Attivo CLOUD

# ADAssessor Sample Report

Virtually all sophisticated attackers whether nation states or criminal syndicates, know the strategic value of Active Directory to an organization. Advanced adversaries can gather hugely valuable situational awareness from AD, and can also use misconfigurations, vulnerabilities and incorrect account permissions to gain advantages during their campaigns.

ADAssessor from Attivo offers organizations a quick and easy way to gain insights into Active Directory and quickly remediate problematic configurations, permissions, delegations and vulnerabilities.

ADAssessor presents hygiene based observations about Active Directory alongside real-time visibility of attacker activity on or against the Domain Controllers. With 70 hygiene detections and 11 real-time detections, it offers the fastest path to value when securing Active Directory.

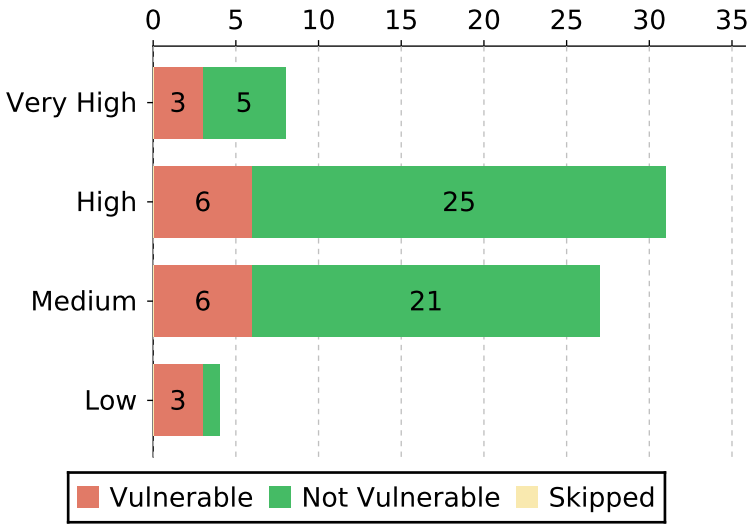
This is a summary report, designed to show the ADAssessor intelligence derived from demonstration environments at Attivo. The top five vulnerabilities are shown in this example report. For a full assessment of your Active Directory, please contact your partner representative.

# Table of Contents

# ADAssessor Executive Summary

This section provides the data for the assessment in summarized form

**labs.sedemo.local**
**Health 75%**
**Low Risk**




| Severity | All | Vulnerable | Not-Vulnerable | Skipped |
|---|---|---|---|---|
| Very High | 8 | 3 | 5 | 0 |
| High | 31 | 6 | 25 | 0 |
| Medium | 27 | 6 | 21 | 0 |
| Low | 4 | 3 | 1 | 0 |
| Total | 70 | 18 | 52 | 0 |

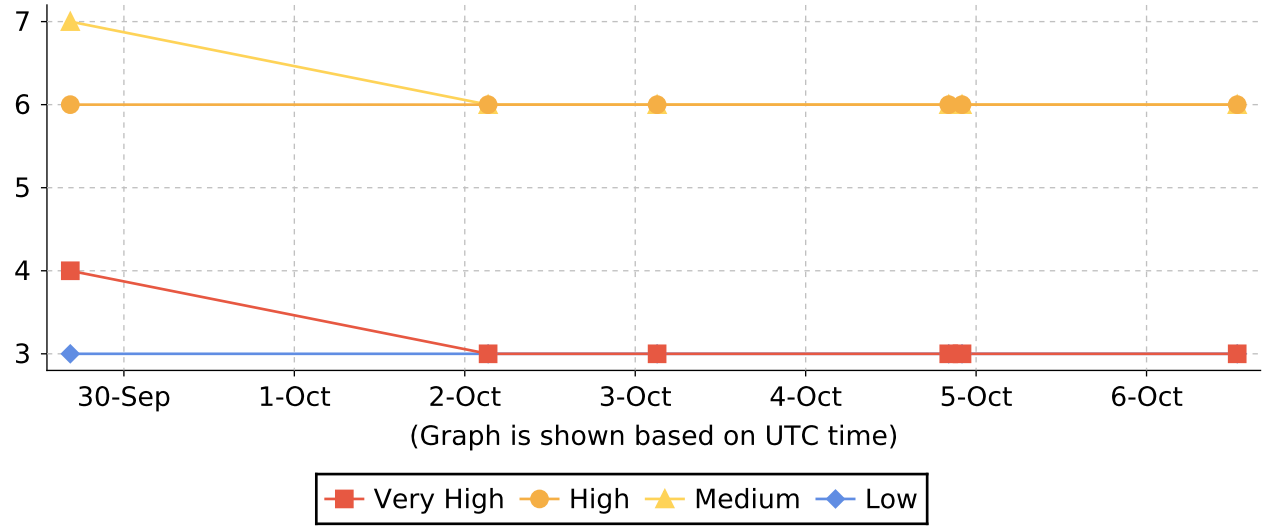
## Mitre ATT&CK

| Persistence | Exfiltration | Execution | Lateral Movement | NA | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Initital Access |
|---|---|---|---|---|---|---|---|---|---|
| 21 | 2 | 1 | 10 | 1 | 43 | 14 | 32 | 4 | 1 |

