Probe Spark

LEVEL 2 · NETWORK

Internal and External Network Penetration Test · **Penetration Test**

Internal and External Network Penetration Test

Prepared for **Northwind Manufacturing** (fictional sample client)

CLIENT	PROVIDER
Northwind Manufacturing (manufacturing, sample equivalent)	ProbeSpark · a SalesSpark / HCD service
WINDOW	**SCOPE**
July 6 to July 15, 2026	Internal 10.0.0.0/24, external johndoe-demo.com and edge IP

CONFIDENTIAL

1. Executive summary

COULD AN ATTACKER TURN ONE WEAK CREDENTIAL INTO ACCESS ACROSS THE ENVIRONMENT

ProbeSpark performed an authorized internal and external network penetration test of the Northwind Manufacturing environment. The engagement enumerated the network, tested exposed services, and validated whether discovered weaknesses could be chained into broader access.

The environment contains several serious exposures. A single default credential on an exposed Telnet service granted administrative access and led to reachability across ten additional systems, a camera recorder, and multiple printers. The findings below are ranked by risk, each backed by reproducible evidence in the technical appendix.

- **One default credential opened the environment.** A default root login on Telnet led to access across ten more systems.
- **Unauthenticated devices are exposed.** Printers and a camera recorder allowed access without valid credentials.
- **The application layer needs hardening.** A public web form does not properly validate input.

How ProbeSpark tested this. This engagement used AI-augmented discovery and correlation with qualified human validation. Automated service and default-credential checks identified the exposures; a tester safely confirmed the default logins and the lateral reach without altering or removing data. Every finding is backed by reproducible evidence in the restricted appendix.

Information governance rating

BUSINESS IMPACT ACROSS THE CIA TRIAD

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Medium Impact	**Medium Impact**	**Medium Impact**

A single default credential produced access across multiple systems, and unauthenticated devices exposed data. The overall impact to confidentiality, integrity, and availability is moderate and readily reduced by the remediation below.

2. Findings overview

6 FINDINGS

1	1	3	1
CRITICAL	HIGH	MEDIUM	LOW

ID	FINDING	SEVERITY	AREA
NF-01	Default root credentials on exposed Telnet, leading to lateral access	Critical	Credentials
NF-02	Camera recorder (DVR) accessible with default credentials	High	Credentials
NF-03	Anonymous access to printers on port 9100	Medium	Exposed services
NF-04	SNMP with default community strings on printers	Medium	Exposed services
NF-05	Weak input validation on a public web form	Medium	Web application
NF-06	Expired TLS certificate on an unused web server	Low	Transport security

3. Detailed findings

VULNERABILITY, IMPACT, AND THE FIX

NF-01

Critical

Default root credentials on exposed Telnet, leading to lateral access

CWE-521 Weak Password Requirements; MITRE ATT&CK T1110 Brute Force

What we found	An internet-of-things-era Telnet service on 10.0.0.87 accepted the default root password. From that access, ten additional internal systems were reachable.
Business impact	A single default credential produces administrative access and a path across the environment. This is the highest-risk finding.
Remediation	Disable Telnet in favor of SSH, reset the default password, enforce a password policy, and segment the reachable hosts. **Owner: IT / Infrastructure.**
Mitigation effort	Reset the default password (about 15 minutes), publish a password policy (about 1 hour), add MFA where supported (about 15 minutes per account), and review whether the ten reachable hosts should intercommunicate (a design session).

NF-02

High

Camera recorder (DVR) accessible with default credentials

CWE-1392 Use of Default Credentials

What we found	A network video recorder (Nightowl-class DVR) exposed a management interface that accepted the default username and password, allowing access to recorded footage.
Business impact	Physical-security footage is viewable by anyone who reaches the device, a privacy and safety concern.
Remediation	Change the default credentials, restrict the device to a management VLAN, and remove it from any internet-reachable path. **Owner: IT / Physical Security.**
Mitigation effort	Change credentials and restrict access (about 30 minutes); VLAN placement may need a short design session.

NF-03

Medium

Anonymous access to printers on port 9100

Exposed unauthenticated service

What we found	Four printers exposed port 9100 with anonymous access, allowing retrieval of print history and the ability to print pages.
Business impact	Print data may be disclosed, and the devices can be abused.
Remediation	Disable anonymous access, require authentication, and limit port 9100 to trusted internal sources. **Owner: IT.**

Mitigation effort	Disable anonymous access (about 15 minutes per device); restricting the port may need a short discovery session.

NF-04

Medium

SNMP with default community strings on printers

CWE-1392; SNMP default community

What we found	Printers responded to SNMP with default community strings, disclosing device and configuration information.
Business impact	Aids reconnaissance and can expose configuration detail.
Remediation	Disable SNMP where unused, or move to SNMPv3 with authentication; remove default community strings. **Owner: IT.**
Mitigation effort	About 15 minutes per device.

NF-05

Medium

Weak input validation on a public web form

OWASP A03 Injection

What we found	A public website form does not properly validate input, allowing crafted input to influence backend handling.
Business impact	Depending on the backend, this can expose or corrupt data.
Remediation	Implement server-side input validation, parameterized queries, and output encoding. **Owner: Web / Engineering.**
Mitigation effort	Web and database development effort; scope confirmed at a short design session.

