Tukkan Consultancy & Analytics

GORA Company

Penetration Testing Report

Business Confidential

Date: March 14th 2025

Table of Contents

Confidentiality Statement

This document and its contents are the exclusive property of **GORA Corp** and **Tukkan Consultancy**. It contains proprietary and confidential information; any duplication, redistribution or use—whether in whole or in part, and in any form—requires the prior written consent of both GORA Corp and Tukkan Consultancy.

GORA Corp may, under a duly executed non-disclosure agreement, share this document with authorized auditors to demonstrate compliance with penetration-testing requirements.

Disclaimer

A penetration test represents a point-in-time evaluation. The findings and recommendations reflect only the information gathered during the engagement period and do not account for any subsequent changes or modifications.

Because time-boxed assessments cannot exhaustively test every security control, Tukkan Consultancy focuses on identifying those controls most susceptible to exploitation. We recommend that GORA Corp undertake comparable assessments—either internally or via an independent third party—on an annual basis to validate and maintain the effectiveness of its security controls.

Pentest Team

Tukkan Red Team

Name	Certification	Report Status
Executive		
John Smith, CEO	CISSP, OSCP	**APPROVED**
Technical Team		
John Smith	OSCP, OSWE, OSCE, CREST CRT	**APPROVED**
Jane Smith	OSCP	**APPROVED**

Assessment Methodology

From February 8 to August 8, 2025, **GORA Corp** retained **Tukkan Consultancy** to assess the security posture of its infrastructure against leading industry benchmarks, including an internal network penetration test. All activities were conducted in accordance with:

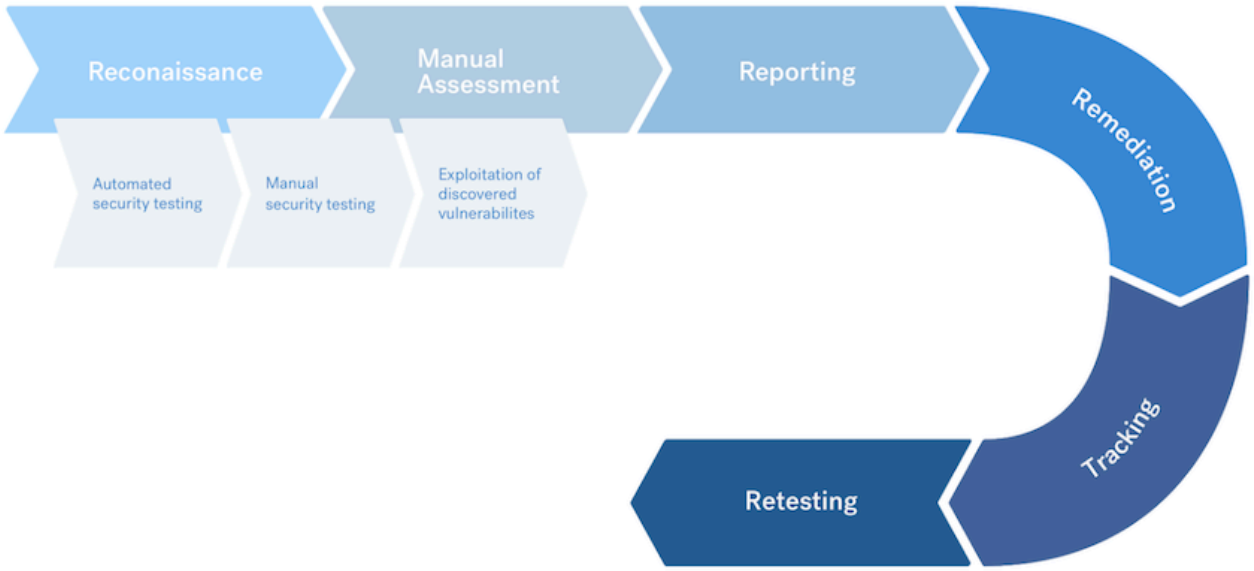
NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment

- **OWASP Testing Guide (v4)**
- Customized testing frameworks tailored to GORA Corp's environment

Penetration Test Phases

1. **Planning**
    - Define engagement scope, objectives and rules of engagement
    - Align on timelines, data handling and communication protocols
2. **Discovery**
    - Conduct network and host scanning
    - Enumerate services, accounts and configurations to identify potential weaknesses
3. **Exploitation**
    - Validate and exploit identified vulnerabilities
    - Leverage any new footholds to further map and assess the internal network
4. **Reporting**
    - Document confirmed vulnerabilities, successful and unsuccessful exploit attempts
    - Highlight strengths, weaknesses and prioritized remediation recommendations

This structured, methodical approach ensured a comprehensive, point-in-time evaluation of GORA Corp's internal defenses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker operating from within the corporate network. The engineer begins by scanning and enumerating the internal environment to discover hosts, services, misconfigurations, and systems still using default or weak credentials (for example, RDP, SSH, printers, or databases). From there, they exploit both common and advanced techniques—LLMNR/NBT-NS poisoning and other man-in-the-middle attacks, Kerberos token impersonation, Kerberoasting, pass-the-hash, and golden-ticket creation—while also probing internally-facing web applications for well-known vulnerabilities such as SQL injection, cross-site scripting (XSS), server-side request forgery (SSRF), and remote code execution (RCE). Once initial access is gained, the engineer moves laterally across the network, harvesting credentials and escalating privileges up to domain-admin level. Finally, they exfiltrate sensitive data to demonstrate the real-world impact of a compromised insider and highlight the combined risk posed by weak credentials and web-application flaws.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Urgent	9.0-10.0	This vulnerability allows an attacker to gain full system-level privileges with minimal effort; apply the recommended patch immediately, implement compensating controls A report for this kind of vulnerability is sent during the pentest.
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Information	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	10.x.x.x/8

