NETWORK SECURITY ASSESSMENT & PENETRATION TESTING

Comprehensive Security Evaluation Report

CLIENT	[Client Organisation Name]
PREPARED BY	Security Assessment Team
DATE	22 April 2026
VERSION	1.0 — DRAFT FOR REVIEW
CLASSIFICATION	CONFIDENTIAL

SATYA TECHNOLOGIES
We Believe in Solutions

TABLE OF CONTENTS

1.	Executive Summary	3
2.	Project Overview & Scope	3
3.	Network Scanning	4
4.	Port Scanning	5
5.	Laptop / Desktop Vulnerability Assessment	6
6.	Penetration Testing — Internal & External	7
7.	Vulnerability Assessment & Penetration Testing (VAPT)	10
8.	Future Security Roadmap	12
9.	Methodology & Standards	14
10.	Deliverables & Timeline	14
11.	Legal & Compliance	15
12.	Terms & Authorisation	15

SATYA TECHNOLOGIES
We Believe in Solutions

1. EXECUTIVE SUMMARY

This document defines the full scope, methodology, and deliverables for the Network Security Assessment and Penetration Testing engagement commissioned by the Client. The engagement is designed to identify vulnerabilities across the Client's network perimeter, internal infrastructure, and endpoint estate before a malicious actor can exploit them. All activities are performed under strict rules of engagement and within the boundaries agreed in writing prior to commencement.

Findings will be presented in a formal report with criticality ratings, evidence screenshots, and actionable remediation guidance prioritised by risk.

2. PROJECT OVERVIEW & SCOPE

Project Title	Network Security Assessment & Penetration Testing
Client	[Client Organisation Name]
Engagement Type	Black-box / Grey-box (as agreed)
Testing Window	[Insert agreed testing dates]
Point of Contact	[Client POC Name, Role, Email, Phone]
Lead Assessor	[Assessor Name & Certification]

Scope Inclusions

- All externally facing IP addresses and domains listed in Appendix A
- Internal network segments as defined in the agreed scope document
- Corporate laptops and desktop endpoints specified by the Client
- Network devices: routers, switches, and firewalls within scope
- Active Directory and authentication infrastructure

Scope Exclusions

- Third-party hosted SaaS platforms not explicitly included
- Production databases unless read-only access is pre-approved
- Physical security assessr

SATYA TECHNOLOGIES
We Believe in Solutions

3. NETWORK SCANNING

Network scanning forms the reconnaissance backbone of the engagement. The objective is to map the Client's external and internal attack surface accurately before any active exploitation attempts are made.

1. Name Server Response Examination

•Query DNS servers to enumerate hostnames, MX records, SPF/DKIM/DMARC entries, zone-transfer vulnerabilities, and subdomain exposure.

- Identify misconfigured resolvers that may allow cache poisoning or amplification attacks.
- Validate DNSSEC implementation where applicable.

2. Outer Wall / Perimeter Review

- Map the external network boundary including all public-facing IP ranges.
- Identify internet-exposed management interfaces, VPN gateways, and remote access portals.
- Assess firewall rule-sets for unnecessary exposure and egress filtering gaps.

3. Target Organisation Track Review

•Perform passive OSINT gathering using public sources (WHOIS, certificate transparency logs, Shodan, LinkedIn).

- Correlate gathered intelligence to identify shadow IT, forgotten assets, and legacy systems.
- Document all discovered assets in a consolidated inventory for further active testing.

4. Information Leak Review

- Check for sensitive data in public repositories (GitHub, Pastebin, code leaks).
- Identify metadata leakage in published documents (PDF, DOCX, XLSX author fields, GPS data).
- Review job postings and technical forums for inadvertent technology disclosures.
- Assess web application headers for server version banners and debug information.

SATYA TECHNOLOGIES
We Believe in Solutions

4. PORT SCANNING

Systematic port scanning identifies listening services and their versions across all in-scope hosts, forming the basis for targeted vulnerability analysis.

