CyberSec Pro cyber-sec-pro.com

Technical Report — Sample

Technical Report

REPORT DATE
2026-09-27 06:07 UTC
SCANS PERFORMED
3 scan(s)
TOTAL FINDINGS
14
RISK LEVEL
Critical

CONFIDENTIAL — AUTHORIZED RECIPIENTS ONLY

Generated by CyberSec Pro | cyber-sec-pro.com
© 2026 CyberSec Pro. All rights reserved.

Table of Contents

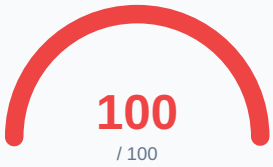
Technical Report — Sample

CyberSec Pro cyber-sec-pro.com

Technical Report

Generated: 2026-09-27 06:07 UTCScans: 3Findings: 14 **Risk: Critical**

Risk Assessment



Overall Risk Score: 100/100

The risk score is calculated based on the severity and quantity of findings discovered during the assessment.

CRITICAL

2

14.3%

HIGH

4

28.6%

MEDIUM

6

42.9%

LOW / INFO

2

7.1%

Executive Summary

The assessment targeted **1** using the following tools: **Nmap, SSL Labs / testssl.sh, Nikto**. Targets scanned: `demo.cyber-sec-pro.com`.

This security assessment was conducted on **2026-09-27** covering **3 scan(s)** across the target infrastructure. A total of **14 finding(s)** were identified, including **2 critical**, **4 high**, **6 medium**, and **1 low** severity issues. The overall risk level is assessed as **Critical**.

Scan Results

Scan #1: Nmap → demo.cyber-sec-pro.com

Tool	Nmap
Target	demo.cyber-sec-pro.com
Started	2026-09-27 05:55
Completed	2026-09-27 06:07
Scan ID	`sample-nmap`

FINDINGS (7)

CRITICAL **23/tcp open telnet — Telnet service exposed**

Telnet transmits credentials and session data in cleartext. Anyone on the path can read them.

HOW TO FIX THIS

Telnet is exposed and transmits credentials in cleartext

Risk if left unfixed: Anyone on the network path can capture the login and session, taking full control of the device.

1. Disable the Telnet service.
2. Enable SSH instead and restrict it to known management IPs.
3. If a device only supports Telnet, place it behind a VPN or management VLAN.

References: CIS Controls v8 4.1 · NIST SP 800-52r2

HIGH **3389/tcp open ms-wbt-server — RDP reachable from the internet**

Remote Desktop is directly reachable and is a primary target for credential stuffing and ransomware operators.

HOW TO FIX THIS

Remote Desktop (RDP) is exposed

Risk if left unfixed: RDP is heavily targeted by brute-force and exploit campaigns (e.g. BlueKeep) and is a common ransomware entry point.

1. Do not expose RDP to the internet — require a VPN.
2. Enable Network Level Authentication.
3. Enforce account lockout and MFA.
4. Keep the host patched against known RDP CVEs.

References: CISA guidance on RDP · CIS Controls v8 4.6

HIGH **445/tcp open microsoft-ds — SMB exposed**

SMB should never be reachable from an untrusted network.

HOW TO FIX THIS

SMB file sharing is reachable

Risk if left unfixed: SMB has a history of wormable vulnerabilities (EternalBlue) and often exposes shares or allows null sessions.

1. Block SMB (445/139) at the network perimeter.
2. Disable SMBv1 entirely.
3. Require authentication and remove anonymous/guest share access.
4. Patch against known SMB CVEs.

References: CISA: Disable SMBv1 · CIS Controls v8 4.8

MEDIUM **21/tcp open ftp — FTP without TLS**

vsftpd 3.0.3 accepting plaintext logins.

HOW TO FIX THIS

FTP is exposed and transmits credentials and data in cleartext

Risk if left unfixed: Credentials and transferred files can be intercepted; anonymous FTP may expose files directly.

1. Replace FTP with SFTP (over SSH) or FTPS (over TLS).
2. Disable anonymous access if it is not required.
3. Restrict access to trusted source addresses.