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

GORA Corp provided Tukkan Consultancy the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

Tukkan Consultancy assessed **GORA Corp**'s internal security posture via a penetration test conducted from **February 8 to August 8, 2025**. The sections that follow deliver a high-level summary of identified vulnerabilities, successful and unsuccessful exploitation attempts, and the organization's key strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten
6 months include business days.

Testing Summary

The network assessment examined **GORA Corp**'s internal security posture. From an insider vantage point, the **Tukkan Consultancy** team conducted comprehensive vulnerability scans across all IP ranges provided by GORA Corp to gauge overall patching efficacy. In parallel, the team executed common Active Directory–centric attacks—Link-Local Multicast Name Resolution (LLMNR) poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting—to validate exploitability. Beyond scanning and AD attacks, Tukkan Consultancy evaluated additional risk vectors, including open file shares, default or weak credentials on servers and network devices, and disclosure of sensitive information, in order to form a holistic view of the network's defenses.

Key findings included:

- **LLMNR enabled (Finding IPT-001):** Allowed interception of user hashes via poisoning, which were subsequently cracked offline using dictionary attacks—evidence of a weak password policy (Finding IPT-005).
- **Overly permissive user accounts:** Cracked credentials granted access to multiple hosts.
- **WDigest enabled on legacy systems (Finding IPT-009 & IPT-003):** Facilitated recovery of cleartext credentials.
- **Reused local account hashes (Finding IPT-002):** Enabled lateral compromise via pass-the-hash across multiple machines.

These results highlight critical gaps in credential management, patching cadence, and authentication hardening that warrant prioritized remediation.

From February 8 to August 8, 2025, the **Tukkan Consultancy** team leveraged credentials harvested via WDigest and hash dumps to pivot laterally across GORA Corp's network. They ultimately landed on a host where a Domain Administrator account was exposed in cleartext through WDigest. Using that account, the team authenticated to the domain controller and achieved full domain compromise (see Finding IPT-025 for a detailed walkthrough).

Additional critical observations included:

- **Kerberos delegation abuse (Finding IPT-004):** Enabled user impersonation via delegation attacks.
- **SMB relay susceptibility (Finding IPT-007):** Occurred because SMB signing was disabled.
- **Unrestricted IPv6 traffic (Finding IPT-006):** Created a path for LDAPS relaying and potential domain takeover.

Remaining critical findings centered on patch management failures, with outdated software (Finding IPT-008), legacy operating systems (Finding IPT-009), and unpatched Microsoft remote-code-execution flaws (Findings IPT-010 through IPT-013) present throughout the environment.

The balance of findings fell into high, medium, low, or informational severity tiers. For a comprehensive breakdown, please refer to the Technical Findings section.

Tester Notes and Recommendations

The assessment of **GORA Corp**'s internal network reflects the typical challenges of a first-time penetration test. Many identified issues stem from Active Directory features enabled by default—LLMNR poisoning, IPv6 relaying, and Kerberoasting.

Two themes dominated our findings: a weak password policy and inconsistent patching. The weak password policy provided our initial foothold, allowing **Tukkan Consultancy** to crack over 2,200 user passwords—including most Domain Administrator accounts—via basic dictionary attacks. We recommend GORA Corp enforce a minimum of **15-character** passwords for standard users and **30-character** passwords for Domain Administrators, implement password blacklisting (we will supply the cracked-password list for review), and consider deploying a Privileged Access Management solution.

Outdated operating systems and lax patching enabled compromise of dozens of hosts. While additional remote-code-execution exploits (e.g. MS17-010) were available, both teams agreed further exploitation was unnecessary once the domain controller was owned, to avoid unintended service disruption. We advise GORA Corp to review the patching recommendations in the Technical Findings section and the accompanying Nessus scan data, then strengthen patch-management policies and procedures to mitigate future risk.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

3	13	5	6	0	1
Urgent	Critial	High	Moderate	Low	Informatioal

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: MS17-010 (EternalBlue) RCE	Urgent	Apply the Microsoft patch immediately to all affected systems and verify successful remediation.
IPT-002: CVE-2020-1472 (Zerologon)	Urgent	Deploy the August 2020 patch on all domain controllers without delay; enable enforcement mode and validate DC-to-DC secure channel integrity.
IPT-003: Internet-Facing SSH	Urgent	Disable password logins, enforce key-based authentication, and limit access via firewall/allow-lists.
IPT-004: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.

