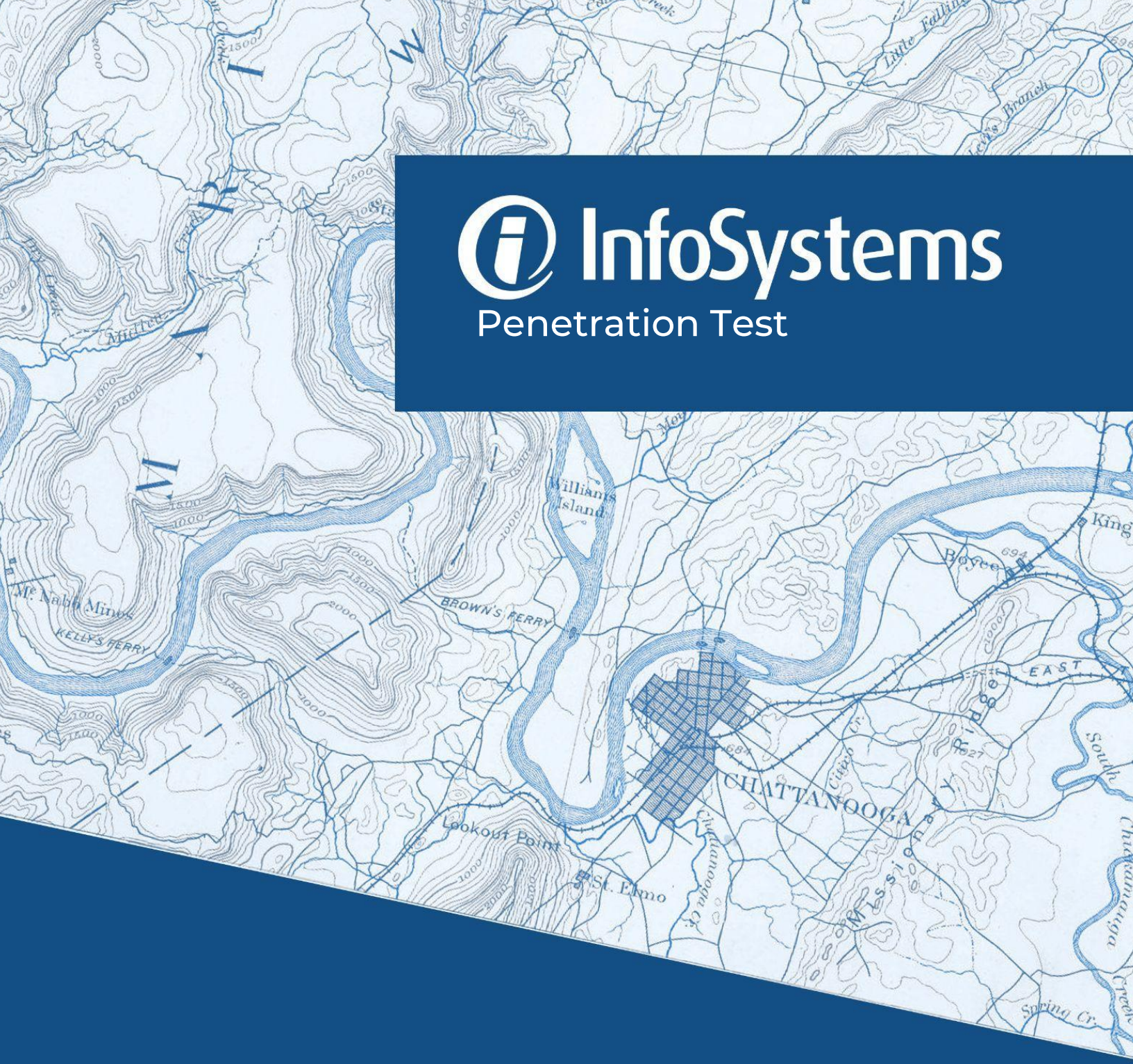


Demo, Inc.

Date: 01/21/2026

Version: v1

Table of Contents

InfoSystems

Confidentiality Statement

This document contains information that is confidential and intended solely for the designated recipient(s). The contents include findings and methodologies related to a security assessment (penetration test) of “” systems. Unauthorized access, disclosure, copying, distribution, or use of this document or any of its contents is strictly prohibited. If you are not the intended recipient, please notify the sender immediately and delete all copies. The information in this report must be handled according to applicable data protection policies and guidelines.

