Nanobyte Security

nanobytesecurity.com

Penetration Test Report

External / Host Assessment - ”Bastion” Lab Host

Client	Example Corp (demonstration)
Assessment	Internal network penetration test (single host, gray box)
Testing window	2026-09-22 to 2026-09-24
Report date	2026-09-28
Version	1.0
Classification	CONFIDENTIAL

Document Control

Version history

Version	Date	Author	Notes
0.1	2026-09-25	A. Dalzell	Initial draft, findings and evidence.
0.9	2026-09-26	A. Dalzell	Internal QA review.
1.0	2026-09-28	A. Dalzell	Final release to client.

Distribution list

Name	Role	Organization
Jordan Rivera	IT Director	Example Corp
Sam Okafor	Security Lead	Example Corp

Nanobyte Security contacts

Name	Role	Contact
A. Dalzell	Lead Penetration Tester	reports@nanobytesecurity.com

Contents

Document Control 1

1 Executive Summary 4

1.1 Findings by severity 4

2 Scope and Objectives 5

2.1 In-scope targets 5

3 Methodology 6

4 Constraints and Limitations 7

5 Attack Narrative 8

6 Findings Summary 9

7 Detailed Findings 10

NB-001: Recoverable Stored Credentials in Remote-Management Tool Lead to Full Administrative Compromise 10

7.1 Description 10

7.2 Business impact 10

7.3 Steps to reproduce 10

7.4 Walkthrough 11

7.5 Recommended remediation 11

7.6 References 11

NB-002: Unauthenticated SMB Share Exposes a Full System-Image Backup 12

7.7 Description 12

7.8 Business impact 12

7.9 Steps to reproduce 12

7.10 Walkthrough 13

7.11 Recommended remediation 13

7.12 References 13

8 Remediation Roadmap **15**

9 Appendices **16**

9.1 Risk rating methodology 16

9.2 Tools Used 16

9.3 Artifacts and Cleanup Log 17

1 Executive Summary

Nanobyte Security performed a gray-box penetration test of a single Windows host (“Bastion”) for Example Corp (demonstration) between 22 and 24 September 2026. The objective was to determine whether an attacker with network access to the host could reach sensitive data or obtain administrative control.

The host was fully compromised. Testing identified a chain of two issues that together allowed an unauthenticated attacker to progress from network access to complete administrative control of the system:

- An SMB file share was reachable without authentication and exposed a full Windows system-image backup. The backup contained the local account database, from which stored password material for a local user was recovered offline.
- Credentials for a highly privileged account were stored by a locally installed remote-management application in a form that could be trivially reversed back to plaintext. These credentials granted full administrative access.

Neither issue required a sophisticated technique or custom tooling; both rely on well-understood weaknesses in default configurations and credential storage. The overall risk to the host is assessed as **High**.

What held up. The host was patched against remotely exploitable service vulnerabilities; no unpatched public exploit was needed at any stage. The compromise was achieved entirely through exposed data and recoverable stored credentials rather than memory-corruption exploitation.

Strategic recommendations.

1. Remove anonymous and guest access to all SMB shares, and ensure backup media is never exposed on a general-purpose file share.
2. Treat system-image backups as crown-jewel assets: restrict access, encrypt at rest, and store them off the production host.
3. Replace any remote-management tooling that stores recoverable credentials, or configure it to use per-user secret storage; rotate all credentials that were held in it.

1.1 Findings by severity

Severity	Count
Critical	1
High	1
Medium	0
Low	0
Informational	0
Total	**2**

2 Scope and Objectives

The engagement covered a single in-scope host provided by Example Corp (demonstration). The objective was to assess the host's resistance to an attacker positioned on the same network segment and to determine the impact of any successful compromise.

Testing was authorized against the host and services listed below only. No social engineering, physical access, or denial-of-service testing was in scope. Testing was performed from a Nanobyte Security-controlled system on the same network segment as the target.