IPT-005: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-006: Security Misconfiguration – Wdigest	Critical	Disable WDigest via GPO.
IPT-007: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-008: Insufficient Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-009: Security Misconfiguration – IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO.
IPT-010: Insufficient Hardening – SMB Signing Disabled	Critical	Enable SMB signing on all Demo Corp domain computers.
IPT-011: Insufficient Patch Management – Software	Critical	Update to the latest software version.
IPT-012: Insufficient Patch Management – Operating Systems	Critical	Update Operating Systems to the latest version.
IPT-013: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI	Critical	Apply the appropriate Microsoft patches to remediate the issue.
IPT-014: Insufficient Patching – MS12-020 – Remote Desktop RCE	Critical	Apply the appropriate Microsoft patches to remediate the issue.
IPT-015:Unconstrained Kerberos Delegation	Critical	Audit and remove any accounts or services configured for unconstrained or protocol-transition delegation; reconfigure only as constrained delegation where strictly necessary and monitor ticket-granting ticket (TGT) requests.
IPT-016: Insufficient Patching – CVE- 2019-0708 - BlueKeep	Critical	Apply the appropriate Microsoft patches to remediate the issue.

Finding	Severity	Recommendation

IPT-017: Insufficient Privileged Account Management – Kerberoasting	High	Use Group Managed Service Accounts (GMSA) for privileged services.
IPT-018: Security Misconfiguration – GPP Credentials	High	Apply vendor patching. Do not use GPP cpasswords.
IPT-019: Insufficient Authentication - VNC	High	Enable authentication on the VNC Server.
IPT-020: Default Credentials on Web Services	High	Change default credentials or disable unused accounts.
IPT-021: Insufficient Hardening – Listable Directories	High	Restrict access and conduct web app assessment.
IPT-022: Unauthenticated SMB Share Access	Moderate	Disable SMB share or require authentication.
IPT-023: Insufficient Patch Management – SMBv1	Moderate	Upgrade to SMBv3 and apply latest patching.
IPT-024: IPMI Hash Disclosure	Moderate	Disable IPMI over LAN if it is not needed.
IPT-025: Insufficient SNMP Community String Complexity	Moderate	Disabled SNMP if not required.
IPT-026: Insufficient Data in Transit Encryption - Telnet	Moderate	Migrate to TLS protected protocols.
IPT-027: Insufficient Terminal Services Configuration	Moderate	Enable Network Level Authentication (NLA) on the remote RDP server.
IPT-028: Steps to Domain Admin	Informational	Review action and remediation steps.

