# Ranger AD Report

Assessment Date: 11:25:46 September 28, 2022 UTC

Report Created Date: 11:42:11 September 28, 2022 UTC

# Table of Contents

## Ranger AD Executive Summary

This section provides the data for the Ranger AD results in summarized form.

LONDON.UK.
EUROPE.local

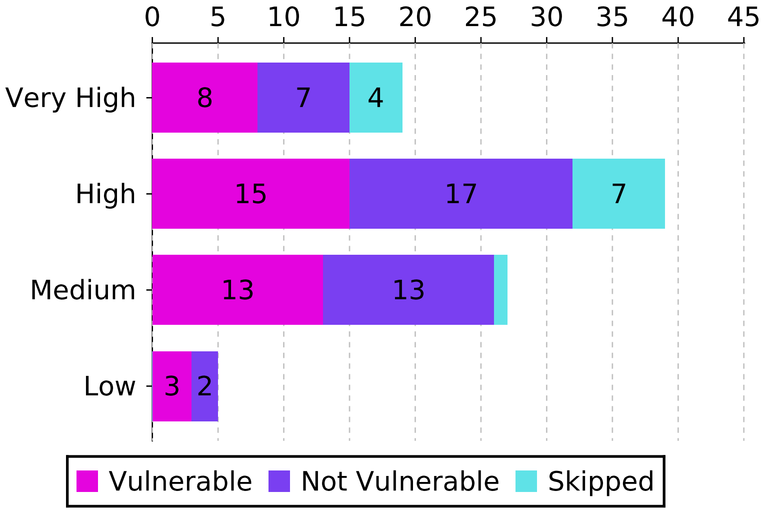
Domain

57%

Health

Medium

Risk



| Severity | All | Vulnerable | Not Vulnerable | Skipped |
|---|---|---|---|---|
| Very High | 19 | 8 | 7 | 4 |
| High | 39 | 15 | 17 | 7 |
| Medium | 27 | 13 | 13 | 1 |
| Low | 5 | 3 | 2 | 0 |
| Total | 90 | 39 | 39 | 12 |

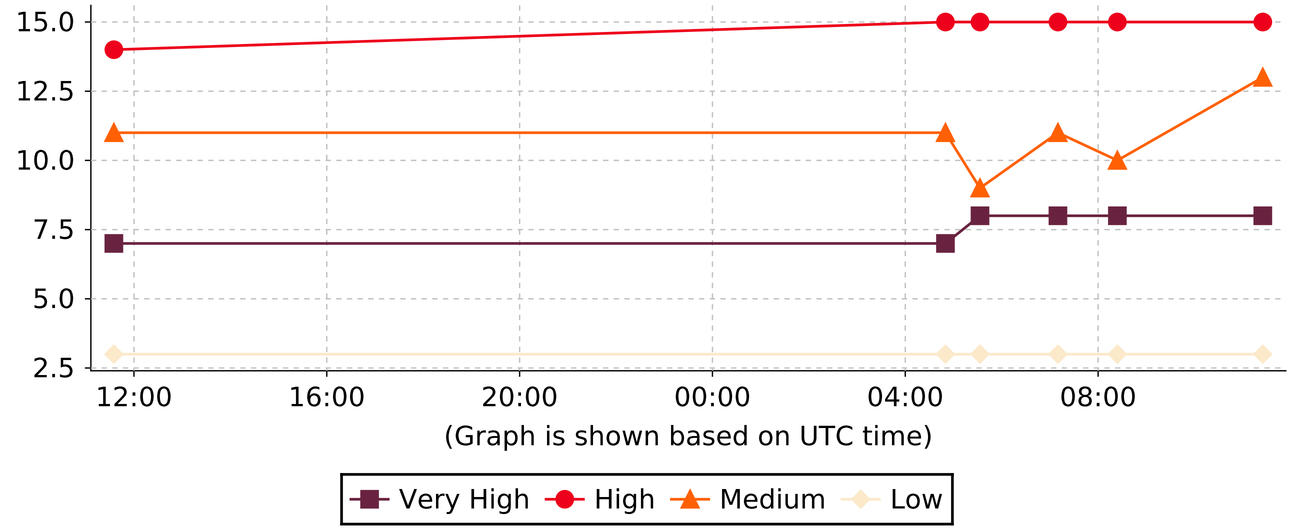
## Mitre ATT&CK

| Persistence | Exfiltration | Impact | Lateral Movement | Execution | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Initial Access | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| 30 | 2 | 1 | 18 | 1 | 60 | 19 | 35 | 4 | 4 | 1 |

## Most Vulnerable Assessments

| Assessment Name | Affected Objects count |
|---|---|
| Unusual Accounts with Replication Permissions (DCSync) | 1 |
| Default Permission Changes on Domain Partition | 4 |
| Weak Krbtgt Account – Golden Ticket | 1 |
| Security Hardening Recommendations for Domain Controllers | 17 |
| Zerologon Vulnerable Domain Controllers | 2 |
| Domain Controller Owner Permissions Changes | 3 |
| Weak Default Administrator Account | 2 |
| Dangerous Access Rights Delegation on Critical Objects | 6 |
| Default Administrator Account Hardening | 1 |
| Computer Accounts in Privileged Groups | 4 |

## Ranger AD Tests



## 1. Domain Controller with Print Spooler Enabled (PrintNightmare)

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Domain Controllers running the Print Spooler service are vulnerable to the PrintNightmare vulnerability if not updated with the latest security patch.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - T0004 (Persistence, Privilege Escalation, Defense Evasion)<br>https://attack.mitre.org/techniques/T0004/ |
| **References** | Windows Print Spooler Remote Code Execution Vulnerability<br>PrintNightmare, Critical Windows Print Spooler Vulnerability \| CISA |

**Manual Remediation Steps**

1. The recommendation is to disable the Print Spooler service on all domain controllers if unused.
 a. Disable the Print Spooler service through Group Policy:
  i. On a domain controller, open the group policy management tool (GPMC.MSC).

  ii. Navigate to the Domain Controllers OU.
  iii. Right-click and create a new group policy.
  iv. Right-click your new Group Policy Object and select the Edit option.

  v. Expand the Computer configuration folder and locate the following item:

   Computer Configuration > Policies > Windows Settings > Security Settings > System Services
  vi. Find Print Spooler and set it to Disabled.
  vii. Click Apply.
  viii. Expand the Computer configuration folder and locate the following item:

   Computer Configuration > Policies > Administrative Templates > Printers

  ix. Find the setting Allow print spooler to accept client connections and set it to Disabled.
  x. Click Apply.
2. Install the security patch.
 a. Windows Print Spooler Remote Code Execution Vulnerability
3. Configure the security settings recommended by Microsoft KB5005010:

 a. Restricting installation of new printer drivers after applying the July 6, 2021 updates

| | |
|---|---|
| **Affected Objects** | Domain_Controller_with_Print_Spooler_Enabled_(PrintNightmare)_1.csv |

## 2. Domain Controller Owner Permissions Changes

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Domain controller computer accounts must be owned by Domain Admins, Enterprise Admins, or built-in Administrator accounts. Standard users owning DCs allows for an easy compromise of the domain.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts - T1078 (Persistence, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/002/ |
| **Known Attack Tools** | Bloodhound |
| **References** | Take ownership of files or other objects (Windows 10) - Windows security \| Microsoft Docs |
| **Manual Remediation Steps** | 1. Review the domain controllers reported by Ranger AD.<br>2. Modify the owner of these domain controllers accounts.<br>3. Click Local Backup.<br>a. Open Active Directory Users and Computers MMC (Windows > Run > DSA.MSC).<br>b. Right-click on a domain controller account and select Properties.<br>c. In the Security tab, click Advanced.<br>d. Click Change adjacent to the Owner field, enter Domain Admins, click Check Names, and then click OK.<br>e. Save the changes. |
| **Affected Objects** | Domain_Controller_Owner_Permissions_Changes_1.csv |

## 3. Weak Krbtgt Account – Golden Ticket

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

An attacker who can steal the credentials of the krbtgt account can obtain domain dominance by forging the ticket granting ticket (TGT) of any user account in the domain, including Domain Admins.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets: Golden Ticket - T1558/001 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1558/001/ |
| **Known Attack Tools** | Mimikatz - Kerberos Golden Ticket |
| **References** | Golden Ticket Attack |
| **Manual Remediation Steps** | Reset the krbtgt account password at least every 180 days.<br>1. Open Active Directory Users and Computers.<br>2. Locate the krbtgt account and reset the password twice to any string, waiting at least the maximum ticket lifetime (10 hours by default) between resets. |
| **Affected Objects** | Weak_Krbtgt_Account_–_Golden_Ticket_1.csv |

## 4. Default Permission Changes on Domain Partition

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

A compromised user account with modified access to the domain partition in a forest can create new objects or make changes that propagate to newly created objects in AD. Inappropriate permissions can result in a DCSync attack leading to a full domain compromise.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Access Token Manipulation - T1134 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1134/ |
| **Known Attack Tools** | Bloodhound<br>Powerview |
| **References** | Active Directory Access Control List – Attacks and Defense |
| **Manual Remediation Steps** | 1. Verify the users and permissions reported by Ranger AD for the domain partition.<br><br>2. Check the security descriptor on Active Directory.<br>3. Open Active Directory Users and Computers MMC (Windows > Run > DSA.MSC).<br><br>4. Right-click the domain name and select properties.<br>5. In the Security tab, verify and remove the non-privileged users reported by Ranger AD. |
| **Affected Objects** | Default_Permission_Changes_on_Domain_Partition_1.csv |

## 5. LDAP Unsigned Connections Allowed

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Unsigned network traffic is susceptible to both replay attacks and man-in-the-middle (MITM) attacks.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Privilege Escalation, Lateral Movement)<br>https://attack.mitre.org/tactics/TA0004/ |
| **References** | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing. |
| **Manual Remediation Steps** | 1. Click Start > Run, type GPMC.MSC and then Click OK.<br>2. Right-click on the GPO linked on the Domain Controllers OU and click Edit.<br><br>3. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies, and then select Security Options.<br>4. Right-click the policy Domain controller: LDAP server signing requirements, and then select Properties.<br>5. In the Domain controller: LDAP server signing requirements Properties dialog box,<br><br>a. Enable Define this policy setting.<br>b. Select Require signing in the Define this policy setting list.<br>c. Click OK.<br>6. In the Confirm Setting Change dialog box, click Yes. |
| **Affected Objects** | LDAP_Unsigned_Connections_Allowed_1.csv |

## 6. Security Hardening Recommendations for Domain Controllers

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

Security policies on Domain Controllers help protect the Domain controller from various attacks and security risks. Group Policy Objects (GPOs) that are linked to the Domain Controllers OU are evaluated to ensure they contain the appropriate security hardening settings.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** Very High

**MITRE ATT&CK** Privilege Escalation - T1543 (Persistence, Privilege Escalation)
https://attack.mitre.org/techniques/T1543/

**References** Securing Domain Controllers Against Attack | Microsoft Docs

**Manual Remediation Steps**

1. Patch the domain controllers with the latest security fixes and update rollups

2. Configure each group policy object linked to the Default Domain Controllers OU with the following settings:
  Computer Configuration/Policies/Windows Settings/Security Settings/Security Options/Audit Policy/
    Audit account logon events Setting: Success, Failure
    Audit account management Setting: Success, Failure
    Audit logon events Setting: Success, Failure
    Audit privilege use Setting: Success, Failure
  Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/User Rights Assignments/
    Access this computer from the network Setting: Administrators, Authenticated Users, Enterprise Domain Controllers
    Add workstations to domain Setting: Administrators
    Allow log on locally Setting: Administrators, Enterprise Domain Controllers

    Allow log on through Remote Desktop Services Setting: Administrators

    Backup file and directories Setting: Administrators, Backup Operators, Server Operators (Backup Operators if a backup agent is required)

    Bypass traverse checking Setting: Not Defined
    Deny access to this computer from the network Setting: Guests, NT AUTHORITY\Local Account
    Deny log on as a batch job Setting:  Guests
    Deny log on through Remote Desktop Services Setting: Guests, NT AUTHORITY\Local Account
    Logon as a batch job Setting: Not Defined
    Log on as a service Setting: Only specific accounts that require this right should be listed here
    Restore file and directories Setting: Administrators, Backup Operators, Server Operators (Backup Operators if a backup agent is required)

    Shut down the system Setting: Administrators
  Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options/
    Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Setting: Enabled
    Devices: Prevent users from installing printer drivers Setting: Enabled
    Domain controller: Allow server operators to schedule tasks Setting: Disabled

    Domain member: Require strong (Windows 2000 or later) session key Setting: Enabled
    Microsoft network client: Digitally sign communication (always) Setting: Enabled

    Microsoft network server: Digitally sign communication (always)

Setting: Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares Setting: Enabled

Network Security: LAN Manager authentication level Setting: Send NTLMv2 response only. Refuse LM & NTLM

Network security: Minimum session security for NTLM SSP based (include secure RPC) clients Setting: Require NTLMv2 session security, Require 128-bit encryption

Network security: Minimum session security for NTLM SSP based (include secure RPC) servers Setting: Require NTLMv2 session security, Require 128 bit encryption

Network Security: Restrict NTLM: Audit Incoming NTLM Traffic Setting: Enable auditing for all accounts

Network Security: Restrict NTLM: Audit NTLM authentication in this domain Setting: Enable all

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Account Logon/

Audit Credential Validation Setting: Success & Failure

Audit Kerberos Authentication Service Setting: Success & Failure

Audit Kerberos Service Ticket Operations Setting: Success & Failure

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Account Management/

Audit Computer Account Management Setting: Success & Failure

Audit Other Account Management Events Setting: Success & Failure

Audit Security Group Management Setting: Success & Failure

Audit User Account Management Setting: Success & Failure

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Detailed Tracking/

Audit DPAPI Activity Setting: Success & Failure

Audit Process Creation Setting: Success & Failure

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/DS Access/

Audit Directory Service Access Setting: Success & Failure

Audit Directory Service Changes Setting: Success & Failure

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Logon and Logoff/

Audit Account Lockout Setting: Success

Audit Logoff Setting: Success

Audit Logon Setting: Success & Failure

Audit Special Logon Setting: Success & Failure

Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/System/

Audit IPsec Driver Setting: Success & Failure

Audit Security State Change Setting: Success & Failure

Audit Security System Extension Setting: Success & Failure

Audit System Integrity Setting: Success & Failure

The following registry changes can be deployed via GPO Computer Preferences:

Lsass.exe audit mode

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe\

Value: AuditLevel REG_DWORD:00000008.

