Penti

Penetration Testing Report - SAMPLE

Representative Findings from Actual Customer Engagements
Assessment Period: Q4 2023 - Q1 2025

Report Type: Sample Report - Compilation of Representative Findings
Testing Date Range: October 31, 2023 - January 7, 2025

Report Status: Completed

Table of Contents

1. Scoping
2. Methodology
3. Scanner Factors
4. Risk Rating Methodology
5. Remediation Proposal Methodology
6. Executive Summary
7. Scope
8. Our Tools
9. Manual Assessment Results
10. Prioritized Remediation
11. Re-testing
12. Disclosure
13. Our Certifications

Scoping

Penti conducts its tests following the best practices and compliance regulations for each Industry sector and follows the roadmap below.

Assessment Type: Manual Penetration Testing
Frameworks Applied:

- OWASP Top 10 & ASVS
- MITRE ATT&CK Enterprise
- NIST Cybersecurity Framework
- Industry-specific compliance requirements

Testing Phases:

1. Reconnaissance & Information Gathering
2. Vulnerability Assessment
3. Exploitation & Validation
4. Post-Exploitation & Lateral Movement
5. Documentation & Reporting
6. Remediation Support

Methodology

Our penetration testing methodology follows industry best practices and incorporates techniques from:

- OWASP Testing Guide - Web application and API security
- MITRE ATT&CK Framework - Real-world adversary tactics and techniques
- PTES (Penetration Testing Execution Standard) - Comprehensive testing methodology
- NIST SP 800-115 - Technical guide to information security testing

All testing is performed manually by certified penetration testers with expertise in:

- Network penetration testing (external and internal)
- Active Directory and domain security
- Credential-based attacks
- Lateral movement and privilege escalation
- Post-exploitation techniques

Finding Factors

All findings in our assessments are assigned two measurement factors:

Severity

Severity indicates the impact of the findings on technical and business operations. Findings are classified according to severity as Critical, High, Medium, Low, or Informational. This reflects the likely impact of each issue for a typical organization.

Confidence

Findings are also classified according to confidence as Certain, Firm, or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

Note: All findings in this report are manually validated and confirmed by our penetration testing team, resulting in Certain confidence levels.

Risk Rating Methodology

Penti follows the OWASP approach in risk analysis, which uses standard methodologies and is customized for application security. Such an approach is used for prioritizing findings based on calculated scores for each. This is done by multiplying the estimated scores of Likelihood (confidence) and Impact (severity) by each other.

Risk Calculation Formula

```
Risk Score = Likelihood × Impact
```

Risk Level Classification

- Critical (9-10): Immediate action required
- High (7-8.9): Should be resolved as soon as possible
- Medium (4-6.9): Should be resolved in a reasonable timeframe
- Low (1-3.9): Should be resolved when resources permit

Remediation Proposal Methodology

After the risks to the application have been classified by Risk Rating Methodology, Penti produces a prioritized list of proposed remediations. As a general rule, the most severe risks should be fixed first; however, Penti helps prioritize and balance high impact security findings with lower impact to make sure your overall security posture improves over time.

Our remediation approach includes:

1. Immediate Actions - Critical findings requiring urgent attention
2. Short-term Fixes - High and medium findings with clear remediation paths
3. Long-term Improvements - Architectural changes and security enhancements
4. Continuous Monitoring - Ongoing validation and re-testing

Executive Summary

Report Composition

This report represents a curated compilation of the most relevant and representative penetration testing findings from actual customer engagements conducted by Penti between October 2023 and January 2025.

To demonstrate our comprehensive penetration testing capabilities, we have selected high-impact findings across multiple enterprise client assessments, showcasing our expertise in:

- External and internal network penetration testing
- Active Directory and domain security assessments
- Assumed breach scenarios and lateral movement testing
- Post-exploitation techniques and credential-based attacks
- Multi-quarter engagements with remediation validation

All customer-identifying information has been redacted to protect client confidentiality. The technical findings, methodologies, and remediation guidance presented are authentic examples from real-world penetration testing engagements.

Assessment Overview

This penetration test was conducted against several customers' production network infrastructure, including external perimeter testing and internal network assessment with assumed breach scenarios. The engagement spanned multiple quarters and involved comprehensive manual testing by certified penetration testers.

Key Findings Summary

Critical Risk Findings: 13
High Risk Findings: 5
Medium Risk Findings: 1
Low Risk Findings: 1
Informational/Passed Tests: 15

Most Significant Findings

1. Active Directory DCSync Attack - Critical
   Active Directory domain controllers vulnerable to credential replication attacks, allowing complete domain compromise.
2. LDAP Relay Attack to Domain Controller - Critical
   NTLM relay attacks possible against domain controllers, enabling unauthorized domain access.
3. VPN Network Segmentation Bypass - High
   VPN users can access restricted internal VLANs including Security, AV, and Guest networks.
4. Memory-Based Credential Extraction (LSASS) - High
   Domain credentials can be extracted from memory on compromised systems.
5. SMB Relay Attack (Missing Signature Requirement) - High
   Internal network vulnerable to SMB relay attacks due to missing signing requirements.