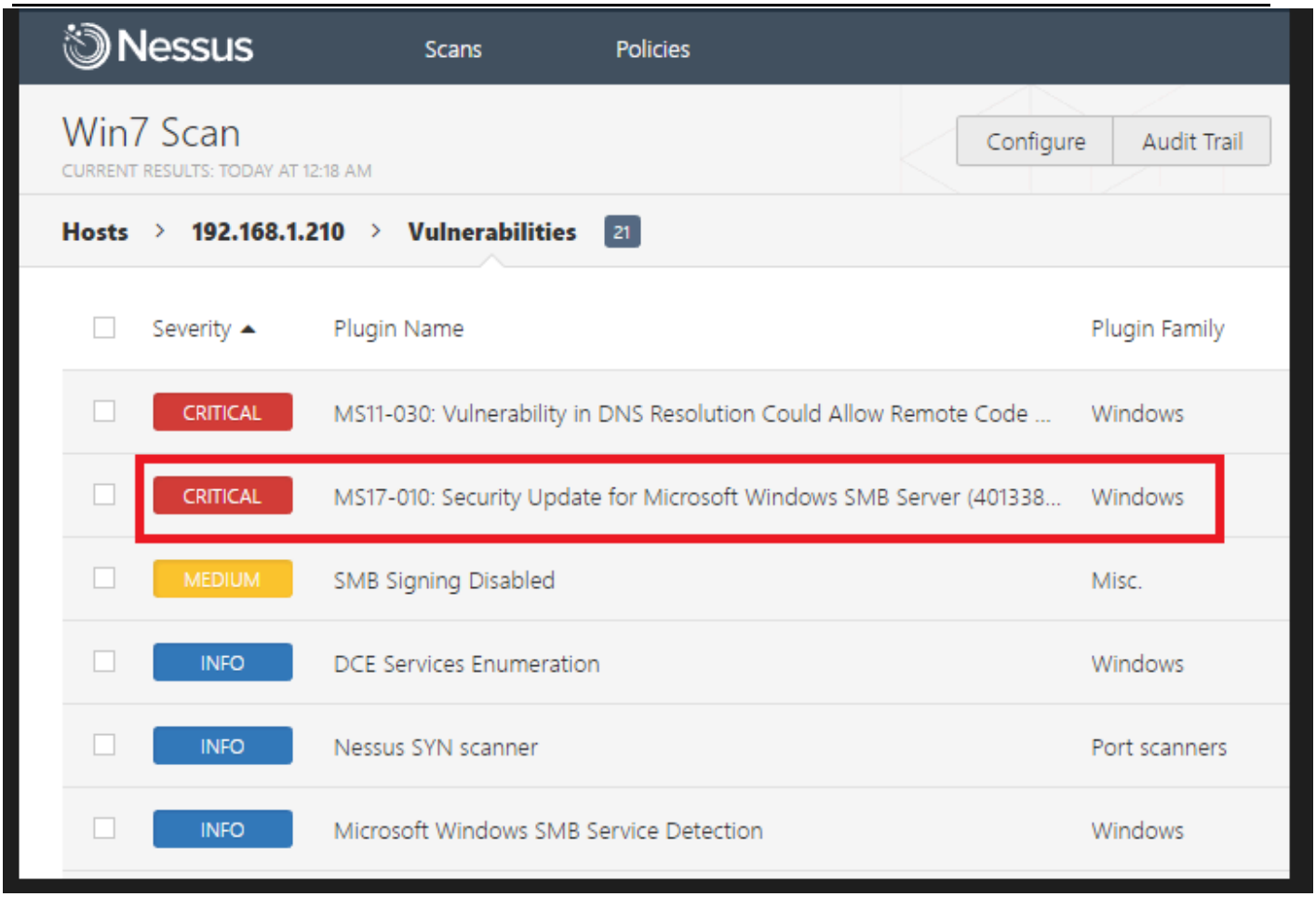
Technical Findings

Internal Penetration Test Findings

Finding IPT-001: IPT-001: MS17-010 (EternalBlue) RCE (Urgent)

Description:	GORA Corp's SMBv1 service was unpatched and susceptible to the MS17-010 vulnerability. Tukkan Consultancy leveraged an EternalBlue exploit to achieve remote code execution and system-level access on affected hosts, leading directly to full domain compromise.
Risk:	**Likelihood:** High – EternalBlue exploits unpatched SMBv1 on exposed hosts with minimal prerequisites, making successful compromise highly probable. **Impact:** Very High – Remote code execution at SYSTEM level enables full host takeover, lateral movement, and potential domain-wide compromise.
System:	All
Tools Used:	Metasploit (EternalBlue), Nessus
References:	- Microsoft Security Bulletin MS17-010 - CVE-2017-0144 - NIST SP 800-53 r4 CM-7: Least Functionality

Evidence



Remediation

1. **Apply Patches:**
   - Immediately install the Microsoft MS17-010 security update on all Windows hosts.
   - Verify patch status via WSUS, SCCM, or manual inspection.
2. **Disable SMBv1:**

Remove or disable the SMBv1 protocol on servers and workstations:

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

   - Reboot systems where required to complete removal.
3. **Enforce Network-Level Authentication (NLA):**
   - Require NLA for all Remote Desktop Services by setting `Require user authentication for remote connections by using Network Level Authentication` to **Enabled** in Group Policy.
4. **Restrict SMB Access:**

- Block inbound SMB (TCP 445) on the perimeter firewall.
- Limit SMB access internally via VLAN segmentation and access control lists.

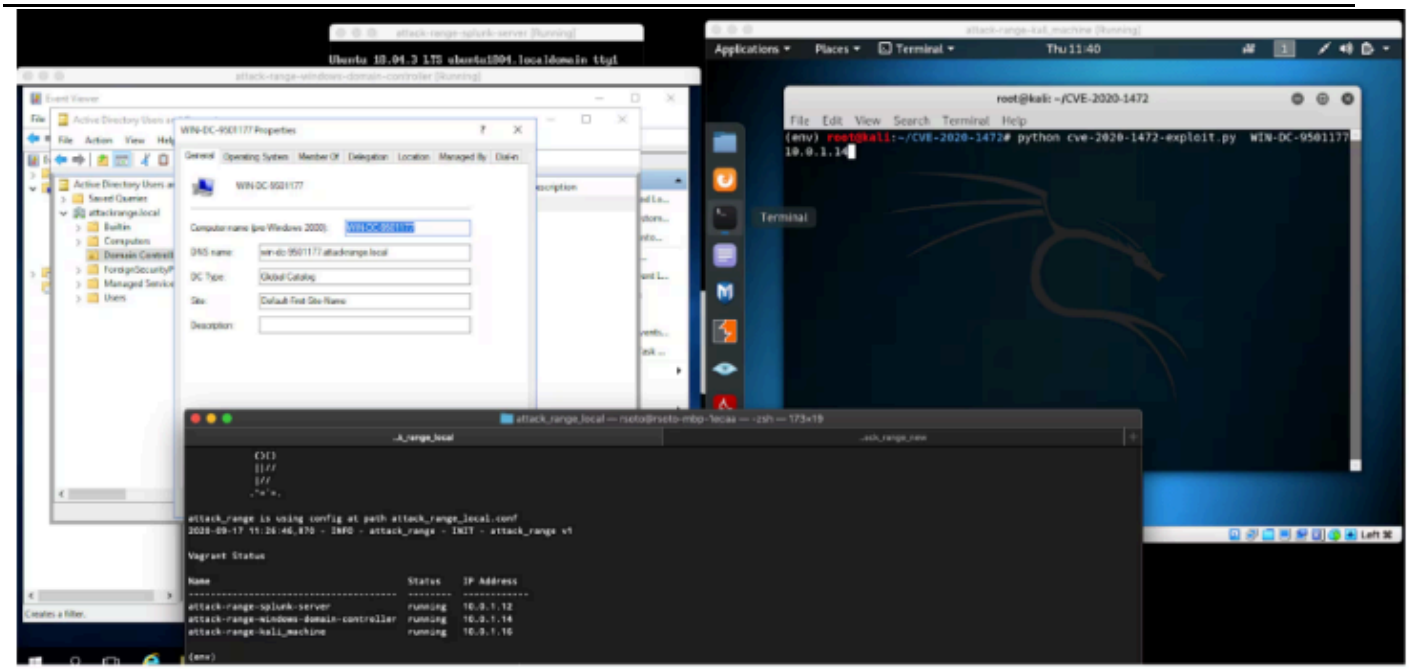
5. **Post-Remediation Validation:**
   - Run vulnerability scans to confirm MS17-010 is no longer detected.
     Test SMB connectivity to ensure business-critical file shares remain accessible under SMBv2/SMBv3.