Enable LSA Protection

Key: HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\Lsa\

Value: RunAsPPL REG_DWORD:1

WDigest Authentication (disabling may require KB2871997)

Key: HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\

Value: UseLogonCredential REG_DWORD:0

**Affected Objects** Security_Hardening_Recommendations_for_Domain_Controllers_1.csv

## 7. Unusual Accounts with Replication Permissions (DCSync)

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Accounts with replication permissions have full control of the complete Active Directory database by impersonating a domain controller.  Consequently, they're also able to receive password hashes.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | OS Credential Dumping: DCSync - T1003/006 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1003/006/ |
| **Known Attack Tools** | Mimikatz<br>DCSync |
| **References** | Protecting Against Active Directory DCSync Attacks - SentinelOne |
| **Manual Remediation Steps** | 1. Open the Active Directory Users and Computers MMC.<br>2. Click on View > Advanced Features.<br>3. Right-click on the domain object, such as "company.com", and then click Properties.<br>4. Click on the Security tab.<br>5. Select the desired user account, found in this exposure's CSV file, and then click Remove.<br>6. Click OK.<br>7. Close the snap-in. |
| **Affected Objects** | Unusual_Accounts_with_Replication_Permissions_(DCSync)_1.csv |

## 8. Zerologon Vulnerable Domain Controllers

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

The Netlogon Elevation of Privilege Vulnerability (CVE-2020-1472), also known as Zerologon, allows an unauthenticated attacker to elevate privileges and obtain administrative access to the domain.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Very High |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts - T1078/002 (Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/002/ |
| **Known Attack Tools** | Mimikatz |
| **References** | CVE-2020-1472 - Security Update Guide - Microsoft - Netlogon Elevation of Privilege Vulnerability |
| **Manual Remediation Steps** | Follow the guidelines provided by Microsoft in the link below:<br>https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e |
| **Affected Objects** | Zerologon_Vulnerable_Domain_Controllers_1.csv |

## 9. Lack of Recent Active Directory Backup

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Regular Active Directory backups can help to recover the domain in case of a disaster or restore objects in case of an attack.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Encrypt Sensitive Information - https://attack.mitre.org/mitigations/M1041/ (Defense Evasion)<br>https://attack.mitre.org/mitigations/M1041/ |
| **References** | AD Forest Recovery - Backing up a full server |

**Manual Remediation Steps**

To perform a backup with Windows Server Backup:

1. Open Server Manager > Tools > Windows Server Backup or Start > Administrative Tools > Windows Server Backup and follow the procedure below.

2. Click Local Backup.

3. Select Action > Backup once. Just as a reference, the steps are provided for a one-time backup with regular options. If needed, you can also schedule regular backups

4. In the Backup Once Wizard, on the Backup options page, click Different options, and click Next.

5. On the Select backup configuration page, click Full server (recommended), and then click Next.

6. On the Specify destination type page, click Local drives, or remote shared folder, and then click Next.

7. Specify the storage location for the backup.

8. On the Confirmation screen, click Backup.

**Affected Objects** Lack_of_Recent_Active_Directory_Backup_1.csv

## 10. Dangerous Access Rights on RODC KDC Account

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Any unwanted permissions on the RODC KDC account can lead to credential exposure.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts -<br>https://attack.mitre.org/techniques/T1078/002/ (Credential Access, Privilege<br>https://attack.mitre.org/techniques/T1078/002/ |
| **Known Attack Tools** | Mimikatz |
| **References** | Attacking Read-Only Domain Controllers (RODCs) to Own Active Directory |

**Manual Remediation Steps**

1. Review the permissions on the krbtgt_#### accounts reported by Ranger AD and remove those permissions identified as extraneous.
2. Open Active Directory Users and Computer MMC (Start > Run > dsa.msc)

  a. Right-click on the identified krbtgt_#### user and select Properties.
  b. On the Security tab, remove the specific permissions for the objects identified in the exposure.
  c. Save the changes.

**Affected Objects** Dangerous_Access_Rights_on_RODC_KDC_Account_1.csv

## 11. Protected Users Group Not Created or Not Used

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

### Summary

Not adding privileged accounts to the Protected Users group can lead to potential credential exposure. The Protected Users group security-hardens privileged user accounts by preventing common attack vectors that lead to these accounts being compromised.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Permission Groups Discovery - T1069 (Credential Access, Privilege Escalation, Defense Evasion)<br>https://attack.mitre.org/techniques/T1069/ |
| **Known Attack Tools** | Mimikatz |
| **References** | Protected Users Security Group<br>Scanning for Active Directory Privileges & Privileged Accounts |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computer MMC.<br>2. Find the Security Group "Protected Users" Group.<br>3. Navigate to "Members" Tab.<br>4. Add all the privileged users to this group. |
| **Affected Objects** | Protected_Users_Group_Not_Created_or_Not_Used_1.csv |

## 12. Weak Default Administrator Account

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Default Administrator accounts are common targets for attackers. Configuring the Password Never Expires option or a weak password can lead to complete domain compromise.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Mimikatz – Cached Credential/Logon Passwords |
| **References** | User Account Control: Admin Approval Mode for the Built-in Administrator account |
| **Manual Remediation Steps** | 1. Configure a password of at least 15 characters in length.<br>2. Regularly change the password of the default Administrator account.<br>3. Use the Administrator account only when absolutely required.<br>4. Do not allow logging on with the Administrator account on workstations and laptops.<br>a. Appendix D - Securing Built-In Administrator Accounts in Active Directory \| Microsoft Docs |
| **Affected Objects** | Weak_Default_Administrator_Account_1.csv |

## 13. Kerberos Delegation on Privileged Accounts

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Privileged accounts configured with unconstrained delegation can lead to attacks like Kerberoasting and Silver Ticket Attack.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets - T1558 (Lateral Movement, Persistence, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1558/ |
| **Known Attack Tools** | Nishang<br>kekeo |
| **References** | Kerberos Unconstrained Delegation (or How Compromise of a Single Server Can Compromise the Domain) |
| **Manual Remediation Steps** | 1. Limit the number of privileged administrators.<br>2. Do not configure delegation on any administrator account.<br>3. Do not register SPN on any privileged account. |
| **Affected Objects** | Kerberos_Delegation_on_Privileged_Accounts_1.csv |

## 14. Accounts with Risky User Account Control Parameters

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Users' accounts configured with incorrect parameters can reduce the security of those accounts, resulting in easy compromise.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Persistence, Privilege Escalation, Defense Evasion)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Mimikatz |
| **References** | UserAccountControl Attribute |
| **Manual Remediation Steps** | 1. Make sure accounts do not have the following values in the User Account Control attribute:<br>a. PASSWD_NOTREQD<br>b. ENCRYPTED_TEXT_PWD_ALLOWED<br>c. DONT_EXPIRE_PASSWORD<br>d. PASSWORD_EXPIRED<br>2. Modify the attribute of the user to NORMAL_ACCOUNT. |
| **Affected Objects** | Accounts_with_Risky_User_Account_Control_Parameters_1.csv |

## 15. Accounts with Never Expiring Passwords

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

If the Password Never Expires flag is enabled on accounts, it decreases the security of those accounts and makes them susceptible to brute force attacks.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Persistence)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Impacket |
| **References** | Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync – Active Directory Security (adsecurity.org) |
| **Manual Remediation Steps** | 1. Identify accounts that have Password Never Expires by checking the User Account Control Value DONT_EXPIRE_PASSWORD.<br>2. Modify the accounts to remove the DONT_EXPIRE_PASSWORD.<br>3. Reset the passwords of these accounts immediately.<br>Note: If the account is used for a service, scheduled task, mapped drive, etc., update the password accordingly where used. |
| **Affected Objects** | Accounts_with_Never_Expiring_Passwords_1.csv |

## 16. Default Administrator Account Hardening

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Without any hardening, the default Administrator account is weak and can be easily compromised.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts: Default Accounts - T1078/001 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/001/ |
| **Known Attack Tools** | Mimikatz |
| **References** | Securing Built-In Administrator Accounts in Active Directory |

**Manual Remediation Steps**

1. Open Active Directory Users and Computers MMC (DSA.MSC)
2. Check the default Administrator account located in the default Users container. Note: For exact location refer to the DN Path in Ranger AD Exposure Affected Objects.
   a. Right-click on the Account and Click Properties.
   b. Navigate to Account tab.
   c. Under Account Options.
      i. Uncheck Password Never Expires if checked.
      ii. Check Account is sensitive and cannot be delegated if unchecked.
      iii. Uncheck Do not required Kerberos pre-authentication if checked.
      iv. Uncheck Store password using reversible encryption If checked.
      v. Uncheck Use Kerberos DES Encryption types for this account If checked.

   d. Under the Delegation tab:
      i. Select Do not trust this user for delegation. Note: If the delegation tab is not available, you can skip this step.
   e. Under Attributes tab:
      i. Scroll down to servicePrincipalName and select it.
      ii. Click Edit.
      iii. Select and remove all the SPNs listed.
      iv. Click OK and Apply.
3. Open Group Policy Management (GPMC.MSC).
   a. Check the policies linked to the domain.
   b. Right-click on the GPO and click Edit.
   c. Navigate to Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
   d. Ensure at-least one GPO has the following settings configured with the Administrator account.
      i. Deny access to this computer from the network
      ii. Deny log on as a batch job
      iii. Deny log on as a service
      iv. Deny log on through Remote Desktop Services

| | |
|---|---|
| **Affected Objects** | Default_Administrator_Account_Hardening_1.csv |

## 17. Domain Controllers with Unwanted Shares and Files Stored

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

This detection looks for any unusual shares on domain controllers. DCs host standard shares like Sysvol and Netlogon, which are needed for group policy. You must investigate any other shares created on a DC along with any files in these shares that are not related to a Group Policy Object.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Network Share Discovery - T1135 (Lateral Movement, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1135/ |
| **Known Attack Tools** | Powersploit |
| **References** | Securing Domain Controllers to Improve Active Directory Security |
| **Manual Remediation Steps** | Review the shares and files identified in the exposure:<br>1. Remove unwanted shares:<br>a. Open Computer Management (Run > compmgmt.msc) on the corresponding domain controller.<br>b. Go to System Tools > Shared Folders > Shares.<br>c. Verify each share.<br>d. If a share is not required, right-click and select Stop Sharing.<br>2. Delete unwanted files:<br>a. In the corresponding domain controller, navigate to the folder identified in the exposure.<br>b. After careful consideration, delete all unwanted files. |
| **Affected Objects** | Domain_Controllers_with_Unwanted_Shares_and_Files_Stored_1.csv |

## 18. Accounts with Pre-Authentication Disabled

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

Reduces the security of the accounts resulting in ASREPROAST attacks.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** High

**MITRE ATT&CK** Steal or Forge Kerberos Tickets: Golden Ticket - T1558/001 (Credential Access, Privilege Escalation)
https://attack.mitre.org/techniques/T1558/001/

**Known Attack Tools** Mimikatz
Rubeus

**References** Roasting AS-REPs

**Manual Remediation Steps**

1. Identify the accounts that do not require pre-authentication by checking the User Account Control value DONT_REQ_PREAUTH.

```
  Get-ADUser -Filter * -Properties * | Where { $_.UserAccountControl -band 0x8000 }
```

2. Modify accounts to remove the DONT_REQ_PREAUTH flag.

```
  Get-ADUser -Filter * -Properties * | Where { $_.UserAccountControl -band 0x8000 }
| Set-ADAccountControl -UseDESKeyOnly $False
```

**Affected Objects** Accounts_with_Pre_Authentication_Disabled_1.csv

## 19. KRBTGT Account with Resource-Based Constrained Delegation (RBCD) Enabled

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

KRBTGT account should not be configured with any delegations.  Any kind of delegation on this account is a security risk for the entire domain.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets - https://attack.mitre.org/techniques/T1558/ (Privilege Escalation)<br>https://attack.mitre.org/techniques/T1558/ |
| **Known Attack Tools** | Rubeus |
| **References** | Attacking Kerberos: Resource Based Constrained Delegation (notsoshant.io)<br>Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory \| Shenanigans Labs<br>Attacking Read-Only Domain Controllers (RODCs) to Own Active Directory |
| **Manual Remediation Steps** | 1. Review the KRBTGT accounts reported by Ranger AD.<br>2. Remove all delegation to these KRBTGT accounts.<br>a. Open Windows PowerShell as a Domain Admin and run the commands below:<br>i. Import-Module ActiveDirectory<br>ii. Set-ADuser -Identity KRBTGT -PrincipalsAllowedToDelegateToAccount $null |
| **Affected Objects** | KRBTGT_Account_with_Resource_Based_Constrained_Delegation_(RBCD)_Enabled_1.csv |

## 20. Computer Accounts in Privileged Groups

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Computer accounts that are a member of a privileged group, if compromised, can then act as a member of that group.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Permission Groups Discovery - T1069 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1069/ |
| **Known Attack Tools** | Bloodhound<br>Mimikatz |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computers MMC (Windows > Run > dsa.msc) and locate the privileged security groups as reported in the Affected Objects -View in Ranger AD.<br>2. Open the Members tab of each of those privileged groups.<br>3. Remove the computer objects as reported in the Affected Objects – View in Ranger AD by selecting the computer names and clicking on Remove.<br>4. Click OK to save the changes.<br>5. Validate the remediation by using the Re-run Assessment option in Ranger AD. |
| **Affected Objects** | Computer_Accounts_in_Privileged_Groups_1.csv |

## 21. Privileged Users with Service Principal Names Defined

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Privileged user accounts with a Service Principal Name (SPN) registered are high-risk for Kerberos-based attacks, which could result in privilege escalation. By adding a SPN to a privileged user account, an attacker can request a Kerberos service ticket for this user which can then be cracked offline (kerberoasting).

