



Tenable Cyber Exposure Study - Identity and Access Management

Last Revised: February 28, 2024



Table of Contents

Overview	3
How Tenable Can Help	4
Tenable Vulnerability Management	5
Active Directory Settings	6
Domain Controllers	8
Group and File Permissions	11
Cryptographic Controls	13
Tenable Identity Exposure	16
Identifying Exposure	19
Identification	20
Users and Groups	22
Service and Default Accounts	23
User Access Controls	25
User Accounts	26
Privileged Accounts	28
Dormant Accounts	29
Active Directory Settings	30
Domain Controllers	32
Group and File Permissions	35
Cryptographic Controls	37
Maintenance	40
Learn More	43



Overview

Compromised identities are a key aspect of most successful cybersecurity data breaches. Identification, authentication, and authorization controls, also known as provision and deprovision processes, must be aligned with business requirements and maintained appropriately, as user roles evolve over time. Very often, organizations have outdated user accounts because of ineffective deprovisioning processes. Two primary challenges organizations face in achieving basic cyber hygiene are limited budgets and a lack of staff with security expertise.

Many exploits require local access to be executed. A common attack path is to trick a user with legitimate local access into executing malware code through phishing attacks or other fraudulent means. Vulnerabilities that an organization may consider to be low risk pose a much higher risk through such attacks.

Microsoft Active Directory servers – a key component of many networks – contain data about users, computers, applications, and shared resources, among other information. These identity management servers are a favorite target for attackers.



How Tenable Can Help


Leveraging Tenable Security Center (formerly Tenable.sc), Tenable Vulnerability Management (formerly Tenable.io), and Tenable Identity Exposure (formerly Tenable.ad) solutions enables organizations to close attack paths, making the organization a more difficult target to attack. Tenable solutions provide organizations the data needed to identify and evaluate exposures in the environment. Tenable Security Center is an on-premises solution, powered by Nessus, that provides a risk-based view of the organization's IT, security and compliance posture. Tenable Vulnerability Management (formerly Tenable.io) provides similar functions in a cloud-based solution. Tenable Identity Exposure is a fast, agent-less Active Directory security solution that helps organizations analyze their complex Active Directory environment, predict what matters most to reduce risk, and eliminate attack paths before they can be exploited.



Tenable Vulnerability Management

Tenable Security Center and Tenable Vulnerability Management enable security teams to focus on the vulnerabilities and assets that matter most to the organization, while deprioritizing the vulnerabilities that attackers are unlikely to ever exploit.

As information about new vulnerabilities is discovered and released into the public domain, Tenable Research designs [plugins](#) to detect and evaluate the risks posed by these vulnerabilities. The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of security exposures. Tenable Research has published many plugins which detect account issues, as shown below:

 **Plugins** Settings ▾

[Plugins Pipeline](#)
[Newest](#)
[Updated](#)
[Search](#)
[Nessus Families](#)
[WAS Families](#)
[NNM Families](#)
[LCE Families](#)
[Tenable.ot Families](#)
[About Plugin Families](#)
[Nessus Release Notes](#)
[Audits](#)
[Tenable.cs Policies](#)
[Tenable.ad Indicators](#)
[Attack Path Techniques](#)

[Plugins / Search](#)

Plugins Search

Add Filter ▾Relevance ▾

<< PreviousPage 1 of 54 • 2683 TotalNext >>

ID	Name	Product	Family	Published	Updated	Severity
108903	Debian DLA-1342-1 : Idap-account-manager security update	Nessus	Debian Local Security Checks	4/10/2018	1/11/2021	MEDIUM
25798	Yahoo! Widgets YDP YDPCTL.YDPControl.1 ActiveX (YDPCTL.dll) Buffer Overflow	Nessus	Windows	7/27/2007	11/15/2018	HIGH
162762	Debian DSA-5177-1 : Idap-account-manager - security update	Nessus	Debian Local Security Checks	7/6/2022	3/23/2023	HIGH
62989	NetIQ Privileged User Manager Detection	Nessus	CGI abuses	11/21/2012	11/22/2019	INFO
94868	Fedora 25 : python-proteus / tryton / trytond / trytond-account / etc (2016-d961441913)	Nessus	Fedora Local Security Checks	11/15/2016	1/11/2021	MEDIUM

