🛡️ Vulnerability Assessment Report

📄 Executive Summary

This vulnerability assessment was conducted on the target system `10.138.16.109` using automated tools such as **Nmap**and **Nikto**, followed by manual testing of select vulnerabilities. The goal was to identify open ports, services, and any associated vulnerabilities. The system exposed several high-risk issues, including weak SSL protocols, outdated web servers, and unsecured FTP access. These findings indicate a high-risk level due to ease of exploitation and potential for significant impact.

🛠️ Tools & Methodology

1. **Nmap Scans**
    - Command: `nmap -sS -sV -T4 -p- 10.138.16.109`
    - Purpose: Discover all open ports and running services.
    - Command: `nmap --script vuln 10.138.16.109`
    - Purpose: Identify known vulnerabilities using Nmap NSE scripts.
2. **Nikto Scan**
    - Command: `nikto -h http://10.138.16.109`
    - Purpose: Scan the web server for misconfigurations and known vulnerabilities.
3. **Manual Verification**
    - Tool: `ftp 10.138.16.109`
    - Purpose: Attempted login with anonymous credentials.

🔍 Key Findings

1. Anonymous FTP Access

- **Tool**: Manual (FTP)
- **Finding**: Anonymous login successful.
- **Risk**: **High**
- **Justification**: Unauthorized access to the file system. Attackers can potentially upload/download malicious files.
- **Remediation**: Disable anonymous FTP or use secure authentication.

2. Apache 2.2.8 (Ubuntu) Web Server

- **Tool**: Nikto

- **Finding**: Outdated Apache version; vulnerable to multiple known exploits.
- **Risk**: **High**
- **Justification**: Publicly known vulnerabilities like directory listing, information disclosure.
- **Remediation**: Upgrade to a supported Apache version (2.4.54+).

3. SSL POODLE Vulnerability (CVE-2014-3566)

- **Tool**: Nmap
- **Finding**: SSLv3 supported, enabling POODLE attacks.
- **Risk**: **High**
- **Justification**: Allows attacker to decrypt sensitive data via CBC padding oracle.
- **Remediation**: Disable SSLv3 support; enforce TLS 1.2+.

4. SSL CCS Injection (CVE-2014-0224)

- **Tool**: Nmap
- **Finding**: Vulnerable OpenSSL version allows MITM attacks.
- **Risk**: **High**
- **Justification**: Enables attackers to hijack sessions.
- **Remediation**: Patch OpenSSL to the latest version.

5. Slowloris DoS Vulnerability (CVE-2007-6750)

- **Tool**: Nmap
- **Finding**: HTTP server vulnerable to Slowloris DoS.
- **Risk**: **Medium**
- **Justification**: Attacker can starve web server resources.
- **Remediation**: Use a reverse proxy/load balancer or timeout protections.

6. RMI Registry Remote Code Execution

- **Tool**: Nmap
- **Finding**: RMI port 1099 open; default config allows RCE.
- **Risk**: **High**
- **Justification**: Remote code execution without authentication.
- **Remediation**: Restrict RMI access; enforce secure class loading.

7. Web Application Vulnerabilities (Nikto)

- **Tool**: Nikto
- **Findings**:
    - Directory indexing enabled
    - phpinfo() exposed
    - X-Frame-Options and X-Content-Type headers missing
- **Risk**: **Medium**
- **Justification**: Enables info disclosure and client-side attacks.

- **Remediation**: Harden HTTP headers and restrict access to sensitive files.

🧩 Screenshots

All relevant screenshots of terminal output and test results have been captured and stored, including:

- Nmap service scan
- Vuln script output
- Nikto web server scan
- FTP manual login
- POODLE and CCS injection detection
- Web vulnerabilities like phpinfo.php and directory indexing

---

🩹 Remediation Tips Summary

Vulnerability	Suggested Fix
Anonymous FTP	Disable anonymous access / use secure auth
Outdated Apache Server	Upgrade to latest supported version
SSL POODLE (CVE-2014-3566)	Disable SSLv3, use TLS 1.2+
SSL CCS Injection (CVE-2014-0224)	Update OpenSSL to patched version
Slowloris (CVE-2007-6750)	Use reverse proxy / limit keep-alive time
RMI RCE	Secure RMI configs, restrict access
Web Misconfigurations	Hide phpinfo, disable directory listing, set headers