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets https://attack.mitre.org/techniques/T1558/003/ (Credential Access)<br>https://attack.mitre.org/techniques/T1558/003/ |
| **Known Attack Tools** | Mimikatz<br>Rubeus |
| **References** | Sneaky Persistence Active Directory Trick #18: Dropping SPNs on Admin Accounts for Later Kerberoasting |
| **Manual Remediation Steps** | 1. Review the accounts reported by Ranger AD for any dependency or if they are used by any application.<br>2. To remove the SPN on a privileged user account:<br>a. Open Active Directory Users and Computers MMC (Start > Run > dsa. msc)<br>b. Find the privileged user account in its OU.<br>c. Right-click and select Properties > Attribute Editor.<br>d. Locate the servicePrincipalName attribute and remove the SPNs.<br>e. Click OK to save. |
| **Affected Objects** | Privileged_Users_with_Service_Principal_Names_Defined_1.csv |

## 22. AdminCount Attribute Set on Standard Users

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Accounts previously part of privileged groups might retain the adminCount value 1, though they are disabled and removed from those privileged groups. Such accounts are treated special and can be easy targets for attackers.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Privilege Escalation - https://attack.mitre.org/tactics/TA0004/ (Privilege Escalation, Persistence)<br>https://attack.mitre.org/tactics/TA0004/ |
| **References** | Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights |

**Manual Remediation Steps**

1. Review the accounts reported by Ranger AD for any dependencies or if they are used by any application.
2. To clear the adminCount value of a user account:
   a. Open the Active Directory Users and Computers MMC (Start > Run > dsa. msc)

   b. Make sure View > Advanced Features is enabled.
   c. For each account reported by Ranger AD:
      1. Open the account's Properties after selecting the user in their OU.
      2. Right-click and select Properties > Attribute Editor.
      3. Locate the adminCount attribute and set its value to <not set>.
      4. Click OK to save the change.
3. Re-enable inheritance.
   a. Open the Active Directory Users and Computers MMC (Start > Run > dsa. msc)

   b. Make sure View > Advanced Features is enabled.
   c. For each account reported by Ranger AD:
      1. Open the account's Properties after selecting the user in their OU.
      2. Right-click the user and and select Properties.
      3. Click on the Security tab > Advanced button.
      4. Click on the Enable inheritance button.
      5. Click OK and then OK again to save the change.

| | |
|---|---|
| **Affected Objects** | AdminCount_Attribute_Set_on_Standard_Users_1.csv |

## 23. Dangerous Access Rights Delegation on Critical Objects

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Standard users with access rights on critical Active Directory objects have been found. These accounts, if exploited, can lead to an Active Directory domain compromise.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Exfiltration, Lateral Movement, Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | Bloodhound |
| **References** | BloodHound 1.3 – The ACL Attack Path Update |
| **Manual Remediation Steps** | Remove all standard and non-privileged users from the critical objects listed in the detection:<br>1. You can view the assigned permissions on an Organizational Unit (OU) in the graphical user interface. You can also use Active Directory Users and Computers console with Advanced Features enabled in the View menu.<br>2. After enabling, right click on OU (for example OU=NewYork), select Properties.<br>3. Now select the Security tab, then click the Advanced button.<br>4. In the Permissions tab (alternate name - "Discretionary Access Control List - DACL") you can see ACE lists<br>5. Select the ACE you want to remove and click Remove |
| **Affected Objects** | Dangerous_Access_Rights_Delegation_on_Critical_Objects_1.csv |

## 24. User Primary Group ID

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Validate that users' primary group has not been modified. Modifying the primary group can lead to privilege escalation.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Account Discovery - T1087 (Discovery)<br>https://attack.mitre.org/techniques/T1087/ |
| **Known Attack Tools** | Bloodhound<br>Mimikatz DCShadow |
| **References** | Primary Group ID Attribute |
| **Manual Remediation Steps** | 1. Open the Active Directory Users and Computers MMC.<br>2. Find the accounts listed in the exposure.<br>3. Navigate to the Member Of tab.<br>4. Change the Primary Group to Domain Users.<br>5. Click Apply and OK.<br>6. Repeat this task on all user accounts listed in the exposure. |
| **Affected Objects** | User_Primary_Group_ID_1.csv |

## 25. Domain with Advanced Audit Policy Disabled

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

Configuring the right auditing level helps granular-level detection of any malicious activity. If auditing is not enabled, then it leads to inappropriate security monitoring.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** Medium

**MITRE ATT&CK** Impair Defenses - T1562 (Defense Evasion)
https://attack.mitre.org/techniques/T1562/

**Known Attack Tools** Mimikatz
LSADump

**References** Advanced Audit Policy Configuration

**Manual Remediation Steps**

1. Logon to a domain controller.
2. Launch Group policy management editor using Server Manager > Tools > Group Policy Management or using the command "GPMC.MSC"
3. Expand Domain Controllers Policy.
4. Right-click on Default Domain Controllers Policy and select Edit.
5. Go to Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.
6. Configure the following policy Settings:
   a. Account Logon
      i. Audit Credential Validation: Success & Failure
      ii. Audit Kerberos Authentication Service: Success & Failure
      iii. Audit Kerberos Service Ticket Operations: Success & Failure
   b. Account Management
      i. Audit Computer Account Management: Success & Failure
      ii. Audit Other Account Management Events: Success & Failure
      iii. Audit Security Group Management: Success & Failure
      iv. Audit User Account Management: Success & Failure
   c. Logon and Logoff
      i. Audit Account Lockout: Success
      ii. Audit Logoff: Success
      iii. Audit Logon: Success & Failure
      iv. Audit Special Logon: Success & Failure
   d. DS Access
      i. Audit Directory Service Access: Success & Failure
      ii. Audit Directory Service Changes: Success & Failure
   e. Detailed Tracking
      i. Audit DPAPI Activity: Success & Failure
      ii. Audit Process Creation: Success & Failure
   f. System
      i. Audit IPsec Driver: Success & Failure
      ii. Audit Security State Change: Success & Failure
      iii. Audit Security System Extension: Success & Failure
      iv. Audit System Integrity: Success & Failure
7. Wait for the Group Policy to update or force an update using the command gpupdate /force
8. Re-run the assessment to validate the exposure is remediated.

**Affected Objects** Domain_with_Advanced_Audit_Policy_Disabled_1.csv

## 26. Regular Users Can Add New Computers into the AD Domain

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

Standard users are allowed to join computers to the Active Directory domain without administrative access.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** Medium

**MITRE ATT&CK** Privilege Escalation - TA0004 (Credential Access, Privilege Escalation, Defense Evasion)
https://attack.mitre.org/tactics/TA0004/

**Known Attack Tools** Mimikatz

**References** Securing Domain Controllers to Improve Active Directory Security

**Manual Remediation Steps**

1. Open Group Policy Management Console (Start > Run > gpmc.msc).
2. Locate Domain Controllers OU and find Default Domain Controllers Policy.

3. Edit Default Domain Controllers Policy.
4. Expand Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
5. From right pane right-click on Add workstations to domain > Properties > Remove Authenticated Users and add the user or group that you are delegating domain joining permissions.
6. Click Apply and then OK to close the Properties window.

**Affected Objects** Regular_Users_Can_Add_New_Computers_into_the_AD_Domain_1.csv

## 27. Disabled Accounts in Privileged Groups

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Accounts that are not used anymore or disabled that are still part of privileged groups may facilitate Silver Ticket attacks.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Persistence)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Mimikatz - Silver Ticket |
| **References** | Scanning for Active Directory Privileges & Privileged Accounts |

**Manual Remediation Steps**

1. Identify the members of the privileged groups below:
   a. Enterprise Admins
   b. Schema Admins
   c. Domain Admins
   d. Group Policy Creator Owners
   e. Administrators
   f. Account Operators
   g. Server Operators
2. Check for disabled accounts in these groups by getting the Properties of each and checking the Members tab.
3. Remove all disabled and unwanted accounts from the groups listed above.

| | |
|---|---|
| **Affected Objects** | Disabled_Accounts_in_Privileged_Groups_1.csv |

## 28. Weak SMB Signing

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

SMBv1 is enabled and SMB traffic is not signed & not encrypted. This can result in man-in-the-middle (MITM) attacks.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** Medium

**MITRE ATT&CK** Network Share Discovery - T1135 (Lateral Movement)
https://attack.mitre.org/techniques/T1135/

**Known Attack Tools** Relayer
SMBetray

**References** SMB Signing not required vulnerability

**Manual Remediation Steps**

1. Log on to a domain controller.
2. Run Group Policy Management Console GPMC.MSC.
3. Open Domain Controller Policy.
4. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Polices > Security Options.
   a. Microsoft network server: Digitally sign communications (always): Enabled

   b. Microsoft network server: Digitally sign communications (if client agrees): Enabled
   c. Microsoft network client: Digitally sign communications (always): Enabled

   d. Microsoft network client: Digitally sign communications (if server agrees): Enabled
5. It's recommended to enable this policy domain wide.
6. Disable SMBv1 by following the steps in the article below:
   How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows | Microsoft Docs

**Affected Objects** Weak_SMB_Signing_1.csv

## 29. Use Legacy Built-in Groups in AD

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

User accounts that are members of the Account Operators and Server Operators groups are potentially overprivileged.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Permission Groups Discovery - T1069 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1069/ |
| **Known Attack Tools** | Mimikatz |
| **References** | 5 ways Attackers Exploit Account Operators :: Security Frameworks by David Rowe (secframe.com)<br>Server Operators - SecOps.cc |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computers MMC (Start > Run > dsa.msc).<br>2. Find Security Groups:<br>a. Account Operators<br>b. Server Operators<br>3. Click on the Members tab.<br>4. Remove all the users from these two groups.<br>Note: We are unable to provide guidance on what access you should delegate for your substitute groups, as that depends on the tasks that those users need access to perform. |
| **Affected Objects** | Use_Legacy_Built_in_Groups_in_AD_1.csv |

## 30. Standard User Accounts as DNS Admins

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Standard users are part of the DNSAdmins group. If these user accounts are compromised, it can lead to an escalation of privileges on domain controllers.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Permission Groups Discovery - T1069 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1069/ |
| **Known Attack Tools** | Powerview<br>Mimikatz |
| **References** | From DNSAdmins to Domain Admin, When DNSAdmins is More than Just DNS Administration<br>Feature, not bug: DNSAdmin to DC compromise in one line<br>Abusing DNSAdmins privilege for escalation in Active Directory |
| **Manual Remediation Steps** | 1. Open the Active Directory Users and Computers MMC (Windows > Run > dsa.msc)<br>2. Locate the DnsAdmins security group.<br>3. Open the Properties dialog of DnsAdmins.  In the Members tab, remove the user accounts mentioned in the Affected Objects.<br>4. Click OK to save the change.<br>5. To validate the remediation, use the "Re-run Assessment" option in Ranger AD. |
| **Affected Objects** | Standard_User_Accounts_as_DNS_Admins_1.csv |

## 31. Guest Account Is Enabled

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Enabling a guest account is a security risk and allows passwordless access to Active Directory.

|  |  |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Valid Accounts: Default Accounts - T1078 (Discovery)<br>https://attack.mitre.org/techniques/T1078/001/ |
| **References** | Securing Active Directory Administrative Groups and Accounts \| Microsoft Docs |

**Manual Remediation Steps**

Disable Guest Accounts in Active Directory
1. Open Active Directory Users and Computers MMC (Start > Run > dsa.msc).

