India Nippon Electricals Limited

Active Directory Security Review

January 2023

Draft Report

Building a better working world

Table of Content

1. Introduction

1.1 Background

EY was engaged by India Nippon Electricals Limited (henceforth referred to as "INEL") to perform a security review of its Information Technology (IT) infrastructure. The findings in this report result from EY's attempts to discover and validate vulnerabilities that were considered within the project's scope and duration. The recommendations provided in this report are structured to facilitate remediation of the identified security risks. The security review involved activities related to active directory security review targeting the in-scope components. The active directory security review was conducted between 12th December 2022 and 23rd December 2022.

1.2 Engagement Scope

Active Directory Security Review

Review the security posture of active directory and analyse the configuration of security sensitive parameters against industry security best practices.

The list of assets identified for the active directory security review has been provided in table 1 below.

Table 1: In-Scope assets for Active Directory Security Review

#	Domain
1.	inelhosur.com
2.	inelpondy.com
3.	inelrewari.com
4.	ineltech.com

1.3 Limitations

The reviews were performed:

- As zero knowledge exercise without detailed information about the target IT infrastructure.
- Without any access to the design or source code of the websites or other hosted applications.

The observations of the exercise reflect the security posture of the targeted assets as ascertained by our assessment carried out between 12th December 2022 and 23rd December 2022.

1.4 Disclaimer

This report is solely for the information of INEL management and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

The gaps identified in this report are based on the technical assessment conducted by us. We made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

We have reported all significant vulnerabilities and risks identified during the period of our review. However, due to the point-in-time nature of security assessments, there is no assurance that additional vulnerabilities, issues or risks will arise after the period of the review given the volatility of changes in information technology and emerging threats and vulnerabilities.

In carrying out our work and preparing the report, we have worked for INEL's purposes only. Consequently, we make no representation regarding the sufficiency of the procedures performed either for the purpose for which the report has been requested or for any other purpose.

Further our report may not have considered issues relevant to any third parties, any use such third parties may choose to make of our report is entirely at their own risk and we shall have no responsibility whatsoever in relation to any such use.

The recommendations provided in this report should be tested in a test environment prior to implementing in the production environment.

2. Approach & Methodology

2.1 Active Directory Security Review

The Active Directory Security Review consisted of the activities listed in the table below.

Table 2: Activities constituting the active directory security review

Description	Objective	Procedure
Group Policy Walkthrough	▪ Identify weaknesses in the Group Policy Preferences (GPP). ▪ Review the Group Policy Object (GPO) defined to the Group of Users. ▪ Kerberos Ticket – Key Distribution Centre (KDC) Review	▪ Analyse Domain & Domain Controller Policy including review of account lockout, Kerberos, user assignment policies ▪ Inspect Password and Audit Log Policy. ▪ Inspect Weak Encryption and Hashing Mechanisms for NetBIOS and SMB services. ▪ Review Folder/File permissions based on Read/Write/Execute access. ▪ Review Firewall/Internet Connection Sharing (ICS) and Integrity Check Policies. ▪ Review Kerberos Policy for Service and User Ticket Lifetime. ▪ Inspect Kerberos user Ticket Renewal from Ticket Granting Server (TGS). ▪ Review Logon Restriction of Kerberos Tickets.
Forest Security	▪ Creation & Maintenance of secure pristine AD DS forest.	▪ Review of forests/domains/zones for segregation and securing critical assets ▪ Review of trust relationships.
Authentication & Password Management	▪ Enforce strong password management policies and practices on Domain Controllers.	▪ Use Digital signing to prevent spoofing/impersonation attacks ▪ Protect service passwords and other key AD passwords including DSRM (Directory Service Restore Mode (DSRM) ▪ Use strong authentication algorithms and avoid use of LM & NTLM algorithms ▪ Use strong password policies including complex passwords and password expiry/updates for all administrator and user passwords

