Microsoft Active Directory Assessment

By SmartProfiler Assessment

Version 5.4.1.1

{consulting firm name here}

Assessment date: {date of assessment}

Phone: {consulting firm Telephone}

Direct: {Direct phone}

Email: {Email Address}

Project: {enter project name here}
Customer: {enter customer name here}
Effective Date: {enter project effective date here}

1. Introduction

This Introduction contains a global summary of the health and security scans performed on the company infrastructure with SmartProfiler for Active Directory Assessment. Detailed information about the scans can be found in the Health & Security Maturity Framework and Technical Findings sections of this report. The assessment was performed according to ANSSI and MITRE ATT&CK definition. ANSSI is French National Agency for the Security of Information Systems. For more information, please check out here: https://www.cert.ssi.gouv.fr/uploads/guide-ad.html. There are tests that also recommended by Microsoft have been performed too.

The scans reflect a quick analysis of customer's overall health & risk assessment program. The findings expressed through a Maturity Model construction provide a highlevel rating. This report is not meant to be a detailed control review. However, it is intended to provide an overall review of the programmatic aspects of the organization's health & risk assessment program in an all-up approach to determine whether it is aware of the risks revealed by SmartProfiler AD Assessment Tool.

SmartProfiler Assessment has been done in below categories:

- **Active Directory Reporting**: Tests in this category are executed to get data for reporting purposes.
- **Account Policies:** Tests in this category are executed to get data for Account and Lockout Policies.
- **AD DNS:** Tests in this category are executed to get DNS Configuration and issues identified on the AD DNS Servers.
- **AD Forest:** Tests executed in this category are executed to find issues in AD Forest.
- **Configuration-Domain:** Tests in this category are executed to check if configuration for overall domain is as per Microsoft best practices.
- **Configuration-Domain Controller:** Tests in this category are executed to check configuration on domain controllers such as DNS Loopback, Multihomed Tests, NIC Dynamic Updates tests, Domain Controllers OU tests and so on.
- **Configuration-Forest:** Tests in this category are executed to check if AD Sites and Site Links are configured as per Microsoft best practices. There are 12 tests executed in the Configuration-Forest category.
- **Domain Controller:** Tests such as Undefined Subnets, local disks, DNS configuration, Event Log settings, DCDiag, Roles and features, and other tests are executed. There are more than 22 tests executed for each domain controller.
- **Group Policy:** Group Policy Category tests include checking Disabled GPO, GPO Application, Block Inheritance, and permissions assigned to GPO.
- **Security and Risk:** Security and Risk category contains more than 50 tests and most of the tests are compliant with ANSSI and MITRE.
- **Time Sync:** Time Sync test is executed to check time sync configuration on all domain controllers.
- **NIST-CIS Domain Controllers Settings:** CIS and NIST Security Controls defined for Domain Controllers.

2. Organization Overview

During the creation of this report, the following summary information was gathered.

ORGANIZATION	
CUSTOMER NAME	{enter customer name here}
CUSTOMER ADDRESS	{enter customer address here}

CUSTOMER OPERATION BRANCHES	{enter customer operation branches here}
NUMBER OF EMPLOYEES	{enter number of employees here}

3. Participants

During the creation of this report, the following summary information was gathered.

PARTICIPANT NAMES	COMPANY	PROJECT ROLE
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}
{ENTER PARTICIPANT NAME HERE}	{enter Participant Company here}	{enter Participant Project Role here}

4. Recommendations

Organizations should be proactive in avoiding the risks and health issues associated with ***Active Directory*** by establishing policies around securing and maintaining the IT environment. It is critical that an organization's plan include protocols governing cybersecurity and how it's managed relative to the amount of risk an organization is comfortable in assuming (since there is no such thing as zero risk).

Because the mitigation of cybersecurity risks and management of the threats is so challenging and can pose such a significant threat to an organization, IT security is a top-level strategic issue requiring executive leadership participation as stakeholders in the process.

- Senior Management must support and enforce establishment of Security Policies. Policies allow for standards to be mandated resulting in guidelines and procedures that will ultimately decrease risk to the organization.
- A Patch Management policy needs to be created and supported by upper level management to provide a more consistent monthly patching process for all customer's Internal Networks. This will decrease risk within the organization.
- The IT department's use of a firewall, email encryption, anti-malware application and a Mobile Device Management system demonstrate a desire to secure and control the environment. However, significantly more technical controls and security awareness training are needed to combat the high level of risk within the organization and to prevent future security incidents and breaches.
- All of the security compliance and risk items must be reviewed carefully in the ***Active Directory*** section and actions to be taken accordingly.

5. Active Directory Components Issues Summary

The SmartProfiler software product was used to perform a complete health & security assessment of ***Active Directory*** of customer. The finiding helps you know the current health status and critical, high and medium issues that have been uncovered. The finding also provides recommendations to fix the issues. Though the report does not contain affected objects, it helps you know the overall health & security status of ***Active Directory*** environment.

5.1 Active Directory Assessment Categories Status

AD CATEGORY	# of FINDINGS	PASSED
AD FEATURES	5	1
RISKY ITEMS	11	12
AD SECURITY RISKS-USERS	11	4
AD SECURITY RISKS-COMPUTERS	3	4
AD SECURITY RISKS-ADMINS	0	2
AD SECURITY RISKS-OBJECTS OWNERSHIP	3	0
SENSITIVE CHANGES	2	5
CRITICAL ACCOUNTS STATUS	5	4
PRIVILEGED ACCOUNTS	7	9
DOMAIN POLICIES	3	1
DC SECURITY	4	11
DC CONFIGURATION	7	15
DC ROLES/SERVICEs	3	11
AD SITES	5	9
TIME SYNC AND FSMO	2	2
AD OBJECTS	6	8
AD GPO	10	6
AD DNS	0	3

5.2 Microsoft Active Directory Components Summary

This section provides information about Microsoft Active Directory environment such as Active Directory Forest, Domains, FSMO, Active Directory Sites, Domain Account Policies and so on. The following information is provided in this section:

- AD Forest Forest Information
- Active Directory Forest Summary
- Active Directory Organizational Units Summary
- Active Directory Domains Information
- Active Directory NetBIOS Information
- Active Directory FSMO Information
- Active Directory Domain Controllers Information
- Active Directory Sites Information
- Active Directory Site and Subnet Information
- Active Directory Forest Site and Link Information
- Active Directory Domain Password Policies
- Active Directory Domain Lockout Policies
- Active Directory Features Status

5.2.1 Active Directory Forest Information

Item	Remark
Active Directory Forest	DynamicPacks.net
Forest Functional Level	Windows2016Forest
Domains	child.Dynamicpacks.net Dynamicpacks.net
Root Domain	Dynamicpacks.net
Domain Naming Master	DC1.Dynamicpacks.net
Schema Master	DC1.Dynamicpacks.net
Global Catalog	3
Application Partitions	3
Active Directory Sites	2

5.3 Active Directory Domain Controllers Information

Item	value
Total writable domain controllers	2
Total read only domain controllers	1
Total global catalog servers	3

5.3.1 Active Directory Domain Functional Level Information

Domain	NetBIOS Name	Functional Level
child.Dynamicpacks.net	CHILD	Windows2016Domain
Dynamicpacks.net	**DYNAMICPACKS**	**Windows2016Domain**

5.3.2 Active Directory FSMO Information

Domain	PDC Emulator	RID Master	Infrastructure Master
child.Dynamicpacks.net	DCChild.child.Dynamicpacks.net	DCChild.child.Dynamicpacks.net	DCChild.child.Dynamicpacks.net
Dynamicpacks.net	**DC1.Dynamicpacks.net**	**DC1.Dynamicpacks.net**	**DC1.Dynamicpacks.net**

5.4 Active Directory Site ISTG and Domain Controllers Information

Ad Site	Current ISTG Server	Total Servers	Total Bridgehead Servers
Default-First-Site-Name	DC1.Dynamicpacks.net	2	1
London	**DCChild.child.Dynamicpacks.net**	**1**	**1**

5.5 Active Directory Site and Subnet Information

Ad Site	Total Subnets	In Site Links
Default-First-Site-Name	1	1
London	**0**	**1**

5.6 Active Directory Forest Site and Link Information

AD Site Link	Total AD Sites
DEFAULTIPSITELINK	**2**

5.7 Active Directory Domain Password Policies

AD Domain	Password Complexity	Maximum Password Age	Minimum Password Age	Password History Count
child.Dynamicpacks.net	True	42.00:00:00	1.00:00:00	24
Dynamicpacks.net	**True**	**42.00:00:00**	**1.00:00:00**	**24**

5.8 Active Directory Domain Lockout Policies

AD Domain	Lockout Duration	Lockout Observation Window	Lockout Threshold Value
child.Dynamicpacks.net	00:10:00	00:10:00	0
Dynamicpacks.net	**00:10:00**	**00:10:00**	**0**

5.9 Active Directory Features Status

AD FEATURE	SEVERITY	STATUS
Protected Users Group Status	High	Total Domains Not Using Protected Users Group:2
AD Recycle Bin Status	Medium	AD Recycle Bin Status:Disabled

Privileged Management Status	Medium	Privileged Access Management Status:Disabled
Managed Service Accounts Status	Medium	Managed Service Accounts Status:Are not in use
gMSA Accounts Status	Low	Total Domains With gMSA Accounts:0
Missing Microsoft LAPS in AD Forest	Passed	Microsoft LAPS Status:Deployed

6 URGENT Action Needed

After carrying out a complete health assessment of the ***Active Directory Environment***, the following issues have been identified and require urgent attention. We recommend that these items especially CRITICAL and HIGH are acted on with the highest priority for each focus area. More details about each issue listed in table below can be found in their respective category section in **Section 8. Technical Findings By Category** in this document.