Impact Assessment

The combination of findings discovered during this assessment reveals a CRITICAL overall risk posture. An attacker gaining initial access through any of the identified external vectors (VPN, exposed services, default credentials) could:

- Compromise the entire Active Directory domain
- Extract all user and service account credentials
- Move laterally across the network without restriction
- Access sensitive data across multiple network segments
- Establish persistent backdoor access
- Exfiltrate sensitive information

Positive Security Controls Observed

- Modern endpoint detection and response (EDR) systems deployed
- Network monitoring and logging capabilities in place
- Patch management processes for critical systems
- Segmentation controls partially implemented (requires improvement)

Recommendations Priority

1. Immediate (24-48 hours):
    - Disable DCSync capabilities for non-admin accounts
    - Enable SMB signing across all systems
    - Implement LDAP signing and channel binding
2. Short-term (1-2 weeks):
    - Enhance VPN network segmentation
    - Deploy credential guard on all Windows systems
    - Implement LAPS for local administrator passwords
3. Medium-term (1-3 months):
    - Active Directory security hardening
    - Privileged Access Workstation (PAW) implementation
    - Enhanced network segmentation and micro-segmentation

Scope

Production Environment

External Perimeter:

- External IP ranges: [REDACTED]
- VPN endpoints
- Public-facing services
- Cloud infrastructure (Azure)

Internal Network:

- Corporate network segments (VLANs 1-10)
- Production servers and workstations
- Active Directory infrastructure
- Internal applications and services
- Network appliances (printers, access points, security devices)

IP Address Ranges Tested:

- External: 203.0.113.0/24, 198.51.100.0/24 [REDACTED/SAMPLE]
- Internal: 192.168.50.0/24, 10.10.100.0/24, 172.16.5.0/29 [REDACTED/SAMPLE]
- VPN: Multiple remote access segments

Staging

No staging environment was included in this assessment.

Development

No development environment was included in this assessment.

Testing Windows:

- External testing: All hours (non-intrusive)
- Internal testing: Business hours with coordination
- Assumed breach: Controlled after-hours testing

Our Tools

Manual Tools (Not Exhaustive)

Network Reconnaissance:

- Nmap - Advanced port scanning and service enumeration
- Masscan - High-speed port scanning
- Netcat - Manual service interaction
- Custom Python/Bash scripts

Web Application Testing:

- Burp Suite Professional - Manual web application testing
- Ffuf - Content discovery and fuzzing
- SQLMap - SQL injection testing
- 403Bypasser - Authorization bypass testing
- Ghauri - Advanced SQL injection
- Custom exploitation scripts

Active Directory Attacks:

- Bloodhound - Active Directory path analysis
- Impacket Suite - SMB and credential attacks
- Mimikatz - Credential extraction
- Responder - LLMNR/NBT-NS poisoning
- Rubeus - Kerberos attacks
- CrackMapExec - Lateral movement

Credential Attacks:

- Hydra - Brute force attacks
- John the Ripper - Password cracking
- Hashcat - GPU-accelerated cracking
- Custom wordlists

Post-Exploitation:

- PowerShell Empire - Windows post-exploitation
- Metasploit Framework - Exploitation and payload delivery

- Covenant - .NET command and control
- Custom persistence mechanisms

VPN & Network Testing:

- IKE-Scan - VPN endpoint discovery
- OpenVPN tools - VPN configuration analysis
- Custom network pivoting scripts

Information Gathering:

- Google Dorking - OSINT and exposed file discovery
- Shodan/Censys - Internet-wide asset discovery
- LinkedIn/OSINT - Social engineering reconnaissance

Manual Assessment Results

We have researched and confirmed the highest priority findings from manual penetration testing:

Summary of Manual Findings

#	Title of Finding	Status	Risk
1	Active Directory DCSync Attack	Active	Critical
2	LDAP Relay Attack to Domain Controller	Active	Critical
3	Memory-Based Credential Extraction (LSASS)	Active	High
4	DPAPI Secret Extraction (Saved Credentials)	Active	High
5	SMB Relay Attack (Missing Signature Requirement)	Active	High
6	VPN Network Segmentation Bypass	Remediated	High
7	Unauthenticated FTP Access	Remediated	Critical
8	Unauthenticated Shell Access via Telnet	Remediated	Critical
9	Network Device Default Credential Vulnerability	Remediated	Critical
10	Unauthenticated SMB Access	Remediated	Critical
11	Lateral Movement Capability Assessment	Validated	Medium
12	SNMP Brute Force Attack	Remediated	Critical
13	Ivanti Connect Secure - Authentication Bypass (CVE-2023-46805)	Not Vulnerable	Critical

Detailed Findings

Finding #1: Active Directory DCSync Attack

Description:

The Active Directory environment is vulnerable to DCSync attacks. DCSync is a technique that allows an attacker with certain Active Directory permissions to impersonate a domain controller and request password data from other domain controllers via the Directory Replication Service (DRS). This attack allows complete compromise of the entire domain.

During testing, we identified that standard user accounts or compromised service accounts could potentially escalate to DCSync permissions through various attack paths. Once achieved, an attacker can:

- Extract NTLM hashes for all domain users including Domain Admins
- Extract Kerberos keys
- Replicate the entire Active Directory database
- Create Golden Tickets for persistent access

Testing Date: January 7, 2025

Risk Level: CRITICAL

Level of Effort: High (requires remediation of AD permissions, tiering, and monitoring)

Status: Active - Requires immediate remediation

Affected Resources:

- Internal Network: 10.10.100.0/24
- Active Directory Domain Controllers
- All domain user accounts

Remediation:

Immediate Actions:

1. Audit all accounts with Replicating Directory Changes permissions
2. Remove DCSync rights from non-DC computer accounts
3. Implement alerts for DCSync attempts (Event IDs 4662, 5136)

4. Review and restrict membership in high-privilege groups

Long-term Actions:

1. Implement Active Directory tiering model (Tier 0, 1, 2)
2. Deploy Privileged Access Workstations (PAWs) for administrators
3. Enable Advanced Threat Analytics or Microsoft Defender for Identity
4. Regular audits of AD permissions using Bloodhound/Purple Knight

Solution:

```
None
# Audit current DCSync permissions
Import-Module ActiveDirectory
(Get-Acl "AD:\DC=domain,DC=com").Access |
  Where-Object {$_.ObjectType -eq
"1131f6aa-9c07-11d1-f79f-00c04fc2dcd2" -or
                $_.ObjectType -eq
"1131f6ad-9c07-11d1-f79f-00c04fc2dcd2"} |
  Select-Object IdentityReference,
ActiveDirectoryRights

# Enable auditing
auditpol /set /subcategory:"Directory Service Access"
/success:enable /failure:enable
```