InfoSystems

Project Contact Information

Customer Contacts:
Jane Doe
CEO

InfoSystems Contacts:

InfoSystems

Executive Summary

InfoSystems evaluated the security posture at Demo, Inc. by performing an internal penetration test. By attacking these networks, the InfoSystems team identified vulnerabilities in the Customer's environments that will be listed below. It is recommended to address these vulnerabilities as soon as possible. The identified vulnerabilities were detected within the specified time frame. It is important to note that there may be additional or newly emerging vulnerabilities beyond this period.

Penetration Testing Approach

All testing was executed in several related phases:

- In the planning phase, the rules of engagement were identified, scope of testing and test windows were agreed upon, and testing goals were set.
- The discovery phase included automated vulnerability scanning along with manual testing to explore and understand the testing target and any vulnerabilities that could be detected by automated tools.
- The attack phase comprised efforts to exploit any vulnerabilities detected, and to synthesize knowledge gained about the environment, its technology, its users, and its function into an escalation of privilege beyond that intended by the Customer.
- The final phase recorded all findings in a manner that supports risk assessment and remediation by the Customer. This included the writing of this report.

Additionally, the attack phase comprised several distinct steps, executed iteratively as information was discovered.

- Gained access to the system or environment in a way that was not intended.
- Escalated privileges to move from regular or anonymous user to a more privileged position.
- Browsed to explore the newly accessed environment and identify useful assets and data.
- Deployed tools to attack further from the newly gained vantage point.
- Exfiltrated data.

Project Scope

Site	Details	Exclusions
Internal	10.10.10.0/24	None

Assessment Summary and Recommendations

InfoSystems Cyber conducted a comprehensive security assessment of Demo, Inc. in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use. This assessment harnessed penetration testing techniques to provide Demo, Inc. management with an understanding of the risks and security posture of their corporate environment.

The test for this engagement included 10.10.10.5 from 01/20/2026 to 01/24/2026. InfoSystems resources performed the assessment using industry-standard penetration testing tools and frameworks, including and more.

InfoSystems

Results

The table below includes the overall results of penetration testing these environments. The score rating was determined using the Findings Severity Table in Appendix A.

Scope	Score Rating
Internal	Critical

InfoSystems
Technical Findings

Score	9.9
Title	Domain Admin Compromise via Kerberoasting
Description	Kerberoasting is an attack technique targeting Kerberos service accounts within an Active Directory environment. Attackers request Service Principal Name (SPN) tickets for accounts that use Kerberos for authentication. These tickets are encrypted with the service account's NTLM hash, allowing attackers to perform offline brute-force or dictionary attacks to recover the plaintext password. In this assessment, the tester identified at least one service account (svc_db) configured with a weak password. Using standard Kerberoasting tooling from an internal network position, the attacker successfully extracted a Kerberos TGS ticket and cracked it offline. The recovered password allowed escalation to high-privilege permissions within the domain, which ultimately enabled full domain compromise. This vulnerability indicates systemic issues with service account password hygiene, account governance, and Kerberos configuration.
Impact	Critical
Affected Host(s)	10.10.10.5
Remediation	Rotate all service account passwords immediately. Enforce long, random passwords (≥ 25 characters). Disable RC4-HMAC encryption. Implement Managed Service Accounts or Group Managed Service Accounts (gMSA).

Evidence:

```
└─ [*]$ impacket-GetUserSPNs -dc-ip 10.10.10.5 examplecorp.local/user1:'Welcom
e123!' -request
```

Kerberoast attack

```
ServicePrincipalName               Name          MemberOf  PasswordLastSet
LastLogon
---------------------              -----------   --------  -------------------
----------
MSSQLSvc/DB01.examplecorp.local    svc_db        {}        2025-05-10 11:20:00
2026-01-15 09:11:00

[*] Requesting SPN Ticket for svc_db
$krb5tgs$23$*svc_db$EXAMPLECORP.LOCAL$MSSQLSvc/DB01.examplecorp.local*$2b$19JvOJ
37HhndkslS92kfhs87...REDACTED...
[*] Hash written to svc_db.kirbi
``
```

