# CODINGBOLT

# NETWORK PENETRATION TEST

Public Sample / Illustrative Deliverable

NOT A REAL CLIENT ASSESSMENT

External & Internal Network Security Assessment

| | |
|---|---|
| Document Type | Public Sample Report |
| Client | CodingBolt Sample Environment (Fictional) |
| Assessment Type | Illustrative External + Internal Network Penetration Test |
| Assessment Period | 01–05 August 2026 (Illustrative) |
| Report Version | v1.0 |
| Prepared By | CodingBolt Cyber Security Team |
| Classification | Public Sample — For Demonstration Purposes Only |

Public-use disclaimer: This document is a fictional sample created by CodingBolt to demonstrate the structure, methodology, evidence presentation, severity classification, remediation guidance, and retesting approach used in penetration-testing deliverables. All organization names, assets, IP addresses, findings, evidence, dates, statuses, and results are illustrative. They do not represent a real client assessment.

# 1. Document Control

Document Owner

Cyber Security Assessment Team

Document Purpose

External and internal network penetration testing deliverable

Classification

Confidential

Version

1.0

Status

Sample / Draft for Client Review

Distribution

## 1.1 Assessment Objective

The objective is to identify and validate security weaknesses across internet-facing infrastructure and the internal network while using non-disruptive validation wherever possible.

## 1.2 Assessment Requirements

The supplied requirements call for annual third-party testing of internet-facing systems, infrastructure and services, including vulnerability scanning and appropriate non-disruptive validation/exploitation. Internal testing should evaluate attack paths, privilege escalation opportunities, network segmentation and common misconfigurations. Medium, High and Critical findings are expected to be remediated.

# 2. Executive Summary

A combined external and internal network penetration test was performed against a representative enterprise environment. Testing focused on perimeter exposure, reachable services, infrastructure configuration, internal attack paths and network segmentation.

In this sample scenario, six findings were identified. The most significant risks were Internet-exposed remote administration, legacy TLS protocols, insufficient SMB signing enforcement and inadequate segmentation. The findings demonstrate how an attacker with an initial foothold could potentially expand access if compensating controls are not present.

Overall risk rating: HIGH

Severity

Count

Illustrative Status

Critical

0

N/A

High

3

Remediated / Validation Pending

Medium

2

Remediated

Low

1

Remediated

Key observations

■ External exposure: A remote administration service was reachable from the public Internet.

■ Cryptographic posture: Legacy TLS versions were accepted by an internet-facing service.

■ Internal infrastructure: SMB signing was not enforced on a representative server.

■ Segmentation: Workstation-to-management and workstation-to-server connectivity was broader than intended.

# 3. Scope & Rules of Engagement

## 3.1 External Network Scope

Asset

Type

Purpose

Status

203.0.113.10

Public IPv4

Internet-facing gateway / application edge

In scope

203.0.113.11

Public IPv4

VPN / remote access gateway

In scope

203.0.113.0/28

Public subnet

Perimeter address space

In scope

## 3.2 Internal Network Scope

Network

Representative Purpose

Assessment Coverage

10.20.10.0/24

Server VLAN

Service discovery, configuration validation, attack paths

10.20.20.0/24

User / workstation VLAN

Reachability and segmentation validation

10.20.30.0/24

Management VLAN

Access-control and segmentation validation

10.20.40.0/24

Infrastructure / network services

Common misconfiguration checks

## 3.3 Rules of Engagement

■ Testing assumes written authorization from the asset owner.

■ Validation is non-destructive unless controlled exploitation is explicitly approved.

■ Denial-of-service, stress testing, destructive payloads and data modification are excluded.

- Any suspected production impact is stopped and escalated immediately.
- Evidence is limited to what is required to demonstrate the condition.

# 4. Methodology

The assessment follows a structured penetration testing lifecycle aligned with the supplied external and internal network requirements.