Reproduction Steps:

1. Compromise a domain user account with elevated permissions
2. Use Impacket's secretsdump.py or Mimikatz:

```
None
secretsdump.py DOMAIN/user:password@DC-IP
```

3. Extract all NTLM hashes including Domain Admin accounts
4. Use extracted hashes for Pass-the-Hash or crack them offline

Testing Process:

1. Enumerated Active Directory using Bloodhound
2. Identified privilege escalation paths to DCSync permissions
3. Validated permissions using LDAP queries
4. Simulated DCSync attack in controlled manner
5. Confirmed ability to extract credential material

Compliance Impact:

- NIST: AC-6 (Least Privilege), AU-2 (Audit Events)
- MITRE ATT&CK: T1003.006 (OS Credential Dumping: DCSync)
- PCI DSS: Requirement 7 (Restrict Access), 10 (Track and Monitor)
- SOC 2: CC6.1 (Logical Access Controls)

Finding #2: LDAP Relay Attack to Domain Controller

Description:

The Active Directory domain controllers do not enforce LDAP signing or LDAP channel binding, making them vulnerable to NTLM relay attacks. An attacker on the internal network can perform a man-in-the-middle attack to relay NTLM authentication attempts to the domain controller's LDAP service.

This vulnerability allows an attacker to:

- Relay credentials from any domain-joined system
- Create new domain user accounts
- Add users to privileged groups (Domain Admins)
- Modify domain security settings
- Achieve full domain compromise without cracking passwords

Combined with techniques like LLMNR/NBT-NS poisoning or SMB relay, this represents a critical path to domain compromise.

Testing Date: January 7, 2025

Risk Level: CRITICAL

Level of Effort: Medium (configuration changes on domain controllers)

Status: Active - Requires immediate remediation

Affected Resources:

- Internal Network: 10.10.100.0/24
- All Domain Controllers
- All domain-joined systems

Remediation:

Immediate Actions:

1. Enable LDAP signing on all domain controllers
2. Enable LDAP channel binding
3. Disable LLMNR and NBT-NS via Group Policy

4. Enable SMB signing on all systems

Configuration Steps:

Enable LDAP Signing:

```
None
Computer Configuration > Policies > Windows Settings >
Security Settings > Local Policies > Security Options
- Domain controller: LDAP server signing requirements =
Require signing
- Network security: LDAP client signing requirements =
Require signing
```

Enable Channel Binding:

```
None
# Set LDAP server channel binding to "Always"
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=domain,DC=com"
-Replace @{"msDS-LdapServerChannelBinding"=2}
```

Disable LLMNR/NBT-NS:

```
None
Computer Configuration > Administrative Templates >
Network > DNS Client
- Turn off multicast name resolution = Enabled

Computer Configuration > Windows Settings > Scripts >
Startup
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameter
```

```
s" /v NodeType /t REG_DWORD /d 2 /f
```

Solution:

Deploy the following Group Policy Objects:

1. LDAP Signing Enforcement GPO
2. LDAP Channel Binding GPO
3. LLMNR/NBT-NS Disable GPO
4. SMB Signing Enforcement GPO

Reproduction Steps:

1. Position attacker on internal network segment: 10.10.100.0/24
2. Start Responder to capture LLMNR/NBT-NS requests:

```
None
responder -I eth0 -wrf
```

3. Use ntlmrelayx to relay captured credentials to DC:

```
None
ntlmrelayx.py -t ldap://DC-IP --escalate-user normaluser
```

4. Wait for authentication event (user browsing, service authentication)
5. Relay credentials grant Domain Admin privileges to controlled account

Testing Process:

1. Verified LDAP signing not enforced using ldapsearch
2. Confirmed channel binding not configured
3. Deployed Responder for LLMNR poisoning
4. Configured ntlmrelayx targeting domain controller
5. Successfully relayed credentials and escalated privileges
6. Validated domain admin access

Compliance Impact:

- MITRE ATT&CK: T1557.001 (LLMNR/NBT-NS Poisoning), T1212 (Exploitation for Credential Access)
- NIST: IA-5 (Authenticator Management), SC-8 (Transmission Confidentiality)
- PCI DSS: Requirement 4 (Encrypt Transmission), 8 (Identify and Authenticate)
- ISO 27001: A.9.4.2 (Secure log-on procedures)

Finding #3: VPN Network Segmentation Bypass

Description:

The VPN infrastructure provides excessive network access, allowing VPN-connected users to reach restricted internal network segments. During testing from a standard VPN user connection, we successfully accessed the following VLANs that should be restricted:

- VLAN 5 (Corporate Internal): 192.168.50.0/24
- Security Management VLAN
- AV/Video Conferencing VLAN
- Guest Network VLAN
- Server Management VLAN

This violates the principle of least privilege and creates significant risk. A compromised VPN account (through phishing, credential stuffing, or stolen laptop) provides an attacker with:

- Direct access to critical infrastructure
- Ability to scan internal networks
- Lateral movement opportunities
- Access to sensitive data and systems

Testing Date: April 4, 2025

Risk Level: HIGH

Level of Effort: High (requires network redesign and access control implementation)

Status: Completed - Remediation verified

Affected Resources:

- VPN Gateway: [REDACTED]
- Internal VLANs: 192.168.50.0/24 and additional segments
- All VPN user accounts

Remediation:

Implemented Solution:

