**VULNERABILITY ASSESSMENT &**

**PENETRATION TESTING REPORT**

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

PROXY SERVER INFRASTRUCTURE

*Comprehensive Security Assessment*

|  |  |
| --- | --- |
| **Document Classification** | CONFIDENTIAL |
| **Report Version** | 1.0 |
| **Assessment Date** | [DD/MM/YYYY] - [DD/MM/YYYY] |
| **Report Date** | 12/02/2026 |
| **Prepared By** | [Your Name / Team Name] |
| **Prepared For** | [Client / Organization Name] |
| **Target System** | Proxy Server ([IP Address]) |
| **Assessment Type** | Grey-Box VAPT |

# Table of Contents

*Note: Right-click > Update Field in Word to populate TOC.*

# 1. Executive Summary

This report presents the findings of a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) engagement conducted against the proxy server infrastructure. The assessment was designed to identify security weaknesses, misconfigurations, and exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the proxy server and the broader network infrastructure it serves.

The VAPT engagement followed industry-standard methodologies including OWASP Testing Guide v4.2, PTES (Penetration Testing Execution Standard), NIST SP 800-115, and OSSTMM 3.0. Testing was conducted from both external (black-box) and internal (grey-box) perspectives using Kali Linux as the primary attack platform.

**Overall Risk Rating:** [CRITICAL / HIGH / MEDIUM / LOW] (To be filled after assessment)

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Count** | **Resolved** | **Open** |
| **Critical** | [X] | [X] | [X] |
| **High** | [X] | [X] | [X] |
| **Medium** | [X] | [X] | [X] |
| **Low** | [X] | [X] | [X] |
| **Informational** | [X] | [X] | [X] |

# 2. Scope and Objectives

## 2.1 Scope

The following assets were included in the scope of the assessment:

• Proxy Server (IP: [X.X.X.X], Ports: all TCP/UDP)

• Proxy Management Interface (HTTP/HTTPS admin panel)

• Proxy Authentication Mechanisms (Basic, Digest, NTLM, LDAP)

• SSL/TLS Configuration and Certificate Chain

• Access Control Lists (ACLs) and URL Filtering Rules

• Caching Mechanisms and Cache Storage

• Network Segment and Adjacent Infrastructure

• Operating System and Installed Packages

• Logging, Monitoring, and Alerting Configuration

## 2.2 Objectives

• Identify and exploit vulnerabilities in the proxy server and its configuration

• Assess the effectiveness of access controls and authentication mechanisms

• Evaluate network-level protections and segmentation around the proxy

• Test for proxy-specific attacks: open proxy abuse, SSRF, cache poisoning, HTTP smuggling

• Assess SSL/TLS implementation for cryptographic weaknesses

• Verify compliance with CIS benchmarks and industry best practices

• Determine the potential business impact of discovered vulnerabilities

• Provide actionable remediation recommendations prioritized by risk

## 2.3 Out of Scope

The following items were explicitly excluded: social engineering attacks, physical security testing, denial-of-service attacks impacting production (unless authorized), and testing of third-party CDN or upstream provider infrastructure.

# 3. Testing Methodology

The assessment followed a structured 8-phase approach combining automated scanning with manual penetration testing. Each phase builds on the findings of the previous one, ensuring thorough coverage of the attack surface.

|  |  |  |
| --- | --- | --- |
| **Phase** | **Name** | **Description** |
| **Phase 1** | Information Gathering & Reconnaissance | Passive and active recon to map the attack surface, identify services, and enumerate technologies. |
| **Phase 2** | Proxy-Specific Enumeration | Targeted enumeration: open proxy testing, HTTP method analysis, header inspection, protocol support. |
| **Phase 3** | Vulnerability Assessment | Automated scanning with OpenVAS/Nessus combined with manual verification. SSL/TLS and system auditing. |
| **Phase 4** | Authentication & Access Control | Brute-force, credential stuffing, authentication bypass, session management, and ACL circumvention. |
| **Phase 5** | Injection & Application-Level | SQLi, XSS, SSRF, HTTP smuggling, CRLF injection, cache poisoning, and directory enumeration. |
| **Phase 6** | Network & Protocol-Level | Packet analysis, MitM, ARP spoofing, DoS resilience, and firewall/IDS evasion testing. |
| **Phase 7** | Post-Exploitation & Priv Esc | Exploitation, privilege escalation, lateral movement, configuration review, and credential hunting. |
| **Phase 8** | Compliance & Hardening | CIS benchmarks, security headers, rootkit detection, and regulatory compliance validation. |