1. Error Checking

- Validate scan results against known false-positive patterns.
- Cross-reference open ports against expected service profiles for anomaly detection.

2. System & Port Enumeration

- Full TCP SYN scan across all 65,535 ports on in-scope hosts.
- UDP scan targeting high-risk services (DNS 53, SNMP 161/162, TFTP 69, NTP 123).
- Service and version detection using banner grabbing and protocol fingerprinting.
- Operating system fingerprinting to build a host profile inventory.

3. Protocol Response Verification

- Validate HTTP/HTTPS, FTP, SSH, Telnet, SMTP, RDP, and SMB service responses.
- Identify deprecated or insecure protocol versions (SSLv3, TLSv1.0, SMBv1).
- Test for default credentials on all discovered services.

4. Packet-Level Response Analysis

- Capture and analyse raw packet responses to detect firewall evasion opportunities.
- Assess TCP/IP stack behaviour for OS-level vulnerability indicators.
- Identify fragmentation handling weaknesses that may allow bypass of packet inspection.

5. Port Sweep (Multi-Host)

- Conduct horizontal port sweeps to identify hosts listening on high-risk ports (e.g., 445, 3389, 22, 23).
- Detect rogue or unauthorised services running on non-standard ports.
- Identify potential pivot points and lateral movement paths within the internal network.

SATYA TECHNOLOGIES
We Believe in Solutions

5. LAPTOP / DESKTOP VULNERABILITY ASSESSMENT

Endpoint devices represent a primary attack vector in modern threat landscapes. This phase assesses the security posture of corporate workstations and laptops.

1. Service Detection

- Enumerate all running services and background processes on assessed endpoints.
- Identify unnecessary or high-risk services (e.g., RDP, SMB, WMI, LLMNR, NBT-NS).
- Assess application allow-listing and execution control enforcement.
- Verify endpoint detection & response (EDR) agent presence and configuration.

2. Patch Verification

- Audit OS patch levels against vendor security bulletins (Microsoft Patch Tuesday, etc.).
- Identify missing critical and high-severity CVEs on operating systems and applications.
- Assess third-party software (browsers, Java, Adobe, Office) for update compliance.
- Review automatic update policy enforcement via Group Policy or MDM.

3. Vulnerability Scanning

- Run authenticated vulnerability scans using industry-standard tooling (Nessus / OpenVAS).
- Identify configuration weaknesses: weak ciphers, insecure registry settings, open shares.
- Assess local firewall rules and host-based intrusion prevention system (HIPS) effectiveness.
- Test for credential caching vulnerabilities, including NTLM hash exposure.
- Review USB and removable media policies for data exfiltration risk.

SATYA TECHNOLOGIES
We Believe in Solutions

6. PENETRATION TESTING — INTERNAL & EXTERNAL

Penetration testing moves beyond identification to active exploitation of discovered vulnerabilities in a controlled and authorised manner. The goal is to determine the true business impact of each vulnerability and validate the effectiveness of existing defensive controls.

1. Password Cracking

- Offline cracking of harvested password hashes using rule-based and dictionary attacks.
- Test account lockout policies and password complexity enforcement.
- Assess password reuse across services and credential stuffing resilience.
- Review service accounts for weak or default credentials.

2. IDS / IPS Evasion Testing

- Evaluate detection fidelity of intrusion detection and prevention systems.
- Test signature-based evasion using fragmentation, encoding, and timing techniques.
- Assess alerting thresholds and security operations centre (SOC) response SLAs.

3. Router, Switch & Firewall Testing

- Attempt access to management interfaces using default and brute-forced credentials.
- Test for known CVEs in router and switch firmware versions.
- Review ACL rule-sets and assess for rule-base misconfigurations.
- Assess VLAN hopping, STP manipulation, and ARP spoofing opportunities.
- Evaluate firewall policy against principle of least-privilege access.

4. DoS / DDoS Resilience Testing

- Conduct controlled denial-of-service simulation against agreed targets only.
- Test SYN flood, ICMP flood, and UDP amplification resilience.
- Assess rate-limiting and traffic-scrubbing capabilities.
- Review upstream ISP-level DDoS mitigation agreements and failover procedures.