1. Network Segmentation Enforcement:
    - Created dedicated VPN VLAN with restricted access
    - Implemented firewall rules limiting VPN to authorized resources only
    - Deployed role-based access control (RBAC) for VPN users
2. Access Control Lists (ACLs):

```
None

# Example ACL structure implemented
permit tcp VPN_SUBNET ALLOWED_SERVERS eq 443
permit tcp VPN_SUBNET ALLOWED_SERVERS eq 3389
deny ip VPN_SUBNET INTERNAL_MGMT_VLAN
deny ip VPN_SUBNET SECURITY_VLAN
deny ip VPN_SUBNET AV_VLAN
permit ip VPN_SUBNET AUTHORIZED_RESOURCES
deny ip any any log
```

3. Zero Trust Network Access (ZTNA):
    - Implemented application-level access control
    - Deployed multi-factor authentication for VPN
    - Implemented device posture checking
4. Monitoring & Alerting:
    - Deployed SIEM rules for unauthorized VPN access attempts
    - Implemented network flow monitoring
    - Created alerts for lateral movement from VPN segment

Solution:

The organization successfully implemented:

- Network micro-segmentation
- Role-based VPN access policies
- Enhanced monitoring and alerting
- Regular access reviews

Reproduction Steps (Original Finding):

1. Connect to corporate VPN with standard user credentials
2. Perform network discovery:

```
None
nmap -sn 192.168.0.0/16
```

3. Identify accessible VLANs
4. Scan discovered segments for services:

```
None
nmap -sV -p- 192.168.50.0/24
```

5. Successfully accessed restricted management interfaces
6. Demonstrated ability to reach Security VLAN, AV VLAN, etc.

Testing Process:

1. Obtained VPN credentials for standard user account
2. Connected to VPN and analyzed network routing
3. Performed network enumeration across multiple subnets
4. Documented accessible VLANs and services
5. Attempted access to management interfaces (successful)
6. Validated lack of network segmentation controls
7. Retest: Confirmed remediation blocks unauthorized access

Compliance Impact:

- MITRE ATT&CK: T1590 (Gather Victim Network Information), T1021 (Remote Services)
- NIST: AC-4 (Information Flow Enforcement), SC-7 (Boundary Protection)
- PCI DSS: Requirement 1.2 (Network Segmentation), 1.3 (Restrict Direct Access)
- Zero Trust: Least privilege access, network microsegmentation

Finding #4: Memory-Based Credential Extraction (LSASS)

Description:

Windows systems in the environment do not adequately protect against Local Security Authority Subsystem Service (LSASS) memory dumping. When administrative access is obtained on any Windows system, attackers can extract plaintext passwords, NTLM hashes, and Kerberos tickets from memory.

During testing, we successfully:

- Dumped LSASS process memory
- Extracted domain credentials including privileged accounts
- Recovered plaintext passwords for some accounts
- Obtained Kerberos TGTs for Pass-the-Ticket attacks

This finding enables lateral movement and privilege escalation across the domain once any single workstation or server is compromised.

Testing Date: January 7, 2025

Risk Level: HIGH

Level of Effort: Medium (requires Windows security feature deployment)

Status: Active - Requires remediation

Affected Resources:

- Internal Network: 10.10.100.0/24
- All Windows workstations and servers
- Domain user credentials

Remediation:

Immediate Actions:

1. Enable Credential Guard (Windows 10/11 Enterprise, Server 2016+):

```
None

# Enable via Group Policy
Computer Configuration > Administrative Templates >
System > Device Guard
- Turn On Virtualization Based Security = Enabled
- Credential Guard Configuration = Enabled with UEFI lock
```

2.

Deploy Windows Defender Credential Guard:

- Isolates credentials using virtualization-based security
- Prevents mimikatz and similar tools from accessing LSASS

3. Enable Protected Process Light (PPL) for LSASS:

```
None

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
RunAsPPL /t REG_DWORD /d 1 /f
```

4.

Implement Local Administrator Password Solution (LAPS):

- Randomizes local admin passwords
- Prevents lateral movement with shared credentials

5. Disable WDigest Authentication:

```
None

reg add
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\
WDigest" /v UseLogonCredential /t REG_DWORD /d 0 /f
```

Long-term Solutions:

1. Deploy Privileged Access Workstations (PAWs) for administrators
2. Implement tiered administrative model

3. Monitor for LSASS access attempts (Sysmon Event ID 10)
4. Deploy EDR with memory protection capabilities

Solution:

Comprehensive credential protection strategy:

- Credential Guard deployment via GPO
- LAPS implementation for local admin accounts
- Enhanced auditing and monitoring
- Admin workstation hardening

Reproduction Steps:

1. Gain local administrator access on target system (via various vectors)
2. Dump LSASS process memory using Mimikatz:

```
None
sekurlsa::minidump lsass.dmp
sekurlsa::logonPasswords
```

3. Or use Task Manager to create dump, then parse offline:

```
None
# Create dump
procdump -ma lsass.exe lsass.dmp

# Parse offline on attacker system
mimikatz # sekurlsa::minidump lsass.dmp
mimikatz # sekurlsa::logonPasswords
```

4. Extract credentials including NTLM hashes and plaintext passwords
5. Use credentials for lateral movement via Pass-the-Hash:

```
None
crackmapexec smb 10.10.100.0/24 -u username -H ntlmhash
```

Testing Process:

1. Obtained local admin access on test workstation
2. Used Mimikatz to dump LSASS process
3. Successfully extracted domain credentials
4. Validated credentials using CrackMapExec
5. Demonstrated lateral movement capability
6. Documented all extracted credential types

Compliance Impact:

- MITRE ATT&CK: T1003.001 (LSASS Memory), T1550 (Use Alternate Authentication)
- NIST: IA-5 (Authenticator Management), SC-12 (Cryptographic Key Management)
- PCI DSS: Requirement 8.2 (Unique User IDs), 8.3 (Secure Authentication)
- CIS Controls: 4.3 (Configure Data Access Control Lists), 16.11 (Lock Workstation Sessions)

Finding #5: SMB Relay Attack (Missing Signature Requirement)

Description:

The majority of Windows systems in the environment do not enforce SMB signing, making them vulnerable to SMB relay attacks. This allows an attacker on the internal network to intercept and relay SMB authentication attempts to other systems, gaining unauthorized access without knowing passwords.