Description	Objective	Procedure
Privileged Account Management	▪ Review privileged accounts/groups to minimize abuse of excessive access ▪ Review principle of Least Privilege to avoid abuse of privileged accounts	▪ Review the permissions surrounding the default built-in privilege accounts and Groups. ▪ Review protected accounts, service accounts and groups. ▪ Review accounts that have direct or transitive membership. ▪ Review Administrator Accounts on Domain-Joined Systems. ▪ Review use of secure network & systems used for AD administration e.g. use of JUMP servers, administrative VLAN. ▪ Use of controls for disparate local administrator passwords.
Domain Controller Security	▪ Secure base OS against data theft and various forms of cyberattacks.	▪ Use of secure components such as Trusted Platform Module (TPM) and encryption to protect data at rest ▪ Use of updated OS and Patches. Prevent use of Domain Controllers for Internet access. ▪ Review Windows Registries for Weak Registry entries which includes Encryption Policy, Default Logon, and Memory Management such as ASLR & DEP entries etc. ▪ Minimize Unnecessary Services and Open Ports
Auditing & Logging	▪ Detection of abnormal changes in AD configuration	▪ Configure logging to track important changes to the administrator account ▪ Use of centralized time source to sync time between all DC components ▪ Analyze Event Log to identify Kerberos Ticket issue and access to users, Pull and Push of Group Policies between Server and Client. ▪ Use of Advanced Audit policies and granular auditing.

3. Detailed Report

3.1 Active Directory Security Review

Table 3: Table of Observations (INEL Hosur)

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
1.	High CVSS Score:7.1	Password expire feature has been disabled for around 12 users. Control observed: DONT_EXPIRE_PASSWD set as 'TRUE' It was observed that password had not been changed for more than a year for several accounts. For instance, Password age for Ravinder Sharma - 2217 days Sakthivel.G - 543 days Mariappan.L- 303 days	inelhosur.com	If the password expire feature has not been enabled, same password can be used throughout the lifetime of the account which when exposed leads to domain compromise if it's an admin account.	Password expiration period must be set as per the organization policy.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
2.	Medium CVSS Score:5.7	The 'Impersonate a client after authentication' setting is not configured.	Default Domain Policy	An attacker with the impersonate a client after authentication user right may create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.	Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through: [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment]. STEP 2: <Double-click> on the User Right [Impersonate a client after authentication]. STEP 3: Verify that this user right is limited to appropriate groups only. Recommended guidelines state: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
3.	Medium CVSS Score:5.7	Anonymous access to shares were not restricted in the group policy.	Default Domain Policy	Enabling anonymous access to shares weakens the security posture as any shares listed can be accessed by any network user. This could potentially lead to the compromise of the system and exposure or corruption of sensitive information assets.	Ensure that anonymous access to shares are restricted. Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through the Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/Security options STEP 2: <Double-click> on the security option labelled [Network access: Shares that can be accessed anonymously]. STEP 3: Ensure that a null value is set.
4.	Low CVSS Score:3.3	The administrator account is not renamed with non-guessable usernames. Control observed: Account Name: Administrator Member of groups: Enterprise administrators, Domain Administrators, Administrators	inelhosur.com	If the administrator/guest account is not renamed, an attacker can perform brute force/password guessing attacks to gain access to system Renaming the account makes it more difficult for attackers to guess this username and password combination.	Rename the administrator account by specifying a complex (non-guessable) value.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
5.	Low CVSS Score:3.3	The server has not enabled LDAP server signing requirements settings. Control observed: Domain controller: LDAP server signing requirements - None	Default Domain Controllers Policy	Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures packets between the client and the server, changes the packets, and then forwards them to the server. If this occurs on an LDAP server, an attacker can cause a server to make decisions that are based on forged requests from the LDAP client.	To protect the directory server from replay and forged attacks configure LDAP server signing. For more information, refer: https://support.microsoft.com/en-in/help/935834/how-to-enable-ldap-signing-in-windows-server

Table 4: Table of Observations (INEL Pondy)