Phase

Activities

1. Pre-engagement

Scope, authorization, asset inventory, test windows and contacts.

2. Reconnaissance

Identification of in-scope hosts, services, technologies and management interfaces.

3. Enumeration

Port/service discovery, version identification, protocol enumeration and configuration checks.

4. Vulnerability Assessment

Review of observed versions, configurations and known weaknesses.

5. Controlled Validation

Non-destructive validation of exploitable conditions and attack paths.

6. Internal Assessment

Host discovery, segmentation checks, privilege-path review and common infrastructure validation.

7. Risk Analysis

Severity assignment using likelihood, impact, exploitability and exposure.

8. Retest

Validation of fixes and documentation of residual risk.

## 4.1 Tooling (Illustrative)

Typical tools may include Nmap, vulnerability scanners, OpenSSL/TLS validation utilities, SMB enumeration utilities, traceroute, routing/ACL validation tools and manual protocol testing. Automated scanner output is not treated as proof of vulnerability; material findings are manually reviewed and validated where safe.

# 5. Risk Rating Methodology

Severity is determined from technical impact, exploitability, exposure, attack prerequisites and likely business consequence. CVSS can be used as a supporting metric, while final severity should reflect the client's environment and risk appetite.

| Severity | Typical interpretation | Recommended response |
| --- | --- | --- |
| Critical | Direct compromise of highly sensitive systems or severe business impact. | Immediate containment and emergency remediation. |
| High | Meaningful unauthorized access, privilege escalation or strong attack path. | Prioritize remediation. |
| Medium | Security weakness requiring additional conditions or limited impact. | Remediate within standard SLA. |
| Low | Limited impact or defense-in-depth weakness. | Planned hardening. |
| Informational | Observation without direct security impact. | Track where appropriate. |

# EXT-01 — Internet-Exposed Remote Administration Service

Severity

High

CVSS (illustrative)

8.1

Affected Asset

203.0.113.10:3389

Status

Illustrative Remediation / Retest Example

Description

Remote Desktop Protocol (RDP) was observed as reachable from the public Internet. The service provides a direct remote administration interface and increases perimeter attack surface.

Security Impact

Internet exposure makes the service available to opportunistic scanning and credential attacks. If valid credentials are compromised, an attacker could obtain interactive access and potentially use the host as an initial foothold.

Evidence / Validation

```
$ nmap -sV --reason 203.0.113.10
```

3389/tcp open ms-wbt-server exposed to Internet

Validation: exposure confirmed; no password spraying or destructive exploitation performed.

Recommended Remediation

■ Remove direct Internet exposure wherever possible.

■ Restrict RDP to a VPN, zero-trust access gateway or approved management jump host.

■ Enforce MFA for remote administration.

■ Apply network ACLs and dedicated management accounts.

Retest / Closure Criteria

Closure should demonstrate that 3389 is no longer reachable from unauthorized Internet sources and approved remote access requires the secure access path.

# EXT-02 — Legacy TLS Protocols Enabled

Severity

Medium

CVSS (illustrative)

6.5

Affected Asset

203.0.113.10:443

Status

Remediated

Description

An internet-facing TLS endpoint accepted legacy TLS 1.0 and TLS 1.1 connections in the sample configuration.

Security Impact

Legacy protocols weaken the cryptographic baseline and may conflict with organizational standards or compliance requirements.

Evidence / Validation

```
$ ssl-enum-ciphers -p 443 203.0.113.10
```

TLS 1.0 accepted — FINDING

TLS 1.1 accepted — FINDING

TLS 1.2 available — OK

Recommended Remediation

■ Disable TLS 1.0 and TLS 1.1.

■ Retain TLS 1.2 and, where supported, TLS 1.3.

■ Use an approved cipher suite baseline.

■ Retest externally after deployment.

Retest / Closure Criteria

Closure should show legacy protocol negotiation is rejected from an external test point.