Implementing these controls will eliminate the EternalBlue attack vector and strengthen overall SMB security.

Finding IPT-002: CVE-2020-1472 (Zerologon) (Urgent)

Description:	GORA Corp's domain controllers were unpatched and vulnerable to the Zerologon flaw. Tukkan Consultancy leveraged the Impacket ZeroLogon exploit to reset the domain controller's machine account password, allowing immediate domain takeover.
Risk:	**Likelihood:** High – Zerologon requires only network access to a domain controller and can be executed with publicly available tools, making successful exploitation very likely. **Impact:** Very High – Exploitation resets the domain controller's machine account password, enabling full domain takeover and complete compromise of Active Directory.
System:	All domain controllers
Tools Used:	Impacket "zerologon" tool, Nessus
References:	- Microsoft Security Advisory CVE-2020-1472 - CVE-2020-1472 - NIST SP 800-53 r4 AC-2: Account Management - NIST SP 800-53 r4 SC-8: Transmission Confidentiality and Integrity

Evidence



Remediation

Remediation for CVE-2020-1472 (Zerologon):

1. **Apply Microsoft's August 2020 Patch:**
    - Install security update KB 4569509 (or newer) on all domain controllers immediately.
2. **Enable Enforcement Mode:**

After patching, configure DCs to reject legacy Netlogon secure channel sessions:

powershell

```
Set-ItemProperty -Path
"HKLM:\System\CurrentControlSet\services\Netlogon\Parameters" -Name
"RequireSignOrSeal" -Value 2

Restart-Service netlogon
```

3. **Validate Secure Channel Integrity:**

Use Microsoft's NItest or "Test-ComputerSecureChannel" to confirm each DC is enforcing secure RPC:

powershell

```
Test-ComputerSecureChannel -Verbose
```

4. **Review and Rotate Machine Account Passwords:**
    - Force a replication cycle to ensure all DCs share the updated secure channel keys.
    - If you suspect compromise, reset the computer account password for each DC.
5. **Monitor and Audit:**
    - Check security logs for failed Netlogon sign/seal errors (Event ID 5827).
    - Alert on any Netlogon RDP or LDAP authentication failures.
6. **Harden Network Access:**
    - Restrict RPC (TCP 135 and dynamic ports) to trusted management subnets.
    - Use IPsec or firewall rules to limit which hosts can initiate Netlogon sessions

Finding IPT-003: Internet-Facing SSH (Urgent)

Description:	GORA Corp had SSH services exposed to the internet using factory/default or weak passwords. Tukkan Consultancy successfully brute-forced these credentials to gain remote shell access, demonstrating full system takeover potential.
Risk:	Likelihood: High – Internet-reachable SSH endpoints can be rapidly identified and brute-forced with commodity tools against weak or default credentials. Impact: Very High – A successful login grants attackers remote shell (often at privileged level), enabling lateral movement, data exfiltration, or ransomware deployment.
System:	Internet-facing SSH servers (Linux/Unix)
Tools Used:	Nmap, Hydra, Burp Suite (for validation), Nessus
References:	- OWASP A2: Authentication - NIST SP 800-53 r4 AC-17: Remote Access - NIST SP 800-53 r4 IA-5: Authenticator Management

Evidence

```
r00trwx@evil ~ nmap 192.168.0.103

Starting Nmap 7.60 ( https://nmap.org ) at 2018-09-14 00:51 IST
Nmap scan report for 192.168.0.103
Host is up (0.00021s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
```

```
labex:project/ $ hydra -L usernames.txt -P passwords.txt ssh://localhost -t 4 -vV
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-29 11:17:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://localhost:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://admin@127.0.0.1:22
[INFO] Successful, password authentication is supported by ssh://127.0.0.1:22
[ATTEMPT] target localhost - login "admin" - pass "password" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "password123" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123456" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "qwerty" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "letmein" - 5 of 25 [child 2] (0/0)
[ATTEMPT] target localhost - login "root" - pass "password" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "password123" - 7 of 25 [child 1] (0/0)
[ATTEMPT] target localhost - login "root" - pass "123456" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target localhost - login "root" - pass "qwerty" - 9 of 25 [child 2] (0/0)
[ATTEMPT] target localhost - login "root" - pass "letmein" - 10 of 25 [child 3] (0/0)
[ATTEMPT] target localhost - login "testuser" - pass "password" - 11 of 25 [child 0] (0/0)
[ATTEMPT] target localhost - login "testuser" - pass "password123" - 12 of 25 [child 1] (0/0)
[22][ssh] host: localhost   login: testuser   password: password123
[ATTEMPT] target localhost - login "user" - pass "password" - 16 of 25 [child 1] (0/0)
[ATTEMPT] target localhost - login "user" - pass "password123" - 17 of 25 [child 2] (0/0)
[ATTEMPT] target localhost - login "user" - pass "123456" - 18 of 25 [child 1] (0/0)
[ATTEMPT] target localhost - login "user" - pass "qwerty" - 19 of 25 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "letmein" - 20 of 25 [child 3] (0/0)
[ATTEMPT] target localhost - login "guesty" - pass "password" - 21 of 25 [child 2] (0/0)
[ATTEMPT] target localhost - login "guesty" - pass "password123" - 22 of 25 [child 1] (0/0)
[ATTEMPT] target localhost - login "guesty" - pass "123456" - 23 of 25 [child 0] (0/0)
[ATTEMPT] target localhost - login "guesty" - pass "qwerty" - 24 of 25 [child 3] (0/0)
[ATTEMPT] target localhost - login "guesty" - pass "letmein" - 25 of 25 [child 3] (0/0)
[STATUS] attack finished for localhost (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-29 11:17:25
labex:project/ $
```