- **Test**: Shows Test name
- **Risk**: Shows Risk associated with the Test. Risk can be **Critical**, **High**, **Medium**, or **Low**.
- **Indicator**: Shows if belongs to IOC or IOE or both.
- **Practice:** Shows if item is Microsoft-Recommended (MS-RECOMMENDED) or ANSSI or MITRE item.
- **Finding:** Shows number of Objects affected. To get a list of objects refer test CSV file.

TEST	Risk	Practice	Finding
Dangerous Permissions on AdminSDHolder	Critical	vuln1_privileged_members_perm vuln2_privileged_members_perm	AD Domains Affected:1
AdminSDHolder was Modified in last 30 days	Critical	vuln1_permissions_adminsdholder	AdminSDHolder Object was modified in total domains:2
Anonymous or EVERYONE in Pre-Windows 2000 Group	Critical	vuln2_compatible_2000_anonymous	Number of Domains Affected:2
Misconfigured Administrative Accounts Found	Critical	MS-RECOMMENDED	Total Admins Misconfigured:7
Weak Password Policies Affected Admins	Critical	vuln2_privileged_members_password	Total Privileged Account using Weak Password Policy:3
TLS 1.1 Enabled DCs	Critical	MS-RECOMMENDED	Total Domain Controllers with TLS 1.1 Protocol Enabled:3
NTLM Authentication Enabled DCs	Critical	MS-RECOMMENDED	Total Domain Controllers with NTLM Enabled:3
Missing DNS Scavenging DCs	Critical	MS-RECOMMENDED	Total DNS Servers Not Enabled with Server Level Scavenging:3
Print Spooler Service Running DCs	Critical	MS-RECOMMENDED	Total Domain Controllers with Print Spooler Service running:3
No Group Policy Objects to Prevent Domain Admins from logging on to Workstations or Servers Found	Critical	MS-RECOMMENDED	Total AD Domains Affected:2

No Group Policy Objects to Block ISO Execution Found	Critical	MS-RECOMMENDED	Total AD Domains Affected:2
Accounts with Extended Rights to Read LAPS Passwords Found	Critical	MS-RECOMMENDED	Illegal Accounts Found to read LAPS in AD Domains:2
Group Policy Objects with Improper Permissions Found	Critical	MS-RECOMMENDED	Abusable GPO Permissions found in Total AD Domains:1
Group Policy Object Assignments with Improper Permissions Found	Critical	MS-RECOMMENDED	Total Abusable GPO Permissions in AD Domains:3
EVERYONE Full Control Permissions on OUs	Critical	MS-RECOMMENDED	Total Organizational Units with Everyone Full Control Access Rights:3
Protected Users Group Status	High	vuln3_protected_users	Total Domains Not Using Protected Users Group:2
Objects Modified in Last 10 Days	High	MS-RECOMMENDED	Total Objects Modified in AD Domains in last 10 days:2138
Objects Created in Last 10 Days	High	MS-RECOMMENDED	Total Objects Created in AD Domains in last 10 days:2105
Anyone can Join Computers to Domain	High	MS-RECOMMENDED	Total Domains Allowing Normal Users to Join Computers to domain:2
Denied RODC Password Replication Group missing Privileged Accounts	High	vuln3_rodc_denied_group	Total Missing Privileged Groups in Denied RODC Password Replication Group:15
msDS-NeverRevealGroupattribute RODC missing Privileged Accounts	High	vuln3_rodc_never_reveal	Total Privileged Groups Not in PRP Denied List:9
Schema Admin Group members	High	MS-RECOMMENDED	Schema Admins Group contains members:1
Missing Domain Zones Scavenging	High	MS-RECOMMENDED	Total Domain Zones Not Enabled with Scavenging:2
AD Partitions Backup Status	High	MS-RECOMMENDED	Total AD Partitions not backed up since last 7 days:5
Users with LastPasswordSet was never Set	High	vuln2_dont_expire	Total Users with LastPasswordSet was never set in all Domains:6

Users with PWDLastSet to ZERO	High	vuln1_user_accounts_dormant	Total Users with PWDLastSet to ZERO in all Domains:6
Stale User Accounts	High	vuln1_user_accounts_dormant	Total Stale User Accounts in all Domains:5
User Accounts Pass Never Expires	High	vuln2_dont_expire	Total Users with Password Never Expires in all Domains:8
User Accounts Pass Not Required	High	vuln2_dont_expire	Total Users with Password Not Required set in all Domains:2
Computers with SPNs Configured	High	vuln1_spn_priv	Total Computers using ServicePrincipalNames in all Domains:1
Stale Computer Accounts	High	vuln1_user_accounts_dormant	Total Stale Computer Accounts in all Domains:33485
Domain Controllers not owned by Admins	High	vuln1_permissions_dc	Total Domain Controllers owned by non-privileged accounts:2
Computer Objects not managed by Admins	High	vuln3_owner	Total Computers Not Managed By Admins in all Domains:2
Organizational Units not managed by Admins	High	vuln3_owner	Total Organizational Units Not Managed By Admins:2
Sensitive GPOs Modified	High	MS-RECOMMENDED	Sensitive GPOs Status in Last 10 Days:WARNING: Modified
Changes to Privileged Groups in Last 15 days	High	MS-RECOMMENDED	Total Privileged Groups Modified in Last 15 Days in All Domains:2
Built-In Admin Account Not protected	High	MS-RECOMMENDED	Default Administrator Account not protected in all domains:1
Built-In Admin Account Not Disabled	High	MS-RECOMMENDED	Default Admin Account not disabled in Total Domains:2
Built-In Admin Account was used in last 10 days	High	MS-RECOMMENDED	Total Domains in which Default Administrator account was used in last 10 days:1

Guest Account is enabled	High	MS-RECOMMENDED	Total Guest Accounts Enabled in All Domains:1
Guest Account is not renamed	High	MS-RECOMMENDED	Guest Account not renamed in Total Domains:2
Missing Privileged Groups in Protected Users Group	High	vuln3_protected_users	Total Missing Privileged Groups in Protected Users Group:Not In Use
Privileged Accounts Pass Never Expires	High	vuln2_dont_expire	Total Privileged Accounts set to Password Never Expire in all Domains:5
Disabled Admins part of Privileged Groups	High	MS-RECOMMENDED	Total Disabled Admins In Privileged Groups:1
Password Do Not Expire	High	vuln1_dont_expire_priv	Total Admin Accounts set to PasswordNeverExpires :4
Default Domain Policy-Minimum Password Length	High	vuln2_privileged_members_password	Account Policies Not Configured correctly in Total Domains:1
FGPP Policies-Minimum Password Length	High	vuln2_privileged_members_password	FGPP Not Configured Correctly In Domains:Not Created
FGPP Policies Not Applying	High	MS-RECOMMENDED	Total FGPP Not Applying in All Domains:Not Created
AllowNT4Crypto DCs	High	MS-RECOMMENDED	Total DCs with AllowNT4Crypto Enabled:3
RC4 Encryption Enabled DCs	High	MS-RECOMMENDED	Total Domain Controllers With RC4 Encryption Enabled:3
Errors and Warnings in Log DCs	High	MS-RECOMMENDED	Total DCs with Event Log Errors:3
DCDiag Failure DCs	High	MS-RECOMMENDED	Total DCs with DCDiag Failures:2
Out Of Default OUs DCs	High	MS-RECOMMENDED	Total DCs outside of it's Default OU:2
Scheduled Tasks found on Domain Controllers	High	MS-RECOMMENDED	Total Scheduled Tasks on DCs:8
Software Installed on Domain Controllers	High	MS-RECOMMENDED	Total Software Installed on DCs:21
Sites without Subnets Association	High	MS-RECOMMENDED	Total AD Sites Without Subnets:1
Missing Global Catalog Sites	High	MS-RECOMMENDED	Total AD Sites Without Global Catalog Servers

			or No Universal Group Caching Enabled:1
PDC Emulator Time Source	High	MS-RECOMMENDED	Root PDC Time Source:Internal Source
Found Unused Netlogon Scripts	High	MS-RECOMMENDED	Total Unused Scripts In All Domains:1
No Group Policy Objects Defining Log Size and Retention	High	MS-RECOMMENDED	Total AD Domains Affected:2
No Group Policy Objects to Mitigate SMBv1 Found	High	MS-RECOMMENDED	Total AD Domains Affected:2
No Group Policy Objects Enforcing UAC Prompt for Elevation Found	High	MS-RECOMMENDED	Total AD Domains Affected:2
No Group Policy Objects to Mitigate Accidental Script Execution	High	MS-RECOMMENDED	Total AD Domains Affected:2
No Group Policy Objects to Mitigate NTLMv1 Protocol	High	MS-RECOMMENDED	Total AD Domains Affected:2
High Value Targets Found	High	MS-RECOMMENDED	Total High Value Targets Found:10
Dangerous Permissions Found on Naming Contexts	High	vuln_permissions_naming_context	AD Domains Affected:1
Pre-Windows 2000 Compatible Access Group is not empty	High	vuln_compatible_2000_anonymous	Number of AD Domains Affected:2
Normal Users Full Control Permissions on OUs	High	MS-RECOMMENDED	Total Normal User Accounts with Full Control Rights to Organizational Units in all Domains:2
AD Recycle Bin Status	Medium	MS-RECOMMENDED	AD Recycle Bin Status:Disabled
Privileged Management Status	Medium	MS-RECOMMENDED	Privileged Access Management Status:Disabled
Managed Service Accounts Status	Medium	MS-RECOMMENDED	Managed Service Accounts Status:Are not in use
Users With DES encryption	Medium	vuln2_kerberos_properties_deskey	Total Users with DES Encryption in all Domains:4
Users With Reversible Encryption	Medium	vuln3_reversible_password	Total Users with Reversible Encryption set in all Domains:4
Users With Kerberos Pre-Authentication	Medium	vuln1_kerberos_properties_preauth_priv vuln2_kerberos_properties_preauth	Total Pre-Authentication Users in all domains:4
Users Disabled	Medium	vuln_user_accounts_dormant	Total Disabled Users in all Domains:2
Users Expired	Medium	MS-RECOMMENDED	Total Expired Users in all Domains:1