SMB relay attacks are particularly dangerous because:

- No password cracking required
- Can relay to any system without SMB signing
- Can be combined with LLMNR/NBT-NS poisoning
- Enables immediate lateral movement
- Can lead to full domain compromise when relayed to domain controllers

During testing, we successfully:

- Relayed SMB authentication to multiple servers
- Gained administrative access to systems
- Deployed remote shells via relay
- Dumped SAM database and credentials

Testing Date: January 7, 2025

Risk Level: HIGH

Level of Effort: Medium (requires GPO deployment and testing)

Status: Active - Requires remediation

Affected Resources:

- Internal Network: 10.10.100.0/24
- All Windows workstations and servers without SMB signing
- Estimated 85% of internal systems affected

Remediation:

Immediate Actions:

1. Enable SMB Signing via Group Policy:
   For Domain Controllers (already required by default):

```
None

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
```

2.
   For All Other Systems:

```
None

Computer Configuration > Policies > Windows Settings >
Security Settings > Local Policies > Security Options
- Microsoft network server: Digitally sign communications
(if client agrees) = Enabled
- Microsoft network client: Digitally sign communications
(if server agrees) = Enabled
```

3.
   Phased Rollout Strategy:
   - Phase 1: Enable on all servers (required)
   - Phase 2: Enable on all workstations (required after testing)
   - Phase 3: Monitor for compatibility issues
   - Phase 4: Enforce on all systems
4. Disable LLMNR/NBT-NS (already covered in Finding #2)
5. Monitor for SMB Relay Attempts:
   - Deploy Sysmon or EDR

- Monitor for suspicious SMB connections
- Alert on authentication anomalies

Solution:

Deploy comprehensive SMB security controls:

```
None
# PowerShell script to enable SMB signing
$GPOName = "SMB-Signing-Enforcement"
$OU = "OU=Computers,DC=domain,DC=com"

# Create/configure GPO
Set-GPRegistryValue -Name $GPOName -Key
"HKLM\System\CurrentControlSet\Services\LanmanServer\Pa
rameters" -ValueName "RequireSecuritySignature" -Type
DWord -Value 1

Set-GPRegistryValue -Name $GPOName -Key
"HKLM\System\CurrentControlSet\Services\LanmanWorkstati
on\Parameters" -ValueName "RequireSecuritySignature"
-Type DWord -Value 1

# Link GPO to OU
New-GPLink -Name $GPOName -Target $OU
```

Reproduction Steps:

1. Position attacker on internal network: 10.10.100.0/24
2. Start Responder to poison LLMNR/NBT-NS:

```
None
responder -I eth0 -rv
```

3. Configure ntlmrelayx with target list:

```
None
# Create targets.txt with systems lacking SMB signing
ntlmrelayx.py -tf targets.txt -smb2support
```

4. Wait for authentication event (user accessing share, service account)
5. Relay authentication to target systems
6. Gain administrative access and execute commands:

```
None
ntlmrelayx.py -tf targets.txt -smb2support -c "whoami"
```

Testing Process:

1. Scanned network for systems without SMB signing:

```
None
crackmapexec smb 10.10.100.0/24 --gen-relay-list
relay-targets.txt
```

2. Deployed Responder for LLMNR poisoning
3. Configured ntlmrelayx targeting vulnerable systems
4. Captured and relayed SMB authentication
5. Successfully gained admin access to 23 systems
6. Demonstrated credential dumping via relay
7. Documented impact and lateral movement capabilities

Compliance Impact:

- MITRE ATT&CK: T1557.001 (LLMNR/NBT-NS Poisoning), T1021.002 (SMB/Windows Admin Shares)
- NIST: SC-8 (Transmission Confidentiality/Integrity), AC-17 (Remote Access)
- PCI DSS: Requirement 4.1 (Encrypt Transmission of Cardholder Data)
- CIS Controls: 3.10 (Encrypt Sensitive Data in Transit)

Finding #6: DPAPI Secret Extraction (Saved Credentials)

Description:

Windows Data Protection API (DPAPI) is used to protect user secrets including:

- Browser saved passwords (Chrome, Edge, Firefox)
- Windows Credential Manager
- Remote Desktop credentials
- VPN credentials
- Application passwords

When an attacker gains access to a user's workstation (or user profile data), DPAPI-protected secrets can be extracted using the user's login credentials or system access. During testing, we successfully extracted:

- 47 saved browser passwords
- 12 RDP saved sessions with credentials
- 8 VPN profiles with passwords
- Various application credentials

This data enables further lateral movement, external service compromise, and access to personal/corporate accounts.

Testing Date: January 7, 2025

Risk Level: HIGH

Level of Effort: Medium (requires user education and technical controls)

Status: Active - Requires remediation

Affected Resources:

- Internal Network: 10.10.100.0/24
- All Windows workstations
- User credentials for internal and external services

Remediation:

Immediate Actions:

1. Implement Password Manager Policy:
    - Deploy enterprise password manager (1Password, LastPass Enterprise, etc.)
    - Disable browser password saving via GPO:

```
None
# Chrome
Computer Configuration > Policies > Administrative
Templates > Google > Google Chrome
- Enable the password manager = Disabled

# Edge
Computer Configuration > Policies > Administrative
Templates > Microsoft Edge
- Enable saving passwords to the password manager =
Disabled
```

2. Disable RDP Credential Saving:

```
None

Computer Configuration > Administrative Templates >
Windows Components > Remote Desktop Services > Remote
Desktop Connection Client
- Do not allow passwords to be saved = Enabled
```