2.1 In-scope targets

Asset	Type	Notes
`10.10.10.134`	Windows host (SMB, WinRM)	Single in-scope host, hostname "Bastion".

3 Methodology

Nanobyte Security testing follows industry-recognized frameworks, including the Penetration Testing Execution Standard (PTES), the OWASP Web Security Testing Guide (WSTG), and NIST SP 800-115. Each engagement proceeds through these phases:

1. **Pre-engagement.** Scope, rules of engagement, and points of contact are confirmed in writing.
2. **Intelligence gathering.** Public and provided information about in-scope assets is collected.
3. **Threat modeling.** Likely attackers and high-value assets are identified to prioritize testing.
4. **Vulnerability analysis.** Automated and manual techniques identify potential weaknesses.
5. **Exploitation.** Weaknesses are validated in a controlled manner to confirm real-world impact.
6. **Post-exploitation.** Access is assessed for its potential to reach sensitive data or systems.
7. **Reporting.** Findings are documented with evidence, risk ratings, and remediation guidance.

4 Constraints and Limitations

The following constraints applied to this engagement and should be considered when interpreting the results:

- **Single host.** Only one host was in scope. Lateral movement to other systems, domain-level attacks, and network-wide exposure were not assessed.
- **Point-in-time.** Results reflect the configuration observed during the 22-24 September 2026 window only.
- **Testing window.** Active testing was limited to business hours on the agreed dates; an attacker without those constraints may progress faster.
- **No destructive testing.** Denial-of-service and other disruptive techniques were excluded by agreement. Availability impact ratings are therefore theoretical.
- **Evidence handling.** Screenshots in this demonstration report are redacted placeholders. In a live engagement, evidence is captured, sanitized of secrets, and retained per the Nanobyte Security data-handling policy.

5 Attack Narrative

This section describes the end-to-end path used to compromise the host, so that the defensive team can understand not just the individual findings but how they combined.

1. Enumeration. A service scan of the host identified SMB file sharing and a Windows remote-management service exposed on the network. SMB was enumerated first.

2. Anonymous share access (see NB-002). One of the SMB shares was accessible without valid credentials. Browsing the share revealed a Windows system-image backup — a full copy of the host's system volume stored as virtual hard disk files.

[SCREENSHOT REDACTED]

Directory listing of the exposed backup share

3. Offline credential recovery. The backup's virtual disk was mounted read-only on the testing system. Because a system image includes the operating system's local account database, the stored password material for a local user account was recovered and cracked offline, away from any account-lockout or monitoring controls on the host.

4. Foothold. The recovered credentials were valid for interactive access to the host, giving a first, low-privileged foothold.

5. Stored credential recovery (see NB-001). With a foothold established, a locally installed remote-management application was found to hold saved connection profiles. The application stored the associated credentials in a form that could be reversed back to plaintext using only information available on the host. One profile contained credentials for a highly privileged account.

[SCREENSHOT REDACTED]

Remote-management application showing a saved privileged connection profile

6. Full compromise. The recovered privileged credentials granted complete administrative control of the host, including access to all data on the system. At this point the objectives of the assessment were met and testing was stopped.

The path relied entirely on exposed data and recoverable stored secrets. No memory-corruption exploit or unpatched service vulnerability was involved at any stage.

6 Findings Summary

ID	Finding	Severity	CVSS	Status
NB-001	Recoverable Stored Credentials in Remote-Management Tool Lead to Full Administrative Compromise	Critical	9.9	Open
NB-002	Unauthenticated SMB Share Exposes a Full System-Image Backup	High	7.5	Open

7 Detailed Findings

NB-001 — Recoverable Stored Credentials in Remote-Management Tool Lead to Full Administrative Compromise

NB-001 | Recoverable Stored Credentials in Remote-Management Tool Lead to Full Administrative Compromise

Severity	**Critical** Critical (CVSS 9.9)
CVSS 3.1 vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H`
CWE	CWE-257 - Storing Passwords in a Recoverable Format; CWE-522 - Insufficiently Protected Credentials
MITRE ATT&CK	T1555 (Credentials from Password Stores); T1078 (Valid Accounts)
Affected assets	`10.10.10.134 (WinRM)`
Status	Open

7.1 Description

A remote-management application installed on the host stored saved connection profiles containing account credentials. The application stored these credentials in a form that can be reversed to plaintext using only information available on the host itself. When a profile relies on the application's default protection, no additional secret is required to recover the stored password.