Computers Disabled	Medium	vuln_user_accounts_dormant	Total Disabled Computer Accounts in all Domains:5
Privileged Groups Contained Computer Accounts	Medium	MS-RECOMMENDED	Total computer accounts part of privileged groups:1
Not Enough Free Space DCs	Medium	MS-RECOMMENDED	Total DCs with Low Disk Space:5
Missing SSL Authentication DCs	Medium	MS-RECOMMENDED	Total DCs without SSL:3
Manual Replication Connection Objects	Medium	MS-RECOMMENDED	Total Manual Replication Connection Objects:1
AD Sites Redundancy	Medium	MS-RECOMMENDED	Total AD Sites with Only One Domain Controller:1
Domain FSMO Placement	Medium	MS-RECOMMENDED	[ItemCAllSN83]
Unprotected OUs	Medium	MS-RECOMMENDED	Total Ous not protected:4
Disabled GPOs	Medium	MS-RECOMMENDED	Total Disabled GPOs:3
GPOs not Linked to OUs	Medium	MS-RECOMMENDED	Total OUs without GPO Linked:10000
Access Control Lists on Security Groups Found	Medium	MS-RECOMMENDED	Found Dangerous Group Permissions in AD Domains:2
Access Control Lists on Users Found	Medium	MS-RECOMMENDED	Found Dangerous User Permissions:0
gMSA Accounts Status	Low	MS-RECOMMENDED	Total Domains With gMSA Accounts:0
Password Expiration is missing for smart card users	Low	vuln_smartcard_expire_passwords	AD Domains Affected:1
Additional Roles and Features DCs	Low	MS-RECOMMENDED	Total Domain Controllers with Additional Roles and Features:3
Replication Interval Not Optimized Sites	Low	MS-RECOMMENDED	Replication Interval is not optimized for Site Links:1
Ogranizational Units without Objects	Low	MS-RECOMMENDED	Total Empty Organizational Units In All Domains:10004
Security Groups without Objects	Low	MS-RECOMMENDED	Total Empty Security Groups In All Domains:50061
Users without UPN specified	Low	MS-RECOMMENDED	Total Users with UPN Blank in all Domains:10

Missing Location Text in AD Sites	Low	MS-RECOMMENDED	Total AD Sites Not Defined With Location:2
GPO Description	Low	**MS-RECOMMENDED**	**Number of GPOs not set with Description:4**

7 NIST/CIS Security Benchmark

The Windows CIS Benchmarks are written for Active Directory domain-joined systems using Group Policy, not standalone/workgroup systems. Adjustments/tailoring to some recommendations will be needed to maintain functionality if attempting to implement CIS hardening on standalone systems or a system running in the cloud. Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark.

SmartProfiler for Active Directory offers more than 50 tests to check if domain controllers are configured with necessary security options, policy settings and audit settings. The below table lists the security status for domain controllers in Active Directory forest environment. The settings mentioned in this document are approved by organiations such as NIST and CIS. These settings must be implemented in the Default Domain Controllers Policy or the Group Policy Object which is linked to the “Domain Controllers” Organizational Unit where all domain controllers reside.

Note: Please note that any domain controller outside its default Organizational Unit (“Domain Controllers”) must be moved to its default Organizational Unit.

7.1 NIST/CIS Security Settings Status for Domain Controllers

GPO Setting	Risk	REMARK
Lock screen camera status	High	Setting Status:Missing
Lock screen slide show status	High	Setting Status:Missing
Passwords to be saved status	High	Setting Status:Missing
Always prompt for password upon connection status	High	Setting Status:Missing
Require secure RPC communication status	High	Setting Status:Missing
Set client connection encryption level status	High	Setting Status:Missing
Windows Defender SmartScreen status	High	Setting Status:Missing
AutoPlay status	High	Setting Status:Missing
Default behavior for AutoRun status	High	Setting Status:Missing
UNC Paths Hardened status	High	Setting Status:Missing
Insecure guest logons status	High	Setting Status:Missing
Audit- Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings status	High	Setting Status:Missing
Domain controller- LDAP server signing requirements status	High	Setting Status:Missing

Domain controller- Refuse machine account password changes status	**High**	Setting Status:Missing
Domain member- Digitally encrypt or sign secure channel data (always) status	**Passed**	Setting Status:Found
Domain member- Digitally encrypt secure channel data (when possible) status	**High**	Setting Status:Missing
Domain member- Digitally sign secure channel data (when possible) status	**High**	Setting Status:Missing
Domain member- Disable machine account password changes status	**High**	Setting Status:Missing
Domain member- Maximum machine account password age status	**High**	Setting Status:Missing
Domain member- Require strong (Windows 2000 or later) session key status	**High**	Setting Status:Missing
Interactive logon- Machine inactivity limit status	**High**	Setting Status:Missing
Microsoft network client- Digitally sign communications (always) status	**High**	Setting Status:Missing
Microsoft network client- Send unencrypted password to third-party SMB servers status	**High**	Setting Status:Missing
Microsoft network server- Digitally sign communications (always) status	**Passed**	Setting Status:Found
Network access- Do not allow anonymous enumeration of SAM accounts status	**High**	Setting Status:Missing
Network access- Do not allow anonymous enumeration of SAM accounts and shares status	**High**	Setting Status:Missing
Network security- Allow LocalSystem NULL session fallback status	**High**	Setting Status:Missing
Network security- Allow LocalSystem NULL session fallback status	**High**	Setting Status:Missing
Network security- Do not store LAN Manager hash value on next password change status	**Passed**	Setting Status:Found
Network security- LAN Manager authentication level status	**High**	Setting Status:Missing
Network security- LDAP client signing requirements	**High**	Setting Status:Missing
Network security- Minimum session security for NTLM SSP based (including secure RPC) clients status	**High**	Setting Status:Missing
Network security- Minimum session security for NTLM SSP based (including secure RPC) servers status	**High**	Setting Status:Missing
System objects- Strengthen default permissions of internal system objects status	**High**	Setting Status:Missing
User Account Control- Admin Approval Mode for the Built-in Administrator account status	**High**	Setting Status:Missing
User Account Control- Behavior of the elevation prompt for administrators in Admin Approval Mode status	**High**	Setting Status:Missing
User Account Control- Behavior of the elevation prompt for standard users status	**High**	Setting Status:Missing
User Account Control- Detect application installations and prompt for elevation status	**High**	Setting Status:Missing
User Account Control- Only elevate UIAccess applications that are installed in secure locations status	**High**	Setting Status:Missing

User Account Control- Run all administrators in Admin Approval Mode status	**High**	Setting Status:Missing
User Account Control- Virtualize file and registry write failures to per-user locations status	**High**	Setting Status:Missing
Audit Credential Validation status	**High**	Setting Status:Missing
Audit Computer Account Management status	**High**	Setting Status:Missing
Audit Other Account Management Events status	**High**	Setting Status:Missing
Audit Security Group Management status	**High**	Setting Status:Missing
Audit User Account Management status	**High**	Setting Status:Missing
Audit PNP Activity status	**High**	Setting Status:Missing
Audit Process Creation status	**High**	Setting Status:Missing
Audit Directory Service Access status	**High**	Setting Status:Missing
Audit Directory Service Changes status	**High**	Setting Status:Missing
Audit Account Lockout status	**High**	Setting Status:Missing
Audit Group Membership status	**High**	Setting Status:Missing
Audit Logon status	**High**	Setting Status:Missing
Audit Other Logon/Logoff Events status	**High**	Setting Status:Missing
Audit Special Logon status	**High**	Setting Status:Missing
Audit Detailed File Share status	**High**	Setting Status:Missing
Audit File Share status	**High**	Setting Status:Missing
Audit Other Object Access Events status	**High**	Setting Status:Missing
Audit Removable Storage status	**High**	Setting Status:Missing
Audit Audit Policy Change status	**High**	Setting Status:Missing
Audit Authentication Policy Change status	**High**	Setting Status:Missing
Audit MPSSVC Rule-Level Policy Change status	**High**	Setting Status:Missing
Audit Other Policy Change Events status	**High**	Setting Status:Missing
Audit Sensitive Privilege Use status	**High**	Setting Status:Missing
Audit Other System Events status	**High**	Setting Status:Missing
Audit Security State Change status	**High**	Setting Status:Missing
Audit Security System Extension status	**High**	Setting Status:Missing
Audit System Integrity status	**High**	**Setting Status:Missing**

8 Technical Findings by Category

After carrying out a complete health assessment of the ***Active Directory***, the following issues have been identified in each Test Category. The table also lists the impact and recommendation to fix the issues for each test identified. However, table doesn't show the passed items. For passed items in each category please refer Passed Items section in this document.