Remediation

Eliminate Default/Weak Accounts

- Audit all internet-exposed SSH endpoints and remove or rename any accounts using factory defaults.
- Enforce unique, complex credentials or disable local password logins entirely.

Enforce Key-Based Authentication

- In `/etc/ssh/sshd_config`, disable `PasswordAuthentication` and `PermitRootLogin`.
- Require strong SSH key pairs (RSA ≥2048 bits or ED25519), managed via a central key store or certificate authority.

Restrict Port Exposure

- Remove direct internet exposure of the SSH port (default TCP 22).
- If remote access is required, place SSH behind a VPN or bastion/jump host.
- Alternatively, change the listening port and implement port-knocking or Single Packet Authorization to obscure the service.

Implement Multi-Factor Authentication

- Integrate SSH with an MFA solution (e.g., Duo, Azure MFA) to require a second factor on login.

Rate-Limit and Block Brute-Force

- Deploy fail2ban or SSHGuard to detect and ban repeated failed login attempts.
- Configure strict banning thresholds for public-facing endpoints.

Keep SSH Up-to-Date and Hardened

- Regularly apply OS and OpenSSH patches.
- Disable deprecated algorithms and enforce strong ciphers, MACs, and KEX methods in `sshd_config`.

Continuous Monitoring and Audit

- Forward SSH logs to a centralized SIEM for alerting on anomalous access patterns.
- Perform periodic penetration tests and credential audits to validate and refine controls.

Finding IPT-004: Insufficient LLMNR Configuration (Critical)

Description:	GORA Corp allows multicast name resolution on their end-user networks. Tukkan Consultancy captured 20 user account hashes by poisoning LLMNR traffic and cracked 2 with commodity cracking software. The cracked accounts were then used to gain additional access, ultimately leading to the compromise of the Domain Controller.
Risk:	Likelihood: High – This attack is effective in environments allowing multicast name resolution. Impact: Very High – LLMNR poisoning permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
System:	All
Tools Used:	Responder, Hashcat
References:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidence

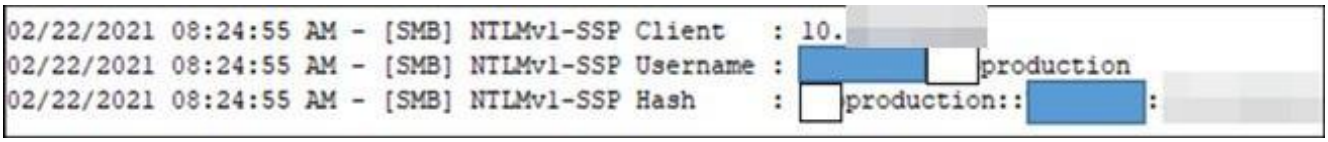


Figure 1: Captured hash of "production"

Figure 2: Cracked hash of "production"

Remediation

Disable multicast name resolution via GPO. For full mitigation and detection guidance, please reference the MITRE guidance here.

The cracked hashes demonstrate a deficient password complexity policy. If multicast name resolution is required, Network Access Control (NAC) combined with application whitelisting can limit these attacks.

Finding IPT-005: Security Misconfiguration – Local Admin Password Reuse (Critical)

Description:	Tukkan Consultancy used local administrator hashes—harvested via the machine access granted by the cracked credentials in Finding IPT-001—to perform pass-the-hash attacks against GORA Corp's endpoints. Because pass-the-hash techniques don't require knowledge of the actual password, the reuse of identical local admin credentials (and therefore identical hashes) across multiple systems enabled the team to authenticate to each host seamlessly. Leveraging this approach, Tukkan Consultancy gained control of approximately 50 machines within GORA Corp's main office. From these footholds, they harvested additional credentials and ultimately compromised the domain controller.
Risk:	Likelihood: High – This attack is effective in large networks with local admin password reuse. Impact: Very High – Pass-the-hash permits an attacker to move laterally and vertically throughout the network.
System:	All
Tools Used:	Impacket, Crackmapexec
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence

Figure 3: Local admin hash used to gain access to machine

Remediation

Utilize unique local admin passwords. Limit local admin users via least privilege. Consider implementing a PAM solution. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-006: Security Misconfiguration – WDigest (Critical)

Description:	GORA Corp maintained legacy operating systems on their network—Windows 7, Windows 8, Server 2008, and Server 2012—that, by default, have WDigest enabled and store currently logged-in users' passwords in clear-text. Tukkan Consultancy used the machine access gained in Findings IPT-004 and IPT-005 to pivot laterally until they located a host where Domain Administrator credentials were exposed via WDigest.
Risk:	Likelihood: Moderate – This attack is effective in networks with older operating systems. Impact: Very High – WDigests credentials are stored in clear text, which can permit the theft of sensitive accounts, such as Domain Administrators.
System:	All systems older than Windows 10 and Server 2016
Tools Used:	Metasploit, Kiwi
References:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than- a-hash/