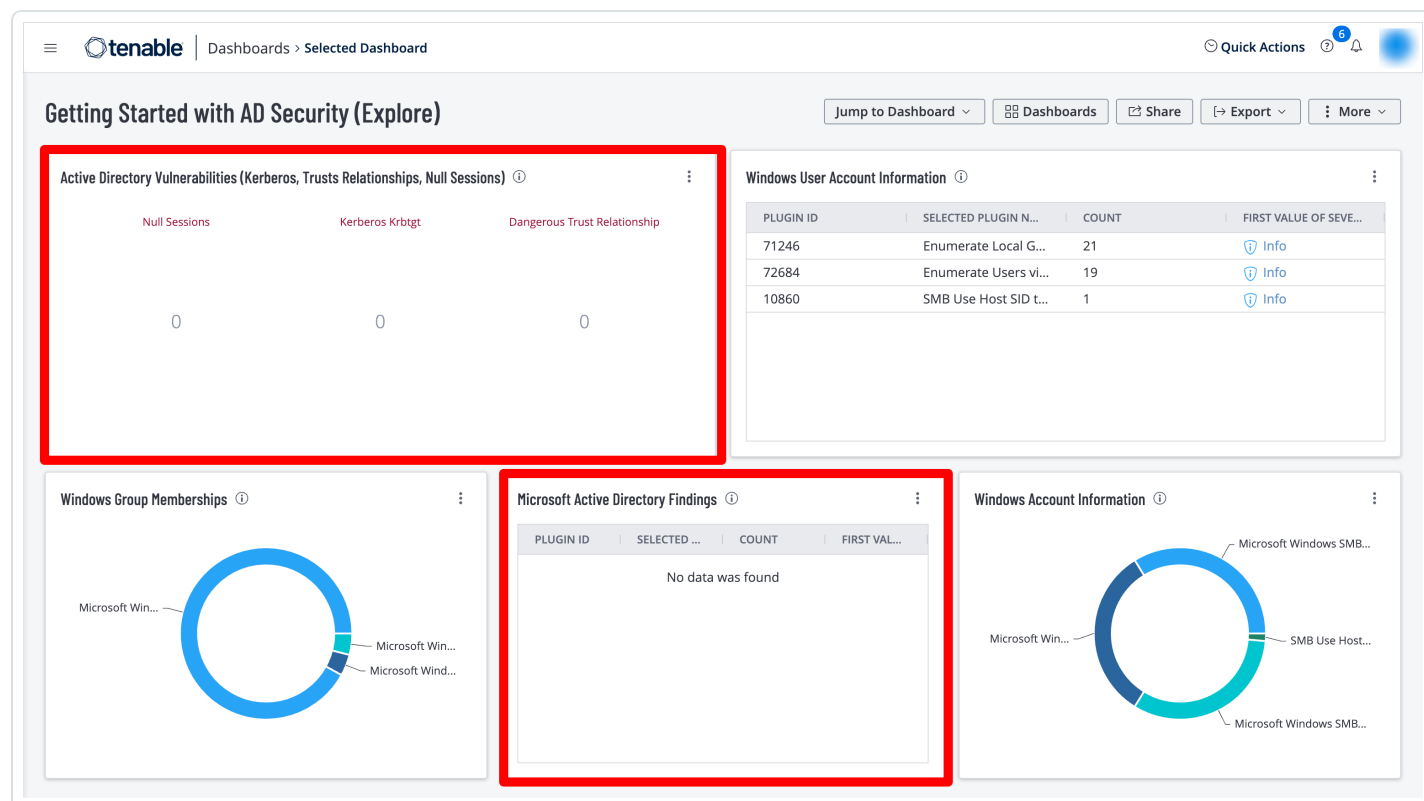


Active Directory Settings

The [Getting Started with AD Security](#) Tenable Vulnerability Management dashboard uses output derived from a set of plugins that are part of the Tenable Active Directory Starter Scan Template to help organizations determine the security posture of their Active Directory Servers using the following widgets:

Active Directory Vulnerabilities (Kerberos, Trusts Relationships, Null Sessions) – This widget uses plugins 150488, 150484, and 150486 to list a total count of findings for assets that were identified with the Active Directory vulnerabilities plugins directly related to Kerberos, Trusts Relationships, and Null Sessions.

Microsoft Active Directory Findings – This widget displays a vulnerability summary for assets that contain any vulnerabilities related to Active Directory. The application CPE filter is used to cross reference Tenable plugins that contain “active_directory”, including those from the AD Starter Scan.