# INT-01 — SMB Signing Not Enforced

Severity

High

CVSS (illustrative)

8.0

Affected Asset

10.20.10.15:445

Status

Illustrative Remediation / Retest Example

Description

SMB message signing was supported but not enforced on a representative internal server.

Security Impact

Where an attacker can position themselves on a suitable internal path, lack of enforced signing can increase exposure to relay-style attacks and credential forwarding. Impact depends on topology and authentication configuration.

Evidence / Validation

```
$ nmap --script smb2-security-mode -p445 10.20.10.15
```

445/tcp open microsoft-ds

Message signing enabled but not required

Validation stopped after configuration evidence.

Recommended Remediation

■ Require SMB signing on servers and clients where feasible.

■ Review NTLM usage and reduce legacy authentication dependencies.

■ Prioritize domain controllers and high-value servers.

■ Monitor abnormal SMB authentication and lateral movement indicators.

Retest / Closure Criteria

Closure should demonstrate that SMB signing is required, not merely supported, on affected systems.

# INT-02 — Insufficient Network Segmentation

Severity

High

CVSS (illustrative)

7.5

Affected Asset

10.20.20.0/24 → 10.20.30.0/24

Status

Illustrative Remediation / Retest Example

Description

Workstation network connectivity to the management network was broader than expected under a least-privilege segmentation model.

Security Impact

An attacker who compromises a workstation may gain unnecessary reachability to management interfaces, making lateral movement and targeting of administrative infrastructure easier.

Evidence / Validation

```
$ nmap -Pn -p 445,3389 10.20.30.0/24
```

Workstation VLAN -> Management VLAN: reachable

Expected: restricted management-plane access

Result: segmentation control requires review.

Recommended Remediation

■ Implement explicit inter-VLAN ACLs/firewall rules.

■ Permit management protocols only from approved administrator/jump-host networks.

■ Deny workstation-to-management access by default.

■ Review allowed flows periodically.

Retest / Closure Criteria

Closure should confirm unauthorized workstation sources can no longer reach management services while approved administrative flows remain functional.

# INT-03 — Excessive Internal Service Exposure

Severity

Medium

CVSS (illustrative)

5.3

Affected Asset

10.20.10.0/24

Status

Remediated

Description

Several internal hosts exposed services that were not required for the documented role of the systems.

Security Impact

Unnecessary services increase the internal attack surface and provide additional opportunities for exploitation after an initial compromise.

Evidence / Validation

Representative validation:

10.20.10.22:21/tcp reachable — service not required

10.20.10.25:8080/tcp reachable — management interface

Finding based on exposure/role mismatch; exploit attempts not required.

Recommended Remediation

■ Disable unused services and remove unnecessary software.

■ Restrict management interfaces to administrative networks.

■ Maintain a current service ownership inventory.

■ Add firewall rules where services are required but should not be broadly reachable.

Retest / Closure Criteria

Closure should demonstrate unnecessary services are disabled or restricted to approved source networks.

# INT-04 — ICMP / Host Discovery Information Disclosure

Severity

Low

CVSS (illustrative)

3.1

Affected Asset

Internal network segments

Status

Remediated

Description

Network hosts responded to ICMP and discovery probes more broadly than required for the sample environment.

Security Impact

ICMP is not inherently a vulnerability. Broad discovery responses can assist host enumeration and network mapping after an attacker gains internal access.

Evidence / Validation

```
$ ping 10.20.20.25
```

10.20.20.25 — response received

Observation: discovery permitted across a broader segment than required.

Recommended Remediation

■ Restrict ICMP between sensitive zones where operationally appropriate.

■ Keep approved monitoring and troubleshooting paths available.

■ Apply zone-based policy rather than disabling ICMP indiscriminately.

Retest / Closure Criteria

Closure should demonstrate that discovery traffic is limited according to documented segmentation policy without disrupting legitimate operations.