2. Locate the Guest account (By default it is placed in the "Users" organizational unit).

3. Double click on the account and make sure "Account is Disabled" is checked.

Disable Guest Accounts on Windows Workstations and Servers
1. Open the Group Policy Management Console MMC (Start > Run > gpmc.msc).

2. Open Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.
3. Set the policy Accounts: Guest account status to Disabled.
4. Close the GPMC MMC.

**Affected Objects** Guest_Account_Is_Enabled_1.csv

## 32. Kerberos Vulnerability Assessment

**Assessment Result** 1 of 1 Domain(s) Vulnerable

**Summary**

Weak Kerberos policy or misconfigured Kerberos settings reduces the security of the overall Active Directory domain.

**Impacted Domains** LONDON.UK.EUROPE.local

**Severity** Medium

**MITRE ATT&CK** Steal or Forge Kerberos Tickets - T1558 (Credential Access, Privilege Escalation)

https://attack.mitre.org/techniques/T1558/

**Known Attack Tools**

DSInternals
Mimikatz

**References** Network security: Configure encryption types allowed for Kerberos

**Manual Remediation Steps**

1. Check all the user accounts reported by Ranger AD that have the attribute msDS-SupportedEncryptionTypes populated with a value. By default, this attribute is <not set>.
2. Check why the attribute msDS-SupportedEncryptionTypes value is configured with a value that supports DES or CBC encryption types.
3. If there are no application dependency, then set the attribute msDS-SupportedEncryptionTypes value to <not set> or any of the below listed values:

   4(0x4)
   8(0x8)
   12(0xC)
   16(0x10)
   20(0x14)
   24(0x18)
   28(0x1C)
4. The ideal configuration of the Kerberos configuration should be via the group policy linked at the domain level.
5. Below is the Kerberos policy setting to be configured:
   a. Open Group Policy Management Console MMC GPMC.MSC.
   b. Find the Default Domain Policy, right-click and click Edit on the policy.

   c. Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
   d. Find the policy setting Network security: Configure encryption types allowed for Kerberos.
   e. Ensure the settings configured in the policy only allow the following encryption types:
      i. RC4_HMAC_MD5
      ii. AES128_HMAC_SHA1
      iii. AES256_HMAC_SHA1
      iv. Future Encryption Types
   f. Any other encryption types allowed should be evaluated and removed if not required.

**Affected Objects** Kerberos_Vulnerability_Assessment_1.csv

## 33. gMSA Accounts with Passwords Not Changed Recently

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

The passwords of gMSA (group Managed Service Accounts) accounts are changed every 30  or as defined in the settings. Unchanged passwords for a longer duration can indicate a stale object used by an attacker to imitate a gMSA object or it may be that the account is compromised and has been manipulated.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Access Token Manipulation - T1134 (Persistence, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1134/ |
| **Known Attack Tools** | Bloodhound |
| **References** | There's Something About Service Accounts |
| **Manual Remediation Steps** | 1. If an account is still needed but hasn't been changed in over 30 days, create a new gMSA account and assign that to the service, then delete the old one.<br>2. If an account is not used anymore, delete it. |
| **Affected Objects** | gMSA_Accounts_with_Passwords_Not_Changed_Recently_1.csv |

## 34. Multiple Issues in the Password Policy

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

A weak password policy in an Active Directory domain can lead to potential password spray or brute force attacks.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Password Policy Discovery - T1201 (Discovery)<br>https://attack.mitre.org/techniques/T1201/ |
| **Known Attack Tools** | Domain Password Spray |
| **References** | Protecting your organization against password spray attacks<br>Password Policy (Windows 10) - Windows security \| Microsoft Learn |
| **Manual Remediation Steps** | 1. Ensure Domain Password Policy is set at a minimum as below<br>a. MinimumPasswordAge = 1<br>b. MaximumPasswordAge = 60<br>c. MinimumPasswordLength = 8<br>d. PasswordComplexity = 1<br>e. PasswordHistorySize = 12<br>2. Protect all Privileged accounts with Fine Grained Password Policy. To create a new Fine Grained Password Policy, refer to the link in the references section "Create a new fine-grained password policy". |
| **Affected Objects** | Multiple_Issues_in_the_Password_Policy_1.csv |

## 35. Privileged Accounts that Are Inactive

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Inactive privileged accounts are common targets which can be easily compromised.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts - https://attack.mitre.org/techniques/T1078/002/ (Credential Access)<br>https://attack.mitre.org/techniques/T1078/002/ |
| **References** | The Most Common Active Directory Security Issues and What You Can Do to Fix Them – Active Directory Security (adsecurity.org) |
| **Manual Remediation Steps** | 1. Review the accounts reported by Ranger AD.<br>2. Remove the user from the corresponding privileged groups.<br>a. Open Active Directory Users and Computers MMC (Windows > Run > dsa. msc)<br>b. Right-click on the privileged group and select Properties.<br>c. In the Members tab, remove the corresponding user accounts.<br>d. Click OK to save the changes. |
| **Affected Objects** | Privileged_Accounts_that_Are_Inactive_1.csv |

## 36. Accounts Using Pre-Windows 2000 Compatible Access Control

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Pre-Windows 2000 Compatible Access group is a legacy built-in security group. Members of this group have reduced security.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Medium |
| **MITRE ATT&CK** | Permission Groups Discovery - T1069 (Lateral Movement, Defense Evasion)<br>https://attack.mitre.org/techniques/T1069/ |
| **Known Attack Tools** | Impacket |
| **References** | Pre-Windows 2000 Compatible Access Group (microsoft.com) |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computer MMC<br>2. Find the Security Group Pre-Windows 2000 Compatible Access<br>3. Navigate to Members Tab<br>4. Remove all the members from the group, including Authenticated users. |
| **Affected Objects** | Accounts_Using_Pre_Windows_2000_Compatible_Access_Control_1.csv |

## 37. Privileged Users Without Fine-Grained Password Policy

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

A Fine-Grained Password Policy defines a password policy for high-privileged users with better security than the Default Domain Policy.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Low |
| **MITRE ATT&CK** | Password Policy Discovery - T1201 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1201/ |
| **Known Attack Tools** | Mimikatz |
| **References** | Fine-Grained Password Policy |
| **Manual Remediation Steps** | 1. To enable Fine-Grained Password Policies (FGPP), you need to open the Active Directory Administrative Center (ADAC), switch to the Tree View and navigate to the System > Password Settings Container.<br>2. Right-click the Password Settings Container object and select New > Password Settings.<br>3. In the Create Password Policy window, fill all the fields that are appropriate.<br>4. Click the Add button in the Directly Applies To section and select the Global Group you want to target.<br>5. Click OK. |
| **Affected Objects** | Privileged_Users_Without_Fine_Grained_Password_Policy_1.csv |

## 38. Dormant User Accounts

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Accounts which have not been used for a very long time, but are enabled in AD, are a risk.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Low |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Persistence)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Mimikatz - Cached Credential/Logon Passwords |
| **References** | Recommendation - Regularly check for and remove inactive user accounts in Active Directory \| Microsoft Docs |
| **Manual Remediation Steps** | 1. Identify which accounts are idle but active which have not logged on in more than 60 days by checking their LastLoginTimestamp value in Active Directory.<br>2. Identify accounts that haven't changed their password in more than 120 days.<br>3. Disable or delete these accounts if no longer required. |
| **Affected Objects** | Dormant_User_Accounts_1.csv |

## 39. Active Directory Event Logs Not Centralized

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Vulnerable |

**Summary**

Security event logs from Active Directory should be centralized. This helps in timely investigation of malicious or inadvertent events.

| | |
|---|---|
| **Impacted Domains** | LONDON.UK.EUROPE.local |
| **Severity** | Low |
| **MITRE ATT&CK** | Indicator Removal on Host: Clear Windows Event Logs - T1070/001 (Defense Evasion)<br>https://attack.mitre.org/techniques/T1070/001/ |
| **References** | Windows Event Log Management Best Practices for 2022 - DNSstuff |

**Manual Remediation Steps**

1. Configuring the Event Log Collector.
2. Enabling WinRM on the Collector.
  a. Run the command Enable-PSRemoting
    Note: To be sure, you can also run the following command from a remote computer.
    Invoke-Command -ComputerName<COLLECTORHOSTNAME> -ScriptBlock {1}

3. Starting the Subscription Collector Service
  a. On the Collector, open Event Viewer.
  b. Click on Subscriptions.
    Note: The first time you open the Subscriptions option, Windows will ask if you want to start the Windows Event Log Collector Service and configured to start automatically.
  c. Click Yes to accept.
4. Setting up the Forwarders GPO
  a. Follow the instructions in the link on how to set up a GPO
    Create a GPO.
  b. Open CMD and run the command wevtutil gl security.
  c. Copy the values (SDDL) displayed under Channel Access.
  d. Create a GPO.
5. Open Group Policy Management console. (Start > Run > gpmc.msc)
6. Navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding > Configure target subscription manager.

7. Set the value for the target subscription manager to the WinRM endpoint on the collector. You will set the Server to be in the format:
  Server=http://<FQDN of the collector>:5985/wsman/SubscriptionManager/WEC,Refresh=60
8. Next, find the SDDL you copied earlier from running wevtutil gl security and paste it into the setting Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security > Configure log access.

9. Once the GPO is created, either link this GPO to an existing OU containing the Windows servers to send event logs from or create a new OU and link the GPO. Any AD computer account you add to this OU will now set up a subscription to the collector.
10. Setting up a Subscription
  a. On the Collector, open the Windows Event Viewer and right-click on Subscriptions, then create subscription.
  b. Select the Source computer-initiated option and then click Select Computer Groups. This is where you will select which computers you like to forward events from.
  c. Select the events to forward. Opening the query filter, select
    Security to forward events to the collector from the Security event log.

  d. Once the Security log is selected, you can filter down even more by
    entering the event ID, keywords, users, and computers.

e. Click OK to exit from the Query Filter.
f. Click Advanced in the Subscription Properties window. Select Minimize Latency.

11. Verifying the WEF configuration
a. Once WEF is set up, you should now check to see if the forwarders actually, checked in by checking the Source Computers column on the main Subscription's page.
b. You can also check the Event Forwarding Plugin Operational log under Applications and Services on the client to make sure everything is working.

| | |
|---|---|
| **Affected Objects** | Active_Directory_Event_Logs_Not_Centralized_1.csv |

## 40. Unprivileged Users in AdminSDHolder ACL

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

The addition of unprivileged users in the AdminSDHolder ACL would allow an attacker to leave hidden Administrator privileges on the domain, without using recognizable privileged accounts.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets: Golden Ticket - T1558/001 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1558/001/ |
| **References** | Five common questions about AdminSdHolder and SDProp |

**Manual Remediation Steps**

1. Review the users and permission in AdminSDHolder container.
  a. Open the Active Directory Users and Computers MMC.
  b. Click on View and make sure that there is a checkmark next to Advanced Features.
  c. Under the domain name, expand System to find the AdminSDHolder container.

  d. Right-click the AdminSDHolder container and click on Properties.
  e. Click on the Security tab.
  f. Select and remove any non-privileged users/groups found.
  g. Click OK to close the Properties sheet.
2. Monitor users and groups with attribute adminCount = 1 to identify objects with ACLs set by SDProp with the following PowerShell commands:

```
  Get-ADUser -Filter {adminCount -eq 1} -Properties adminCount -ResultSetSize $null
  Get-ADGroup -Filter {adminCount -eq 1} -Properties adminCount -ResultSetSize $null
```

3. Change attribute adminCount to 0 on all non-privileged users/groups found. These should be the same that were found in step 1f.
  a. Search for each of the non-privileged users/groups found in Active Directory Users and Computers. Make a note of the users DN attribute.
  b. Using the DN location, open the Properties sheet on that object in the OU where it resides.
  c. Click on the Attribute Editor tab.
  d. Locate the adminCount attribute. Click on Edit and set the value to 0.

  e. Click OK.
  f. Click on the Security tab.
  g. Click on the Advanced button.
  h. Click on the Enable inheritance button.
  i. Click OK.
  j. Repeat steps a-i for each of the remaining users and/or groups.

## 41. Certificates Exposed to ROCA Vulnerability

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.) |

**Summary**

ROCA (Return of Coopersmith Attack) exploits a weakness in certain cryptographic hardware that utilize Infinion Technologies chip sets and the RSALib library. The vulnerable chip sets/library generate low entropy RSA Public/Private key pairs, allowing an attacker to determine the private key by just knowing the public key.Ranger AD scans Active Directory for any stored certificates and determines if they are ROCA vulnerable.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - T1078 (Defense Evasion, Persistence, Privilege Escalation, Initial Access)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | ROCA-Crack<br>Certify<br>Rubeus |
| **References** | Microsoft Security Advisory on ROCA<br>ROCA: Vulnerable RSA generation (CVE-2017-15361)<br>ROCA Offline Checker Tool<br>ROCA Online Checker Tool |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computers from Administrative Tools or run the command DSA.MSC.<br>2. Make sure that under the View menu Advanced Features is selected.<br>3. Check the Distinguished Name of the user reported in the Exposure by Ranger AD.<br>4. Navigate to the OU/Container and select the User Account.<br>5. Right Click on the User Account and Select Properties.<br>6. Select the Published Certificates tab.<br>7. Select the certificate where the Issued To name matches the Certificate Subject Name identified in the exposure.<br>8. Click Remove and then OK.<br>9. Re-run the assessment to verify that the exposure has been remediated. |

## 42. Privileged Accounts with Non-Standard Owners

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Privileged users must be owned by the Domain Admins group and controlled by AdminSDHolder. Privileged users owned by a standard user could be a misconfiguration or might indicate a persistence technique.