## 3.1 Standards and Frameworks

This assessment was conducted in accordance with:

• OWASP Testing Guide v4.2 - Web application security testing methodology

• PTES (Penetration Testing Execution Standard) - End-to-end pentesting framework

• NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

• OSSTMM 3.0 - Open Source Security Testing Methodology Manual

• CVSSv3.1 - Common Vulnerability Scoring System for risk rating

• MITRE ATT&CK Framework - Adversarial tactics and techniques mapping

• CIS Benchmarks - Configuration hardening guidelines

# 4. Detailed Testing Matrix - Tools, Commands & Tests

The following sections provide a comprehensive breakdown of every tool, command, and test performed during each phase. Each entry includes the command syntax, test description, and potential severity rating.

## 4.1 Phase 1: Information Gathering & Reconnaissance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **Nmap** | nmap -sS -sV -O -A -p- <proxy\_ip> | Full TCP port scan with service version detection, OS fingerprinting, and aggressive scan scripts. Identifies all open ports, running services, and OS details on the proxy server. | [To be filled] | **Informational** |
| **Nmap (UDP)** | nmap -sU --top-ports 200 <proxy\_ip> | UDP port scan on top 200 common UDP ports to detect services like SNMP, DNS, TFTP that may be exposed. | [To be filled] | **Informational** |
| **Nmap NSE Scripts** | nmap --script=default,vuln,discovery -p 3128,8080,8443,80,443 <proxy\_ip> | NSE scripts with default, vulnerability, and discovery categories against proxy ports to enumerate banners, detect known CVEs, and gather service metadata. | [To be filled] | **Informational** |
| **Whois / DNSRecon** | whois <proxy\_ip> && dnsrecon -d <domain> | WHOIS lookup and DNS reconnaissance to map domain records, subdomains, mail servers, and name servers associated with the proxy infrastructure. | [To be filled] | **Informational** |
| **theHarvester** | theHarvester -d <domain> -b all -l 500 | OSINT gathering for email addresses, hostnames, employee names, and subdomains from public sources (Google, Bing, Shodan, etc.). | [To be filled] | **Informational** |
| **Shodan CLI** | shodan host <proxy\_ip> | Query Shodan for historical scan data, open ports, banners, vulnerabilities, and geolocation information about the proxy's public IP. | [To be filled] | **Informational** |
| **WhatWeb** | whatweb http://<proxy\_ip>:8080 -a 3 | Web technology fingerprinting to identify proxy software (Squid, Nginx, HAProxy, Apache), version numbers, and web server headers. | [To be filled] | **Informational** |

## 4.2 Phase 2: Proxy-Specific Enumeration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **curl (Open Proxy Test)** | curl -x http://<proxy\_ip>:3128 http://ifconfig.me | Test if proxy is an open proxy by routing external requests. If successful, proxy can be abused for anonymization, spam, or DDoS amplification. | [To be filled] | **Critical** |
| **curl (CONNECT Method)** | curl -x http://<proxy\_ip>:3128 -X CONNECT https://external-site.com:443 | Test if CONNECT method tunnels arbitrary TCP connections, potentially bypassing firewalls and accessing internal networks. | [To be filled] | **High** |
| **Nmap (Proxy Bounce)** | nmap -b <proxy\_ip>:21 <internal\_target> | FTP bounce scan to test if proxy can scan internal/protected network segments not directly accessible. | [To be filled] | **High** |
| **curl (Header Analysis)** | curl -I -x http://<proxy\_ip>:3128 http://target.com | Inspect HTTP response headers for info leakage: Via, X-Forwarded-For, X-Cache, X-Proxy-ID, Server version, internal IPs. | [To be filled] | **Medium** |
| **curl (HTTP Methods)** | for m in GET POST PUT DELETE PATCH OPTIONS TRACE PURGE; do curl -X $m ...; done | Enumerate allowed HTTP methods. Dangerous methods like TRACE (XST), PUT/DELETE (file manipulation), PURGE (cache poisoning) should be disabled. | [To be filled] | **Medium** |
| **Nikto** | nikto -h http://<proxy\_ip>:8080 -useproxy http://<proxy\_ip>:3128 | Web vulnerability scanner for default files, misconfigurations, known vulns, dangerous HTTP methods, and outdated software on proxy interfaces. | [To be filled] | **Medium** |
| **WAFW00F** | wafw00f http://<proxy\_ip>:8080 | Detect WAF presence to tailor testing techniques and identify bypass opportunities. | [To be filled] | **Informational** |