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
1.	Medium CVSS Score:5.7	Anonymous access to shares were not restricted in the group policy.	Default Domain Policy	Enabling anonymous access to shares weakens the security posture as any shares listed can be accessed by any network user. This could potentially lead to the compromise of the system and exposure or corruption of sensitive information assets.	Ensure that anonymous access to shares are restricted. Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through the Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/Security options STEP 2: <Double-click> on the security option labelled [Network access: Shares that can be accessed anonymously]. STEP 3: Ensure that a null value is set.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
2.	Medium CVSS Score:5.7	The 'Impersonate a client after authentication' setting is not configured.	Default Domain Policy	An attacker with the impersonate a client after authentication user right may create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.	Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through: [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment]. STEP 2: <Double-click> on the User Right [Impersonate a client after authentication]. STEP 3: Verify that this user right is limited to appropriate groups only. Recommended guidelines state: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
3.	Low CVSS Score:3.3	The administrator account is not renamed with non-guessable usernames. Control observed: Account Name: Administrator Member of groups: Enterprise administrators, Domain Administrators, Administrators	inelpondy.com	If the administrator/guest account is not renamed, an attacker can perform brute force/password guessing attacks to gain access to system Renaming the account makes it more difficult for attackers to guess this username and password combination.	Rename the administrator account by specifying a complex (non-guessable) value.
4.	Low CVSS Score:3.3	The server has not enabled LDAP server signing requirements settings. Control observed: Domain controller: LDAP server signing requirements - None	Default Domain Controllers Policy	Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures packets between the client and the server, changes the packets, and then forwards them to the server. If this occurs on an LDAP server, an attacker can cause a server to make decisions that are based on forged requests from the LDAP client.	To protect the directory server from replay and forged attacks configure LDAP server signing. For more information, refer: https://support.microsoft.com/en-in/help/935834/how-to-enable-ldap-signing-in-windows-server

Table 5: Table of Observations (INEL Rewari)

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
1.	High CVSS Score:7.1	Password expire feature has been disabled for around 9 users. Control observed: DONT_EXPIRE_PASSWD set as 'TRUE' It was observed that password had not been changed for more than a year for several accounts. For instance, Password age for Rahul Kumar - 556 days Balkishan Yadav - 455 days	inelrewari.com	If the password expire feature has not been enabled, same password can be used throughout the lifetime of the account which when exposed leads to domain compromise if it's an admin account.	Password expiration period must be set as per the organization policy.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
2.	Medium CVSS Score:5.7	The 'Impersonate a client after authentication' setting is not configured.	Default Domain Policy	An attacker with the impersonate a client after authentication user right may create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.	Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through: [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment]. STEP 2: <Double-click> on the User Right [Impersonate a client after authentication]. STEP 3: Verify that this user right is limited to appropriate groups only. Recommended guidelines state: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
3.	Medium CVSS Score:5.7	Anonymous access to shares were not restricted in the group policy.	Default Domain Policy	Enabling anonymous access to shares weakens the security posture as any shares listed can be accessed by any network user. This could potentially lead to the compromise of the system and exposure or corruption of sensitive information assets.	Ensure that anonymous access to shares are restricted. Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through the Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/Security options STEP 2: <Double-click> on the security option labelled [Network access: Shares that can be accessed anonymously]. STEP 3: Ensure that a null value is set.
4.	Low CVSS Score:3.3	The administrator account is not renamed with non-guessable usernames. Control observed: Account Name: Administrator Member of groups: Enterprise administrators, Domain Administrators, Administrators	inelrewari.com	If the administrator/guest account is not renamed, an attacker can perform brute force/password guessing attacks to gain access to system Renaming the account makes it more difficult for attackers to guess this username and password combination.	Rename the administrator account by specifying a complex (non-guessable) value.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
5.	Low CVSS Score:3.3	The server has not enabled LDAP server signing requirements settings. Control observed: Domain controller: LDAP server signing requirements - None	Default Domain Controllers Policy	Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures packets between the client and the server, changes the packets, and then forwards them to the server. If this occurs on an LDAP server, an attacker can cause a server to make decisions that are based on forged requests from the LDAP client.	To protect the directory server from replay and forged attacks configure LDAP server signing. For more information, refer: https://support.microsoft.com/en-in/help/935834/how-to-enable-ldap-signing-in-windows-server