**Severity** Very High

**MITRE ATT&CK** Valid Accounts: Domain Accounts - T1078 (Credential Access)
https://attack.mitre.org/techniques/T1078/002/

**Known Attack Tools** Bloodhound

**Manual Remediation Steps**

1. Review the privileged users reported by Ranger AD.
2. Modify the owner of these privileged user accounts.
  a. Open Active Directory Users and Computer MMC (Windows > Run > DSA.MSC).

  b. Right-click on a privileged account and select Properties.
  c. In the Security tab, click Advanced.
  d. Click Change adjacent to the Owner field, enter Domain Admins, click Check Names, and then click OK.
  e. Click Save to save the changes.

## 43. Default Permissions Changes on Schema Partition

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

An attacker compromising a user with access to the schema partition in a forest can make any changes and propagate those changes in AD. This can potentially weaken the AD security posture.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Access Token Manipulation - T1134 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1134/ |
| **Known Attack Tools** | Bloodhound |
| **References** | Update access to the directory schema must be restricted to appropriate accounts. |

**Manual Remediation Steps**

1. Register the Schema Management DLL by entering the following command:

```
regsvr32 schmmgmt.dll
```

2. Launch Microsoft Management Console by entering the following command:

```
mmc.exe
```

3. Click File > Add/Remove Snap-in.
4. Add Active Directory Schema snap-in and click OK.
5. Select the Active Directory Schema entry in the left-most pane (under Console Root).
6. In the right-most pane, under Actions, click Permissions.
7. Remove non-privileged users from the security object reported by Ranger AD and click OK.

## 44. Anonymous and Unsigned LDAP Allowed

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Allowing Anonymous access to LDAP reduces the security of Directory Services, resulting in open access and reconnaissance attacks by any authenticated user.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | DSInternals<br>Powershell Empire |
| **References** | Anonymous LDAP operations to Active Directory are disabled on domain controllers |
| **Manual Remediation Steps** | 1. Open ADSIEDIT.MSC (Start > Run > ADSIEDIT.MSC).<br>2. Expand the Configuration container > Services > Windows NT.<br>3. Right-click CN=Directory Service and select Properties.<br>4. Double-click the dSHeuristics attribute.<br>5. Set the value to <Not Set> and click OK.<br>6. Close the ADSIEDIT tool. |

## 45. Critical Certificate Templates without Manager Approval

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.) |

**Summary**

Misconfigured permissions on certificate templates allow an attacker to modify or request a certificate that can be used to escalate privileges. If a certificate template performs a critical function, a request workflow requiring manual manager approval should be configured. This puts the certificate request into a pending state until a manager can review the request and determine its legitimacy before approving the request.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Privilege Escalation)<br>https://attack.mitre.org/tactics/TA0004/ |
| **Known Attack Tools** | Certify<br>Rubeus |
| **References** | Certificate Template: Issuance Requirements |

**Manual Remediation Steps**

1. Open the Certificate Authority Manager MMC from Administrative Tools or run the command certsrv.msc.
2. Expand Certificate Authority.
3. Right-click Certificate Templates and click Manage.
4. Select the certificate template listed in the exposure.
5. Right-click on the certificate template and select Properties.
6. Select the Issue Requirements tab.
7. Select CA Certificate Manager Approval.
8. Click Apply and OK.
9. Repeat steps 4 to 8 until all the templates have been corrected.
10. Remove and re-publish the certificate to issue.
    a. To remove the Certificate Template from an issuing CA:
        1) On each issuing CA, right-click each template and click Delete.
    b. To re-publish the Certificate:
        1) On each issuing CA, right-click Certificate Templates and click New.
        2) Click Certificate Template to Issue.
        3) Select all the required Certificate Templates and Click OK.
11. Re-run the assessment to verify that the exposure has been remediated.

## 46. Certificate Templates with Any Purpose

**Assessment Result** 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.)

**Summary**

Misconfigured permissions on certificate templates could allow an attacker to modify or request a certificate to escalate their privileges.

**Severity** Very High

**MITRE ATT&CK** Privilege Escalation - T1078/002 (Defense Evasion, Persistence, Privilege Escalation, Initial Access)
https://attack.mitre.org/techniques/T1078/002/

**Known Attack Tools**

Leghorn
PSPKIAudit
Certify
Certipy
Rubeus
SharpDPAPI
Kekeo
Mimikatz

**References** Enroll for a Certificate

**Manual Remediation Steps**

1. Open the Certificate Authority Manager MMC from Administrative Tools or run the command CERTSRV.MSC.
2. Expand the Certificate Authority.
3. Right-click Certificate Templates and click Manage.
4. Select the Certificate Template listed in the exposure
5. Right-click on the Certificate Template and select Properties.
6. Click on the Security tab.
7. Verify and remove the permissions listed in the exposure by Ranger AD.

8. Click Apply and OK.
9. Repeat from step 4 to 8 until all the exposed templates are corrected.
10. Remove and re-publish the certificate to issue it.
  a. To remove the Certificate Template from an issuing CA:
    i. On each issuing CA, right-click each template and click Delete.
  b. To re-publish the Certificate:
    i. On each issuing CA, right-click Certificate Templates and click New.
    ii. Click Certificate Template to Issue.
    iii. Select all the required Certificate Templates and click OK.
11. Re-run the assessment to verify that the exposure has been remediated.

## 47. Non-Standard Permissions on Agent Certificate Templates

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Misconfigured permission on certificate templates could allow an attacker to modify and then request an enrollment agent certificate. As a certificate enrollment agent, the attacker can escalate their privileges by requesting additional certificates on behalf of other users.

| | |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Privilege Escalation, Lateral Movement)<br>https://attack.mitre.org/tactics/TA0004/ |
| **Known Attack Tools** | Certify<br>Rubeus |
| **References** | Enroll for a Certificate |
| **Manual Remediation Steps** | 1. Open the Certificate Authority Manager MMC from Administrative Tools or run the command CERTSRV.MSC.<br>2. Expand the Certificate Authority.<br>3. Right-click Certificate Templates and click Manage.<br>4. Select the Certificate Template listed in the exposure.<br>5. Right-click on the Certificate Template and select Properties.<br>6. Click on the Security tab.<br>7. Verify and remove the permissions listed in the exposure by Ranger AD.<br><br>8. Click Apply and OK.<br>9. Repeat from step 4 to 8 until all the templates have been corrected.<br>10. Delete the certificate from each CAs published certificates list.<br>11. Re-run the assessment to verify that the exposure has been remediated. |

## 48. Recent Changes to Default Domain Policy or Default Domain Controllers Policy

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Recent changes to the default group policies of the domain have been detected. Changes to domain-wide policies could be a security risk resulting in privileged access to Active Directory.

**Severity** Very High

**MITRE ATT&CK** Domain Policy Modification - T1484 (Lateral Movement)
https://attack.mitre.org/techniques/T1484/

**References** Sneaky Active Directory Persistence #17: Group Policy

**Manual Remediation Steps**

1. Changes to the Default Domain Policy or Default Domain Controllers Policy should be controlled by implementing strict polices or change management and should be tracked.
2. If there are no way to track and understand who made the changes, The best option is to investigate both the policy settings if there are weak security settings enabled, Settings that allow lateral movement or privileged escalation.

3. Possible area of investigation in GPO.
  a. Open GPMC.MSC.
  b. Right Click on Default Domain Policy and Click Edit.
  c. Under Computer Configuration -> Windows settings -> Security Settings Check the following Categories.
    i. Account Policies -> Password Polices
    ii. Local Policies -> Audit Policy, User Rights Assignment, Security Options

    iii. Restricted Groups
    iv. System Services
    v. Public Key Policies
    vi. Software Restriction Policies
    vii. Application Control Policies
    viii. Advanced Audit Policy Configuration
  d. Check if any of settings has been modified, added, or removed.
  e. Right-click on Default Domain Controller Policy and Click Edit.
  f. Under Computer Configuration -> Windows settings -> Security Settings Check the following Categories.
    i. Local Policies -> Audit Policy, User Rights Assignment, Security Options

    ii. Restricted Groups
    iii. System Services
    iv. Public Key Policies
    v. Software Restriction Policies
    vi. Application Control Policies
    vii. Advanced Audit Policy Configuration
4. Alternate approach is if an Active Directory backup is available prior to the change, restore the backup in an isolated environment and compare the settings.

## 49. Dangerous Access Rights that Expose Certificate Authority

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.) |

**Summary**

Misconfigured permissions on certificate authority (CA) related Active Directory containers could allow an attacker to escalate their privileges by enrolling for PKINIT compliant logon certificates.

|  |  |
|---|---|
| **Severity** | Very High |
| **MITRE ATT&CK** | Privilege Escalation - T1078 (Defense Evasion, Persistence, Privilege Escalation, Initial Access)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Leghorn<br>PSPKIAudit<br>Certify<br>Certipy<br>Rubeus<br>SharpDPAPI<br>Kekeo<br>Mimikatz |
| **References** | Securing PKI<br>Certificate Requirements and Enumeration |
| **Manual Remediation Steps** | 1. Open ADSIEDIT.MSC.<br>2. Right Click ADSIEDIT and Select Connect to...<br>3. In the Connection Settings window, under Select a well-known Naming Context select Configuration and Click OK.<br>4. Expand Configuration and navigate to CN=Services -> CN = Public KeyServices.<br><br>5. Check each PKI related Container reported in the exposure.<br>6. Right-click and select Properties, then click the Security tab.<br>7. Review and remove the permissions that are reported in the exposure by Ranger AD.<br>8. Click Apply and then click OK.<br>9. Repeat the steps from 5 to 8 for all the listed containers.<br>10. Additionally, check the altSecurityIdentities attribute on identified user and computer objects and remove the certificate if any listed in the exposure.<br><br>11. Re-run the assessment to verify that the exposure has been remediated. |

## 50. Weak SMBv1 Session Allowed

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

SMBv1 is enabled and SMB traffic is not signed and encrypted. This can result in man-in-the-middle (MITM) attacks.

**Severity** Very High

**MITRE ATT&CK** Network Share Discovery - T1135 (Lateral Movement)
https://attack.mitre.org/techniques/T1135/

**Known Attack Tools** Relayer - SMB Relay Attack Script
SMBetray

**References** SMB Signing not required vulnerability

**Manual Remediation Steps**

1. Enable the following Group Policy at the domain level for all versions of SMB:

   a. Microsoft network server: Digitally sign communications (always)
   b. Microsoft network client: Digitally sign communications (always)

2. Disable SMBv1 and (optionally) enable SMBv2 and/or SMBv3:
   How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows | Microsoft Docs

3. Remove SMBv1 from Windows Server:
   a. On the Server Manager Dashboard of the server where you want to remove SMBv1, under Configure this local server, select Add roles and features.

   b. On the Before you begin page, select Start the Remove Roles and Features Wizard, and then on the following page, select Next.
   c. On the Select destination server page under Server Pool, ensure that the server you want to remove the feature from is selected, and then select Next.

   d. On the Remove server roles page, select Next.
   e. On the Remove features page, clear the check box for SMB 1.0/CIFS File Sharing Support and select Next.
   f. On the Confirm removal selections page, confirm that the feature is listed, and then select Remove.

## 51. Rogue Krbtgt SPN set on regular account

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

The krbtgt account is registered with a unique SPN that is used for password changes. If the same SPN is registered on any standard user account, then the domain is at high risk.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts - T1078 (Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/002/ |
| **Known Attack Tools** | Mimikatz<br>Rubeus |
| **References** | Kerberoasting<br>DS Heuristics |

**Manual Remediation Steps**

1. Review the account(s) reported by Ranger AD.
2. Remove the rogue SPN on the account(s).
   a. Open Active Directory Users and Computers MMC (Start > Run > dsa. msc)

   b. Click the View menu and select Advanced Features
   c. Right-click on the account and select Properties.
   d. In the Attribute Editor tab, edit the servicePrincipalName attribute to
   e. Remove "kadmin/changepw"
   f. Click OK to save the changes.

## 52. Credentials Harvesting from Domain Shares

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Plaintext or reversible passwords in scripts or group policy files, which are stored in the Sysvol or Netlogon shares, are commonly extracted by attackers. An authenticated attacker who successfully exploits this vulnerability could acquire new local or domain administrator credentials and could use them to elevate their privileges.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Unsecured Credentials - T1552 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1552/ |
| **References** | Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486)<br>One more link for Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486) |
| **Manual Remediation Steps** | 1. Review the active Group Policy Preferences identified in the exposure and remove and re-create them.<br>2. Review the Sysvol scripts identified in the exposure and remove the vulnerable passwords.<br>3. Deploy Local Administrator Password Solution (LAPS) for local administrator accounts. |

## 53. Insecure Anonymous Access Settings

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Anonymous access can expose your Active Directory domain to various attacks and result in a loss of sensitive information.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Exfiltration)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | Impacket |
| **References** | Network access: Do not allow anonymous enumeration of SAM accounts and shares<br>Network access: Let Everyone permissions apply to anonymous users<br>Network access: Allow anonymous SID/Name translation |
| **Manual Remediation Steps** | Navigate to Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security Options and disable Anonymous User Configurations by configuring the following GPO Settings:<br>1. Do not allow anonymous enumeration of SAM accounts and shares: Enabled<br>2. Network access: Let Everyone permissions apply to anonymous users: Disabled<br>3. Network access: Allow anonymous SID/Name translation: Disabled |

## 54. Unwanted Privilege for Enterprise Key Admins

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

The Enterprise Key Admins group is granted Full Control on the Domain partition ACL.