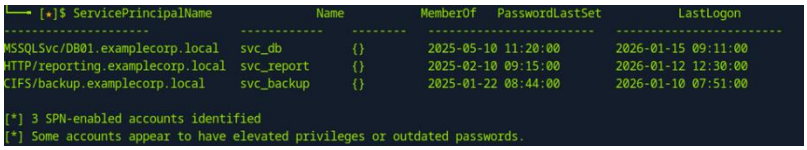
Capturing hash for user svc_db

Score	7.1
Title	Excessive Service Principal Names (SPNs) Exposed to Low-Privilege Users
Description	During enumeration of Active Directory service accounts, it was observed that an excessive number of accounts had Service Principal Names (SPNs) assigned — including accounts not typically associated with network services (e.g., backup, reporting, legacy integration accounts). This condition increases exposure to Kerberoasting, as any account with an SPN is eligible for TGS ticket extraction. The greater the number of SPN-enabled accounts, the wider the attack surface for offline password cracking. Additionally, these SPNs were discoverable by any authenticated user, meaning a low-privileged user could enumerate high-value accounts simply by requesting domain account metadata. This significantly reduces the attacker's effort and improves the success probability of Kerberoasting attempts.
Impact	High
Affected Host(s)	10.10.10.5

Remediation	• Remove Unnecessary SPNs
	  ○ Audit all SPNs and remove or disable any that are not required for service authentication.
	• Limit SPN Assignment to Required Service Accounts Only
	  ○ Service accounts should have SPNs *only* if needed by specific services (e.g., MSSQL, IIS, LDAP services).
	• Use gMSAs for SPN-Bound Accounts
	  ○ Weak passwords
	  ○ Static passwords
	  ○ Manual misconfiguration

Evidence:

Listing accounts with SPNs



Three accounts show having SPNs.

Score	**2.6**
Title	**SMB Signing Not Required**
Description	Several domain-joined workstations were found to have SMB signing set to “enabled” but not “required.” When SMB signing is optional, clients and servers may negotiate unsigned SMB sessions, enabling attackers with network positioning (e.g., on the same VLAN) to perform NTLM relay, man-in-the-middle attacks, or modify SMB communications. This does not directly lead to compromise but can weaken internal network integrity, especially when combined with other vulnerabilities such as LLMNR poisoning or weak NTLM configurations.
Impact	Low
Affected Host(s)	10.10.10.5
Remediation	**Require SMB Signing on All Workstations and Servers** Set via Group Policy: • *Microsoft network client: Digitally sign communications (always)* • *Microsoft network server: Digitally sign communications (always)* **Disable NTLM Where Possible** Prefer Kerberos authentication to reduce NTLM relay risk.

Evidence:

```
Get-SmbServerConfiguration | Select EnableSecuritySignature, RequireSecuritySignature
```

PowerShell command to run to show SMB signing vulnerability.

Score	0.0
Title	Anonymous LDAP Bind Allowed
Description	The domain controller permits anonymous (unauthenticated) LDAP binding. This configuration does not directly enable compromise, but it may expose limited directory metadata — such as domain naming contexts, rootDSE information, and schema properties. Most environments block anonymous LDAP binds by default, but certain legacy applications or misconfigurations may re-enable it.
Impact	Informational
Affected Host(s)	10.10.10.5
Remediation	Disable anonymous LDAP binds unless legacy application requirements exist

Evidence: None

InfoSystems

Appendices

Appendix A – Findings Severity

Severity	Score Range	Definition
Critical	9.0 – 10.0	Vulnerabilities were identified and ability to exploit are possible. It is advised to patch immediately.
High	7.0 – 8.9	Vulnerabilities were identified but deemed more difficult to exploit. It is recommended to patch as soon as possible.
Medium	4.0 – 6.9	Vulnerabilities exist but exploitation is not possible or requires more steps. It is recommended to patch these after the high-priority issues are addressed.
Low	0.1 – 3.9	Vulnerabilities are non-exploitable but would improve Customer's security posture if remediated.

Appendix B – Exploited Hosts

Host	Scope	Method	Notes
10.10.10.5	Internal	Kerberoasting	Kerberoast attack successful on user svc_db

Appendix C – Compromised Users

Username	Type	Method	Notes
svc_db	Domain Service Account	Kerberoasting Attack	Service account was compromised via a kerberoast attack which could lead to lateral movement throughout the domain.