These widgets leverage the following Tenable Nessus plugins:

- 150480 AD Starter Scan - Kerberoasting



- 150484 AD Starter Scan - Kerberos Krbtgt
- 150486 AD Starter Scan - Dangerous Trust Relationship
- 150481 AD Starter Scan - Weak Kerberos encryption
- 150488 AD Starter Scan - Null sessions
- 150489 AD Starter Scan - Blank passwords
- 150485 AD Starter Scan - Unconstrained delegation
- 150482 AD Starter Scan - Kerberos Pre-authentication Validation
- 150483 AD Starter Scan - Non-Expiring Account Password
- 150487 AD Starter Scan - Primary Group ID integrity



Domain Controllers

Organizations can leverage the following Nessus plugins in Tenable Vulnerability Management to identify security issues in Domain Controllers:

- 10413 - Microsoft Windows SMB Registry: Remote PDC/BDC Detection

Organizations can leverage the following Nessus plugins in Tenable Security Center to identify security issues in Domain Controllers:

- 44871 - WMI Windows Feature Enumeration With Vuln Text = Active Directory Domain Services
- 10456 - Microsoft Windows SMB Service Enumeration With Vuln Text = Active Directory Domain Services [NTDS]
- 44401 - Microsoft Windows SMB Service Config Enumeration With Vuln Text = Display name : Active Directory Domain Services

The following [Indicators of Exposure](#) (IoE) in Tenable Identity Exposure can be used to identify exposures in Domain Controllers:

- Unsecured Configuration of Netlogon Protocol (Critical)
- Domain Controllers Managed by Illegitimate Users (Critical)
- Insufficient Hardening Against Ransomware (Medium)
- Domain without Computer-Hardening GPOs (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:

Indicators of Exposure

Search: net X Show all indicators No 4/4 domains >

Unsecured Configuration of Netlogon Protocol
 Critical
 CVE-2020-1472 ("ZeroLogon") affects Netlogon protocol and allows elevation of privilege
 ▲ 4 domains Complexity

Mapped Certificates on Accounts
 Ensures that privileged objects do not have any mapped certificate assigned to them.
 ▲ demo Complexity

Domain Controllers Managed by Illegitimate Users
 Some domain controllers can be managed by non-administrative users due to dangerous access rights.
 ▲ 2 domains Complexity

Verify Sensitive GPO Objects and Files Permissions
 Ensures that the permissions assigned to GPO objects and files linked to sensitive containers, such as the domain controllers or OU, are appropriate and secure.
 ▲ 2 domains Complexity

ADCS Dangerous Misconfigurations
 List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI).
 ▲ demo Complexity

Verify Permissions Related to AAD Connect Accounts
 Ensure the permissions set on AAD Connect accounts are sane
 ▲ demo Complexity

Root Objects Permissions Allowing DCSync-Like Attacks
 Checks for unsafe permissions on root objects that may enable unauthorized users to steal authentication credentials.
 ▲ demo Complexity

Dangerous Kerberos Delegation
 Checks for unauthorized Kerberos delegation, and ensures protection for privileged users against it.
 ▲ 4 domains Complexity

Ensure SDProp Consistency
 Control that the adminSDHolder object is in a clean state.
 ▲ 2 domains Complexity

Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:

Indicators of Exposure | Indicator details X

Search: net

Unsecured Configuration of Netlogon Protocol
 Severity: Critical
 Status: Not compliant
 Latest detection: 15:28:58, 2023-04-17

Information | Vulnerability details | Deviant objects | Recommendations

EXECUTIVE SUMMARY

The vulnerability described by CVE-2020-1472 ("ZeroLogon") allows an unauthenticated attacker to connect to a domain controller to obtain domain administrator access.

IMPACTED DOMAINS

DOCUMENTS

- CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
- How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472
- [MS-NRPC]: Netlogon Remote Protocol
- [Blog] ZeroLogon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)

ATTACKER KNOWN TOOLS

- CVE-2020-1472 POC
Dirk-jan Mollema
- Mimikatz - LsaDump ZeroLogon
Benjamin Delpy