## 4.3 Phase 3: Vulnerability Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **OpenVAS (GVM)** | gvm-cli socket --xml '<create\_target>...' | Full vulnerability assessment with 70,000+ NVT checks: CVE detection, misconfigurations, default credentials, missing patches, SSL/TLS issues, compliance. | [To be filled] | **Critical** |
| **Nessus (if available)** | Launch via Nessus Web UI against <proxy\_ip> | Commercial scanner for authenticated/unauthenticated scans: CVEs, misconfigurations, PCI-DSS/CIS compliance, zero-day heuristics. | [To be filled] | **Critical** |
| **Searchsploit** | searchsploit squid proxy && searchsploit nginx proxy | Search Exploit-DB offline database for known public exploits matching identified proxy software and version. | [To be filled] | **High** |
| **testssl.sh** | testssl.sh --full https://<proxy\_ip>:8443 | Comprehensive SSL/TLS: SSLv2/v3, weak ciphers (RC4, DES, NULL), Heartbleed, POODLE, BEAST, CRIME, DROWN, ROBOT, HSTS, OCSP stapling. | [To be filled] | **High** |
| **SSLyze** | sslyze --regular <proxy\_ip>:443 | SSL/TLS scanner for certificate validation, cipher suite enumeration, protocol analysis, and TLS vulnerability detection. | [To be filled] | **High** |
| **Lynis** | lynis audit system --quick | System audit: kernel hardening, file permissions, user accounts, PAM, firewall rules, logging. Generates hardening index score. (Requires local access.) | [To be filled] | **Medium** |
| **Linux Exploit Suggester** | ./linux-exploit-suggester.sh | Analyze kernel version and packages to suggest local privilege escalation exploits. (Requires shell access.) | [To be filled] | **Medium** |

## 4.4 Phase 4: Authentication & Access Control Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **Hydra** | hydra -L users.txt -P passwords.txt <proxy\_ip> http-proxy / | Online brute-force against proxy auth: common credentials, defaults, dictionary attacks against HTTP Basic/Digest/NTLM authentication. | [To be filled] | **Critical** |
| **Medusa** | medusa -h <proxy\_ip> -U users.txt -P pass.txt -M http -n 3128 | Parallel brute-force with multi-protocol support for testing weak proxy credentials with customizable threading. | [To be filled] | **High** |
| **curl (Auth Bypass)** | curl -x http://<proxy\_ip>:3128 http://internal -H 'X-Forwarded-For: 127.0.0.1' | Authentication bypass by spoofing trusted IP headers (X-Forwarded-For, X-Real-IP). Misconfigured proxies may grant access based on these. | [To be filled] | **Critical** |
| **curl (Default Creds)** | curl -x http://admin:admin@<proxy\_ip>:3128 http://ifconfig.me | Test default credentials: admin/admin, proxy/proxy, squid/squid, root/root, admin/password, admin/123456. | [To be filled] | **High** |
| **Burp Suite** | Burp Suite -> Set upstream proxy -> Intercept & modify | Intercept auth tokens and cookies. Test session fixation, cookie manipulation, token replay, session timeout, and auth logic flaws. | [To be filled] | **High** |
| **curl (ACL Bypass)** | curl -x http://<proxy\_ip>:3128 http://169.254.169.254/latest/meta-data/ | ACL bypass via cloud metadata (AWS/GCP/Azure), internal RFC 1918 addresses, localhost. Checks ACL enforcement. | [To be filled] | **Critical** |

