (UID=0)  
  
Tool Used: Hydra  
Target: SSH (Port 22)  
Attempted Password List: rockyou.txt (Not Found)  
Result: Brute-force attempt failed  
  
All screenshots and session outputs are attached in the appendix.

# Remediation Recommendations

- Disable anonymous FTP access  
- Replace Telnet with SSH or disable if unused  
- Upgrade Apache to latest secure version  
- Apply OpenSSL patches to mitigate SSL vulnerabilities  
- Configure RMI with strict access control  
- Disable directory indexing and remove phpinfo pages  
- Implement firewall rules and network segmentation  
- Conduct regular security audits and patch management

# Appendix

The following screenshots and logs support the findings documented in this report. Screenshots include:  
- Nmap service and vulnerability scans  
- Nikto output for Apache server  
- Wireshark ICMP capture  
- Metasploit exploitation shell  
- Hydra password attack attempt  
- Metasploitable2 web interface and app links