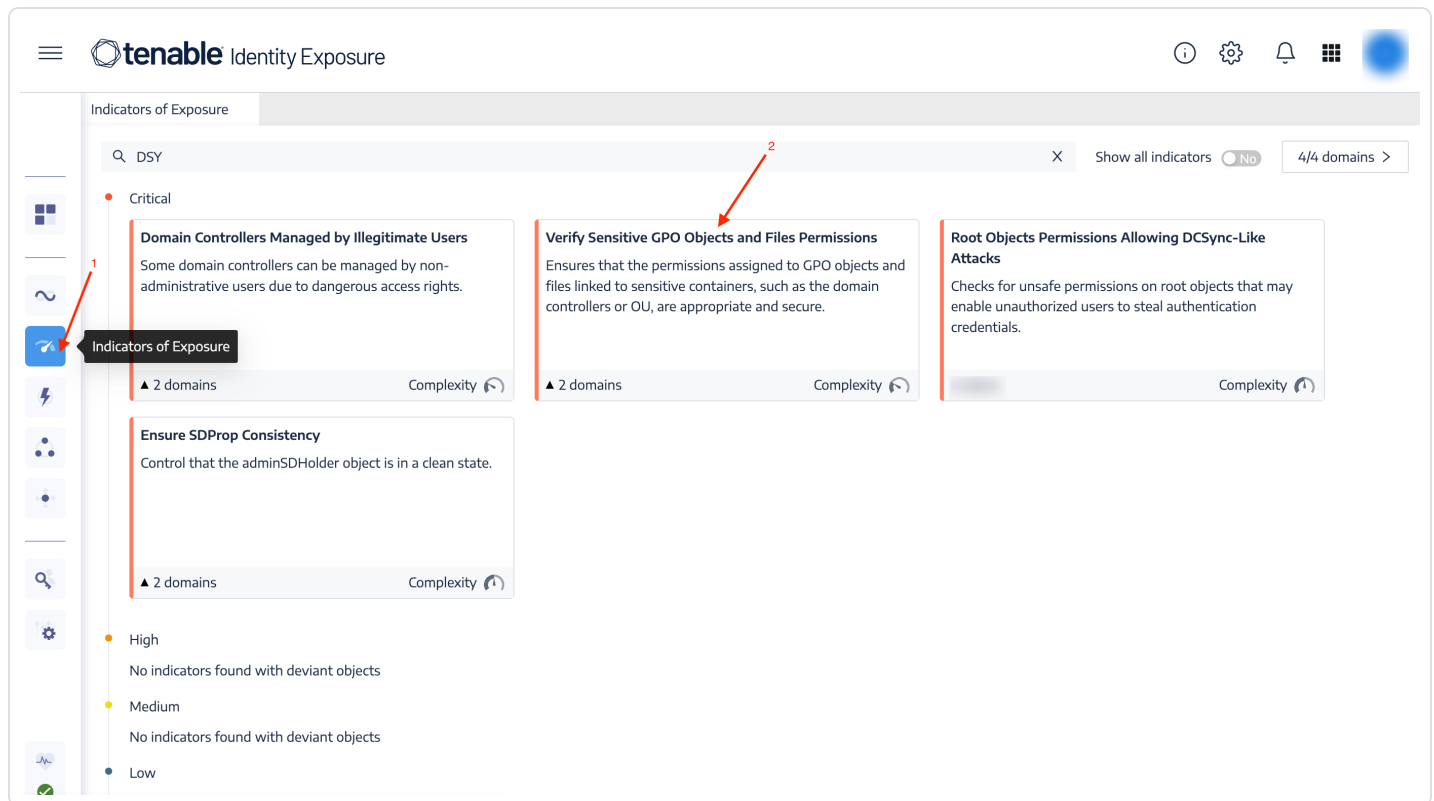


Group and File Permissions

The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be leveraged to determine exposures in group and file permissions:

- Verify Sensitive GPO Objects and File Permissions (Critical)
- User Primary Group (Critical)
- Verify Permissions Related to AAD (Azure Active Directory) Connect Accounts (Critical)
- Root Objects Permissions Allowing DCSync-Like Attacks (Critical)
- Users Allowed to Join Computers to the Domain (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Indicators of Exposure

Indicator details X

DSY

Critical

Domain

Some c

admini

2 do

Ensured

Contro

2 do

Verify Sensitive GPO Objects and Files Permissions

Critical

Not compliant

16:38:02, 2023-05-08

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.

IMPACTED DOMAINS

DOCUMENTS

Group Policy Object reference

ATTACKER KNOWN TOOLS

No tools listed for this indicator



Cryptographic Controls

Applications and servers often support SSL/TLS key exchanges that are cryptographically weaker than recommended. Key exchanges must be recommended by IANA and provide at least 224 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges. Nessus has over 1000 plugins that identify vulnerabilities with SSH/OpenSSH, and other cipher suites.

Tenable Identity Exposure has the following Indicators of Exposure to evaluate cryptographic controls:

- ADCS (Active Directory Certificate Services) Dangerous Misconfigurations (Critical)
- Use of Weak Cryptography Algorithms into Active Directory PKI (Critical)
- Reversible Passwords (Medium)
- Vulnerable Credential Roaming Related Attributes (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Indicators of Exposure

Q Crypto

Critical

Use of Weak Cryptography Algorithms in Active Directory PKI

Identifies weak cryptographic algorithms used in root certificates deployed on an internal Active Directory PKI.

Indicators of Exposure

Complexity

High

No indicators found with deviant objects

Medium

No indicators found with deviant objects

Low

No indicators found with deviant objects

Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Indicators of Exposure

Indicator details

X

Search

Crypto

Critical

Use of Weak Cryptography Algorithms in Active Directory PKI

Identified

certific

dem

High

No indic

Medium

No indic

Low

No indic

Name

Use of Weak Cryptography Algorithms in Active Directory PKI

Severity

Critical

Status

Not compliant

Latest detection

15:30:21, 2023-04-17

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Active Directory instances use a public key infrastructure (PKI) for authentication purposes. The various cryptographic algorithms require correct configuration.