8.1 AD RISKY ITEMS

Test	Severity	Finding	Remark
Dangerous Permissions on AdminSDHolder	**Critical**	AD Domains Affected: 1	**IMPACT:** Found Full Control Permissions on AdminSDHolder Object. Dangerous permissions are set on the adminSDHolder object. Permissions set on this object may grant trusted objects full control over the Active Directory. In a tiered administrative model, these permissions allow compromise of Tier 0 objects from lower trust tiers. **RECOMMENDATION:** Permissions set on the adminSDHolder object are periodically copied to all protected AD objects (privileged built-in group members). By default, only privileged objects are granted access rights on the adminSDHolder object. This mechanism protects the most privileged Active directory users and groups from accidental misconfigurations. Modifying default permissions set on this object is strongly discouraged. Removing dangerous permissions is strongly advised to return the object to its default state. Fixing usually requires using adsiedit.msc or the LDP utility. Please check if a NORMAL USER account has GenericAll Permission on AdminSDHolder Object and remove if not required.
AdminSDHolder was Modified in last 30 days	**Critical**	AdminSDHolder Object was modified in total domains: 2	**IMPACT:** AdminSDHolder was modified in the last 30 days. Active Directory Domain Services uses AdminSDHolder, protected groups and Security Descriptor propagator (SD propagator or SDPROP for short) to secure privileged users and groups from unintentional modification. Unlike most objects in the Active Directory domain, which are owned by the Administrators group, AdminSDHolder is owned by the Domain Admins group. The AdminSDHolder object has a unique Access Control List (ACL), which is used to control the permissions of security principals that are members of built-in privileged Active Directory groups. Every hour, a background process runs on the domain controller to compare manual modifications to an ACL and overwrites them so that the ACL matches the ACL on the AdminSDHolder object. Any changes to AdminSDHolder object is a security risk. **RECOMMENDATION:** Please review why AdminSDHolder was modified and if any user or computer accounts that were added to the security tab of the AdminSDHolder object.
Anonymous or EVERYONE in Pre-Windows 2000 Group	**Critical**	Number of Domains Affected: 2	**IMPACT:** Everyone or Anonymous groups were found in Pre-Windows 2000 compatibility group. The pre-Windows 2000 compatibility mechanism ensures Windows NT domains are still supported. It is enabled by adding the Anonymous SID (S-1-5-7) to the Pre-Windows 2000 Compatible Access group, which allows anonymous access to some of Active Directory contents on domain controllers. **RECOMMENDATION:** It is highly recommended to remove Everyone and anonymous groups from Pre-Windows security group from all affected domains.

Denied RODC Password Replication Group missing Privileged Accounts	**High**	Total Missing Privileged Groups in Denied RODC Password Replication Group: 15	**IMPACT:** Denied RODC Password Replication Group does not contain privileged groups. Some default groups are missing from the Denied RODC Password Replication Group. It is a security risk to expose passwords of privileged groups. **RECOMMENDATION:** The Denied RODC Password Replication Group must include the following members: Domain Controllers, Read-only Domain Controllers, Group Policy Creator Owners, Domain Admins, Cert Publishers, Enterprise Admins, Schema Admins, and KRBTGT groups.
msDS-NeverRevealGroupattribute RODC missing Privileged Accounts	**High**	Total Privileged Groups Not in PRP Denied List: 9	**IMPACT:** Some or all privileged Groups are missing in msDS-NeverRevealGroupattribute Attribute of RODC. Read-only domain controllers (RODCs) are used in the forest with dangerous secret revelation settings. Some default groups are missing from the msDS NeverRevealGroup attribute of some RODCs. **RECOMMENDATION:** The msDS-NeverRevealGroup attribute can be used to list objects whose secrets are prevented from being revealed on a RODC. Read-only domain controllers must have their msDS-NeverRevealGroupattribute set to include, at least: Administrators, Server Operators, Account Operators, Backup Operators, and Denied RODC Password Replication Group.
Schema Admin Group members	**High**	Schema Admins Group contains members: 1	**IMPACT:** Found members in Schema Admins Group. Only members of the Schema Admins group can modify the schema, so accounts should only be added to this group when a change to the Schema is required and removed afterwards. This approach helps prevent an attacker from compromising a Schema Admin account, which could have serious consequences. **RECOMMENDATION:** It is recommended to remove all members from the Schema Admins Group.
Missing Domain Zones Scavenging	**High**	Total Domain Zones Not Enabled with Scavenging: 2	**IMPACT:** Domain Zones do not have DNS Aging enabled. It is important to note that if you do not enable Aging for a Domain Zone DNS Server may result in a huge number of stale DNS records. **RECOMMENDATION:** It is recommended to enable DNS Aging for each Domain Zone.
AD Partitions Backup Status	**High**	**Total AD Partitions not backed up since last 7 days: 5**	**IMPACT: Some AD Partitions have not been backed up for the last 7 days. If AD partitions are not backed up, then restores will be impacted. Each partition must be backed up.** **RECOMMENDATION: Recommended action is to take backups of AD partitions using the standard backup tools. Microsoft ships Windows Server backup tool to process backups of AD Forests.**

8.2 AD SECURITY RISKS-USERS

Test	Severity	Finding	Remark
Users with LastPasswordSet was never Set	High	Total Users with LastPasswordSet was never set in all Domains: 6	**IMPACT:** Found Users accounts with PasswordLastSet not set. These users are either have been set their passwords do not expire or they can accept the blank passwords. **RECOMMENDATION:** Please review the list of users and disable them or force them to change their passwords.
Users with PWDLastSet to ZERO	High	Total Users with PWDLastSet to ZERO in all Domains: 6	**IMPACT:** PWDLastSet is set to ZERO for some users. This flag on an account may be an indication of a stale account or an account created without a password. **RECOMMENDATION:** User accounts can be flagged with pwdlastset=0 under three conditions: Where an account has been created but a password has not been assigned, where an account has been created and the administrator has assigned a password but selected the option to change password at next logon, where the administrator has selected the option to require a user to change their password at the next logon as part of managing that users account, such as after a password reset. This condition is detected by querying the user accounts and finding instances where the value for passwordLastSet is zero.
Stale User Accounts	High	Total Stale User Accounts in all Domains: 5	**IMPACT:** Stale user accounts were found in AD Domains. Refer issue details. **RECOMMENDATION:** Please load and check why these user accounts are not being used. If these user accounts are not in use, then these MUST be disabled to avoid any security risks to AD environment.
User Accounts Pass Never Expires	High	Total Users with Password Never Expires in all Domains: 8	**IMPACT:** Password Never Expires user accounts were found in AD Domains. Every user must be set to renew their password except user accounts which are created for use with applications. Service Accounts can be set to not expire. **RECOMMENDATION:** Please check why passwords for these user accounts are set to not expire.
User Accounts Pass Not Required	High	**Total Users with Password Not Required set in all Domains: 2**	**IMPACT: Users found with Password Not Required. Accounts with weak access controls are often targeted by attackers seeking to move laterally or gain a persistent foothold within the environment.** **RECOMMENDATION: Recommended action is to ensure all users in Active Directory require a password and use the complex password.**

8.3 AD SECURITY RISKS-COMPUTERS

Test	Severity	Finding	Remark

Computers with SPNs Configured	**High**	Total Computers using ServicePrincipalNames in all Domains: 1	**IMPACT:** Found some computer accounts using Service Principals. An attacker could use this to attempt a brute force password cracking attempt, which may succeed for accounts with weak passwords. **RECOMMENDATION:** The servicePrincipalName (SPN) attribute allows linking Kerberos service names to accounts. Whenever an account owns a Kerberos service name, it becomes possible for any user to request a ticket for that service. In that case, the received ticket is encrypted with one of the corresponding account Kerberos encryption keys. Thus, it is possible to start an offline brute-force attack on the ticket to recover the account password if it is not strong enough. By default, only computer accounts have SPNs and the attribute must remain empty for all privileged accounts.
Stale Computer Accounts	**High**	**Total Stale Computer Accounts in all Domains: 33485**	**IMPACT: Found Stale Computer Accounts were found. This type of user or computer accounts are not disabled and did not authenticate against the Active Directory for more than a year. Dormant accounts are either legitimate accounts which are rarely used, or obsolete accounts. Obsolete accounts grant users illegitimate access (e. g. after they leave the company) or be stealthily used by attackers, which is even more problematic if the accounts are privileged. Their mere existence also makes user and access rights accountability much harder.** **RECOMMENDATION: Recommended action is to remove Stale Computer or user accounts or move them to an Organizational Unit and then protect that OU.**

8.4 AD SECURITY RISKS-ADMINS

Test	Severity	Finding	Remark

8.5 AD SECURITY RISKS-OBJECTS OWNERSHIP

Test	Severity	Finding	Remark
Domain Controllers not owned by Admins	**High**	Total Domain Controllers owned by non-privileged accounts: 2	**IMPACT:** Not all Domain Controller computer accounts are owned by privileged accounts. Control of DC machine accounts allows for an easy path to compromising the domain. While Domain Controller objects are typically created during DCPromo by privileged accounts, if an accidental ownership change occurs on a DC object, it can have large consequences for security of the domain, since object owners can change permissions on the object to perform any number of actions. **RECOMMENDATION:** Accounts which are granted permissions on domain controllers must be considered privileged. Therefore, they must be protected through the adminSDHolder mechanism. These accounts must belong to either the Enterprise Admins or the Domain Admins

			group. Please review the list of affected domain controllers and ensure to change ownership.
Computer Objects not managed by Admins	High	Total Computers Not Managed By Admins in all Domains: 2	**IMPACT:** Some objects have non-standard owners. All computer objects must be owned by admin accounts. **RECOMMENDATION:** Please ensure one of the following accounts manages computer accounts in domain: Domain Admins, Enterprise Admins, Administrators, or Local System.
Organizational Units not managed by Admins	High	**Total Organizational Units Not Managed By Admins: 2**	**IMPACT: Some Organizational Units have non-standard owners. All organizational units must be owned by admin accounts.** **RECOMMENDATION: Please ensure one of the following accounts manages computer accounts in domain: Domain Admins, Enterprise Admins, Administrators, or Local System.**