## 4.5 Phase 5: Injection & Application-Level Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **SQLMap** | sqlmap -u 'http://<proxy\_ip>:8080/admin?id=1' --batch --level=5 --risk=3 | SQL injection on proxy management interface: Boolean-based, Time-based, UNION, Error-based, Stacked query across all parameters. | [To be filled] | **Critical** |
| **Burp Suite (XSS)** | Burp Suite Active Scanner on proxy management interface | XSS testing (Reflected, Stored, DOM-based) in error pages, admin panels, and custom deny pages via URL params, headers, forms. | [To be filled] | **High** |
| **curl (SSRF)** | curl -x http://<proxy\_ip>:3128 http://127.0.0.1:22 | SSRF: access internal services (SSH, databases, cloud metadata) through proxy. Tests IPv4, IPv6, URL encoding, DNS rebinding. | [To be filled] | **Critical** |
| **nc (HTTP Smuggling)** | printf 'POST / HTTP/1.1\r\n...' | nc <proxy\_ip> 3128 | HTTP Request Smuggling (CL.TE/TE.CL/TE.TE). Exploits Content-Length vs Transfer-Encoding parsing discrepancies. | [To be filled] | **Critical** |
| **curl (CRLF Injection)** | curl -x http://<proxy\_ip>:3128 'http://target/%0d%0aX-Injected:evil' | CRLF injection for header injection/response splitting. Can cause cache poisoning, session fixation, XSS, log injection. | [To be filled] | **High** |
| **curl (Cache Poisoning)** | curl -x http://<proxy\_ip>:3128 http://target -H 'X-Forwarded-Host: evil.com' | Web cache poisoning via unkeyed headers (X-Forwarded-Host, X-Forwarded-Scheme) to serve malicious cached responses. | [To be filled] | **High** |
| **Gobuster** | gobuster dir -u http://<proxy\_ip>:8080 -w wordlist.txt -x php,html,conf,bak | Directory/file brute-forcing to discover hidden admin panels, config backups (.bak, .old), and debug endpoints. | [To be filled] | **Medium** |

## 4.6 Phase 6: Network & Protocol-Level Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **Wireshark / tcpdump** | tcpdump -i eth0 -w capture.pcap host <proxy\_ip> -c 10000 | Packet capture for cleartext credentials, unencrypted data, DNS leaks, protocol anomalies, ARP poisoning, malformed packets. | [To be filled] | **High** |
| **Responder** | responder -I eth0 -wrf | LLMNR/NBT-NS/MDNS poisoning to intercept NTLMv1/v2 hashes on the proxy network segment for offline cracking. | [To be filled] | **High** |
| **Ettercap (ARP Spoof)** | ettercap -T -q -M arp:remote /<proxy\_ip>// /<gateway>// | ARP spoofing MitM between proxy and gateway. Tests Dynamic ARP Inspection, port security protections. | [To be filled] | **High** |
| **hping3 (SYN Flood)** | hping3 -S --flood -V -p 3128 <proxy\_ip> | SYN flood resilience. Checks SYN cookies, rate limiting, connection limits, firewall protections. (Authorization required.) | [To be filled] | **High** |
| **Slowloris** | slowloris <proxy\_ip> -p 3128 -s 500 | Slow HTTP DoS: partial headers keep connections open to exhaust available connection slots and starve the proxy. | [To be filled] | **Medium** |
| **Nmap (FW Evasion)** | nmap -f -D RND:5 --data-length 24 -sS <proxy\_ip> | Firewall/IDS evasion with fragmented packets, decoys, and random padding to determine if perimeter defenses can be bypassed. | [To be filled] | **Medium** |