IMPACTED DOMAINS

DOCUMENTS

Block Cipher Techniques

ATTACKER KNOWN TOOLS

No tools listed for this indicator

- 15 -



Tenable Identity Exposure

Tenable Identity Exposure provides information about an organization's Active Directory environment in an intuitive dashboard that monitors Active Directory in real-time, enabling organizations to identify at a glance the most critical vulnerabilities and recommended courses of remediation. [Indicators of Exposure](#) and [Indicators of Attack](#) discover underlying issues affecting the organization's Active Directory environment. Some of the Identity Management compliance requirements that Tenable solutions address include:

- Identify all accounts in the environment
- Ensure all active accounts are authorized
- Ensure all accounts are configured to use strong authentication controls
- Delete or disable dormant accounts
- Restrict privileged access to only authorized users
- Ensure group access is appropriately assigned
- Understand configuration exposures, such as dangerous permissions

Indicators of Exposure provides an overview of critical, high, medium, and low risk exposures identified across the organization's domains. From the landing page, security analysts can drill down for more details about which assets are exposed.

tenable.ad | Active Directory

Indicators of Exposure

Search for an indicator Show all indicators

Critical

- Unsecured Configuration of Netlogon Protocol**
CVE-2020-1472 ("ZeroLogon") affects Netlogon protocol and allows elevation of privilege
▲ 4 domains Complexity
- Mapped Certificates on Accounts**
Ensure that no mapped certificate is set on privileged objects
▲ demo Complexity
- Domain Controllers Managed by Illegitimate Users**
Some domain controllers can be managed by non-administrative users due to dangerous access rights.
▲ 2 domains Complexity
- Verify Sensitive GPO Objects and Files Permissions**
Ensure the permissions set on the GPO objects and files that are linked to sensitive containers (like the Domain Controllers OU) are sane
▲ 2 domains Complexity
- ADCS Dangerous Misconfigurations**
List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI)
▲ demo Complexity
- Verify Permissions Related to AAD Connect Accounts**
Ensure the permissions set on AAD Connect accounts are sane
▲ demo Complexity
- Application of Weak Password Policies on Users**
Some password policies applied on specific user accounts are not strong enough and can lead to credentials theft.
▲ 4 domains Complexity
- Root Objects Permissions Allowing DCSync-Like Attacks**
The permissions set on root objects could allow illegitimate users to steal authentication secrets
▲ demo Complexity
- Dangerous Kerberos Delegation**
Check that no dangerous Kerberos delegation (unconstrained, protocol transition, etc.) is authorized, and that privileged users are protected against such delegation
▲ 4 domains Complexity

The Indicators of Attack pane provides a consolidated view of exposures that impact the organization's Active Directory environment. Displayed is an event timeline that shows when attacks occurred and identifies the severity level of the vulnerability targeted: Critical (red-orange), High (light orange), Medium (yellow), and Low (blue). The tiles below the timeline provide details on the top three attacks in the organization's domains.

This view enables security teams to:

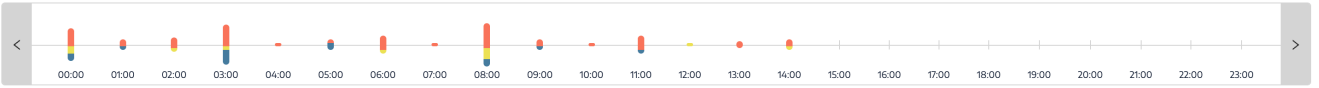
- Visualize every Active Directory threat from an accurate attack timeline
- Analyze in-depth details about an Active Directory attack
- Explore [MITRE ATT&CK](#) descriptions directly from detected incidents



Indicators of Attack

Hour Day Month Year June 5, 2023 📅 🕒

4/4 domains > 17/17 indicators > Refresh

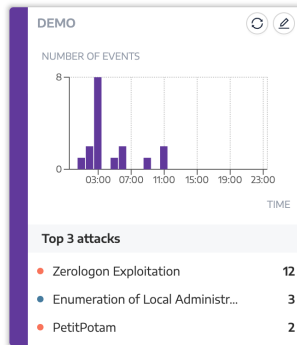
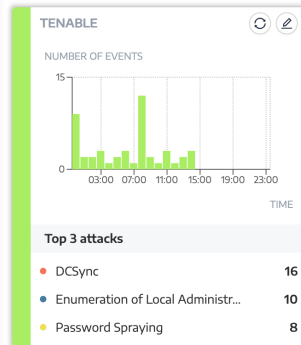