8.6 SENSITIVE CHANGES

Test	Severity	Finding	Remark
Sensitive GPOs Modified	High	Sensitive GPOs Status in Last 10 Days: WARNING: Modified	**IMPACT:** Sensitive Group Policy Objects have been changed in the last 10 days. Changes to the Default Domain Policy or Default Domain Controllers Policy should be accounted for by the administrators. If the change cannot be accounted for, investigate the change looking for potential weakening of security posture and why the change was made. **RECOMMENDATION:** Please ensure the change is made by an Administrator as changing to default domain and domain controller policies is generally not required.
Changes to Privileged Groups in Last 15 days	High	**Total Privileged Groups Modified in Last 15 Days in All Domains: 2**	**IMPACT: Found indicator of exposure found. Recent additions or deletions to privileged group members could be normal operational changes or could indicate attempts at persistence or cleaning up of tracks after an attack.** **RECOMMENDATION: Confirm that any additions/removals from privileged groups are valid and properly accounted for.**

8.7 CRITICAL ACCOUNTS STATUS

Test	Severity	Finding	Remark

Built-In Admin Account Not protected	**High**	Default Administrator Account not protected in all domains: 1	**IMPACT:** Default Administrator account is not protected. Use of a domain's Administrator account should be reserved only for initial build activities, and possibly, disaster-recovery scenarios. To ensure that an Administrator account can be used to effect repairs in the event that no other accounts can be used, you should not change the default membership of the Administrator account in any domain in the forest. Instead, you should secure the Administrator account in each domain in the forest. **RECOMMENDATION:** It is recommended to enable the Account is sensitive and cannot be delegated flag on the administrator account and make sure to change the password.
Built-In Admin Account Not Disabled	**High**	Default Admin Account not disabled in Total Domains: 2	**IMPACT:** Default Administrators account in domains have not been renamed or disabled. Anyone with an administrator account can attempt to log on to domain which will cause Bad Logon Events on domain controllers. **RECOMMENDATION:** Please review the list and make sure to rename and disabled Default Administrator account in each domain.
Built-In Admin Account was used in last 10 days	**High**	Total Domains in which Default Administrator account was used in last 10 days: 1	**IMPACT:** Default Administrator account was used recently in some domains. The default Admin account should only be used for initial Active Directory setup and for disaster recovery purposes. If default admin account is used, then it could indicate that the user has been compromised. **RECOMMENDATION:** If best practices are followed and domain Admin is not used, this would indicate a compromise. Ensure any logins to the built-in Domain Administrator account are legitimate and accounted for. If not accounted for, a breach is likely and should be investigated.
Guest Account is enabled	**High**	Total Guest Accounts Enabled in All Domains: 1	**IMPACT:** Guest Account is not disabled in all domains. Enabling Guest Account is a security risk as all of the users in an Active Directory environment have their own ID to access Active Directory and organization applications. **RECOMMENDATION:** It is recommended to disable Guest account in identified domains.
Guest Account is not renamed	**High**	**Guest Account not renamed in Total Domains: 2**	**IMPACT: Guest account in domains have not been renamed or disabled. The built-in guest account is a well-known user account on all Windows systems and, as initially installed, does not require a password. This can allow access to system resources by unauthorized users. Renaming this account to an unidentified name improves the protection of this account and the system.** **RECOMMENDATION: Please review the list and make sure to rename and disabled Guest account in each domain.**

8.8 PRIVILEGED ACCOUNTS

Test	Severity	Finding	Remark
Misconfigured Administrative Accounts Found	Critical	Total Admins Misconfigured: 7	**IMPACT:** Test has failed. Administrative accounts were found that are not configured to have the 'This account is sensitive and cannot be delegated' option enabled. This leaves the account vulnerable to potential abuse of delegated rights to change the administrative account password disable copy or modify the account properties. **RECOMMENDATION:** This can be remediated by running the following PowerShell command as a privileged user (Domain Admin)
Weak Password Policies Affected Admins	Critical	Total Privileged Account using Weak Password Policy: 3	**IMPACT:** Privileged Users are not using strong password policies. A password length of seven characters can be cracked instantly by various brute force tools. Apart from the danger of account compromise, having a weak password policy also leads to complex problems like regulatory compliance. **RECOMMENDATION:** For privileged accounts, enforcing a password policy with the following requirements is recommended: forced change at most every 3 years and length of 8 or more characters is recommended.
Disabled Admins part of Privileged Groups	High	Total Disabled Admins In Privileged Groups: 1	**IMPACT:** Some Disabled users are part of Privileged Groups. When a user is disabled, it tends to not be monitored as closely as active accounts. If this user is also a privileged user, then it becomes a target for takeover if an attacker can enable the account. **RECOMMENDATION:** Recommended action is to remove Disabled Users from Privileged groups.
Password Do Not Expire	High	**Total Admin Accounts set to PasswordNeverExpires: 4**	**IMPACT: Some privileged accounts have passwords that never expire. If no security mechanism enforces a periodic password rotation, taking over an account allows any malicious user to keep their access rights in the domain for extended periods of time.** **RECOMMENDATION: Passwords should be periodically changed for all privileged group members (at most every 3 years). To enforce application of the domain password policy on these accounts, their DONT_EXPIRE flag should not be set. This account flag should then be unset, usually by unchecking the password never expires option in the "Account" tab of the user properties. Their passwords should then be rolled immediately.""**

8.9 DOMAIN POLICIES

Test	Severity	Finding	Remark
Default Domain Policy-Minimum Password Length	High	Account Policies Not Configured correctly in Total Domains: 1	**IMPACT:** Account Policies are configured correctly. **RECOMMENDATION:**
FGPP Policies-Minimum Password Length	High	FGPP Not Configured Correctly In Domains: Not Created	**IMPACT:** FGPP password parameters are not configured correctly. Minimum password set to 7 or less will not help in providing adequate defense against a brute force attack. **RECOMMENDATION:** Please review the list of FGPP provided and make sure to enable Password Complexity. Please check the account policies parameters and ensure values are correct. The Minimum Password Length recommended is 12 and password complexity must be enabled.
FGPP Policies Not Applying	High	**Total FGPP Not Applying in All Domains: Not Created**	**IMPACT: Some FGPP Policies have been created but they do not apply to any objects. Users will not receive Password Policies from FGPP.** **RECOMMENDATION: Please review the list and make sure FGPP Policies are applying to desired objects.**

8.10DOMAIN CONTROLLER SECURITY

Test	Severity	Finding	Remark
TLS 1.1 Enabled DCs	Critical	Total Domain Controllers with TLS 1.1 Protocol Enabled: 3	**IMPACT:** TLS 1. 1 protocol is not disabled on all domain controllers. Modern cyber-attacks methods often make specific use of legacy protocols in their attack and often utilize them to target organizations that have yet to implement the proper mitigation. **RECOMMENDATION:** To retire the use of legacy protocols, your organization must first discover which internal entities and applications rely on them. Recommendation is to disabled TLS 1.1 protocol on all affected domain controllers by applying a registry fix or using Default Domain Controllers GPO.
NTLM Authentication Enabled DCs	Critical	**Total Domain Controllers with NTLM Enabled: 3**	**IMPACT: Found NTLM enabled on all domain controllers. NTLM and NTLMv2 authentication is vulnerable to various malicious attacks, including SMB replay, man-in-the-middle attacks, and brute force attacks. Reducing and eliminating NTLM authentication from your environment forces the Windows operating system to use more secure protocols, such as the Kerberos version 5 protocol, or different authentication mechanisms, such as smart cards. The main risk of disabling NTLM is the potential usage of legacy or incorrectly configured applications that can still use NTLM authentication.** **RECOMMENDATION: It is recommended to disable NTLM Protocol on domain controllers by using the registry or GPO. Edit the Default Domain Policy, go to the GPO section Computer Configurations, Select**

			Policies, and then take, security Setting from Windows Settings, then choose Local Policies -> Security Options, and find the policy Network Security: LAN Manager authentication level. Configure Send LM & NTLM responses to use NTLMv2 session security if negotiated to apply settings to all domain controllers.

8.11 DOMAIN CONTROLLER CONFIGURATION

Test	Severity	Finding	Remark
Missing DNS Scavenging DCs	**Critical**	Total DNS Servers Not Enabled with Server Level Scavenging: 3	**IMPACT:** Some DNS Servers do not have automatic scavenging enabled. Disabling Scavenging might result in a huge number of stale DNS Entries. **RECOMMENDATION:** Note that if all your Domain Zones are AD Integrated it is recommended to keep Scavenging enabled only on one DNS Server.
DCDiag Failure DCs	**High**	Total DCs with DCDiag Failures: 2	**IMPACT:** DCDiag Test reported errors on domain controllers. DCDiag the checks complete functionality of a domain controller. **RECOMMENDATION:** Please check DCDiag file for that domain controller. The DCDiag result file can be found at C:\Users\Public\SmartProfiler\SmartProfilerAssessment\Data\DCDiagTest location.
Out Of Default OUs DCs	**High**	Total DCs outside of it's Default OU: 2	**IMPACT:** Some domain controllers are located outside Domain Controllers OU. Domain Controller Default GPO might not be applying to domain controllers located outside Domain Controllers OU. Domain controllers pull some security settings only from group policy objects linked to the root of the domain. Because domain controllers share the same account database for the domain, certain security settings must be set uniformly on all domain controllers. **RECOMMENDATION:** Please make sure to move domain controllers back to Domain Controllers OU. The domain controller gathers the list of group policy objects by searching the parent containers of the domain controller's Computer object. The domain controller applies the settings listed earlier only if the group policy object is linked to the Domain container.
Scheduled Tasks found on Domain Controllers	**High**	**Total Scheduled Tasks on DCs: 8**	**IMPACT: Test has failed. Scheduled tasks have been known to be exploited to allow attackers to elevate privileges gain persistence and download and deploy malware. This finding indicates that scheduled tasks were found on the Domain Controllers within the domain queried.** **RECOMMENDATION: Review scheduled tasks listed in the accompanying file(s) for legitimacy and validate that they are needed. Remove any unneeded unnecessary tasks.**