## 4.7 Phase 7: Post-Exploitation & Privilege Escalation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **Metasploit** | msfconsole -> use exploit/unix/http/squid\_ntlm\_authenticate -> exploit | Exploit identified vulnerabilities: RCE, buffer overflows, proxy-specific exploits (Squid NTLM auth, Nginx off-by-slash). | [To be filled] | **Critical** |
| **LinPEAS** | ./linpeas.sh | Privilege escalation enumeration: SUID/SGID, writable cron jobs, sudo misconfig, kernel exploits, credentials in configs, Docker breakouts. | [To be filled] | **High** |
| **pspy** | ./pspy64 -p -i 1000 | Unprivileged process monitoring for exploitable cron jobs, background tasks, and root processes. | [To be filled] | **Medium** |
| **Config Review** | cat /etc/squid/squid.conf | grep -E '(acl|http\_access|auth\_param)' | Manual proxy config review: permissive ACLs, disabled auth, hostname leaks, forwarded-for exposure, insecure cache peers. | [To be filled] | **High** |
| **Log Analysis** | tail -f /var/log/squid/access.log | grep -E '(DENIED|ERR\_)' | Analyze proxy logs for unauthorized access, blocked requests, error patterns, misconfigurations, and IOCs. | [To be filled] | **Medium** |
| **Credential Hunting** | grep -rn 'password\|secret\|api\_key' /etc/squid/ /etc/nginx/ | Search proxy configs for hardcoded credentials, API keys, tokens, and plaintext secrets. | [To be filled] | **High** |

## 4.8 Phase 8: Compliance & Hardening Checks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool** | **Command** | **Test Description** | **Findings** | **Severity** |
| **CIS Benchmark Audit** | CIS-CAT tool or manual audit | Audit against CIS benchmarks: TLS config, access controls, logging, header security, timeouts, buffer sizes, admin access. | [To be filled] | **High** |
| **Nmap (SSL Compliance)** | nmap --script ssl-enum-ciphers -p 443,8443 <proxy\_ip> | Enumerate SSL/TLS cipher suites for PCI-DSS and NIST compliance. Verify TLS 1.2+ and weak ciphers disabled. | [To be filled] | **High** |
| **Security Headers** | curl -sI http://<proxy\_ip>:8080 | grep -iE '(strict-transport|content-security|x-frame)' | Audit HTTP security headers: HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy. | [To be filled] | **Medium** |
| **auditd / ausearch** | ausearch -m AVC,USER\_AUTH,LOGIN --start today | Review audit logs for SELinux denials, authentication events, login attempts, and security-relevant system calls. | [To be filled] | **Medium** |
| **chkrootkit / rkhunter** | chkrootkit && rkhunter --check --skip-keypress | Rootkit detection: known rootkits, suspicious files, hidden processes, backdoors, compromised binaries. | [To be filled] | **Medium** |

# 5. Detailed Findings

Each finding follows a standardized format: severity, CVSS score, affected component, description, evidence, business impact, and remediation.

## 5.1 Finding 1

|  |  |
| --- | --- |
| **Finding ID** | VAPT-PROXY-001 |
| **Title** | [Vulnerability Title] |
| **Severity** | [Critical / High / Medium / Low / Informational] |
| **CVSS v3.1 Score** | [X.X] - [Vector String] |
| **CVE ID** | [CVE-XXXX-XXXXX or N/A] |
| **CWE ID** | [CWE-XXX - Category] |
| **Affected Component** | [e.g., Squid Proxy 5.2 on port 3128] |
| **MITRE ATT&CK** | [Tactic: Technique ID] |
| **Status** | [Open / Remediated / Accepted Risk] |

**Description:** [Detailed technical description of the vulnerability, why it exists, and the attack scenario.]

**Steps to Reproduce:**

1. [Step-by-step instructions] 2. [Exact commands/payloads] 3. [Observed response]