Sort by Criticality ▾

🔍 Search a domain or an attack

Show only domains under attack ☒ Yes

CRITICAL



📄 Export

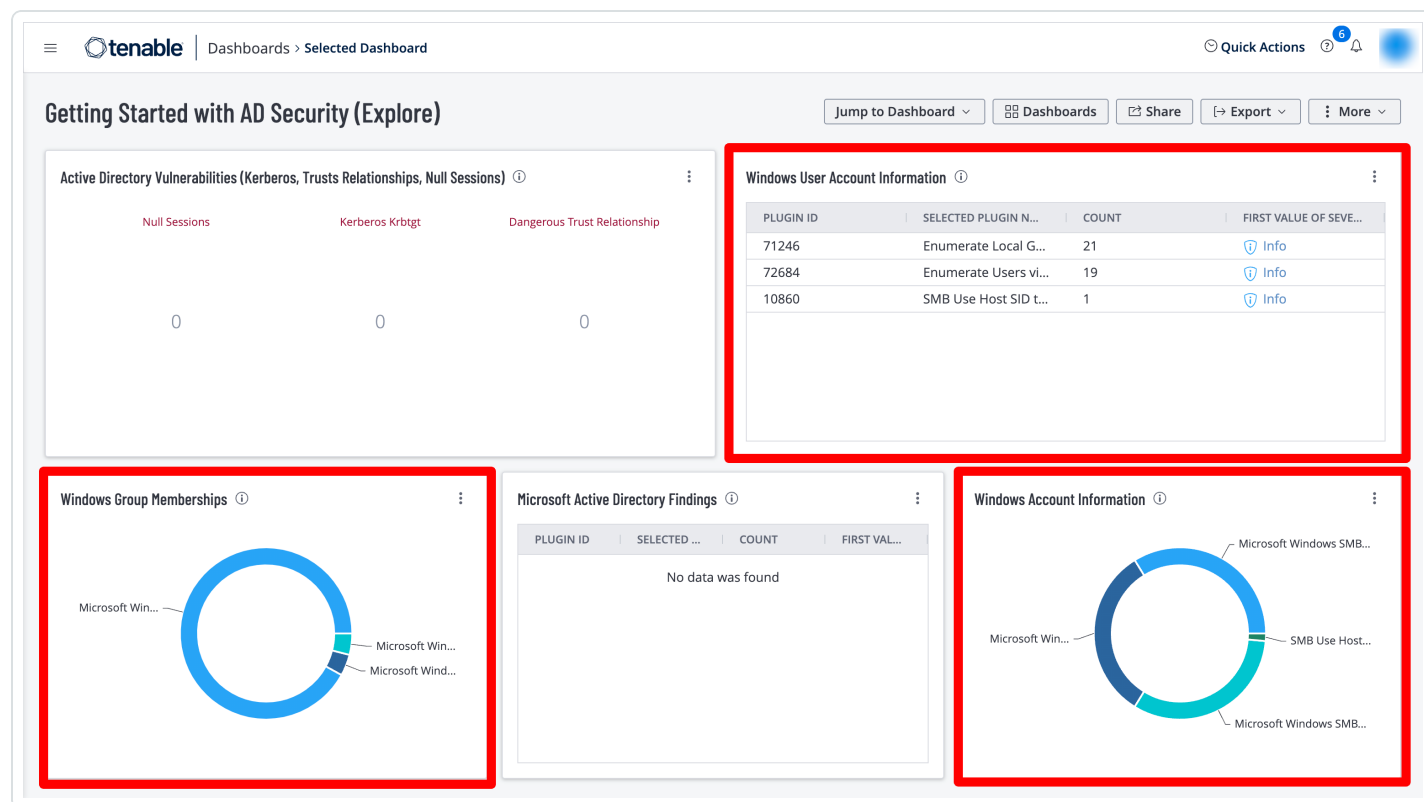


Identifying Exposure

Tenable Identity Exposure provides various methods to access the information collected through the Indicators of Exposure (IoE) and Indicators of Attack (IoA) panes. Tenable Vulnerability Management provides the ability to use the Explore Findings through the use of dashboards and reports.

Identification

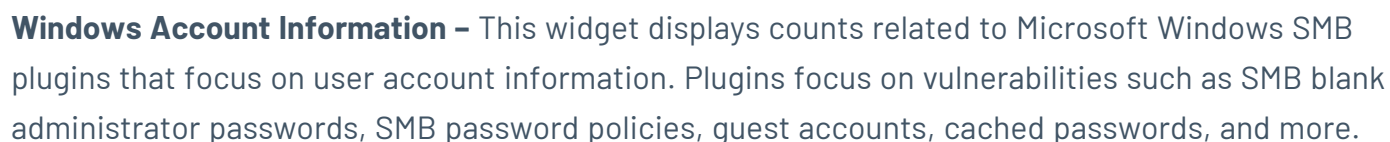
The first step in taking control of the organization's Identity Management is to enumerate every user account in the environment and determine the level of access the account is granted. All user accounts must be uniquely identified and assigned to particular entities, such as users and applications.