Table 6: Table of Observations (INEL Tech Center)

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
1.	High CVSS Score:7.1	The password policies set for the user accounts deviates from leading security practices. Controls observed: Minimum password length - 7 Account lockout threshold - 0 invalid logon attempts	Default Domain Policy	Weak passwords can be compromised by password attacks such as password guessing, password brute force and dictionary attacks. Failure to implement adequately stringent account lockout policies increases the risk of an unauthorized individual being able to compromise the system by executing a brute force dictionary attack against user accounts	Consider modifying the domain group policies to reflect the settings as per organization policies/leading practices. Recommendation as per leading security practices: Minimum password length - 8 Account lockout threshold - 5 invalid logon attempts For more information please refer: https://technet.microsoft.com/en-us/library/hh994572(v=ws.11).aspx

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
2.	Medium CVSS Score:5.7	The 'Impersonate a client after authentication' setting is not configured.	Default Domain Policy	An attacker with the impersonate a client after authentication user right may create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.	Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through: [Windows Settings] > [Security Settings] > [Local Policies] > [User Rights Assignment]. STEP 2: <Double-click> on the User Right [Impersonate a client after authentication]. STEP 3: Verify that this user right is limited to appropriate groups only. Recommended guidelines state: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
3.	Medium CVSS Score:5.7	Anonymous access to shares were not restricted in the group policy.	Default Domain Policy	Enabling anonymous access to shares weakens the security posture as any shares listed can be accessed by any network user. This could potentially lead to the compromise of the system and exposure or corruption of sensitive information assets.	Ensure that anonymous access to shares are restricted. Launch the GPMC (Group Policy Management Console), and then right-click on Default Domain Policy in the left pane and select Edit. Inside the Group Policy Object Editor and follow the below steps to apply the setting. STEP 1: Navigate through the Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/Security options STEP 2: <Double-click> on the security option labelled [Network access: Shares that can be accessed anonymously]. STEP 3: Ensure that a null value is set.
4.	Low CVSS Score:3.3	The administrator account is not renamed with non-guessable usernames. Control observed: Account Name: Administrator Member of groups: Enterprise administrators, Domain Administrators, Administrators	ineltech.com	If the administrator/guest account is not renamed, an attacker can perform brute force/password guessing attacks to gain access to system Renaming the account makes it more difficult for attackers to guess this username and password combination.	Rename the administrator account by specifying a complex (non-guessable) value.

#	Risk Rating	Vulnerability Identified	Policies/Host(s) Affected	Risk/Implication	Recommendation
5.	Low CVSS Score:3.3	The server has not enabled LDAP server signing requirements settings. Control observed: Domain controller: LDAP server signing requirements - None	Default Domain Controllers Policy	Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures packets between the client and the server, changes the packets, and then forwards them to the server. If this occurs on an LDAP server, an attacker can cause a server to make decisions that are based on forged requests from the LDAP client.	To protect the directory server from replay and forged attacks configure LDAP server signing. For more information, refer: https://support.microsoft.com/en-in/help/935834/how-to-enable-ldap-signing-in-windows-server

Appendix – A: Basis of Risk Ratings

The risk grading of the application was based on the CVSS v3 (Common Vulnerability Scoring System) base score. The various metrics used in the scoring system is defined below.

Table 7: Basis for Risks Ratings – CVSS v3 (Common Vulnerability Scoring System)

Metrics	Metrics definition
Attack Vector (AV)	This metric reflects the context (Network, Adjacent, Local, Physical) by which vulnerability exploitation is possible.
Attack Complexity (AC)	This metric describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability.
Privileges Required (PR)	This metric describes the level of privileges an attacker must possess *before* successfully exploiting the vulnerability.
User Interaction (UI)	This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component.
Scope	The Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope.
Confidentiality (C)	This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability.
Integrity (I)	This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information.
Availability (A)	This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.

Table 8: Risks Ratings – CVSS v3 (Common Vulnerability Scoring System)

Risk Rating	Range
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0