An attacker with any foothold on the host — such as the low-privileged access obtained via NB-002 — can read the application's configuration and recover every credential it holds. One stored profile contained credentials for a highly privileged account.

7.2 Business impact

Recovering the stored privileged credentials granted complete administrative control of the host: full access to all data, the ability to alter or disable security controls, and the ability to establish persistence. Because the credentials belonged to a privileged account, this issue turned a limited foothold into total compromise of the system. Where such accounts are reused across systems, the impact can extend well beyond the single host.

7.3 Steps to reproduce

1. From a foothold on the host, locate the remote-management application's saved configuration.
2. Identify a connection profile that stores credentials using the application's default protection.
3. Recover the stored password to plaintext using only material present on the host.
4. Authenticate to the host's remote-management service using the recovered privileged credentials.

7.4 Walkthrough

[SCREENSHOT REDACTED]

Saved connection profile stored by the remote-management application

[SCREENSHOT REDACTED]

Stored credential recovered to plaintext from the profile

[SCREENSHOT REDACTED]

Administrative access confirmed using the recovered credentials

7.5 Recommended remediation

- **Rotate immediately.** Change the password for every account stored in the application, prioritizing the privileged account, and confirm the old credential no longer works.
- **Stop storing recoverable secrets.** Configure the tool so that stored credentials are protected by a per-user secret that is not present on the host, or replace it with tooling that integrates with an enterprise secret store.
- **Least privilege.** Do not save privileged-account credentials in connection profiles on general-purpose hosts. Use just-in-time or vaulted credential issuance for administrative access.
- **Detect reuse.** Verify the privileged credential was not reused on other systems; if it was, rotate it everywhere.

7.6 References

- CWE-257: Storing Passwords in a Recoverable Format — https://cwe.mitre.org/data/definitions/257.html
- CWE-522: Insufficiently Protected Credentials — https://cwe.mitre.org/data/definitions/522.html
- MITRE ATT&CK T1555: Credentials from Password Stores — https://attack.mitre.org/techniques/T1555/

NB-002 — Unauthenticated SMB Share Exposes a Full System-Image Backup

NB-002 | Unauthenticated SMB Share Exposes a Full System-Image Backup

Severity	High High (CVSS 7.5)
CVSS 3.1 vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
CWE	CWE-306 - Missing Authentication for Critical Function; CWE-522 - Insufficiently Protected Credentials
MITRE ATT&CK	T1580 / T1078 (Valid Accounts); T1003 (OS Credential Dumping)
Affected assets	`10.10.10.134 (SMB)`
Status	Open

7.7 Description

The host exposed an SMB file share that could be accessed over the network without valid credentials. The share contained a Windows system-image backup — a complete copy of the host's system volume stored as virtual hard disk (`.vhd`) files.

A Windows system image includes the operating system's local account database. An attacker who can read the backup can mount the virtual disk offline and extract the stored account information, entirely away from the protections that exist on the live host (account lockout, logging, and monitoring). This converts a file-exposure issue into a credential-compromise issue.

7.8 Business impact

Any attacker with network access to the host — including an unauthenticated one — could retrieve a full copy of the system, including its stored account credentials. Recovering a valid local account from the image provided the initial foothold that led to full compromise of the host (see NB-001). Backups are among the most sensitive assets an organization holds precisely because they concentrate this information in one place.

7.9 Steps to reproduce

1. Enumerate SMB shares on the host over the network.
2. Connect to the exposed share without supplying valid credentials.
3. Observe the Windows system-image backup stored on the share.
4. Copy the backup's virtual disk files to the testing system and mount them read-only.
5. Recover the local account database from the mounted image and process it offline.