## Most Vulnerable Assessments

| Assessment Name | Affected Objects count |
|---|---|
| Unusual Accounts with Replication Permissions (DCSync) | 1 |
| Default permissions changes on Domain Partition | 3 |
| Weak KRBTGT Account - Golden Ticket | 1 |
| Weak default Administrator Account | 2 |
| Default Administrator account hardening | 1 |

## ADAssessor Tests



## Assessor Details

### 1. Weak KRBTGT Account - Golden Ticket

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domains Vulnerable |

**Summary**

An attacker can obtain domain dominance by attempting a Golden Ticket Attack or by querying for privileged accounts or privileged accounts with delegation.

| | |
|---|---|
| **Impacted Domains** | labs.sedemo.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** | Reset the krbtgt account password/keys<br>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password<br>Detecting Forged Kerberos Ticket (Golden Ticket & Silver Ticket) Use in Active Directory<br>https://adsecurity.org/?p=1515<br>KRBTGT Account Password Reset Scripts now available for customers<br>https://github.com/microsoft/New-KrbtgtKeys.ps1 |
| **Mitigation Steps** | 1. Prevent Domain Administrators from logging on to any computer other than the domain controllers.<br>2. Reset the KRBTGT account at least once a year.<br>3. Review and filter Security Event ID 4624 and 4672 |
| **Affected Objects** | Weak_KRBTGT_Account_-_Golden_Ticket.csv |

## 2. Default permissions changes on Domain Partition

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domains Vulnerable |

**Summary**

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

| | |
|---|---|
| **Impacted Domains** | labs.sedemo.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 â€“ Attacks and Defense<br>https://techcommunity.microsoft.com/t5/security-compliance-identity/active-directory-access-control-list-8211-attacks-and-defense/ba-p/250315 |
| **Mitigation Steps** | 1. Verify the users & permissions reported by ADAssessor for the domain partition.<br>2. Check the security descriptor on Active Directory.<br>3. Open Active Directory Users and Computers MMC (Windows > Run > dsa.msc).<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 ADAssessor" |
| **Affected Objects** | Default_permissions_changes_on_Domain_Partition.csv |

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

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domains Vulnerable |

**Summary**

Full control to the complete Active Directory Domain Database

| | |
|---|---|
| **Impacted Domains** | labs.sedemo.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 - DCSync |
| **References** | How to grant the Replicating Directory Changes permission for the Microsoft Metadirectory Services ADMA service account<br>https://support.microsoft.com/en-us/help/303972/how-to-grant-the-replicating-directory-changes-permission-for-the-micr |
| **Mitigation Steps** | 1. Open the Active Directory Users and Computers snap-in On the View menu. Click "Advanced Features"<br>2. Right-click the domain object, such as "company.com", and then click Properties.<br>3. Select the desired user account, and then click Remove.<br>4. Alternatively you could select the account and Deselect "Replicating Directory Changes", "Replicating Directory Changes All", "Replicating Directory Changes Filtered set" check box from the list.<br>5. Click Apply, and then click OK.<br>6. Close the snap-in. |
| **Affected Objects** | Unusual_Accounts_with_Replication_Permissions_(DCSync).csv |

## 4. Lack of recent Active Directory Backup

**Assessment Result** 1 of 1 Domains Vulnerable

**Summary**

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

**Impacted Domains** labs.sedemo.local

**Severity** High

**MITRE ATT&CK** Encrypt Sensitive Information - https://attack.mitre.org/mitigations/M1041/ (Defense Evasion)
https://attack.mitre.org/mitigations/M1041/

**References** AD Forest Recovery - Backing up a full server
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-backing-up-a-full-server

Backing Up and Restoring an Active Directory Server
https://docs.microsoft.com/en-us/windows/win32/ad/backing-up-and-restoring-an-active-directory-server

**Mitigation Steps**

1. To perform a backup with Windows Server Backup

Open Server Manager > Tools > Windows Server Backup.

2. In Windows Server 2008 R2 and Windows Server 2008.

Go to Start > Administrative Tools > Windows Server Backup and follow a similar procedure as below.

3. Click Local Backup.

4. 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.

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

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

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

8. Specify the storage location for the backup.

9. On the confirmation screen, click Backup.

**Affected Objects** Lack_of_recent_Active_Directory_Backup.csv

## 5. Protected Users group not created or not used

| | |
|---|---|
| **Assessment Result** | 1 of 1 Domains Vulnerable |

**Summary**

Not adding privileged accounts to the Protected Users group can lead to potential Credential Exposure.

| | |
|---|---|
| **Impacted Domains** | labs.sedemo.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>http://go.microsoft.com/fwlink/?LinkId=298939<br>Scanning for Active Directory Privileges & Privileged Accounts<br>https://adsecurity.org/?p=3658 |
| **Mitigation 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.csv |