8.12DOMAIN CONTROLLER ROLES/SERVICEs

Test	Severity	Finding	Remark
Print Spooler Service Running DCs	Critical	Total Domain Controllers with Print Spooler Service running: 3	**IMPACT: Print Spooler Service is not disabled on all domain controllers. CVE-2021-1675 is weaponized to compromise Domain Controllers. This is actually already happening in the real world, leading to a zero-day vulnerability event. Luckily, the vulnerability can be easily thwarted with a simple configuration change on Domain Controllers by disabling the Print Spooler service.** **RECOMMENDATION: Print spooler services are enabled by default. If not absolutely required, disable the service on all domain controllers. If required, make sure the server is fully patched and follow Microsoft guidance here. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527**

8.13AD SITES

Test	Severity	Finding	Remark
Sites without Subnets Association	High	Total AD Sites Without Subnets: 1	**IMPACT:** Some AD Sites do not have Subnets associated. Application and User authentication is impacted. Users and applications will go to domain controllers in other sites for authentications. **RECOMMENDATION:** It is highly recommended to associate required user/application subnets with AD Sites. If subnets are not associated with AD Sites users in the AD Sites might choose a remote domain controller for authentication.
Missing Global Catalog Sites	High	**Total AD Sites Without Global Catalog Servers or No Universal Group Caching Enabled: 1**	**IMPACT: No Global Catalog Servers found in some AD Sites. It is recommended to designate one Domain Controller as a Global Catalog Server in AD Sites where AD Applications are running. AD Applications might use Global Catalog Server to find objects in the Active Directory.** **RECOMMENDATION: Assign Global Catalog Servers to AD Sites.**

8.14TIME SYNC AND FSMO PLACEMENT

Test	Severity	Finding	Remark
PDC Emulator Time Source	High	Root PDC Time Source: Internal Source	**IMPACT:** Domain Controller Time Synchronization is not correct. Impacts authentication between domain controllers and clients. **RECOMMENDATION:** Please ensure PDC syncs its time from an External NTP Server and other domain controllers sync using the default Time Synchronization settings. All other Domain Controllers must be using NT5DS registry entry.

8.15AD OBJECTS

Test	Severity	Finding	Remark
Found Unused Netlogon Scripts	High	Total Unused Scripts In All Domains: 1	**IMPACT:** **RECOMMENDATION:**
Security Groups without Objects	Low	Total Empty Security Groups In All Domains: 50061	**IMPACT:** Security Groups have been created in Domain, but they do not hold any members. Refer issue details. **RECOMMENDATION:** Please check why empty Security Groups have been created in Domain. The output also contains the pre-defined security groups other than user-defined security groups.
Users without UPN specified	Low	Total Users with UPN Blank in all Domains: 10	**IMPACT:** Some Domain Users do not have UPN filled. UPN is required by other applications. **RECOMMENDATION:** Please review the list and make sure to address the users that do not have the UPN filled.
Missing Location Text in AD Sites	Low	**Total AD Sites Not Defined With Location: 2**	**IMPACT: AD Sites do not have a description text set that defines the AD site location. In a large environment it will be difficult to identify sites or applications will fail to query AD Site description if not defined.** **RECOMMENDATION: It is recommended to set a description text to identify the role of the AD Site. Some applications use AD Site Location text to get the details about the AD Sites.**

8.16AD GPO

Test	Severity	Finding	Remark
No Group Policy Objects to Prevent Domain Admins from logging on to Workstations or Servers Found	Critical	Total AD Domains Affected: 2	**IMPACT:** Test has failed. Group Policy Objects are used to centralize enforcement of configurations and policies for domain user and computer assets. GPO's can be leveraged to remove the ability to perform unsafe actions like logging into a workstation as a Domain

			Admin. These actions increase the risk and likelihood of credential theft and compromise. **RECOMMENDATION:** Create a Group Policy Object to prevent Domain Admins from logging on to Workstations or Servers.
No Group Policy Objects to Block ISO Execution Found	**Critical**	Total AD Domains Affected: 2	**IMPACT:** Test has failed. Group Policy Objects are used to centralize enforcement of configurations and policies for domain user and computer assets. GPO's can be leveraged to disable execution of ISO automatically. **RECOMMENDATION:** Create a Group Policy Object to disable ISO execution.
No Group Policy Objects Enforcing UAC Prompt for Elevation Found	**High**	Total AD Domains Affected: 2	**IMPACT:** Test has failed. Group Policy Objects are used to centralize enforcement of configurations and policies for domain user and computer assets. GPO's can be leveraged to enforce security measures like the User Account Control (UAC) prompt to grant elevated permissions. Enforcing the use of the UAC prompt hinders an attackers ability to silently or programmatically elevate a standard users privileges to administrative permissions. **RECOMMENDATION:** Create a Group Policy Object to enforce UAC prompts for all users.
No Group Policy Objects to Mitigate Accidental Script Execution	**High**	Total AD Domains Affected: 2	**IMPACT:** Test has failed. Groups Policy Objects are used to centralize enforcement of configurations and policies for domain user and computer assets. GPO's can be leveraged to replace the default file associations with a program of your choice. Replacing the default file association of JavaScript (. js) file extensions to a program like notepad will mitigate the risk associated with automated or inadvertent file execution. The following extensions are evaluated **RECOMMENDATION:** Create a Group Policy Object to replace the default file association for JavaScript file extensions.
No Group Policy Objects to Mitigate NTLMv1 Protocol	**High**	**Total AD Domains Affected: 2**	**IMPACT: Test has failed. NTLMv1 is a legacy authentication protocol with weak encryption that allows attackers to easily retrieve credentials from the network and perform NTLM Relay attacks.** **RECOMMENDATION: Create a Group Policy Object to disable NTLMv1 protocols. Additionally, disabling these protocols in a Golden Image is recommended.**

8.17AD DNS

Test	Severity	Finding	Remark

8.18DANGEROUS PERMISSIONS

Test	Severity	Finding	Remark

Accounts with Extended Rights to Read LAPS Passwords Found	**Critical**	Illegal Accounts Found to read LAPS in AD Domains: 2	**IMPACT:** Test has failed. Accounts in an Active Directory with extended or overly permissive rights to OU's and Computers may be granted unintentional permissions to read modify or administer the Local Admin Password Solution (LAPS) on domain objects. **RECOMMENDATION:** Identified accounts should be reviewed to ensure that they are supposed to have the rights to view read or modify LAPS password information. Auditing of LAPS access can be configured by running the PowerShell commands.
Group Policy Objects with Improper Permissions Found	**Critical**	Abusable GPO Permissions found in Total AD Domains: 1	**IMPACT:** Test has failed. Group Policy Objects found with ``Write`` or ``Modify`` permissions granted to Authenticated Users or Everyone groups. **RECOMMENDATION:** Review the identified Group Policy Object permissions.
Group Policy Object Assignments with Improper Permissions Found	**Critical**	Total Abusable GPO Permissions in AD Domains: 3	**IMPACT:** Test has failed. Groups Policy Objects found with 'Write' or 'Modify' permissions granted to Authenticated Users or Everyone groups on the policy enforced objects. (eg Everyone group can modify a file or application assigned via GPO) **RECOMMENDATION:** Review the identified Group Policy Object permissions.
EVERYONE Full Control Permissions on OUs	**Critical**	**Total Organizational Units with Everyone Full Control Access Rights: 3**	**IMPACT: Some Organizational Units have been found with Everyone Full Control. Everyone Full Control to an OU is not an optimal configuration and may lead to security risks.** **RECOMMENDATION: Please review the list provided and make sure Everyone Full Control Permission is removed from the Organizational Units.**

APPENDIX-1: ANSSI Tests Status

The following table lists the Tests that were performed according to ANSSI and MITRE ATT&CK definition. ANSSI is French National Agency for the Security of Information Systems. For more information, please check out here: https://www.cert.ssi.gouv.fr/uploads/guide-ad.html

- **Test**: Shows test name (Test name can be different from ANSSI ID Test)
- **Severity**: Shows Risk/Severity associated with the Test. Risk can be **Critical**, **High**, Medium or **Low**.
- **ANSSI:** Shows ANSSI ID for test.
- **More Information:** More information where you can find link to test recommended by ANSSI.