5. IP Spoofing

- Test ingress and egress filtering for anti-spoofing controls (BCP38/BCP84).
- Attempt source IP spoofing to bypass IP-based access controls.
- Assess SIEM correlation rules for spoofed traffic detection.

6. Trusted System Scanning

- Identify trust relationships between internal systems (Kerberos delegation, SSH trust, DCOM).
- Assess risks arising from overly permissive inter-system trust configurations.
- Test for Pass-the-Hash and Pass-the-Ticket attacks in Active Directory environments.

7. Trojan & Malware Indicator Scanning

- Scan network traffic and endpoint artefacts for indicators of known Trojans and RATs.
- Check for persistence mechanisms: scheduled tasks, registry run keys, WMI subscriptions.
- Test anti-malware solution detection rates against common payload families.

8. Administrator Privilege Escalation Testing

•Attempt local privilege escalation on assessed endpoints via unpatched CVEs and misconfigurations.

- Test for token impersonation, DLL hijacking, and unquoted service path vulnerabilities.

•Assess domain privilege escalation paths: unconstrained delegation, ACL abuse, GPO misconfiguration.

- Attempt Kerberoasting and AS-REP roasting against Active Directory service accounts.

9. Additional Attack Scenarios

- Man-in-the-Middle (MitM) attacks via ARP poisoning and LLMNR/NBT-NS poisoning.
- Lateral movement simulation using discovered credentials and vulnerability chains.
- Data exfiltration simulation to test DLP controls and egress monitoring.
- Social engineering scenarios (phishing simulation) if separately authorised by Client.

SATYA TECHNOLOGIES
We Believe in Solutions

7. VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)

VAPT is a combined discipline that integrates systematic Vulnerability Assessment (VA) with targeted Penetration Testing (PT) into a single, cohesive engagement. Where a standalone vulnerability scan identifies and catalogues weaknesses, VAPT goes further by validating their real-world exploitability, chaining vulnerabilities into attack paths, and quantifying the tangible business impact to the Client's operations, data, and reputation.

The VAPT engagement follows a structured five-phase lifecycle ensuring thorough coverage, controlled risk, and actionable outputs.

Phase	Activity	Key Outputs
1 Planning	Define scope, obtain written authorisation, establish emergency contacts, agree Rules of Engagement.	Signed RoE, NDA, scope document
2 Reconnaissance	Passive OSINT, active network mapping, asset discovery, service fingerprinting.	Asset inventory, attack surface map
3 Vulnerability Assessment	Authenticated and unauthenticated scans, CVE correlation, CVSS scoring, false-positive triage.	VA report with CVSS ratings
4 Exploitation (PT)	Controlled exploitation of confirmed vulnerabilities; privilege escalation; lateral movement; data access proof-of-concept.	Exploitation evidence, attack chains
5 Reporting	Risk-rated findings, remediation roadmap, executive summary, retest plan.	Full VAPT report + roadmap

1. Vulnerability Assessment Activities

•Authenticated network scans using Nessus Professional / OpenVAS against all in-scope hosts.

•Web application scanning (OWASP Top 10): SQL injection, XSS, CSRF, insecure direct object references, misconfigurations.

•Cloud configuration review (AWS/Azure/GCP) for exposed storage buckets, IAM misconfigurations, and public snapshots.

•Database exposure assessment: unnecessary public access, default credentials, unencrypted connections.

•API security assessment: broken object-level authorisation, excessive data exposure, rate-limiting gaps.

•Mobile application assessment (if in scope): insecure data storage, traffic interception, certificate pinning bypass.

• All findings assigned CVSS v3.1 scores and mapped to CWE / MITRE ATT&CK techniques.