7.10 Walkthrough

[SCREENSHOT REDACTED]

Share accessible without valid credentials; backup directory visible

[SCREENSHOT REDACTED]

Virtual hard disk files within the exposed system-image backup

[SCREENSHOT REDACTED]

Local account database recovered from the offline-mounted image

7.11 Recommended remediation

- **Remove anonymous and guest access.** Require authentication on all SMB shares. Disable guest access and confirm that no share grants access to the `ANONYMOUS LOGON` or `Everyone` principals.
- **Relocate backups.** Do not store system-image backups on a general-purpose file share on the same host being backed up. Move backup media to a dedicated, access-controlled backup system.
- **Restrict and encrypt.** Limit read access on backups to the specific service account that needs it, and encrypt backup media at rest so that an exposed file cannot be mounted and read.
- **Rotate exposed credentials.** Treat every credential contained in the exposed image as compromised and rotate it, including the local account recovered during testing.

7.12 References

- CWE-306: Missing Authentication for Critical Function — https://cwe.mitre.org/data/definitions/306.html
- CWE-522: Insufficiently Protected Credentials — https://cwe.mitre.org/data/definitions/522.html

- Microsoft, “Enable or Disable SMB Anonymous/Guest access” — https://learn.microsoft.com/windows-server/storage/file-server/troubleshoot/guest-access-in-smb2-and-smb3-is-disabled

8 Remediation Roadmap

Findings are listed in priority order (severity, then exploitability). Target windows follow the risk-rating guidance in the appendix.

ID	Remediation	Severity	Target
NB-001	Replace or reconfigure tooling that stores recoverable credentials; rotate all stored secrets.	Critical	Immediate
NB-002	Remove anonymous/guest access to SMB shares; relocate and restrict backup media.	High	30 days

9 Appendices

9.1 Risk rating methodology

Findings are rated using the Common Vulnerability Scoring System version 3.1 (CVSS 3.1) base score. The full vector string is provided for each finding so scores can be independently verified.

Severity	CVSS 3.1 Score	Guidance
Critical	9.0 – 10.0	Remediate immediately. Exploitation is likely and impact is severe.
High	7.0 – 8.9	Remediate as a priority, typically within 30 days.
Medium	4.0 – 6.9	Remediate within a planned maintenance cycle, typically within 90 days.
Low	0.1 – 3.9	Remediate as resources allow or accept the risk with documentation.
Informational	0.0	No direct risk. Provided to improve security posture.

CVSS base scores measure technical severity. Nanobyte Security may note where business context raises or lowers the practical priority of a finding.

9.2 Tools Used

The following categories of tooling were used during the engagement. Exact versions are recorded in the Nanobyte Security engagement workbook.

Category	Purpose
Network / service scanner	Host and service discovery
SMB enumeration client	Listing and accessing file shares
Disk-image mount utility	Read-only mounting of the recovered backup
Offline credential-recovery toolkit	Extracting and cracking stored account material
Remote-management client	Authenticating with recovered credentials

All tooling was run from a Nanobyte Security-controlled testing system. No tooling was installed on the target host.

9.3 Artifacts and Cleanup Log

This log records every change Nanobyte Security made to the target environment during testing and confirms its removal, so that Example Corp (demonstration) can verify the host was left in its original state.

Artifact	Location	Created	Removed
Copied backup image	Testing system only	2026-09-22	Securely deleted 2026-09-24
Recovered credential material	Testing system only	2026-09-22	Securely deleted 2026-09-24
Interactive logon sessions	Target host	2026-09-23	Logged off; no accounts or files left behind

No accounts were created, no files were written to the target host, and no persistence mechanisms were installed. Any credentials recovered during testing are listed in the findings and must be rotated by Example Corp (demonstration); Nanobyte Security retains no copy after report delivery.

— End of report —
Nanobyte Security LLC