Test	SEVERITY	ANSSI ID	More Information
Dangerous Permissions on AdminSDHolder	**Critical**	vuln1_privileged_members_perm vuln2_privileged_members_perm	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#permissions_adminsdholder

AdminSDHolder was Modified in last 30 days	Critical	vuln1_permissions_adminsdholder	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#permissions_adminsdholder
Anonymous or EVERYONE in Pre-Windows 2000 Group	Critical	vuln2_compatible_2000_anonymous	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#compatible_2000_anonymous
Weak Password Policies Affected Admins	Critical	vuln2_privileged_members_password	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#privileged_members_password
Protected Users Group Status	High	vuln3_protected_users	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#protected_users
Denied RODC Password Replication Group missing Privileged Accounts	High	vuln3_rodc_denied_group	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#rodc_denied_group
msDS-NeverRevealGroupattribute RODC missing Privileged Accounts	High	vuln3_rodc_never_reveal	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#rodc_never_reveal
Users with LastPasswordSet was never Set	High	vuln2_dont_expire	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire
Users with PWDLastSet to ZERO	High	vuln1_user_accounts_dormant	https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/review-accounts-whose-attribute-pwdlastset-has-a-zero-value
Stale User Accounts	High	vuln1_user_accounts_dormant	https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory
User Accounts Pass Never Expires	High	vuln2_dont_expire	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire
User Accounts Pass Not Required	High	vuln2_dont_expire	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire
Computers with SPNs Configured	High	vuln1_spn_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#spn_priv
Stale Computer Accounts	High	vuln1_user_accounts_dormant	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#user_accounts_dormant
Computer Objects not managed by Admins	High	vuln3_owner	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#owner
Organizational Units not managed by Admins	High	vuln3_owner	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#owner

Missing Privileged Groups in Protected Users Group	High	vuln3_protected_users	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#protected_users
Privileged Accounts Pass Never Expires	High	vuln2_dont_expire	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire
Password Do Not Expire	High	vuln1_dont_expire_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire_priv
Dangerous Permissions Found on Naming Contexts	High	vuln_permissions_naming_context	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Pre-Windows 2000 Compatible Access Group is not empty	High	vuln_compatible_2000_anonymous	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Users With DES encryption	Medium	vuln2_kerberos_properties_deskey	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#kerberos_properties_deskey
Users With Reversible Encryption	Medium	vuln3_reversible_password	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#reversible_password
Users With Kerberos Pre-Authentication	Medium	vuln1_kerberos_properties_preauth_priv vuln2_kerberos_properties_preauth	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#kerberos_properties_preauth_priv
Users Disabled	Medium	vuln_user_accounts_dormant	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_user_accounts_dormant
Computers Disabled	Medium	vuln_user_accounts_dormant	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_user_accounts_dormant
Password Expiration is missing for smart card users	Low	vuln_smartcard_expire_passwords	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Orphaned Admins on AdminSDHolder	Passed	vuln1_permissions_adminsdholder	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#permissions_adminsdholder
Constrained delegation to domain controller service	Passed	vuln1_delegation_a2d2	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#delegation_a2d2
Resource-based constrained delegation on domain controllers	Passed	vuln1_delegation_sourcedeleg	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#delegation_sourcedeleg
Anonymous Access to Active Directory	Passed	vuln1_dsheuristics_bad	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dsheuristics_bad
Allowed RODC Password Replication Group is not empty	Passed	vuln3_rodc_allowed_group	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#rodc_allowed_group

Managed service accounts with passwords unchanged for more than 90 days	**Passed**	vuln_password_change_msa_no_change_90	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Users with SPNs Configured	**Passed**	vuln1_spn_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#spn_priv
Users Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#primary_group_id_nochange
Computers With Unconstrained Delegation	**Passed**	vuln2_delegation_t4d	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#delegation_t4d
Computers Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#primary_group_id_nochange
Admins with SPNs Configured	**Passed**	vuln1_spn_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#spn_priv
KRBTGT Account Password Not Changed	**Passed**	vuln2_krbtgt	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#krbtgt
Too Many Privileged Accounts	**Passed**	vuln_privileged_members	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Inactive Admins	**Passed**	vuln1_user_accounts_dormant	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#user_accounts_dormant
Privileged Groups Contain more than 20 members	**Passed**	vuln1_privileged_members	https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/review-and-reduce-the-number-of-accounts-in-highly-privileged-administrative-groups https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#privileged_members
Kerberos Pre-authentication Disabled	**Passed**	vuln1_kerberos_properties_preauth_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#kerberos_properties_preauth_priv
Passwords Not Changed within 90 days	**Passed**	vuln1_password_change_priv	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_priv
DNSAdmins Group has members	**Passed**	vuln1_dnsadmins and vuln1_permissions_msdn	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dnsadmins
Domain Controllers Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#primary_group_id_nochange
Inconsistent DCs	**Passed**	vuln1_dc_inconsistent_uac	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dc_inconsistent_uac

Secrets not renewed DCs	**Passed**	vuln1_password_change_dc_no_change	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_dc_no_change
Duplicate SPNs	**Passed**	vuln1_delegation_sourcedeleg	https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names
Unauthenticated Servers	**Passed**	vuln2_password_change_server_no_change_90	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_server_no_change_90
Secrets not renewed Servers	**Passed**	vuln3_password_change_server_no_change_45	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_server_no_change_45
AD Forest Schema Not upto date	**Passed**	vuln2_adupdate_bad	https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#adupdate_bad
Dangerous Permissions Found on MicrosoftDNS Container	**Passed**	vuln_permissions_msdns	https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html
Found Groups with SID history Set	**Passed**	**vuln_sidhistory_present**	**https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html**

APPENDIX-2: Passed/Completed Tests

After carrying out a complete health assessment of the ***Active Directory Environment***, the following Tests have been **passed**/completed sucessfully and no issues were found.

Test	Severity	Practice	Finding
Missing Microsoft LAPS in AD Forest	**Passed**	MS-RECOMMENDED	Microsoft LAPS Status:Deployed
Orphaned Admins on AdminSDHolder	**Passed**	vuln1_permissions_adminsdholder	Total Possible Orphaned Admins in all Domains on AdminSDHolder object:0
Constrained delegation to domain controller service	**Passed**	vuln1_delegation_a2d2	Total Computers with Constrained Delegation in all Domains:0
Resource-based constrained delegation on domain controllers	**Passed**	vuln1_delegation_sourcedeleg	Total Computers with Resource-Based Delegation in all Domains:0
Anonymous Access to Active Directory	**Passed**	vuln1_dsheuristics_bad	Anonymous Access To Active Directory:0
Found Hidden Domain Controllers	**Passed**	MS-RECOMMENDED	Total Hidden Domain Controllers:0
Successful Exploit Machine Accounts Found	**Passed**	MS-RECOMMENDED	Total Exploit Machine Accounts:0
Possible User-based Service Accounts found	**Passed**	MS-RECOMMENDED	Total Possible User-Based Service Accounts:0

Domain Trusts Found	**Passed**	MS-RECOMMENDED	Domain Trusts Status:Not Found
Replication Errors DCs	**Passed**	MS-RECOMMENDED	Total DCS in Replication Errors:0
Allowed RODC Password Replication Group is not empty	**Passed**	vuln3_rodc_allowed_group	Total Members in RODC Replication Group:0
Managed service accounts with passwords unchanged for more than 90 days	**Passed**	vuln_password_change_msa_no_change_90	Total Managed Service Accounts Password Unchanged Since last 90 days:0
Unsecure Updates Zones	**Passed**	vuln1_dnszone_bad_prop vuln3_dnszone_bad_prop	Total DNS Zones accepting non-secure updates:0
Users with SPNs Configured	**Passed**	vuln1_spn_priv	Total Users with SPN defined in all Domains:0
Accounts vulnerable to Kerberoasting Found	**Passed**	MS-RECOMMENDED	Total Kerberoasting Accounts Found:0
Users Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	Total Users with PrimaryGroupID Modified in all Domains:0
Users Sending Bad Logons	**Passed**	MS-RECOMMENDED	Total Users sending Bad Logons in all Domains:0
Computers With Unconstrained Delegation	**Passed**	vuln2_delegation_t4d	Total Computers with Unconstrained Delegation in all Domains:0
Computers Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	Total Computers modified with PrimaryGroupID:0
Computers Sending Bad Logons	**Passed**	MS-RECOMMENDED	Total Computers sending Bad Logon Attempts in all Domains:0
Unsupported Operating Systems	**Passed**	MS-RECOMMENDED	Total End Of Life-Unsupported Operating Systems:0
Admins with SPNs Configured	**Passed**	vuln1_spn_priv	Total Admin Accounts With ServicePrincipalName Identified:0
Admins Sending Bad Logons	**Passed**	MS-RECOMMENDED	Total Privileged Users With Bad Logon Attempts:0
Recently Created Privileged Admins	**Passed**	MS-RECOMMENDED	Total Privileged Accounts created in last 10 days in all domains:0
Users Identified with Privileged SIDs in sIDHistory	**Passed**	MS-RECOMMENDED	Total Users containing Admin Accounts in sIDHistory in all Domains:0
Computers Identified with Privileged SIDs in sIDHistory	**Passed**	MS-RECOMMENDED	Total Computers containing Admin Accounts in sIDHistory in all Domains:0
Found Excluded Groups by AdminSDHolder and SDProp	**Passed**	MS-RECOMMENDED	Total Excluded Groups by SDProp Process:0

krbtgt Account with Resource-Based Constrained Delegation	**Passed**	MS-RECOMMENDED	Affected number of Domains:0
Built-In Admin Account Not Renamed	**Passed**	MS-RECOMMENDED	Default Admin Account not renamed in Total Domains:0
Built-In Admin Account Password Not Changed in 90 days	**Passed**	MS-RECOMMENDED	Total Domains in which Default Administrator password not changed since last 90 days:0
KRBTGT Account Password Not Changed	**Passed**	vuln2_krbtgt	Total Domains Using KRBTGT Old Password:0
Administrator Account ServicePrincipalNames Found	**Passed**	MS-RECOMMENDED	Total AD Domains Affected:0
Too Many Privileged Accounts	**Passed**	vuln_privileged_members	Affected AD Domains:0
Inactive Admins	**Passed**	vuln1_user_accounts_dormant	Total Enabled Admin Accounts Not In Use Since Last 30 Days:0
Privileged Groups Contain more than 20 members	**Passed**	vuln1_privileged_members	Privileged Groups Contain More than 20 members:0
Kerberos Pre-authentication Disabled	**Passed**	vuln1_kerberos_properties_preauth_priv	Total Pre-Authentication Admins in all domains:0
Passwords Not Changed within 90 days	**Passed**	vuln1_password_change_priv	Total Admin Accounts Did Not Change Their Passwords Since Last 90 Days:0
DNSAdmins Group has members	**Passed**	vuln1_dnsadmins and vuln1_permissions_msdn	Total Members In DNSAdmins Group In All Domains:0
Privileged Admins missing AdminCount=1 Flag	**Passed**	MS-RECOMMENDED	Total Admins not set with AdminCount=1 flag in all domains:0
Operators Groups are not empty	**Passed**	MS-RECOMMENDED	Operators Groups containing total members in all domains:0
AdminsCount Flag set users not acting as Admins	**Passed**	MS-RECOMMENDED	Total Unknown Admins Found:1
Account Lockout Policies Missing	**Passed**	MS-RECOMMENDED	Total Accounts Locked Out in All Domains:0
Domain Controllers Modified with PrimaryGroupID	**Passed**	vuln3_primary_group_id_nochange vuln1_primary_group_id_1000	Total Domain Controllers modified with PrimaryGroupID:0
SMB 1 Protocol Enabled DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers with SMB1 Server Protocol Enabled:0
SMB 1 Client Protocol Enabled DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers with SMB1 Client Service Enabled:0