2. Penetration Testing Activities

- Exploitation of confirmed high and critical CVEs to establish proof-of-concept access.
- Active Directory attack simulation: Kerberoasting, DCSync, Golden/Silver Ticket forgery.
- Internal network pivot and lateral movement to assess blast radius of initial compromise.
- Simulated data exfiltration to validate DLP and egress monitoring effectiveness.
- Business logic abuse testing on web and API endpoints.
- Social engineering (phishing) simulation against employee subset — only if separately authorised.

3. VAPT Risk Rating Framework

•**Critical (CVSS 9.0–10.0):** Immediate exploitation possible; full system or data compromise likely. Remediate within 24–72 hours.

•**High (CVSS 7.0–8.9):** Significant impact; exploitation feasible with moderate effort. Remediate within 7 days.

•**Medium (CVSS 4.0–6.9):** Limited impact; exploitation requires specific conditions. Remediate within 30 days.

- **Low (CVSS 0.1–3.9):** Minimal direct impact; address in next scheduled maintenance cycle.
- **Informational:** Best-practice observations and hardening recommendations.

4. VAPT Report Contents

•Management summary with risk heat map and overall security posture score.

•Technical findings with: vulnerability description, affected asset, CVSS score, evidence screenshots, proof-of-concept steps, and remediation guidance.

- Attack path diagrams illustrating multi-stage exploitation chains.
- Benchmarking against industry peers and applicable compliance frameworks.
- Remediation tracking spreadsheet for Client's internal use.

SATYA TECHNOLOGIES
We Believe in Solutions

8. FUTURE SECURITY ROADMAP

Beyond identifying current vulnerabilities, this engagement delivers a structured, multi-year security improvement roadmap aligned to the Client's business objectives, risk appetite, and budget. The roadmap translates technical findings into a prioritised programme of work that progressively matures the Client's security posture from its current baseline toward industry best practice.

8.1 Roadmap Overview — Three Horizon Model

The roadmap is structured across three time horizons, ensuring that critical risks are addressed immediately while medium and longer-term strategic improvements are planned and resourced appropriately.

Horizon	Timeframe	Focus	Outcome
H1 — Remediate	0–3 Months	Fix all Critical and High findings. Patch urgent CVEs. Remove unnecessary attack surface.	Immediate risk reduction
H2 — Strengthen	3–9 Months	Implement security controls, harden configurations, improve detection & response capabilities.	Improved defensive posture
H3 — Transform	9–24 Months	Mature security programme, achieve compliance certifications, embed security into SDLC and culture.	Resilient, sustainable security

2. Horizon 1 — Immediate Remediation (Months 0–3)

- Patch or mitigate all Critical and High CVSS vulnerabilities identified during VAPT.
- Disable or restrict all unnecessary services, ports, and protocols exposed to the internet.
- Enforce multi-factor authentication (MFA) on all remote access, VPN, and privileged accounts.
- Reset all default, weak, and reused credentials identified during the assessment.
- Implement emergency network segmentation to isolate the most sensitive systems.
- Deploy or update endpoint detection and response (EDR) tooling across the endpoint estate.
- Conduct emergency security awareness training focused on phishing and social engineering.

SATYA TECHNOLOGIES
We Believe in Solutions

3. Horizon 2 — Security Hardening (Months 3–9)

- Implement a formal vulnerability management programme with monthly scan cadence.
- Deploy a Security Information and Event Management (SIEM) solution with tuned alerting rules.
- Harden Active Directory: tiered administration model, remove legacy protocols (NTLMv1, LDAPv2).
- Implement network access control (NAC) for device onboarding and rogue device detection.
- Establish a patch management policy with defined SLAs by severity tier.
- Deploy web application firewall (WAF) and API gateway for external-facing applications.
- Implement privileged access management (PAM) solution for all administrator accounts.
- Develop and test an Incident Response Plan (IRP) and Disaster Recovery (DR) runbooks.
- Conduct quarterly phishing simulation exercises for all staff.

