PENETRATION TEST | SAMPLE REPORT

Network & Infrastructure Penetration Test

An illustrative sample of the report Offload Security delivers — external and internal findings, an attack-path narrative, remediation, and full PCI / NIST / ISO / CIS / SOC 2 mapping.

Targets	203.0.113.0/24 (external), 10.20.0.0/16 (internal) — illustrative
Engagement	External + internal network penetration test
Standards	PCI DSS 4.0.1 (11.4), NIST 800-53, ISO 27001:2022, CIS Controls v8, SOC 2
Prepared by	Offload Security
Classification	Sample / illustrative data — not a real engagement

This is a **sample document** using illustrative data to demonstrate report structure and depth. It does not describe a real system or engagement.

1. Executive summary

The engagement identified **8 findings** across the external perimeter and internal network: **1 Critical**, **3 High**, **3 Medium** and **1 Low**. An unauthenticated remote code execution flaw on an internet-facing service (NET-01) provided an initial foothold; from there, a flat internal network and shared local-administrator credentials (NET-03) allowed lateral movement to a domain controller within the test window. This chain — external foothold to domain compromise — is the most urgent risk and should be remediated immediately.

Overall risk rating: **High.** Closing NET-01 and enforcing network segmentation (NET-03) would break the demonstrated attack path and materially reduce exposure.

Findings by severity

Severity	Count	Example
Critical	1	Unauthenticated RCE on exposed service
High	3	Flat network / lateral movement; default device credentials; unpatched internal hosts
Medium	3	Deprecated TLS; exposed management interface; weak password policy
Low	1	Verbose service banners disclosing versions

2. Scope & methodology

Scope: external perimeter (203.0.113.0/24) and internal network (10.20.0.0/16). Testing was authorized, time-boxed and non-destructive. **Methodology:** aligned to PTES/OSSTMM — reconnaissance, discovery and enumeration (Nmap-family, OpenVAS), vulnerability analysis, controlled exploitation, and internal post-exploitation / lateral movement. Findings were validated against CVEs and scored with CVSS, enriched by CISA KEV and EPSS.

3. Attack path summary

1. Internet-facing service on 203.0.113.14 running outdated software → unauthenticated RCE (NET-01) → foothold as a service account.
2. No egress or segmentation controls → pivot into internal 10.20.0.0/16 (NET-03).
3. Shared local-admin password recovered → lateral movement across workstations.
4. Kerberoasting & unpatched host → privilege escalation to Domain Admin.

4. Standards coverage

Finding	NIST	ISO 27001	CIS v8	PCI DSS	SOC 2
NET-01 Unauthenticated RCE	RA-5, SI-2	A.8.8	CIS 7	Req 6.3	CC7.1
NET-02 Default device credentials	IA-5	A.5.17	CIS 5	Req 8	CC6.1
NET-03 Flat / no segmentation	SC-7	A.8.22	CIS 12	Req 1.3	CC6.1
NET-04 Deprecated TLS	SC-13	A.8.24	CIS 3	Req 4	CC6.7
NET-05 Unpatched internal hosts	RA-5	A.8.8	CIS 7	Req 6.3	CC7.1

5. Detailed findings

NET-01 — Unauthenticated remote code execution	CRITICAL
Category	External · vulnerable service
Affected host	203.0.113.14:8080 (application server)
Description	The internet-facing service runs an outdated framework with a known unauthenticated RCE vulnerability. A remote attacker can execute arbitrary commands with the service account's privileges.
Evidence	`curl -s http://203.0.113.14:8080/... payload -> id: uid=997(svc-app) — remote command execution confirmed`
Impact	Full compromise of the host and initial foothold into the environment. Directly exploitable without credentials.
Remediation	Patch the affected software to a fixed version immediately. Restrict the service to required networks, run it as a least-privilege account, and place it behind a WAF/reverse proxy as an interim control.
Control mapping	NIST RA-5, SI-2 • ISO A.8.8 • CIS 7 • PCI Req 6.3 • SOC 2 CC7.1 • CVSS 9.8 • EPSS High

NET-03 — Flat network enabling lateral movement	HIGH
Category	Internal · segmentation
Affected host	10.20.0.0/16 (internal network)
Description	The internal network has no meaningful segmentation. From a single compromised host, an attacker can reach workstations, servers and domain controllers without crossing any security boundary.
Evidence	`From 10.20.4.31 (foothold): reachable 10.20.0.10 (DC), 10.20.2.0/24 (workstations), 10.20.8.0/24 (servers)`
Impact	Turns a single-host compromise into full-environment exposure; directly enabled escalation to Domain Admin in testing.
Remediation	Segment the network by function and trust (e.g. user, server, management, PCI zones). Restrict east-west traffic with host firewalls/ACLs and require authentication between segments. Validate with re-testing.
Control mapping	NIST SC-7 • ISO A.8.22 • CIS 12 • PCI Req 1.3 • SOC 2 CC6.1 • CVSS 8.2

NET-04 — Deprecated TLS protocols & weak ciphers	MEDIUM
Category	External · cryptography
Affected host	203.0.113.20:443, 203.0.113.25:443
Description	Public services support TLS 1.0/1.1 and weak cipher suites, exposing sessions to downgrade and interception attacks.
Evidence	`testssl.sh: TLS 1.0 offered (yes), TLS 1.1 offered (yes), weak ciphers (3DES) present`
Impact	Weakens transport security and may fail PCI DSS and modern compliance requirements.
Remediation	Disable TLS 1.0/1.1 and weak ciphers; enforce TLS 1.2+ with strong suites and HSTS.
Control mapping	NIST SC-13 • ISO A.8.24 • CIS 3 • PCI Req 4 • SOC 2 CC6.7 • CVSS 5.9

6. Appendix — tools & methodology

Tool	Purpose	Version
Nmap	Host discovery, port & service enumeration	7.9x
OpenVAS / GVM	Network vulnerability scanning	current
testssl.sh	TLS / certificate analysis	3.2.x
Manual testing	Controlled exploitation, lateral movement, AD testing	—

Severity is scored with CVSS v3.1 and enriched with CISA KEV (known-exploited) and EPSS (exploit-probability) context. All findings in this sample are illustrative.