**Evidence / PoC:** [Sanitized command output, screenshots, request/response pairs.]

**Business Impact:** [Data breach, unauthorized access, service disruption, compliance violation, financial loss.]

**Remediation:** [Specific configuration changes, patches, code fixes, compensating controls.]

**References:** [CVE details, vendor advisories, OWASP guides, CIS benchmarks.]

## 5.2 Finding 2

|  |  |
| --- | --- |
| **Finding ID** | VAPT-PROXY-002 |
| **Title** | [Vulnerability Title] |
| **Severity** | [Critical / High / Medium / Low / Informational] |
| **CVSS v3.1 Score** | [X.X] - [Vector String] |
| **CVE ID** | [CVE-XXXX-XXXXX or N/A] |
| **CWE ID** | [CWE-XXX - Category] |
| **Affected Component** | [e.g., Squid Proxy 5.2 on port 3128] |
| **MITRE ATT&CK** | [Tactic: Technique ID] |
| **Status** | [Open / Remediated / Accepted Risk] |

**Description:** [Detailed technical description of the vulnerability, why it exists, and the attack scenario.]

**Steps to Reproduce:**

1. [Step-by-step instructions] 2. [Exact commands/payloads] 3. [Observed response]

**Evidence / PoC:** [Sanitized command output, screenshots, request/response pairs.]

**Business Impact:** [Data breach, unauthorized access, service disruption, compliance violation, financial loss.]

**Remediation:** [Specific configuration changes, patches, code fixes, compensating controls.]

**References:** [CVE details, vendor advisories, OWASP guides, CIS benchmarks.]

## 5.3 Finding 3

|  |  |
| --- | --- |
| **Finding ID** | VAPT-PROXY-003 |
| **Title** | [Vulnerability Title] |
| **Severity** | [Critical / High / Medium / Low / Informational] |
| **CVSS v3.1 Score** | [X.X] - [Vector String] |
| **CVE ID** | [CVE-XXXX-XXXXX or N/A] |
| **CWE ID** | [CWE-XXX - Category] |
| **Affected Component** | [e.g., Squid Proxy 5.2 on port 3128] |
| **MITRE ATT&CK** | [Tactic: Technique ID] |
| **Status** | [Open / Remediated / Accepted Risk] |

**Description:** [Detailed technical description of the vulnerability, why it exists, and the attack scenario.]

**Steps to Reproduce:**

1. [Step-by-step instructions] 2. [Exact commands/payloads] 3. [Observed response]

**Evidence / PoC:** [Sanitized command output, screenshots, request/response pairs.]

**Business Impact:** [Data breach, unauthorized access, service disruption, compliance violation, financial loss.]

**Remediation:** [Specific configuration changes, patches, code fixes, compensating controls.]

**References:** [CVE details, vendor advisories, OWASP guides, CIS benchmarks.]

*[Add additional findings as discovered. Duplicate the template above for each.]*

# 6. Risk Rating Matrix

Vulnerabilities are rated using CVSSv3.1 scores mapped to the following severity levels:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rating** | **CVSS** | **Description** | **SLA** | **Example** |
| **Critical** | 9.0-10.0 | Immediate exploitation; full system compromise | 24-48 hrs | RCE, Open Proxy, Auth Bypass |
| **High** | 7.0-8.9 | Significant impact; minimal exploitation effort | 7 days | Weak TLS, Brute-forceable Auth |
| **Medium** | 4.0-6.9 | Moderate impact; specific conditions needed | 30 days | Missing Headers, Info Leakage |
| **Low** | 0.1-3.9 | Low impact; difficult to exploit | 90 days | Verbose Errors, Minor Config |
| **Informational** | 0.0 | No direct impact; best practice | Next cycle | Version Disclosure, Banner |

# 7. Remediation Summary and Prioritization

The following table provides a prioritized remediation roadmap ordered by severity and business impact.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Action** | **Severity** | **Ref** | **Effort** | **Owner** | **Status/Due** |
| 1 | [Action] | [Sev] | VAPT-PROXY-001 | [L/M/H] | [Name] | [Status] |
| 2 | [Action] | [Sev] | VAPT-PROXY-002 | [L/M/H] | [Name] | [Status] |
| 3 | [Action] | [Sev] | VAPT-PROXY-003 | [L/M/H] | [Name] | [Status] |
| 4 | [Action] | [Sev] | VAPT-PROXY-004 | [L/M/H] | [Name] | [Status] |
| 5 | [Action] | [Sev] | VAPT-PROXY-005 | [L/M/H] | [Name] | [Status] |