4. Horizon 3 — Security Transformation (Months 9–24)

- Pursue ISO/IEC 27001 certification or equivalent compliance framework alignment.
- Implement Zero Trust Architecture (ZTA) principles across network and application access.
- Establish a Security Operations Centre (SOC) function — internal or managed service.
- Integrate security testing into the Software Development Lifecycle (DevSecOps).
- Deploy Security Orchestration, Automation and Response (SOAR) to accelerate incident handling.
- Establish a Threat Intelligence programme to proactively monitor for emerging threats.
- Implement Data Loss Prevention (DLP) across endpoints, email, and cloud platforms.
- Conduct annual red team exercises to continuously validate security controls.
- Develop a Board-level security reporting dashboard with KPIs and risk metrics.

5. Compliance & Certification Pathway

- ISO/IEC 27001 — Information Security Management System (ISMS) certification.
- Cyber Essentials / Cyber Essentials Plus — baseline government-backed certification.
- PCI-DSS — if the Client processes, stores, or transmits cardholder data.
- SOC 2 Type II — for SaaS or cloud-hosted service providers.
- GDPR Article 32 compliance — technical and organisational security measures.
- NIST Cybersecurity Framework (CSF) maturity assessment and improvement.

6. Security Metrics & KPIs

- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to security incidents.
- Vulnerability remediation rate: percentage of Critical/High findings resolved within SLA.
- Phishing simulation click rate — target reduction of >70% year-on-year.
- Patch compliance rate: percentage of endpoints patched within defined SLA windows.
- Number of security incidents per quarter — trend analysis over rolling 12 months.
- Security awareness training completion rate across all staff.

9. METHODOLOGY & STANDARDS

All testing activities are conducted in alignment with internationally recognised frameworks and standards to ensure consistency, repeatability, and professional quality.

- PTES — Penetration Testing Execution Standard
- OWASP Testing Guide v4 (web components)
- NIST SP 800-115 — Technical Guide to Information Security Testing
- CVSS v3.1 for vulnerability severity scoring
- CIS Benchmarks for endpoint and device configuration review
- MITRE ATT&CK Framework for adversary technique mapping

SATYA TECHNOLOGIES
We Believe in Solutions

10. DELIVERABLES & TIMELINE

#	Deliverable	Description	ETA
1	Kick-off Meeting	Scope confirmation, rules of engagement sign-off	Day 0
2	Reconnaissance Report	OSINT findings, network map, asset inventory	Day 3
3	VAPT Vulnerability Scan	Authenticated scans, CVSS-rated findings, tool output	Day 6
4	Vulnerability Report (Draft)	All identified vulnerabilities with CVSS ratings	Day 8
5	Penetration Test Report	Exploitation evidence, attack chains, impact analysis	Day 12
6	Executive Summary	C-level briefing document — non-technical risk overview	Day 13
7	Remediation Guidance	Prioritised fix list with implementation guidance	Day 13
8	Security Roadmap	12-month phased security improvement programme	Day 14
9	Debrief	Live walkthrough of findings with Client team	Day 14
10	Retest (optional)	Verification of patched vulnerabilities	Day 28

SATYA TECHNOLOGIES
We Believe in Solutions

11. LEGAL & COMPLIANCE

All security testing activities described in this document are performed exclusively within the authorised scope and are conducted in compliance with applicable laws and regulations including, but not limited to:

- Computer Misuse Act 1990 and equivalent legislation in the Client's jurisdiction
- General Data Protection Regulation (GDPR)
- ISO/IEC 27001 Information Security Management requirements
- Any sector-specific regulatory requirements (PCI-DSS, HIPAA, etc.) applicable to the Client

The assessment team will immediately halt all activities and notify the Client's point of contact if any evidence of an active third-party breach is discovered during testing.

12. TERMS & AUTHORISATION

This project plan is subject to a separate Rules of Engagement (RoE) agreement and Non-Disclosure Agreement (NDA) which must be signed by authorised representatives of both parties prior to commencement of any testing activity.

On behalf of the Client	On behalf of the Assessment Team
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

Document generated: 22 April 2026 | Classification: CONFIDENTIAL | This document contains commercially sensitive information and must not be shared without written authorisation.

SATYA TECHNOLOGIES
We Believe in Solutions