Evidence

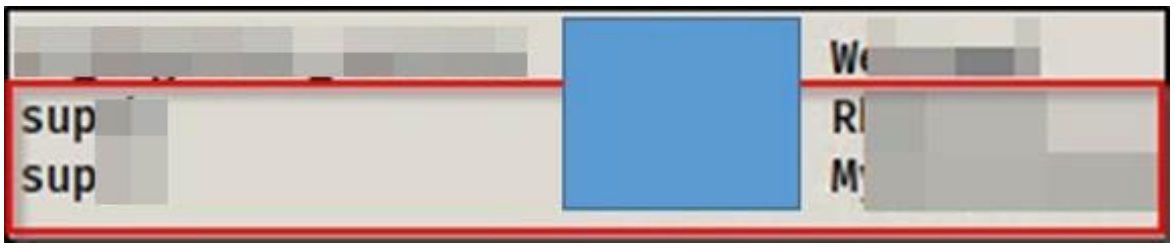


Figure 4: Cleartext passwords of Domain Administrators

Remediation

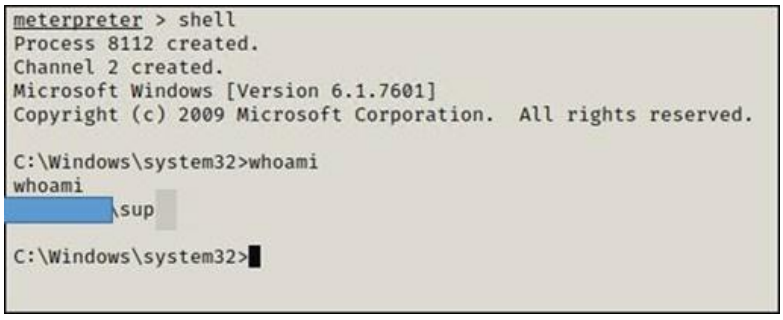
Disable WDigest via GPO. For full mitigation and detection guidance, please reference the guidance here.

Finding IPT-007: Insufficient Hardening – Token Impersonation (Critical)

Description:	Tukkan Consultancy impersonated the token of **supcb**, successfully elevating to Domain Administrator privileges.
Risk:	Likelihood: High – The penetration tester viewed and impersonated tokens with the use of open-source tools. Impact: Very High - If exploited, an attacker gains domain administrator access.
System:	All
Tools Used:	Metasploit, Incognito
References:	NIST SP800-53 r4 CM-7 - Least Functionality NIST SP800-53 r4 AC-6 - Least Privilege https://docs.microsoft.com/en-us/windows-server/identity/ad- ds/manage/how-to-configure-protected-accounts

Evidence

Figure 5: Impersonation of "sup"



F igure 6: Shell access as Domain Admin "sup"

Remediation

Restrict token delegation.Please reference the MITRE guidance here.

Finding IPT-008: Insufficient Password Complexity (Critical)

Description:	Tukkan Consultancy extracted user hashes from GORA Corp's domain controller and executed dictionary-based and low-effort brute-force attacks against all accounts. In total, 2,226 passwords were recovered, including 17 with Domain Administrator privileges.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks base on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting Demo Corp ability to operate.
System:	All
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

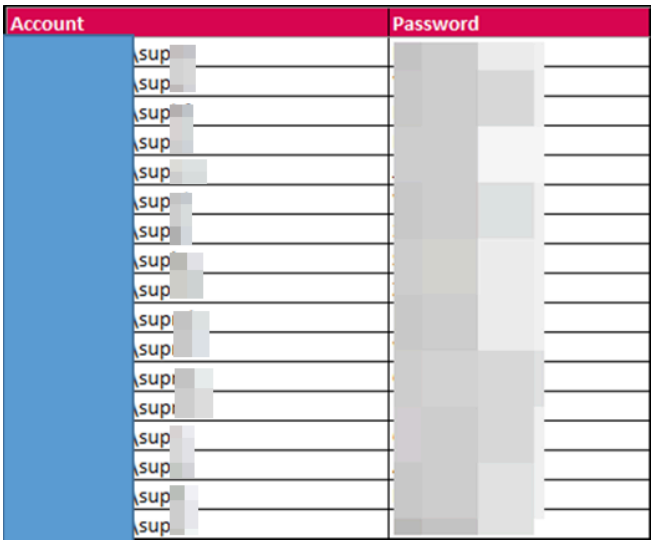


Figure 7: Excerpt of cracked domain hashes

Remediation

Implement CIS Benchmark password requirements / PAM solution.