# 8. Complete Kali Linux Tool Inventory

Master list of all tools used or recommended for this proxy server VAPT engagement, organized by category.

|  |  |
| --- | --- |
| **Category** | **Tools** |
| **Reconnaissance & OSINT** | Nmap, Masscan, Unicornscan, theHarvester, Recon-ng, Maltego, DNSRecon, DNSenum, Fierce, Sublist3r, Amass, WhatWeb, Shodan CLI, Censys |
| **Vulnerability Scanning** | OpenVAS (GVM), Nessus, Nikto, Wapiti, Arachni, Vega, W3af, Searchsploit, testssl.sh, SSLyze, SSLScan, Lynis, Linux Exploit Suggester |
| **Proxy & Web Testing** | Burp Suite, OWASP ZAP, mitmproxy, curl, wget, HTTPie, Gobuster, Dirb, ffuf, Feroxbuster, WFuzz, WAFW00F, Arjun, ParamSpider |
| **Authentication Attacks** | Hydra, Medusa, Ncrack, John the Ripper, Hashcat, CeWL, Crunch, Cupp, Patator, BruteSpray |
| **Injection & Exploitation** | SQLMap, Commix, XSSer, BeEF, Metasploit Framework, ExploitDB, MSFVenom, PowerSploit |
| **Network Analysis & MitM** | Wireshark, tcpdump, Ettercap, Bettercap, arpspoof, Responder, mitmproxy, SSLstrip, dnschef, hping3 |
| **Post-Exploitation** | LinPEAS, WinPEAS, pspy, GTFOBins, Mimikatz, CrackMapExec, Impacket, Chisel, Ligolo-ng |
| **DoS Testing** | Slowloris, HOIC, LOIC (authorized only), hping3, T50, GoldenEye |
| **Compliance & Hardening** | Lynis, CIS-CAT, chkrootkit, rkhunter, AIDE, Tiger, OpenSCAP, Nmap compliance scripts |
| **Reporting** | Dradis, Faraday, Serpico, CherryTree, Pipal, Cutycapt |

# 9. Conclusion

This VAPT assessment provided a thorough evaluation of the proxy server's security posture across eight distinct testing phases encompassing network-level, application-level, authentication, injection, protocol, and compliance testing domains.

Key findings summary:

• [X] Critical vulnerabilities requiring immediate remediation within 24-48 hours

• [X] High-severity vulnerabilities to be addressed within 7 days

• [X] Medium-severity vulnerabilities with a 30-day remediation window

• [X] Low-severity and informational findings for continuous improvement

A retest is recommended within [30/60/90] days of remediation to verify all vulnerabilities have been addressed and no regressions introduced.

# 10. Appendices

## Appendix A: Raw Tool Outputs

[Attach raw Nmap scans, OpenVAS reports, testssl.sh output, Burp Suite logs, and tool-generated evidence.]

## Appendix B: Screenshots and Evidence

[Insert numbered screenshots with captions documenting each vulnerability with timestamps and request/response pairs.]

## Appendix C: Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **VAPT** | Vulnerability Assessment and Penetration Testing |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **CWE** | Common Weakness Enumeration |
| **SSRF** | Server-Side Request Forgery |
| **XSS** | Cross-Site Scripting |
| **CRLF** | Carriage Return Line Feed |
| **ACL** | Access Control List |
| **MitM** | Man-in-the-Middle |
| **TLS** | Transport Layer Security |
| **DoS** | Denial of Service |
| **RCE** | Remote Code Execution |
| **HSTS** | HTTP Strict Transport Security |
| **CSP** | Content Security Policy |

## Appendix D: Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Changes** |
| 1.0 | [Date] | [Your Name] | Initial VAPT report |
| 1.1 | [Date] | [Name] | Retest findings and remediation updates |

# Disclaimer

This report is provided for informational purposes and represents a point-in-time assessment. Findings are based on conditions observed during the testing window. New vulnerabilities may emerge after the assessment. This report is CONFIDENTIAL and should be distributed only to authorized personnel. The testing team is not responsible for unauthorized use of the techniques, tools, or findings described herein.