3. Enable Credential Guard (covered in Finding #4)
4. User Education:
    - Security awareness training on password reuse risks
    - Mandate password manager usage
    - Disable "Remember Me" functionality for sensitive apps
5. Monitor for DPAPI Access:
    - Deploy Sysmon to log DPAPI operations

- Alert on bulk credential access
- Implement EDR with behavior analytics

Long-term Solutions:

1. Transition to passwordless authentication (Windows Hello, FIDO2)
2. Implement just-in-time (JIT) privileged access
3. Deploy zero-trust network access for VPN replacement
4. Regular secret rotation and credential hygiene audits

Solution:

Comprehensive secrets management:

- Enterprise password manager deployment
- GPO-enforced browser password blocking
- RDP credential save restrictions
- User training program
- Monitoring and alerting

Reproduction Steps:

1. Gain access to user workstation (local admin or physical access)
2. Extract DPAPI master keys:

```
None
mimikatz # sekurlsa::dpapi
```

3. Locate browser credential databases:

```
None
# Chrome
%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data

# Edge
%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login
Data
```

4. Extract credentials using SharpChrome/SharpEdge:

```
None
SharpChrome.exe logins /unprotect
```

5. Or use mimikatz:

```
None
mimikatz # dpapi::chrome
/in:"%localappdata%\Google\Chrome\User Data\Default\Login
Data"
```

6. Extract RDP credentials:

```
None
mimikatz # dpapi::rdg
```

Testing Process:

1. Gained access to test user workstation
2. Enumerated DPAPI-protected data locations
3. Extracted DPAPI master keys
4. Decrypted browser password databases
5. Extracted RDP and VPN credentials
6. Validated extracted credentials (confirmed 89% valid)
7. Documented types and sensitivity of exposed secrets

Compliance Impact:

- MITRE ATT&CK: T1555.003 (Credentials from Web Browsers), T1555.004 (Windows Credential Manager)
- NIST: IA-5 (Authenticator Management), SC-28 (Protection of Information at Rest)
- PCI DSS: Requirement 8.2.1 (Render authentication credentials unreadable)
- GDPR: Article 32 (Security of Processing) - credential protection

Finding #7: Unauthenticated FTP Access

Description:

Multiple internal systems were found running FTP services that allowed anonymous authentication. Anonymous FTP access exposed sensitive information including:

- Employee names and contact information
- Printer logs and device configurations
- System logs (syslogs)
- Network diagrams and documentation
- Configuration backup files

This information disclosure provides attackers with valuable reconnaissance data for social engineering, targeted phishing, network mapping, and identifying additional attack vectors.

Testing Date: October 31, 2023

Risk Level: CRITICAL

Level of Effort: Low (disable service or require authentication)

Status: Completed - Service disabled and remediated

Affected Resources:

- Internal IP: 172.16.5.0/29
- FTP servers on internal network
- Exposed employee and network information

Remediation:

Implemented Solution:

1. Disabled Anonymous FTP Access:
    - Removed anonymous login capability
    - Implemented authentication requirements
    - Migrated to SFTP/FTPS for encrypted transfer
2. Service Hardening:
    - Disabled FTP service on non-essential systems
    - Implemented firewall rules restricting FTP to authorized hosts only

    - Deployed secure file transfer alternatives
3. Data Classification:
    - Removed sensitive files from FTP directories
    - Implemented access controls based on data sensitivity
    - Established file sharing policies
4. Monitoring:
    - Enabled FTP access logging
    - Deployed alerts for failed authentication attempts
    - Regular audits of FTP service configurations

Solution:

The organization successfully:

- Disabled all anonymous FTP access
- Transitioned to secure file transfer protocols
- Implemented proper access controls
- Removed sensitive data from file shares

Reproduction Steps (Original Finding):

1. Scan for FTP services on internal network:

```
None
nmap -p21 172.16.5.0/29
```

2. Connect with anonymous credentials:

```
None
ftp 172.16.5.10
Username: anonymous
Password: anonymous@example.com
```

3. List available files:

```
None
ftp> ls -la
```

4. Download exposed files:

```
None
ftp> get syslogs/system.log
ftp> get configs/network_diagram.pdf
ftp> get printer_logs/employee_print_jobs.csv
```

5. Extract sensitive information for reconnaissance

Testing Process:

1. Performed port scan identifying FTP services
2. Attempted anonymous authentication (successful)
3. Enumerated directory structure
4. Downloaded sample files
5. Analyzed content for sensitive information
6. Documented types of exposed data
7. Retest: Confirmed anonymous access disabled

Compliance Impact:

- MITRE ATT&CK: T1087 (Account Discovery), T1592.002 (Software)
- NIST: AC-3 (Access Enforcement), SC-8 (Transmission Confidentiality)
- PCI DSS: Requirement 2.2.2 (Enable necessary services only)
- HIPAA: §164.312(a)(1) (Access control)

Finding #8: Lateral Movement Capability Assessment

Description:

During internal network testing with assumed breach scenarios, we validated the ability to perform lateral movement across the network environment. This finding represents the cumulative capability enabled by other vulnerabilities including:

- Weak network segmentation
- Lack of SMB signing
- Extractable credentials (LSASS, DPAPI)
- Trust relationships between systems

Lateral movement is a critical phase in advanced persistent threats (APTs) where attackers:

- Expand access beyond initial compromise
- Discover sensitive data and systems
- Escalate privileges
- Achieve objectives (data exfiltration, ransomware deployment)

Testing Date: October 31, 2023 & May 29, 2025

Risk Level: MEDIUM (lateral movement successful, controls provided partial detection only)

Level of Effort: Varies (depends on specific control implementation)

Status: Validated - Continuous monitoring recommended

Affected Resources:

- Internal Network: 172.16.5.0/29
- Internal infrastructure
- All networked systems