Finding IPT-009: Security Misconfiguration – IPv6 (Critical)

Description:	Through IPv6 DNS poisoning, the Tukkan Consultancy team successfully relayed credentials to the GORA Corp domain controller.
Risk:	Likelihood: High – IPv6 is enabled by default on Windows networks. The tools and techniques required to perform this task are trivial. Impact: Very High - If exploited, an attacker can gain domain administrator access.
System:	All
Tools Used:	Mitm6, Impacket
References:	https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via- ipv6/

Evidence

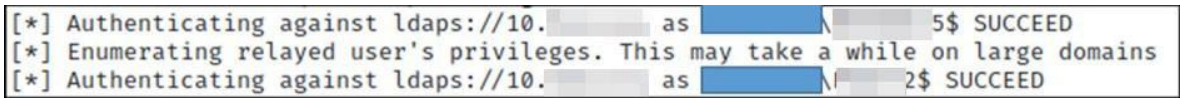


Figure 8: Successfully relayed LDAP credentials via mitm6

Remediation

1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you do not use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
    a. (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
    b. (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    c. (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6- Out)
2. If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
3. Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.

Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

Finding IPT-010: Insufficient Patch Management – Software (Critical)

Description:	Demo Corp permitted various deprecated software in their network. This includes: • Apache version < 2.4.46 • Apache Tomcat version < 7.0.100, 8.5.51, 9.0.31 • Cisoco AireOS version 8.5.151.10 • CodeMeter version 3.05 (5.21.1478.500) • Dropbear SSH Server version 2015.68 • Dell iDRAC7 version 2.63.60.62.01 • Dell iDRAC8 version 2.63.60.61.06 • Dell iDRAC9 version 3.36.36.36.21 • ESXi version 5.5 • ESXi version 6.5 build 15256549 • Flexera FlexNet Publisher version 11.16.0 • IIS version 7.5 • ISC BIND version 9.6.2-P2 • Microsoft DNS Server version 6.1.7601.24261 • Microsoft SQL Server version 11.0.6594.0 • Netatalk OpenSession version < 3.1.12 • PHP version < 7.3.11 • Rockwell Automation RSLinx Classic Above lists all critical and high-rated deprecated software, the majority of which permit serious vulnerabilities, such as remote code execution. For a full patching list, please review the provided Nessus scan documentation.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: Very High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Remediation

Update to the latest software version. For a full list of vulnerable systems, versions, and patching requirements, please see the below document. (Appendix-A)

Finding IPT-019: Unauthenticated SMB Share Access (Medium)

Description:	GORA Corp exposed multiple servers with unauthenticated file server access.
Risk:	Likelihood: Moderate – Adversaries will discover these shares with low-noise, basic reconnaissance techniques. Impact: Moderate – Attackers learn about the environment through information leaks.
System:	10.x.x.x
Tools Used:	Nessus, smbclient
References:	NIST SP800-53r4 AC-6(3) - Least Privilege NIST SP800-53 r4 SC-4 - Information in Shared Resources

Evidence

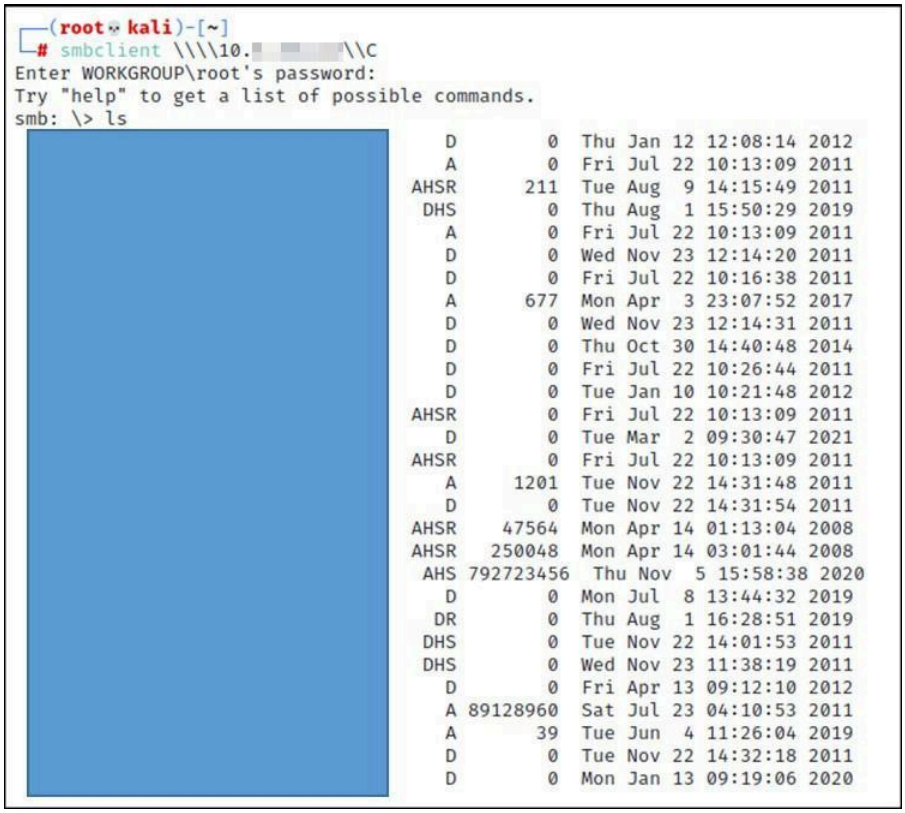


Figure 19: Unauthenticated Share access

Remediation

Disable SMB share or require authentication. Enabling authentication on the share will protect the confidentiality of the stored information. Exporting authentication logs to a SIEM solution will give incident response teams insights to brute force login attempts.

Tukkan
Consultancy & Analytics

Last Page