LAN Manager password hashes Enabled DCs	**Passed**	MS-RECOMMENDED	Total DCs with LAN Manager Password Hashes:0
SMB Signing Disabled DCs	**Passed**	MS-RECOMMENDED	Total Domains Controller Without SMB Signing:0
LDAP Signing Disabled DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers Without LDAP Signing:0
Inconsistent DCs	**Passed**	vuln1_dc_inconsistent_uac	Total Domain Controllers in Inconsistent State:0
Secrets not renewed DCs	**Passed**	vuln1_password_change_dc_no_change	Total Domain Controllers Not Changed Password Within 45 Days In All Domains:0
Missing Updates DCs	**Passed**	MS-RECOMMENDED	Total DCs Not Updated Since Last 45 Days:0
Missed Reboot Cycles DCs	**Passed**	MS-RECOMMENDED	Total DCs Not Rebooted Since Last 30 Days:0
No Contacts with Domain Controllers in Last Three Months	**Passed**	MS-RECOMMENDED	Total Domain Controllers not contacted since last three months:0
Orphaned DCs	**Passed**	vuln1_dc_inconsistent_uac	Total Orphaned Domain Controllers:0
Missing DNS Forwarders DCs	**Passed**	MS-RECOMMENDED	Total DNS Servers Do Not Have Forwarders Configured:0
Missing Root Hints DCs	**Passed**	MS-RECOMMENDED	Total DNS Servers Do Not Have Root Hints Configured:0
Missing Host Records DCs	**Passed**	MS-RECOMMENDED	Total DCs Missing Host Records in DNS:0
Loopback Address Missing DCs	**Passed**	MS-RECOMMENDED	Total DCs not configured with Loopback Address:0
Multihomed DCs	**Passed**	MS-RECOMMENDED	Total DCS in Multihomed State:0
NTFS Replication DCs	**Passed**	vuln2_sysvol_ntfrs	Total Domain Controllers utilizing NTFRS for AD Replication:0
Strict Replication Disabled DCs	**Passed**	MS-RECOMMENDED	Total DCs with Strict Replication Consistency not enabled:0
Unsupported OS DCs	**Passed**	MS-RECOMMENDED	Total DCs running Unsupported Operating Systems:0
Missing Enough DNS Servers in NIC DCs	**Passed**	MS-RECOMMENDED	Total DCs With inadequate Number Of DNS Servers in NIC Property:0
Not Enough Local Disks DCs	**Passed**	MS-RECOMMENDED	Total DCs Not Configured With Recommended Disk Configuration:0

Missing DNS Dynmaic Registration on NIC DCs	**Passed**	MS-RECOMMENDED	Total DCS NIC Dynamic Updates Not Enabled:0
Missing _msdcs Zone DCs	**Passed**	MS-RECOMMENDED	Total DNS Servers Missing _msdcs Zone:0
Event Log Config Not Correct DCs	**Passed**	MS-RECOMMENDED	Total DCs with Event Log misconfiguration:0
Event Log Size Not Optimized DCs	**Passed**	MS-RECOMMENDED	Total DCs with Event Log Size not optimal:0
Fax Server role installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have Fax Server Installed::0
Microsoft FTP service installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have FTP Server Installed::0
Peer Name Resolution Protocol installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have Peer Name Resolution Protocol Installed::0
Simple TCP-IP Services installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have Simple TCP/IP Services Installed::0
Telnet Client installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have Telnet Client Installed::0
TFTP Client installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have TFTP Client Installed::0
Server Message Block (SMB) v1 protocol Installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have SMB 1.0/CIFS File Sharing Support Installed::0
Windows PowerShell 2.0 installed DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers have Windows PowerShell 2.0 Engine Installed::0
ADWS Service Set to Manual DCs	**Passed**	MS-RECOMMENDED	Total DCs ADWS Not Set to Start Automatic:0
DHCP Service Running DCs	**Passed**	MS-RECOMMENDED	Total Domain Controllers with DHCP Server running:0
AD Services not running DCs	**Passed**	MS-RECOMMENDED	Total DCs with Services Not Running:0
Total Undefined Subnets	**Passed**	MS-RECOMMENDED	Total Undefined Subnets in AD Forest:0
Sites without ISTG Role	**Passed**	MS-RECOMMENDED	Total AD Sites Do Not Have ISTG Defined:0
Missing AD Sites Coverage	**Passed**	MS-RECOMMENDED	Total AD Sites Not Covered:0
Duplicate Site Links	**Passed**	MS-RECOMMENDED	Total Duplicate Site Links:0
Sites Missing Bridgehead Server	**Passed**	MS-RECOMMENDED	Number Of AD Sites Without Bridgehead Servers:0

Sites With Manual Bridgehead Server	**Passed**	MS-RECOMMENDED	Number Of AD Sites With Manual Bridgehead Servers:0
Sites creating Mesh Topology	**Passed**	MS-RECOMMENDED	Total AD Site Links Containing More than Two AD Sites:0
AD Sites without Site Link	**Passed**	MS-RECOMMENDED	Total AD Sites Not In Site Links:0
AD Sites without Domain Controller	**Passed**	MS-RECOMMENDED	Total AD Sites Without Domain Controllers:0
Domain Controllers Time Source	**Passed**	MS-RECOMMENDED	Total DCs Not Defined With Correct Time-Source:0
Domain Naming Master and Schema Master Placement	**Passed**	MS-RECOMMENDED	Status:Hosted on same computer
Managed Service Accounts Not Linked	**Passed**	MS-RECOMMENDED	Total Managed Service Accounts are not Linked:0
TombstoneLifeTime Modified?	**Passed**	MS-RECOMMENDED	Current TombstoneLifeTime Value:180
Check AD Forest Functional Level	**Passed**	MS-RECOMMENDED	AD Forest Functional Level:Dynamicpacks.net is Windows2016Forest
Check AD Domain Functional Level	**Passed**	MS-RECOMMENDED	Status:Ok
Duplicate SPNs	**Passed**	vuln1_delegation_sourcedeleg	Total Duplicate SPNs in AD Domains:0
Unauthenticated Servers	**Passed**	vuln2_password_change_server_no_change_90	Total Servers Not Authenticated Within 90 Days in All Domains:0
Secrets not renewed Servers	**Passed**	vuln3_password_change_server_no_change_45	Total Servers Not Changing Password within 45 days in all Domains:0
AD Forest Schema Not upto date	**Passed**	vuln2_adupdate_bad	Current Forest Schema Version Status:OK:88
GPOs not Applying	**Passed**	MS-RECOMMENDED	Total GPOs not applying correctly in All Domains:0
Orphaned GPO Containers	**Passed**	MS-RECOMMENDED	Total Orphaned Group Policy Objects:0

APPENDIX-3: Tests Scoring and Methodology

SmartProfiler adds severity to each test it executes based on the test weight and outcome. For example, if there are only 10 domain users which are disabled it doesn't necesserily mark that item as "High" severity. On the other hand if there are more than 100 users disabled in domain then test is marked as "High". The scoring is done based on

- The number of affected objects
- Is the affected object a System Object?
- Can affected objects be isolated based on the test executed?
- Is test impacting all users in Active Directory?

In Active Directory assessment, severity levels are used to classify the impact or seriousness of a particular issue or vulnerability. Here are definitions of critical, high, medium, and low severity in the Active Directory context:

Severity	CATEGORY
CRITICAL	Critical severity refers to issues or vulnerabilities that have the highest level of impact on the active directory environment. These issues pose an immediate and significant threat to the security, stability, or functionality of the ad infrastructure. Critical severity issues often result in system-wide disruptions, compromise of sensitive data, or unauthorized access to critical resources. They require immediate attention and remediation to mitigate the risks they pose.
HIGH	High severity denotes issues or vulnerabilities that have a significant impact on the active directory environment. While not as severe as critical issues, high severity problems can still lead to serious consequences. They may involve the potential compromise of important data, unauthorized access to resources, or disruptions to ad operations. High severity issues require prompt action to address and mitigate the risks they present.
MEDIUM	Medium severity indicates issues or vulnerabilities that have a moderate impact on the active directory environment. While not as critical or high, medium severity issues still possess the potential to impact the security, stability, or functionality of the ad infrastructure. They may include vulnerabilities that could be exploited to gain unauthorized access, expose sensitive information to certain users, or cause disruptions to non-critical services. While they require attention and remediation, they may not demand immediate action as critical or high severity issues.
LOW	Low severity refers to issues or vulnerabilities that have minimal impact on the active directory environment. These issues are generally less critical and do not pose an immediate threat to the security, stability, or functionality of the ad infrastructure. Low severity issues may include minor misconfigurations, weak security settings, or issues that have limited consequences or can be easily mitigated. While they should not be ignored, low severity issues can often be addressed during regular maintenance or scheduled updates.