NF-06

Low

Expired TLS certificate on an unused web server

Certificate hygiene

What we found	An external web server presented an expired TLS certificate.
Business impact	Erodes trust and can mask other issues; the server appears unused.
Remediation	Replace the certificate or decommission the unused server. **Owner: Platform.**
Mitigation effort	About 30 minutes to replace, or a short session to confirm decommissioning.

Proven attack path

HOW THE COMPROMISE UNFOLDED, STEP BY STEP

1. **Internal foothold.** Testing began from an authorized internal host (10.0.0.205), simulating a compromised workstation.
2. **Host discovery.** The internal range was enumerated and host 10.0.0.87 was identified.
3. **Service scan.** A TCP port scan of 10.0.0.87 found a Telnet service exposed on port 23.
4. **Default-credential check.** An automated default-credential pass was run against the exposed service.
5. **Access.** The default root credential succeeded, granting local administrative access to the host.
6. **Lateral movement.** From that foothold, ten additional internal systems, a camera recorder, and several printers were reachable through default or anonymous access. Testing stopped at proof; no data was altered or removed.

4. Remediation roadmap

SEQUENCED BY RISK

Do first (0 to 30 days)

- Reset all default credentials (Telnet host, DVR, printers) and disable Telnet in favor of SSH
- Publish and enforce a password policy; add MFA where supported
- Disable anonymous printer access and default SNMP community strings

Do next (30 to 90 days)

- Segment the internal network so a single foothold cannot reach ten systems
- Fix the web form input validation; replace or decommission the expired-certificate server
- Move to a recurring cadence so new exposures are caught between full tests

Methodology and effort disclosure

TRANSPARENCY ON HOW THE WORK WAS PERFORMED

ITEM	DETAIL
Service classification	Penetration Test
Lead tester	Jordan A. Reyes, OSCP
Independent peer reviewer	M. Okafor, OSWE (independent review and sign-off)
Manual tester hours	26
AI-assisted analysis hours	7
Reporting and QA hours	4
Retest hours	3
Tools and tool classes	Nmap service/version and default-credential NSE scripts, targeted credential validation, ProbeSpark AI correlation; manual confirmation of access and lateral reach
Testing window and source	July 6 to July 15, 2026; source [allowlisted ProbeSpark IP]

Test disposition

WHAT WAS TESTED, PARTIALLY TESTED, OR EXCLUDED

AREA	DISPOSITION
Internal host and service discovery	Fully tested
Default and weak credential validation	Fully tested (findings)
Exposed device services (printers, DVR, SNMP)	Fully tested (findings)
External perimeter and web form	Tested (finding)
Deep Active Directory attack-pathing	Available as an add-on where a domain is in scope
Social engineering	Not in scope (separate module)

5. Letter of Attestation

THE COMPLIANCE-FACING SUMMARY

This letter attests that ProbeSpark, a service of HC Development, Inc., performed an authorized internal and external network penetration test for Northwind Manufacturing during July 6 to July 15, 2026 under a signed scope, using AI-augmented methods with qualified human validation. The engagement identified 1 Critical, 1 High, 3 Medium, and 1 Low findings, and demonstrated a proven attack path from a single default credential to lateral access across the environment. This is a point-in-time assessment and does not identify every possible risk. Findings should be remediated and re-tested; changes may expose additional issues.

Jordan A. Reyes, OSCP

Lead Penetration Tester, ProbeSpark · HC Development, Inc.

Signed July 17, 2026

Technical Evidence Appendix

REPRODUCIBLE PROOF FOR THE CLIENT TECHNICAL TEAM

NF-01 · Default root credentials on exposed Telnet, leading to lateral access

Affected asset	10.0.0.87 tcp/23 (Telnet, Security DVR/host OS)
Preconditions	Authorized internal position (assumed compromised workstation).
Evidence	The default root credential authenticated over Telnet. From that host, ten additional systems responded to the same or related default access. Full session evidence retained in the engagement store, redacted here.
Reproduction (safe)	1) From an internal position, port-scan 10.0.0.87. 2) Connect to Telnet on tcp/23. 3) Authenticate with the vendor default root credential. 4) Enumerate reachable internal hosts. No data was altered or removed.
CVSS rationale	Adjacent/internal vector, low complexity, no privileges, high confidentiality and integrity impact given administrative access and lateral reach.

NF-02 · Camera recorder (DVR) accessible with default credentials

Affected asset	10.0.0.87 tcp/23 (Security DVR, Nightowl-class)
Preconditions	Reachable from the internal network.
Evidence	The DVR management interface accepted the documented default credential and returned access to camera footage. No footage was retained.
Reproduction (safe)	Connect to the DVR management service and authenticate with the vendor default credential.

NF-03 · Anonymous access to printers on port 9100

Affected asset	Four internal printers, tcp/9100
Preconditions	Reachable from the internal network.
Evidence	Port 9100 accepted anonymous connections; print history was retrievable on the affected devices.

NF-04 · SNMP with default community strings on printers

Affected asset	Internal printers, udp/161 (SNMPv1)
Preconditions	Reachable from the internal network.
Evidence	SNMP responded to a default community string with device information.

NF-05 · Weak input validation on a public web form

Affected asset	johndoe-demo.com contact form
Preconditions	Unauthenticated, external.
Evidence	Crafted input altered the form response in a way consistent with insufficient validation.

NF-06 · Expired TLS certificate on an unused web server

Affected asset	External edge web server
Preconditions	External.
Evidence	The server presented an expired certificate.