**Severity** High

**MITRE ATT&CK** Privilege Escalation - TA0004 (Credential Access, Privilege Escalation)
https://attack.mitre.org/tactics/TA0004/

**Known Attack Tools** Bloodhound

**References** ADPREP Bug in Windows Server 2016

**Manual Remediation Steps**

1. Open Active Directory Users and Computers MMC (DSA.MSC) from a domain controller.
2. Right-click on the Domain Name and click Properties.
3. Select the Security tab and click Advanced.
4. In the list of permission entries, find Enterprise Key Admins. Select and click Remove and click Apply.
5. Click Add and then click Select a Principal.
6. Type Enterprise Key Admins and then click Check Names and Click OK.

7. In the permissions and properties dialog box, only select List contents,

   a. Read All properties
   b. Read msDS-KeyCredentialLink
   c. Write msDS-KeyCredentialLink.
8. Click OK > click Apply > click OK > click OK on the Properties screen.

As an alternate option, you could run the DSACLS command below to achieve the same result:

1. Remove the ACE with Enterprise Key Admins group:
   dsacls "dc=<domain>,dc=<domain>,dc=<domain>" /R "<domain>\Enterprise Key Admins"
2. Add a new ACE with Enterprise Key Admins group only granting Read and Write Property on the ms-DS-Key-Credential-Link attribute:
   dsacls "dc=<domain>,dc=<domain>,dc=<domain>" /G "<domain>\Enterprise Key Admins":RPWP;msDS-KeyCredentialLink /I:T

## 55. Detect LAPS Backdoor Vulnerability

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

The LAPS DLL file is poisoned and creates a backdoor that allows attackers to read the password in plaintext.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts: Local Accounts - T1078/003 (Credential Access, Privilege Escalation, Lateral Movement)<br>https://attack.mitre.org/techniques/T1078/003/ |
| **Known Attack Tools** | AdmPwd |
| **References** | Malicious use of Microsoft LAPS<br>Dump LAPS password in clear text |

**Manual Remediation Steps**

1. Connect to a domain controller via LDAP using LDP.exe.
2. Query the Schema partition for the below object:
CN=ms-MCS-AdmPwd,CN=Schema,CN=configuration,DC=<Domain>,DC=<Name>

3. Check to see if the searchflags attribute value is 776 (0x308)
4. Set the value of searchflags to 904 (0x388)
5. Check and validate the integrity/signature of admpwd.dll.
  a. Validate that the LAPS DLL exists (in PowerShell):
    Get-ChildItem 'c:\program files\LAPS\CSE\Admpwd.dll'
  b. Check the file hash and hashing algorithm of the DLL:
    Get-FileHash 'c:\program files\LAPS\CSE\Admpwd.dll'
  c. Check for digital signature on the DLL:
    Get-AuthenticodeSignature 'c:\program files\LAPS\CSE\Admpwd.dll'
  d. Compare the file hash and digital signature to the file hash and the digital signature of a known good version of the LAPS Admpwd.dll.
  e. If they don’t match, you will need to replace the system Admpwd.dll with the known good copy.

## 56. Verify Sensitive GPO Objects and File Permissions

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Access rights to modify the GPO files in the SYSVOL share should be limited. Unwanted privileges on GPO scripts can be used by an attacker to spread ransomware or escalate privileges.

**Severity** High

**MITRE ATT&CK** Domain Policy Modification - T1484 (Lateral Movement, Privilege Escalation)

https://attack.mitre.org/techniques/T1484/

**References**

Group Policy Storage | Microsoft Docs
Red Team Guide to GPOs

**Manual Remediation Steps**

1. Review the files reported by Ranger AD.
2. Modify the permission on these files:
  a. Right-click on the file and select Properties.
  b. Check the permissions in the Security tab.
  c. Remove any additional permissions other than the following:
    i. Domain Admins (Full Control)
    ii. Enterprise Admis (Full Control)
    iii. Enterprise Domain Controllers (Read & Execute)
    iv. Authenticated Users (Read & Execute)
  v. SYSTEM (Full Control)
    vi. Administrators (Full Control)
    vii. Server Operators (Read & Execute)
  d. Click OK to save the change.

## 57. Dangerous Access Control Rights on Logon Scripts

|  |  |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Access rights to modify the files in the scripts folder of the Sysvol share should be limited. Unwanted privileges on the scripts can be used by an attacker to spread ransomware or escalate privileges.

|  |  |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Domain Policy Modification - T1484 (Lateral Movement, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1484/ |
| **Known Attack Tools** | Bloodhound |
| **References** | Sneaky Active Directory Persistence #17: Group Policy |

**Manual Remediation Steps**

1. Review the files reported by Ranger AD.
2. Modify the permissions on these files.
   a. Right-click on the file and select Properties.
   b. Check the permissions in the Security tab.
   c. Remove any additional permissions other than the following:
      i. Domain Admins (Full Control)
      ii. Enterprise Admis (Full Control)
      iii. Enterprise Domain Controllers (Read & Execute)
      iv. Authenticated Users (Read & Execute)
      v. SYSTEM (Full Control)
      vi. Administrators (Full Control)
      vii. Server Operators (Read & Execute)
   d. Save the changes.

## 58. Standard Users with GMSA Password Read Permission

|  |  |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Misconfiguration of a Group Managed Service Account (GMSA) can result in unauthorized users reading the GMSA password. An attacker can discover users who have permission to read the password and obtain the GMSA's credentials as a hash or clear text password. Once the attackers gain access to the hash, they can perform Pass the Hash (PtH) techniques and move laterally.

|  |  |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | OS Credential Dumping - T1003 (Credential Access, Lateral Movement, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1003/ |
| **Known Attack Tools** | DSInternals<br>Mimikatz<br>GMSAPasswordReader |
| **References** | GMSA Overview<br>Attacking Active Directory Group Managed Service Accounts (GMSAs) |
| **Manual Remediation Steps** | 1. Verify the GMSA Accounts listed in the detection to see who has permission to read the password.<br>2. User accounts and groups should be removed unless required by the applications service.  (Only computer accounts should be allowed to read the password.) |

## 59. Accounts with a Hidden Privileged SID

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

### Summary

Using a SIDHistory attribute indicates that the attacker could be trying to hide a higher privileged group membership, like Domain Admins, in a lower privileged account to conceal a post-exploitation, domain persistent backdoor.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | DeathStar<br>DSInternals<br>SIDCloner<br>Powershell Empire |
| **References** | Sneaky Active Directory Persistence #14: SID History |
| **Manual Remediation Steps** | 1. Review the user objects with SIDHistory and check if the SID is that of a privileged user.<br>2. Clear the SIDHistory attribute of the suspicious user.<br>3. Audit for Following Events ID's<br>a. 4765: SID History was added to an account.<br>b. 4766: An attempt to add SID History to an account failed |

## 60. Dangerous Access Rights that Expose Certificate Templates

**Assessment Result** 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.)

**Summary**

Misconfigured permission on certificate templates allows an attacker to modify or request a certificate and attacker could use the certificate to escalate privileges.

**Severity** High

**MITRE ATT&CK** Privilege Escalation - TA0004 (Privilege Escalation, Credential Access)
https://attack.mitre.org/tactics/TA0004/

**Known Attack Tools** Certify
Rubeus

**References** Planning for certificate template permissions for certificate profiles in Configuration Manager

**Manual Remediation Steps**

1. Open the Certificate Authority Manager MMC from Administrative Tools or run the command CERTSRV.MSC.
2. Expand the Certificate Authority.
3. Right-click Certificate Templates and click Manage.
4. Select Certificate Template listed in the exposure.
5. Right click on the Certificate Template and select Properties.
6. Select the Security tab.
7. Verify and remove the permissions listed in the exposure by Ranger AD.

8. Click Apply and Ok.
9. Repeat from step 4 to 8 until all the templates have been corrected.
10. Remove the template from the Certificate Templates container and re-publish the new certificate template to re-issue certificates.
  a. To publish the certificate, right-click Certificate Templates and click New.

  b. Click Certificate Template to Issue.
  c. Select all the required certificate templates and click OK.
11. Re-run the assessment to check exposure is remediated.

## 61. Rogue Domain Controllers

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

A rogue domain controller is a persistence technique of registering an attacker's computer as a domain controller for the purposes of stealing Active Directory data, like credentials, or modifying the Active Directory database to escalate privileges. This is also known as a DCShadow attack.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Rogue Domain Controller - T1207 (Execution, Defense Evasion, Privilege Escalation, Persistence)<br>https://attack.mitre.org/techniques/T1207/ |
| **Known Attack Tools** | Mimikatz<br>Set-DCShadowPermissions.ps1 |
| **References** | DC Shadow |

**Manual Remediation Steps**

1. Validate that the suspected rogue Domain Controller is not a legitimate DC.

2. If no longer valid or unknown, remove the server object from the Configuration partition:

   a. Open ADSI Edit.
   b. Click on Action.
   c. Click on Connect to....
   d. From the Select a Well Known Naming Context:
      i. Select Configuration.
      ii. Click OK.
   e. Expand CN=Configuration,DC=yourdmain,DC=com
      i. Expand CN=Sites.
      ii. Expand CN="<the site indicated in the exposure>"
         1. Expand CN=Servers.

## 62. Dangerous computer accounts delegation

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

### Summary

Unconstrained delegation can lead to credential theft, and an attacker can gain privileged access to the domain. A computer that is trusted for delegation, stores in the LSASS process the Kerberos credential of a user who has previously authenticated to the computer. If an attacker compromises the computer that is trusted for delegation, they can dump the LSASS stored credentials and use them for lateral movement.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Lateral Movement, Persistence, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | Nishang<br>kekeo<br>Rubeus |
| **References** | Kerberos Unconstrained Delegation (or How Compromise of a Single Server Can Compromise the Domain)<br>Hunting in Active Directory: Unconstrained Delegation & Forests Trusts |
| **Manual Remediation Steps** | 1. Locate all the servers that have delegation configured as identified in the exposure.<br>2. Configure constrained delegation for servers that require delegation by adding only those services for which delegation is allowed.<br>3. Configure all privileged computer accounts to be "Account is sensitive and cannot be delegated". |

## 63. Certificate Authority with Weak Cryptography

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.) |

**Summary**

The National Security Agency recommends setting up a Certificate Authority with SHA256 and longer keys. Weak cryptography like SHA-1, lower-key length is older cryptography, that is susceptible to an attacker compromising the Certificate Authority (CA) by creating an SHA-1 Collision or performing an SHA Attack. This in turn results in the attacker being able to exploit any certificate issued.

|  |  |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Privilege Escalation, Lateral Movement, Persistence)<br>https://attack.mitre.org/tactics/TA0004/ |
| **Known Attack Tools** | Certify<br>Rubeus |
| **References** | Certify |

**Manual Remediation Steps**

1. Renew or issue a new Certificate for the CA.
2. Ensure the issuing CA can issue a certificate satisfying the below conditions:

   a. Key Length is greater than or equal to 2048 bits.
   b. Signature algorithm sha256 or higher.
   c. Hashing algorithm is greater than SHA1.
3. Log onto your Issuing CA and open the Certificate Authority MMC (Certsrv.mmc).

4. Right-click on your Issuing CA > All Tasks > Renew CA Certificate.
5. Click Yes to Stop AD Certificate Services.
6. Press Yes to Generate a new Public/Private Pair.
7. Make sure the computer name is the FQDN of your Issuing CA and select your Root CA as your Parent CA.
8. On the C: drive now, you should have a REQ file. Copy this to your Root CA.

9. Go to your Root CA and open the Certificate Authority MMC (Certsrv.mmc).

10. Right-click your Root CA > All Tasks > Submit New Request.
11. Select the REQ file you just copied onto the Root CA and click OK.
12. Select Pending requests and issue the Certificate Requested.
13. Select Issued certificates.
14. Double-click the certificate issued and go to the Details tab and select Copy to file.
15. Export the certificate as CER file and copy the certificate over to the Issuing CA.

16. Now connect to your Issuing CA, right-click your CA > All Tasks > Install CA Certificate.
17. Press Yes to Stop AD Certificate Services.
18. Change the File Extension from P7B to CER and select your Certificate File.

19. Press Open and your Issuing CA Cert should be renewed.
20. Re-run the assessment to verify that the exposure has been remediated.

## 64. High-Risk Trust Relationships

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Trust across forests and between domains can reduce the security of the Active Directory environment, because they allow access between forests and domains.