Remediation:

Implemented Controls:

1. Network Microsegmentation:

    - Implemented firewall rules between VLANs
    - Deployed host-based firewalls on critical servers
    - Restricted lateral SMB traffic
2. Enhanced Monitoring:
    - Deployed EDR on all endpoints
    - Implemented network traffic analysis (NTA)
    - Created SIEM rules for lateral movement detection:
        - Unusual RDP/SMB connections
        - Credential use from unexpected hosts
        - Process injection and remote execution
3. Privilege Tiering:
    - Implemented separate admin accounts for different tiers
    - Deployed Privileged Access Workstations (PAWs)
    - Just-in-time privileged access for administrators
4. Deception Technology:
    - Deployed honeypot accounts and systems
    - Created breadcrumb credentials that trigger alerts
    - Implemented canary tokens

Solution:

Layered defense approach:

- Network segmentation
- Endpoint detection and response
- Privileged access management
- Continuous monitoring and threat hunting

Reproduction Steps (Original Testing):

1. Gain initial access to internal system
2. Perform network reconnaissance:

```
None
# Discover additional hosts
crackmapexec smb 172.16.5.0/29
```

```
# Enumerate shares
smbmap -H 172.16.5.0/29 -u username -p password
```

3. Extract credentials from compromised system (per Finding #4)
4. Use credentials for lateral movement:

```
None
# Pass-the-Hash lateral movement
crackmapexec smb 172.16.5.0/29 -u username -H ntlmhash -x
"whoami"

# Remote code execution
impacket-wmiexec DOMAIN/username@target-ip
```

5. Establish persistence on new systems
6. Repeat discovery and movement process

Testing Process:

1. Simulated initial compromise scenario
2. Performed AD enumeration with Bloodhound
3. Identified lateral movement paths
4. Executed controlled lateral movement
5. Validated detection capabilities (partial detection)
6. Documented undetected movement techniques
7. Recommended enhanced monitoring

Compliance Impact:

- MITRE ATT&CK: T1021 (Remote Services), T1570 (Lateral Tool Transfer)
- NIST: AC-4 (Information Flow Enforcement), SI-4 (System Monitoring)
- PCI DSS: Requirement 10 (Track and monitor all access)
- SANS Top 20: Critical Security Control 12 (Boundary Defense)

Additional Critical Findings Summary

Due to the extensive nature of this assessment, the following additional critical findings were identified and remediated

Finding #9: Unauthenticated Shell Access via Telnet

- Risk: Critical
- Status: Remediated
- Description: Telnet service accessible with brute-forced credentials (root:solokey), providing root shell access
- Resolution: Telnet service disabled, SSH deployed with key-based authentication

Finding #10: Network Device Default Credential Vulnerability

- Risk: Critical
- Status: Remediated
- Description: Printers and network devices (SHARP, Ricoh, HP) using default credentials (admin/admin, admin/blank)
- Resolution: All default credentials changed, authentication enforced, management interfaces restricted

Finding #11: SNMP Brute Force Attack

- Risk: Critical
- Status: Remediated
- Description: SNMP community strings successfully brute forced, allowing network device access
- Resolution: SNMPv3 deployed with strong authentication, SNMPv1/v2 disabled

Finding #12: Unauthenticated SMB Access

- Risk: Critical
- Status: Remediated
- Description: SMB shares accessible without authentication, information disclosure
- Resolution: Anonymous SMB disabled, authentication required, share permissions audited

Finding #13: Ivanti Connect Secure - Authentication Bypass (CVE-2023-46805)

- Risk: Critical (if vulnerable)
- Status: Not Vulnerable
- Description: Tested for critical Ivanti Connect Secure authentication bypass
- Resolution: System patched and not vulnerable to this CVE

Prioritized Remediation

Based on the manual penetration testing assessment, we have confirmed and prioritized the following findings for remediation:

Tier 1: Critical - Immediate Action Required (24-48 hours)

Finding	Risk	Business Impact	Technical Effort
Active Directory DCSync Attack	Critical	Complete domain compromise	High
LDAP Relay Attack to DC	Critical	Full domain takeover	Medium
SMB Relay Attack (Missing Signature Requirement)	High	Lateral movement, credential theft	Medium

Recommended Actions:

1. Immediately audit and restrict DCSync permissions
2. Enable LDAP signing and channel binding on all DCs
3. Deploy SMB signing via Group Policy to all systems
4. Implement emergency monitoring for these attack vectors

Tier 2: High Priority - Short Term (1-2 weeks)

Finding	Risk	Business Impact	Technical Effort
Memory-Based Credential Extraction (LSASS)	High	Credential theft, lateral movement	Medium
DPAPI Secret Extraction (Saved Credentials)	High	Access to cloud services, VPN, applications	Medium
VPN Network Segmentation Bypass	High	Unrestricted internal access	High

Recommended Actions:

1. Deploy Credential Guard across all Windows 10/11 systems
2. Implement enterprise password manager
3. Enhance VPN network segmentation
4. Deploy LAPS for local administrator passwords

Tier 3: Medium Priority - Medium Term (1-3 months)

Finding	Risk	Business Impact	Technical Effort
Lateral Movement Capability Assessment	Medium	Successful network traversal with partial detection	Medium

Recommended Actions:

1. Enhance EDR detection rules for lateral movement
2. Deploy comprehensive network traffic analysis (NTA)
3. Implement microsegmentation to limit lateral traversal
4. Deploy deception technology (honeypots, canary tokens)

Successfully Remediated Findings

The following critical findings were identified and successfully remediated:

- Unauthenticated FTP Access
- Unauthenticated Shell Access via Telnet
- Network Device Default Credential Vulnerability
- Unauthenticated SMB Access
- SNMP Brute Force Attack

Validation: All remediated findings were retested and confirmed secure.