The [Getting Started with AD Security](#) dashboard in Tenable Vulnerability Management contains the following widgets to enumerate user accounts:

Windows User Account Information – This widget displays counts for user accounts and security identifiers (SID). Plugins report on potential user account vulnerabilities such as disabled accounts, accounts that have never logged in, accounts with passwords that have never changed, and more.

Windows Group Memberships – This widget displays information for Windows default groups such as administrators, server operators, account operators, backup operators, print operators, and replicator groups.



Organizations can use the **CSF - Account and Group Information** widget located in the **CIS Control 4/5: Secure Configurations & Group Memberships** dashboard in Tenable Security Center, which leverages plugins that enumerate Windows account information.

- 21 -



Users and Groups

While Active Directory is typically used by most organizations, there are many other accounts for non-Windows platforms that must be identified. Tenable Nessus contains a number of [plugins](#) and plugin families that help organizations enumerate users and groups on the network. The **Windows: User management** plugin family contains nearly 30 plugins that enumerate Microsoft Windows users and groups. Other useful Nessus plugins for user and group enumeration include:

- **10894 Microsoft Windows Users Group List** – This plugin uses the supplied credentials to retrieve the list of groups each user belongs to. Groups are stored for further checks.
- **126527 Microsoft Windows SAM user enumeration** – This plugin enumerates domain users on the remote Windows system using Security Account Manager.
- **95928 Linux User List Enumeration** – This plugin enumerates local users and groups on the remote host.
- **95929 macOS and Mac OS X User List Enumeration** – This plugin extracts the member lists of 'Admin' and 'Wheel' groups on the remote host.

A number of other Nessus plugins that contain the key words "User Enumeration" in a [plugin name search](#) using the Plugin Name filter identify WordPress, VMware, LDAP, and other software applications that maintain user accounts, as shown in the following image:

The screenshot shows the Tenable Nessus interface with the 'Plugins' section selected. The 'Search' tab is active, displaying a search results page for 'User Enumeration'. The search results are as follows:

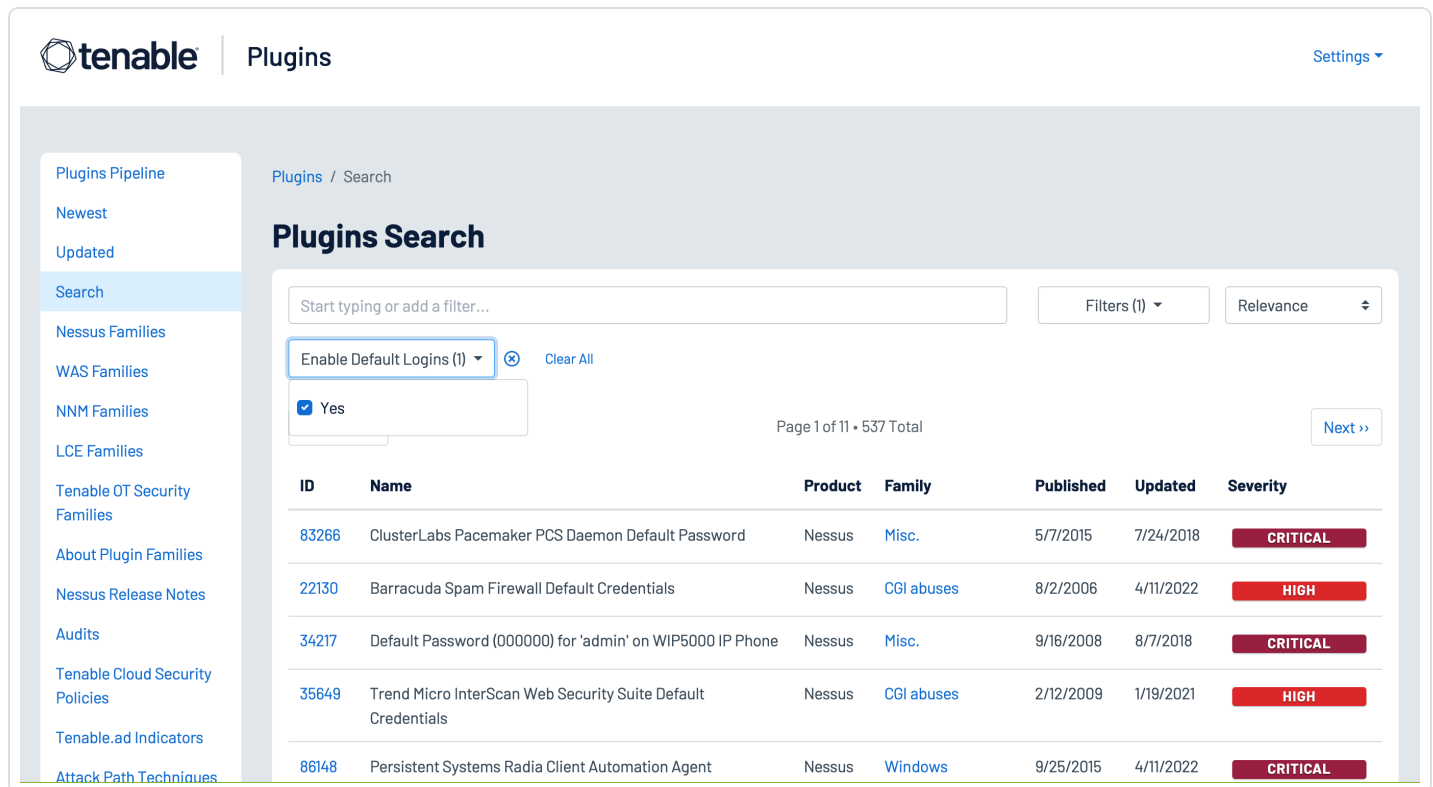
ID	Name	Product	Family	Published	Updated	Severity
45478	LDAP User Enumeration	Nessus	Misc.	4/9/2010	4/25/2023	INFO
90067	WordPress User Enumeration	Nessus	CGI abuses	3/21/2016	4/11/2022	MEDIUM
29187	Plumtree Portal User Object User Enumeration	Nessus	CGI abuses	12/4/2007	4/11/2022	MEDIUM
59358	Drupal Portal R10 User Enumeration	Nessus	CGI abuses	6/6/2012	4/11/2022	MEDIUM