**Severity** High

**MITRE ATT&CK** Domain Trust Discovery - T1482 (Lateral Movement, Credential Access, Privilege Escalation, Defense Evasion)
https://attack.mitre.org/techniques/T1482/

**Known Attack Tools**
ADRecon
PowerView
Mimikatz

**References**
Hunting in Active Directory: Unconstrained Delegation & Forests Trusts
Kerberos Unconstrained Delegation (or How Compromise of a Single Server Can Compromise the Domain)

**Manual Remediation Steps** Follow the mitigations steps below depending on the exposure on the trusts.

Warning: Modifying any trust related information can have significant impact on authentication and accessing resources across forests/domains. Please review the links carefully and understand the full impact before making any changes and test this in your environment before making any production changes.

1. Enabling SID Filtering for External Trust
  a. Execute the command below to enable SID Filtering
  b. In this scenario Users are not allowed to use SID History to access resource in the forest.
    i. Command:

```
    netdom trust <TrustingDomainName>/domain:<TrustedDomainName>
/quarantine:Yes /usero:<domainadministratorAcct>
/passwordo:<domainadminpwd>
```

    Note: Replace <> with actual values relevant to your Domain or Trust.

2. Enabling SID Filtering for Forest Trust
  a. Execute the command below to enable SID Filtering
  b. In this scenario Users are not allowed to use SID History to access resource in the forest.
    i. Command:

```
    netdom trust <trustingDomain> /domain:<trustedDomain> /enableSIDhistory:no
/usero:<domainadministratorAcct> /passwordo:<domainadminpwd>
```

    Note: Replace <> with actual values relevant to your Domain or Trust.

3. Modifying a Trust from Domain-Wide Authentication to Selective Authentication

  Execute the command below to change the authentication type to Selective Authentication. Once authentication has been changed to Selective, only resources configured with "Allowed to Authenticate" can be accessed over a trust. Read the articles below and understand the implications before making the change.

    i. Command:

```
    netdom trust <TrustingDomainName>
    /domain:<TrustedDomainName> /SelectiveAUTH:Yes
    /usero:<domainadministratorAcct> /passwordo:<domainadminpwd>
```

    Note: Replace <> with actual values relevant to your Domain or Trust.

4. Modifying a Trust from Two-Way Trust to One-Way Trust
  Once the trust is changed to one-way, the trusted domain can only access resources and not both ways.
Modifying the trust requires the trust to be removed and created again.

Follow the instructions in the reference articles section to remove and create a trust.

## 65. Authentication Certificate Templates Allowed with Custom Subject

**Assessment Result** 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.)

**Summary**

Misconfigured certificate templates allow an attacker to modify or request a certificate, and an attacker could use a certificate generated from it to escalate privileges. If a security template allows the subject name to be provided at certificate request, an attacker could map the subject name to another AD user with the aim of using that certificate to impersonate the user.

**Severity** High

**MITRE ATT&CK** Privilege Escalation - TA0004 (Privilege Escalation, Credential Access, Persistence)

https://attack.mitre.org/tactics/TA0004/

**Known Attack Tools** Certify
Rubeus

**References** Certify, Rubeus

**Manual Remediation Steps**

1. Open the Certificate Authority Manager MMC from Administrative Tools or run the command certsrv.msc.
2. Expand the Certificate Authority.
3. Right-click Certificate Templates and click Manage.
4. Select Certificate Template listed in the Exposure.
5. Right Click on the Certificate Template and select Properties.
6. Click on the Subject Name tab.
7. Select Build from this Active Directory Information and select the appropriate Subject Name Format.
8. Click Apply and OK.
9. Repeat from steps 4 to 8 until all the templates are corrected.
10. Remove and re-publish the certificate templates to re-issue certificates:

    a. To remove the Certificate Template from an issuing CA:
      i. On each issuing CA, right-click each template and click Delete.
    b. To re-publish certificates:
      i. On each issuing CA, right-click Certificate Templates and click New.
      ii. Click Certificate Template to Issue.
      iii. Select all the required Certificate Templates and Click OK.
11. Re-run the assessment to verify that the exposure has been remediated.

## 66. Anonymous NSPI Access Allowed to Active Directory

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Allowing anonymous Name Service Provider Interface (NSPI) access reduces the security of Directory Services resulting in open access and reconnaissance attacks.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | DSInternals<br>Powershell Empire |
| **References** | DANGEROUS DSHEURISTICS PARAMETERS |

**Manual Remediation Steps**

1. Windows > Run > adsiedit.msc.
2. Right-click on ADSI Edit and select Connect to....
3. From the Select a well-known Naming Context list, select Configuration and click OK.
4. Click on and expand Configuration.
5. Click on and expand CN=Configuration,DC=Domain,DC=Name.
6. Similarly, click and expand in the following sequence: Services > Windows NT > Directory Service.
7. Right-click Directory Service and select Properties.
8. Locate the attribute dSHeuristics and edit it to change its value to "<not set>".

9. Save the changes.

## 67. User Accounts with Sensitive Certificates

|  |  |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (ADCS not applicable for child domain.) |

**Summary**

Users configured with sensitive certificates are targeted by attackers to gain privileged access.  Alternatively, attackers use this approach to store a compromised certificate for maintaining persistence in the Active Directory domain.

|  |  |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Persistence - TA0003 (Command and Control, Credential Access, Privilege Escalation, Persistence)<br>https://attack.mitre.org/tactics/TA0003/ |
| **Known Attack Tools** | Certify<br>Mimikatz<br>Rubeus |
| **References** | Certificate Requirements and Enumeration |
| **Manual Remediation Steps** | 1. Open Active Directory Users and Computers from Administrative Tools or run the command DSA.MSC<br>2. Click on the View menu and select Advanced Features<br>3. Check the Distinguished Name of the user reported in the exposure.<br>4. Navigate to the OU/Container and select the user account.<br>5. Right-click on the user account and select Properties.<br>6. Select the Attribute Editor tab.<br>7. Find the attribute userCertificate and click Edit.<br>8. Review and then remove the certificate reported in the exposure.<br>9. Click OK.<br>10. Click Apply and click OK.<br>11. Additionally check the user’s altSecurityIdentities attribute and remove any certificates listed in the exposure.<br>12. Re-run the assessment to verify that the exposure has been remediated |

## 68. Domain Controllers with Passwords Not Changed Recently

|  |  |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Not changing the passwords of Domain Controllers may be an indication that a Domain Controller is not functioning properly, and such Domain Controllers could be easily compromised.

|  |  |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Rogue Domain Controller - T1207 (Privilege Escalation)<br>https://attack.mitre.org/techniques/T1207/ |
| **References** | Use Netdom.exe to reset machine account passwords of a Windows Server domain controller |

**Manual Remediation Steps**

1. Log on to an identified Domain Controller.
2. Open a command prompt and run the command below after you change the domain name in this command. This command resets the password:

```
  netdom resetpwd /s:<server> /ud:<domain\User> /pd:*
```

3. Enter the password when prompted.
4. The following message is displayed if the trust reset is successful.
  “Command completed successfully.”

## 69. DSRM Login Enabled

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (WinRM Exception) |

### Summary

Misconfigured Directory Services Restore Mode (DSRM) settings can lead to full domain compromise. Attackers can gain Domain Admin level access and maintain persistence in the Active Directory Domain using techniques like Pass-the hash or DCSync.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Use Alternate Authentication Material - T1550 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1550/ |
| **Known Attack Tools** | DSInternals<br>Mimikatz |
| **References** | Sneaky Active Directory Persistence Tricks |
| **Manual Remediation Steps** | 1. Open Regedit (Start, Run, Regedit.msc).<br>2. Navigate to the HKLM\System\CurrentControlSet\Control\Lsa\<br>3. Double-click the DsrmAdminLogonBehavior key.<br>4. Set the value to 0, then click OK.<br>5. Close the Regedit tool. |

## 70. Malicious Security Provider

**Assessment Result** 1 of 1 Domain(s) Skipped (WinRM Exception)

**Summary**

Malicious security support providers (SSPs) loaded on a domain controller can result in an attacker compromising a domain, resulting in domain persistence.

**Severity** High

**MITRE ATT&CK** OS Credential Dumping - T1003 (Credential Access, Privilege Escalation)
https://attack.mitre.org/techniques/T1003/

**Known Attack Tools** DSInternals
Mimikatz

**References** Sneaky Active Directory Persistence #12: Malicious Security Support Provider (SSP)

**Manual Remediation Steps**

1. Open Regedit.
2. Navigate to the hive:
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Security Packages\
3. Remove any non-default or non-standard security providers from the list.

Default list of security Providers:
a. Kerberos
b. Msv1_0
c. Schannel
d. Tspkg
e. Pku2u

## 71. Shadow Admins Outside of Privileged Groups

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Privileged users have permissions on AD objects through privileged groups.  If any user has explicit permission on any AD Object, this is an unwanted permission.

**Severity** High

**MITRE ATT&CK** Privilege Escalation - TA0004 (Credential Access, Privilege Escalation)
https://attack.mitre.org/tactics/TA0004/

**Known Attack Tools** Bloodhound

**References** BloodHound 1.3 – The ACL Attack Path Update

**Manual Remediation Steps** Remove all standard and non-privileged users from the Critical Objects listed in the detection.

1. Open Active Directory Users and Computer MMC (Windows > Run > DSA.MSC).

   Note: Ensure that you’ve enabled Advanced Features under View.

2. After enabled, right click on the OU (for example OU=NewYork), select Properties.
3. Now, select the Security tab, then click Advanced button. In the Permissions tab (other name is Discretionary Access Control List - DACL), you can see ACEs lists.

4. Select the ACE (standard user account entry) you want to remove and click Remove.

## 72. Skeleton Key Vulnerability Assessment

**Assessment Result** 1 of 1 Domain(s) Skipped (WinRM Exception)

**Summary**

Adversaries may patch the authentication process on a domain controller to bypass the typical authentication mechanisms and enable login to all user accounts with a common password. The normal user password is not affected and can still be used.

**Severity** High

**MITRE ATT&CK** Modify Authentication Process: Domain Controller Authentication - T1556/001 (Credential Access, Defense Evasion)
https://attack.mitre.org/techniques/T1556/001/

**Known Attack Tools** Mimikatz

**Manual Remediation Steps**

1. Reduce the number of Domain Admins and Administrators.
2. Enable LSA protection

To enable LSA protection using Group Policy:

a. Open the Group Policy Management Console (GPMC).
b. Create a new GPO that is linked at the domain level or that is linked to the organizational unit that contains your computer accounts. Alternatively, you can select a GPO that is already deployed.
c. Right-click the GPO, then click Edit to open the Group Policy Management Console.
d. Expand Computer Configuration.
e. Expand Preferences.
f. Expand Windows Settings.
g. Right-click Registry, point to New, then click Registry Item.
h. The New Registry Properties dialog box appears.
i. In the Hive list, expand HKEY_LOCAL_MACHINE.
j. In the Key Path list, browse to: SYSTEM\CurrentControlSet\Control\Lsa
k. In the Value name box, type: RunAsPPL
l. In the Value type box, click: REG_DWORD
m. In the Value data box, type: 00000001
n. Click OK.

## 73. Domain Controllers with Certificates Deployed through Group Policy

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Insecure certificates deployed to Domain Controllers via Group Policy can reduce the security of Domain Controllers, resulting in a domain compromise.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Persistence - TA0003 (Privilege Escalation, Persistence)<br>https://attack.mitre.org/tactics/TA0003/ |
| **Known Attack Tools** | Certify<br>Rubeus |
| **References** | Active Directory Certificate Services a big security blindspot \| CSO Online |

**Manual Remediation Steps**

1. Open GPMC.MSC on a Domain Controller.
2. Identify the GPO detected by Ranger AD, right-click and select Edit.
3. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.
4. Locate the container where the certificate has been deployed.
5. Identify the certificate by the serial number provided by Ranger AD.
6. Remove the certificate from the policy if not required.
7. Repeat this step until all certificates are removed.
8. Wait for the GPO to apply on the Domain Controller or force the Group Policy update on the Domain Controller by running the command "gpupdate /force".

9. Re-run the assessment to verify that the exposure has been remediated.

## 74. Service Accounts that Have Shadow Admin Privileges

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Service Accounts are used for application authentication and do not require permission on AD objects, if such accounts are compromised it can lead to complete domain takeover.

| | |
|---|---|
| **Severity** | High |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/tactics/TA0004/ |
| **Known Attack Tools** | Bloodhound |
| **References** | BloodHound 1.3 – The ACL Attack Path Update |

**Manual Remediation Steps**

Remove all permission for services accounts from the critical objects listed in the detection.

1. We can view the assigned permissions on an Organizational Unit (OU) in the graphical user interface, also we can use the Active Directory Users and Computers console, but we must enable Advanced Features under View.

2. After enabled, right-click on an OU (for example OU=NewYork) and select Properties.
3. Select the Security tab, then click the Advanced button.
   a. In Permissions tab (other name is Discretionary Access Control List - DACL), you can see ACEs list.
4. Select the ACE you want remove and click Remove.