References: OWASP Transport Layer Protection Cheat Sheet

MEDIUM **161/udp open snmp — SNMPv1 responds to the default community string**

SNMPv1 has no encryption and 'public' returns the full device inventory.

HOW TO FIX THIS

SNMP is reachable

Risk if left unfixed: SNMP with a default community string discloses interfaces, routes, processes and serial numbers, and v1/v2c sends them in cleartext.

1. Change default community strings; never leave "public" or "private".
2. Move to SNMPv3 with authentication and privacy.
3. Restrict SNMP to the monitoring host only.

References: NIST SP 800-53 SC-8

CONFIDENTIAL

LOW **22/tcp open ssh — OpenSSH 7.4**

Reachable from any source address.

HOW TO FIX THIS

SSH is reachable from this network

Risk if left unfixed: SSH is the usual route to a shell on the host, so it is a standing target for credential stuffing and for any CVE in the running version.

1. Restrict SSH to known management addresses with a firewall rule or security group.
2. Disable password authentication and use keys: PasswordAuthentication no.
3. Disable direct root login: PermitRootLogin no.
4. Keep OpenSSH patched, and remove accounts that no longer need shell access.
5. If the host must be reachable from the internet, put SSH behind a VPN or bastion instead.

References: CIS Benchmark — OpenSSH Server · NIST SP 800-123

INFO **80/tcp open http — plaintext HTTP**

Serves content without TLS.

HOW TO FIX THIS

The service answers over plaintext HTTP

Risk if left unfixed: Anything sent over HTTP — credentials, session cookies, form data — can be read or altered by anyone on the network path.

1. Serve the site over HTTPS with a valid certificate.
2. Redirect HTTP to HTTPS, and keep the redirect relative or hardcoded to https.
3. Add Strict-Transport-Security once HTTPS is confirmed working.
4. Mark session cookies Secure and HttpOnly.

References: OWASP Transport Layer Protection Cheat Sheet · RFC 6797

RAW TOOL OUTPUT

```
Starting Nmap 7.94 ( https://nmap.org )
Nmap scan report for demo.cyber-sec-pro.com
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.3
22/tcp    open  ssh         OpenSSH 7.4 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
80/tcp    open  http        nginx 1.18.0
445/tcp   open  microsoft-ds Samba smbd 4.6.2
3389/tcp  open  ms-wbt-server xrdp
161/udp   open  snmp        SNMPv1 server
```

Scan #2: SSL Labs / testssl.sh → demo.cyber-sec-pro.com

Tool	SSL Labs / testssl.sh
Target	demo.cyber-sec-pro.com
Started	2026-09-27 05:55
Completed	2026-09-27 06:07
Scan ID	`sample-testssl`

FINDINGS (4)

CRITICAL SSLv3 is offered — POODLE

CVE-2014-3566

SSLv3's CBC padding can be decrypted a byte at a time by an active network attacker.

HOW TO FIX THIS

An obsolete SSL protocol (SSLv2/SSLv3) is enabled

Risk if left unfixed: SSLv3 is broken (POODLE); an attacker can decrypt session data.

1. Disable SSLv2 and SSLv3 on the server.
2. Enable only TLS 1.2 and TLS 1.3.
3. Re-test with an SSL scanner to confirm the weak protocols are gone.

References: RFC 7568 (SSLv3 deprecation) · Mozilla Server Side TLS

HIGH TLS 1.0 is still enabled

Deprecated by RFC 8996 and disallowed by PCI DSS.

HOW TO FIX THIS

A deprecated TLS version (1.0/1.1) is enabled

Risk if left unfixed: TLS 1.0/1.1 have known weaknesses and fail PCI-DSS and modern compliance baselines.

1. Disable TLS 1.0 and TLS 1.1.
2. Enable TLS 1.2 and TLS 1.3 only.
3. Update cipher suites to remove RC4, 3DES and CBC-only suites.

References: PCI-DSS v4.0 4.2.1 · Mozilla Server Side TLS

MEDIUM Certificate is self-signed

No client can verify this certificate, so every TLS warning becomes noise users learn to click through.

HOW TO FIX THIS

The TLS certificate is self-signed

Risk if left unfixed: Clients cannot verify the server's identity, which enables man-in-the-middle attacks.