# 12. Remediation Roadmap

Illustrative prioritization; adapt to the client's actual SLA and risk acceptance process.

| Priority | Action | Owner | Target |
| --- | --- | --- | --- |
| P1 | Remove Internet exposure of RDP; secure remote-access path and MFA. | Infrastructure / IAM | Immediate |
| P1 | Enforce SMB signing and review NTLM/relay exposure. | Windows / Infrastructure | Immediate |
| P1 | Restrict workstation-to-management paths. | Network Security | Immediate |
| P2 | Disable TLS 1.0/1.1 and standardize TLS configuration. | Infrastructure | 7–14 days |
| P2 | Remove/restrict unnecessary internal services. | Infrastructure | 14–30 days |
| P3 | Tune ICMP/discovery controls. | Network Security | 30–60 days |

# 13. Evidence Appendix

The following images are simulated evidence created for this sample report. In a real engagement, replace each image with an authorized screenshot captured during testing and include the affected asset, timestamp and evidence reference.

Figure 1 — External service exposure validation — SIMULATED EVIDENCE

This public sample does not represent real client evidence. Replace with an authorized screenshot from the relevant engagement in a client-specific report.

SIMULATED EVIDENCE NOTICE: Any evidence shown or described in this public sample is illustrative and must not be interpreted as evidence from an actual customer environment.

Figure 2 — TLS protocol validation — SIMULATED EVIDENCE

This public sample does not represent real client evidence. Replace with an authorized screenshot from the relevant engagement in a client-specific report.

SIMULATED EVIDENCE NOTICE: Any evidence shown or described in this public sample is illustrative and must not be interpreted as evidence from an actual customer environment.

Figure 3 — SMB signing validation — SIMULATED EVIDENCE

This public sample does not represent real client evidence. Replace with an authorized screenshot from the relevant engagement in a client-specific report.

SIMULATED EVIDENCE NOTICE: Any evidence shown or described in this public sample is illustrative and must not be interpreted as evidence from an actual customer environment.

Figure 4 — Internal segmentation validation — SIMULATED EVIDENCE

This public sample does not represent real client evidence. Replace with an authorized screenshot from the relevant engagement in a client-specific report.

SIMULATED EVIDENCE NOTICE: Any evidence shown or described in this public sample is illustrative and must not be interpreted as evidence from an actual customer environment.

# 14. Retest & Closure Template

A remediation retest should validate the original condition from an equivalent network position and record whether the issue is Closed, Partially Remediated or Still Open.

Finding

Original State

Retest Result

Evidence

Status

EXT-01

RDP Internet exposure

[Result]

[Screenshot / scan]

[Closed/Open]

EXT-02

TLS 1.0/1.1 enabled

[Result]

[TLS scan]

[Closed/Open]

INT-01

SMB signing not required

[Result]

[SMB validation]

[Closed/Open]

INT-02

Broad workstation→management access

[Result]

[ACL/connectivity]

[Closed/Open]

INT-03

Unnecessary services

[Result]

[Service scan]

[Closed/Open]

INT-04

Discovery exposure

[Result]

[Connectivity test]

[Closed/Open]

# 15. Conclusion

This sample demonstrates a complete third-party network penetration testing deliverable covering both internet-facing and internal network requirements. The structure separates executive-level risk communication from technical evidence, remediation guidance and retest criteria.

For an actual engagement, all illustrative assets, findings, screenshots, CVSS values, dates and statuses must be replaced with verified assessment results. Findings should not be reported solely from automated scanner output; material issues should be manually reviewed and validated where safe.

# PUBLIC SAMPLE NOTICE

This report is published by CodingBolt for demonstration and marketing purposes. It is not evidence of a penetration test performed against any real organization. A real client deliverable must use verified scope, authorization, timestamps, evidence, findings, severity, remediation status, and retest results from that engagement.

For authorized penetration testing and security assessment services, visit codingbolt.in.