## 75. Use of Explicit Denied Access on Containers

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Organizational Units or Containers in Active Directory where explicit deny is defined can prevent security settings from being applied.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Impair Defenses: Disable or Modify Tools - T1562 (Defense Evasion, Persistence)<br>https://attack.mitre.org/techniques/T1562/ |
| **Known Attack Tools** | Bloodhound |
| **References** | Hiding Active Directory Objects and Attributes |
| **Manual Remediation Steps** | 1. Open the Active Directory Users and Computers MMC.<br>2. Find the OU listed in the detection.<br>3. Right-click on the OU and go to the Security tab.<br>4. Delete the Deny permission defined on the OU.<br>5. Click Apply and OK.<br>6. Repeat the task on all OUs and Containers listed in the exposure. |

## 76. Domain Using a Dangerous Backward Compatibility Configuration

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Misconfigured attributes on dsHeuristics impacts the security of the Active Directory.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Credential Access, Privilege Escalation, Defense Evasion)<br>https://attack.mitre.org/tactics/TA0004/ |
| **References** | AD Permissions: The AdminSDHolder Mechanism |
| **Manual Remediation Steps** | 1. Open ADSIEDIT.MSC.<br>2. Connect to the Configuration Partition.<br>3. Navigate to CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<Domain>,DC=<name>.<br>4. Right-click on Directory Service and select Properties.<br>5. Find dSHeuristics and set it <Not Set>. |

## 77. Domains Have an Outdated Functional Level

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Domains with an outdated or low functional level reduces the security of the domain.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Defense Evasion - TA0005 (Defense Evasion)<br>https://attack.mitre.org/tactics/TA0005/ |
| **Known Attack Tools** | PowerShell Empire<br>Metasploit |
| **References** | How to raise Active Directory domain and forest functional levels |
| **Manual Remediation Steps** | 1. Raise the domain functional level:<br>Raise the domain functional level: Active Directory \| Microsoft Docs<br>2. Raise the forest functional level:<br>Raise the forest functional level: Active Directory \| Microsoft Docs |

## 78. Non-Use of Managed Service Accounts

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Managed Service Accounts protect your Active Directory from Kerberoasting attacks, of which regular service accounts are vulnerable.

**Severity** Medium

**MITRE ATT&CK** Steal or Forge Kerberos Tickets: Golden Ticket - T1558/001 (Persistence)
https://attack.mitre.org/techniques/T1558/001/

**Known Attack Tools** Patator
Kerberoast

**References** There's Something About Service Accounts
Group Managed Service Accounts Overview

**Manual Remediation Steps**

1. Determine which applications use service accounts.
2. Check if those applications are compatible with Managed Service Accounts (MSA) or Group Managed Service Accounts (GMSA); you may need to talk to the application vendor.
3. If your application is standalone and only on a single server, use a MSA. If your application is clustered and multi node, then use a GMSA account.

4. To use a Group Managed Service Account please review below given link

Getting Started with GMSAs

5. Additionally, the Key Distribution Services KDS Root Key needs to be created, using the following command:

```
Add-KdsRootKey -EffectiveImmediately
```

6. To create a new Managed Service Account, follow the detailed use case and scenario given below matching your business requirements.
use case and scenario
7. To create a Group Managed Service Account, follow the use case and appropriate deployment model given below.
use case and appropriate deployment model
8. Remove the Service Principal Name (SPN) from a regular service account that is being replaced by a managed service account.
9. Disable / delete the regular service accounts that are no longer used. Note: Test the applications thoroughly in a test environment before moving to production.

## 79. LAPS Solution Not Enabled

|  |  |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

The Microsoft Local Administrator Password Solution (LAPS) helps protect local Administrator accounts by regularly changing the password to random values for each machine in the organization.

|  |  |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Valid Accounts - T1078 (Persistence, Lateral Movement, Privilege Escalation)<br>https://attack.mitre.org/techniques/T1078/ |
| **Known Attack Tools** | Psexec<br>Priv2Admin |
| **References** | Local Administrator Password Solution (LAPS) Implementation Hints and Security Nerd Commentary |
| **Manual Remediation Steps** | Enable the LAPS Solution:<br>1. Follow these Microsoft guidelines for deploying LAPS:<br>Step by Step How to Deploy LAPS |

## 80. Non-canonical ACE on Objects

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Active Directory objects with a non-canonical ACE, that is, with Access Control Entries (ACEs) listed in a non-standard way of grants before denies, can be unexpectedly accessed.

**Severity** Medium

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

**Known Attack Tools** PowerShell Empire

**References** Why does canonical order for ACEs put deny ACEs ahead of allow ACEs?

**Manual Remediation Steps** 1. The ACE listed in the Ranger AD's detection needs to be verified on the AD object.

2. Remove the ACE and add it again.
3. Ensure the ACE is listed in the correct order.  Deny ACEs should be listed before the granting ACEs.

## 81. Trust Accounts Passwords Have Not Changed

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

Trust passwords that haven’t been changed in the past year are a problem, especially since they should automatically be changed around every 30 days.  Trust accounts should be protected equally as privileged users accounts, as they allow authentication across trusts. This could be an indication of an orphaned trust.

**Severity** Medium

**MITRE ATT&CK** Valid Accounts - T1078 (Initial Access)
https://attack.mitre.org/techniques/T1078/

**References** AD Forest Recovery - Resetting a trust password | Microsoft Docs

**Manual Remediation Steps**

1. Log on to the Domain Controller

2. Run the following command in command prompt after you modify the example domain name

   a. netdom trust /d:Northamerica USA-Chicago /Ud:Northamerica\admin /reset

   Note: In the above example the trust password is reset for the one-way trust between Northamerica and USA-Chicago.

3. Enter the password when prompted.

4. Following message is displayed if the password reset is successful "Trust between Northamerica and USA-Chicago" been successfully reset and verified. Command completed successfully.

## 82. Organizational Units Are Blocking Applying Group Policy

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Organizational units are not applying the required security policy.  It is being prevented due to one or more deny permissions set on it.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Domain Policy Modification - T1484 (Persistence)<br>https://attack.mitre.org/techniques/T1484/ |
| **Known Attack Tools** | Responder |
| **References** | 10 Common Problems Causing Group Policy To Not Apply - TechNet Articles - United States (English) - TechNet Wiki (microsoft.com) |
| **Manual Remediation Steps** | 1. For the OUs reported by Ranger AD, review the ACLs configured with the Deny permission for the SYSTEM account, Authenticated Users, or Domain Users.<br>2. Remove any accounts or groups with deny permission from the ACLs. |

## 83. Computer Account Takeover Through Kerberos Resource-Based Constrained Delegation (RBCD)

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Detects if Resource Based Constrained Delegation (RBCD) is configured that could allow takeover of a computer account.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Steal or Forge Kerberos Tickets - https://attack.mitre.org/techniques/T1558/ (Privilege Escalation)<br>https://attack.mitre.org/techniques/T1558/ |
| **Known Attack Tools** | Rubeus |
| **References** | Wagging the Dog: Abusing Resource-Based Constrained Delegation to Attack Active Directory<br>Kerberos Resource-based Constrained Delegation: Computer Object Takeover<br>Kerberos Constrained Delegation Overview<br>Revisiting Constrained Delegation<br>Attacking Kerberos Resourced Based Constrained Delegation |
| **Manual Remediation Steps** | 1. Review the computer accounts reported by Ranger AD.<br>2. Remove the delegation on these accounts by running Windows PowerShell as an administrator and the issuing these commands:<br>a. Import-Module ActiveDirectory<br>b. Set-ADComputer -Identity <computer name> -PrincipalsAllowedToDelegateToAccount $null |

## 84. Group Policy Objects - Unlinked, Disabled, or Orphaned

**Assessment Result** 0 of 1 Domain(s) Vulnerable

### Summary

Group Policy objects which are unlinked, disabled, or orphaned could lead to administrative issues. Also, attackers might modify these GPOs to bypass or evade detection.

**Severity** Medium

**MITRE ATT&CK** Domain Policy Modification - T1484 (Defense Evasion)
https://attack.mitre.org/techniques/T1484/

**Manual Remediation Steps**

1. Open Group Policy Management Console (GPMC.MSC).
2. Review the GPOs reported by Ranger AD.
3. Check with others to see if the GPO is unlinked or disabled for a business reason.

4. If the GPO is no longer required, delete the link of the GPO from the respective OU and then delete the GPO itself.

## 85. Computers Accounts with Their Password Not Changed Recently

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

The passwords for computer accounts are changed every 30 days or as defined by a GPO policy. Unchanged passwords using a longer change duration may indicate that the computer object is being used by attackers to imitate a valid computer object or the secure channel of the computer is broken to tamper evidence.

**Severity** Medium

**MITRE ATT&CK** Valid Accounts: Domain Accounts - T1078 (Credential Access)
https://attack.mitre.org/techniques/T1078/002/

**Known Attack Tools** Powerview

**References** Secure Channel Explained

**Manual Remediation Steps**

1. Check the list of computer accounts reported by Ranger AD.
2. Verify if each of these computer accounts are objects of real systems.
3. Connect to each machine and validate if the secure channel is proper using the following command:

```
nltest /sc_verify:<domain name>
Example: nltest /sc_verify:acme.com
```

If "Access denied" is returned, disjoin, and rejoin the computer to the domain.

4. Refer to the following article to join a computer to a domain:
Join a Computer to a Domain

## 86. Check for WDigest

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domain(s) Skipped (WinRM Exception) |

**Summary**

Domains with WDigest enabled allows an attacker to read credentials from memory in cleartext.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | OS Credential Dumping - T1003 (Credential Access)<br>https://attack.mitre.org/techniques/T1003/ |
| **Known Attack Tools** | Mimikatz |
| **References** | An Overview of KB2871997<br>Red Team/Blue Team Practice on Wdigest |

**Manual Remediation Steps**

1. Install the security fix as below:
   https://support.microsoft.com/en-in/help/2871997

2. After you install this security update, you can control how installed WDigest credentials can be saved by using a registry setting. To prevent WDigest credentials from being stored in memory, a Group Policy setting can be applied to the UseLogonCredential registry entry under the following

subkey:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest

3. If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.

## 87. Servers with Passwords Unchanged for More Than 60 Days

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

The passwords of server accounts are changed every 30 days or as defined by the policy. Unchanged passwords for a longer duration can indicate it is a server being used by attackers to imitate a computer object or the secure channel of the server is broken to tamper evidence.

| | |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Valid Accounts: Domain Accounts - T1078 (Credential Access)<br>https://attack.mitre.org/techniques/T1078/002/ |
| **Known Attack Tools** | Powerview |
| **References** | Secure Channel Explained |

**Manual Remediation Steps**

1. Check the list of Server accounts reported by Ranger AD.
2. Verify if each of these computer accounts are objects of real systems. If the computers are no longer needed, they can be safely deleted. Prior to deleting, make sure to reset the computer’s local administrator password so you can still login after removal.
3. Connect to the machine and validate if the secure channel is proper using the following command:

```
nltest /sc_verify:<domain name>
Example: nltest /sc_verify:acme.com
```

4. If Access denied is returned, disjoin and rejoin the computer to the domain.

5. Refer to the following article to join a computer to a domain:
   Join a Computer to a Domain

## 88. Service Accounts that Are Inactive for More Than 60 Days

|  |  |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Inactive service accounts are common targets, which can be easily compromised.

|  |  |
|---|---|
| **Severity** | Medium |
| **MITRE ATT&CK** | Privilege Escalation - TA0004 (Credential Access, Privilege Escalation)<br>https://attack.mitre.org/tactics/TA0004/ |
| **Known Attack Tools** | Mimikatz - Cached Credential/Logon Passwords |
| **References** | How to Manage and Secure Service Accounts: Best Practices \| BeyondTrust |

**Manual Remediation Steps**

1. Verify the service accounts detected by the exposure.
2. Check for the service accounts that have not logged in for more than 60 days by checking their Lastlogintimetimestamp attribute in Active Directory.

3. Check for the accounts that have not changed the password for more than 60 days.

4. Disable or delete these accounts if no longer required.

## 89. Enable the Active Directory Recycle Bin

**Assessment Result** 0 of 1 Domain(s) Vulnerable

**Summary**

User, Computer, Service Accounts, or any object in AD cannot be recovered if the Active Directory Recycle Bin is not enabled.

**Severity** Low

**MITRE ATT&CK** Inhibit System Recovery - T1490 (Impact)
https://attack.mitre.org/techniques/T1490/

**References** The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting

**Manual Remediation Steps**

1. Open Server Manager.
2. Open the Active Directory Administrative Center. From the Server Manager go to tools and select Active Directory Administrative Center.
3. Within the Active Directory Administrative Center click on your local domain then click on Enable Recycle Bin.
4. Click OK to confirm.
5. Click OK on the next pop-up.

## 90. Computers Running an Obsolete OS

| | |
|---|---|
| **Assessment Result** | 0 of 1 Domain(s) Vulnerable |

**Summary**

Legacy operating systems are vulnerable and don't have enhanced security features. Windows Server 2008 R2, Windows 7, and earlier are considered legacy.

| | |
|---|---|
| **Severity** | Low |
| **MITRE ATT&CK** | System Information Discovery - T1082 (Discovery, Lateral Movement, Defense Evasion)<br>https://attack.mitre.org/techniques/T1082/ |
| **Known Attack Tools** | Metasploit |
| **References** | How Forgotten Legacy Systems Could Be Your Downfall - Infosecurity Magazine (infosecurity-magazine.com) |
| **Manual Remediation Steps** | 1. Decommission the older operating systems identified by the detections. |