1. Replace the self-signed certificate with one from a trusted CA.
2. For internal services, distribute your internal CA to clients instead of self-signing per host.

References: NIST SP 800-52r2

MEDIUM Certificate expired 34 days ago

Browsers hard-fail an expired certificate.

HOW TO FIX THIS

The TLS certificate has expired

Risk if left unfixed: Clients see security warnings and may refuse to connect; trust in the service is broken.

1. Renew the certificate with your CA (or Let's Encrypt).
2. Install the full chain, not just the leaf certificate.
3. Automate renewal so this does not recur (e.g. certbot, ACME).

References: CA/Browser Forum Baseline Requirements

RAW TOOL OUTPUT

```
Testing protocols via sockets
SSLv2      not offered (OK)
SSLv3      offered (NOT ok)
TLS 1      offered (deprecated)
TLS 1.2    offered (OK)
TLS 1.3    not offered
```

Scan #3: Nikto → demo.cyber-sec-pro.com

Tool	Nikto
Target	demo.cyber-sec-pro.com
Started	2026-09-27 05:55
Completed	2026-09-27 06:07
Scan ID	`sample-nikto`

FINDINGS (3)

HIGH **Content-Security-Policy header is missing**

Nothing constrains where scripts may be loaded from, so any injected markup executes.

HOW TO FIX THIS

No Content-Security-Policy is set

Risk if left unfixed: Without a CSP, an injected script runs with full page privileges — the main defence against XSS is absent.

1. Define a CSP starting from `default-src 'self'`.
2. Remove inline scripts or allow them with a nonce/hash rather than 'unsafe-inline'.
3. Deploy in report-only mode first to find violations before enforcing.

References: OWASP Content Security Policy Cheat Sheet

MEDIUM **Strict-Transport-Security header is missing**

A first request over plaintext HTTP can be intercepted and downgraded.

HOW TO FIX THIS

HTTP Strict Transport Security (HSTS) is not set

Risk if left unfixed: Users can be downgraded to plaintext HTTP by an on-path attacker before the redirect to HTTPS.

1. Send `Strict-Transport-Security: max-age=31536000; includeSubDomains`.
2. Only enable after confirming every subdomain serves HTTPS.
3. Consider HSTS preloading once stable.

References: OWASP HSTS Cheat Sheet

MEDIUM **X-Frame-Options header is missing — clickjacking**

The page can be framed by a third-party site and overlaid.

HOW TO FIX THIS

The X-Frame-Options / frame-ancestors protection is missing

Risk if left unfixed: The page can be framed by a malicious site and used for clickjacking.

1. Send `Content-Security-Policy: frame-ancestors 'none'` (or a trusted origin).
2. For older clients, also send `X-Frame-Options: DENY`.

References: OWASP Clickjacking Defense Cheat Sheet

RAW TOOL OUTPUT

```
- Nikto v2.5.0
+ Target: https://demo.cyber-sec-pro.com
+ The anti-clickjacking X-Frame-Options header is not present.
+ The site does not send a Content-Security-Policy header.
+ Strict-Transport-Security header not present.
```

Recommendations

CRITICAL:2 critical finding(s) require immediate remediation. Patch vulnerable services, rotate exposed credentials, and assess blast radius.

HIGH:4 high-severity issue(s) found. Schedule remediation within 7 days. Review service configurations and update vulnerable software versions.

MEDIUM:6 medium-severity finding(s). Plan remediation within 30 days. Harden configurations and implement defense-in-depth controls.

LOW:1 low-severity issue(s). Address during next maintenance window. These represent informational findings and best-practice improvements.

Methodology

This assessment was performed using **CyberSec Pro**, a cloud-based offensive security platform running **183 Kali Linux tools** across 18 categories. All scans were conducted with proper authorization.

Platform	CyberSec Pro v4.0
Report Template	Technical Report
Generated	2026-09-27 06:07 UTC
Classification	Confidential
Data residency	Canada

Automated assessment

Content digest

This report is confidential and intended only for authorized recipients.
© 2026 CyberSec Pro. All rights reserved.