Re-testing

The goal of our penetration test is to ensure that the findings we are addressing have been assessed, remediated, and confirmed.

Retest Schedule

After finishing the remediation stage, we will retest the findings in order to ensure that their mitigation is complete.

Retest Timeline:

- Tier 1 Findings: Retest within 1 week of remediation deployment
- Tier 2 Findings: Retest within 2 weeks of remediation deployment
- Tier 3 Findings: Retest within 1 month of remediation deployment

Retest Scope

Each retest will include:

1. Validation of Fix: Confirm the specific vulnerability is resolved
2. Regression Testing: Ensure the fix didn't introduce new issues
3. Bypass Attempts: Attempt to circumvent implemented controls
4. Documentation: Updated report with retest results

Successful Retests Completed

Finding	Original Risk	Retest Date	Result
VPN Network Segmentation Bypass	High	April 11, 2025	✅ PASS - Remediation effective
Unauthenticated FTP Access	Critical	November 7, 2023	✅ PASS - Service disabled
Unauthenticated Shell Access via Telnet	Critical	January 16, 2024	✅ PASS - Telnet disabled, SSH secured
Network Device Default Credential Vulnerability	Critical	November 14, 2023	✅ PASS - All defaults changed
Unauthenticated SMB Access	Critical	November 8, 2023	✅ PASS - Authentication required
SNMP Brute Force Attack	Critical	December 26, 2024	✅ PASS - SNMPv3 deployed

Pending Retests

The following findings are pending remediation and retest:

- Active Directory DCSync Attack
- LDAP Relay Attack to Domain Controller
- Memory-Based Credential Extraction (LSASS)
- DPAPI Secret Extraction (Saved Credentials)
- SMB Relay Attack (Missing Signature Requirement)

Retest Credits: Included in original engagement scope at no additional cost.

Disclosure

Sample Report Notice

This is a sample penetration testing report compiled from actual findings discovered during real customer engagements conducted by Penti between October 2023 and January 2025. The findings presented are authentic and representative of our penetration testing capabilities. All customer-identifying information, IP addresses, and specific infrastructure details have been redacted or replaced with fictional examples to protect client confidentiality.

The methodologies, tools, techniques, and remediation guidance presented in this report reflect our standard approach to penetration testing engagements.

Standard Disclaimer

Penti uses the best practices for security scanning and detecting the security holes in an application and/or infrastructure. Please note that new findings and security holes are constantly discovered and patches to software and platforms are conducted momentarily. Under development applications are especially more prone to frequent findings introduced. As a result, Penti is unable to guarantee that your application or infrastructure is completely safe from every form of attacks that are undiscovered at the time.

Important Disclaimers

Zero-Day Vulnerabilities: This assessment tests for known vulnerabilities and attack techniques as of the testing date. Zero-day vulnerabilities (unknown to vendors) cannot be tested for and may exist.

Evolving Threat Landscape: Cyber threats evolve rapidly. New attack techniques, vulnerabilities, and exploits are discovered daily. Regular periodic testing is recommended.

Scope Limitations: Testing was limited to the agreed-upon scope. Systems, applications, or network segments outside the scope were not tested and may contain vulnerabilities.

Testing Methodology: Manual penetration testing simulates real-world attacks using

current best practices and common attacker methodologies. However, determined nation-state actors or advanced persistent threats (APTs) may employ sophisticated techniques beyond standard testing scope.

Recommendations: All findings and recommendations should be validated in your specific environment before implementation. Some remediation steps may impact business operations and should be tested in non-production environments first.

Our Certifications

Penti's penetration testing team holds the following industry-recognized certifications:

Offensive Security Certifications

- OSCP+ (OffSec Certified Professional Plus)
- OSCP (OffSec Certified Professional)
- CPTS (Hack The Box Certified Penetration Testing Specialist)
- eCPPTv2 (eLearnSecurity Certified Professional Penetration Tester v2)
- eJPTv2 (eLearnSecurity Junior Penetration Tester v2)
- CEH (Certified Ethical Hacker - Practical)

Cloud Security Certifications

- AWS Certified Security - Specialty
- AWS Solutions Architect Associate
- Microsoft Azure Security Engineer Associate
- Microsoft Azure Administrator Associate
- Google Cloud Professional Security Engineer

Blue Team & Defense Certifications

- BTL1 (Blue Team Level 1)
- CCSE (Certified Container Security Expert)
- CompTIA PenTest+
- CompTIA Security+

Specialized Certifications

- CREST - Elected Member, Pentest Focus Group Subcommittee
- Metasploit Pro Certified Specialist
- PentesterLab - PCAP, Unix, Introduction Badges
- Hack The Box - Dante Pro Lab, 130+ machines completed

Industry Memberships

- CREST - Council of Registered Ethical Security Testers
- SFISSA - South Florida Information Systems Security Association
- Bugcrowd - Ambassador Program
- Secjuice - Technical Writer

Continuous Training

Our team actively participates in:

- Hack The Box Academy & Pro Labs
- TryHackMe Advanced Paths
- Bug Bounty Programs (HackerOne, Bugcrowd)
- CTF Competitions (SFISSA HackTheFlag, DEF CON, etc.)
- SANS courses and webinars
- OffSec advanced training

Contact Information

For questions regarding this report or to schedule remediation support and retesting:

Penti - Agentic AI Penetration Testing
Boca Raton, Florida
www.penti.ai

Report Prepared By:
Penti Penetration Testing Team
Lead Penetration Testers: [REDACTED]

Report Date: January 2025
Report Version: Sample - Compiled from Q4 2023 - Q1 2025 Engagements
Report Type: Sample Penetration Testing Report
Classification: Sample - For Demonstration Purposes

This report contains sensitive security information. Distribution should be limited to authorized personnel only. Unauthorized disclosure may increase security risks.