Service and Default Accounts

Operating Systems and applications are often distributed with service and default accounts that are either not password-protected or have a default password that is well-known. Tenable Nessus and Tenable Identity Exposure help identify these accounts, enabling organizations to review and disable any unnecessary accounts to reduce the attack surface. Organizations can leverage the following Nessus plugins to enumerate service and default accounts:

- **Plugin Family: Default Unix Accounts** – This plugin family contains over 170 Nessus plugins that check for the existence of default accounts/passwords on a number of devices. In addition, there are many plugins that check for simple passwords such as “0000”, “1234”, and more commonly identified password combinations for “root” or administrator accounts.
- **171959 Windows Enumerate Accounts** – This plugin enumerates all Windows Accounts

Several hundred plugins can be identified by searching for “Default Account” from the Nessus Plugins Search page using the [Enable Default Logins](#) filter. Nessus default account plugins are available for Databases, Web Servers, SCADA devices, Unix/Linux devices, Cisco devices and more. Many of the plugins are associated with the Default Unix Account Nessus family, however, many are in other families as well.



The screenshot displays the Tenable Nessus Plugins Search interface. On the left, a sidebar contains navigation links: Plugins Pipeline, Newest, Updated, Search (selected), Nessus Families, WAS Families, NNM Families, LCE Families, Tenable OT Security Families, About Plugin Families, Nessus Release Notes, Audits, Tenable Cloud Security Policies, Tenable.ad Indicators, and Attack Path Techniques. The main content area is titled 'Plugins / Search' and 'Plugins Search'. It features a search bar with the text 'Start typing or add a filter...', a filter dropdown set to 'Enable Default Logins (1)', and a 'Clear All' link. Below the filter, a checkbox labeled 'Yes' is checked. The results are displayed in a table with columns: ID, Name, Product, Family, Published, Updated, and Severity. The table shows five results, all with a severity of CRITICAL or HIGH. The first result is 'ClusterLabs Pacemaker PCS Daemon Default Password' (ID 83266, Family Misc., Severity CRITICAL). The second is 'Barracuda Spam Firewall Default Credentials' (ID 22130, Family CGI abuses, Severity HIGH). The third is 'Default Password (000000) for 'admin' on WIP5000 IP Phone' (ID 34217, Family Misc., Severity CRITICAL). The fourth is 'Trend Micro InterScan Web Security Suite Default Credentials' (ID 35649, Family CGI abuses, Severity HIGH). The fifth is 'Persistent Systems Radia Client Automation Agent' (ID 86148, Family Windows, Severity CRITICAL). The interface also shows 'Page 1 of 11 • 537 Total' and a 'Next >>' button.

ID	Name	Product	Family	Published	Updated	Severity
83266	ClusterLabs Pacemaker PCS Daemon Default Password	Nessus	Misc.	5/7/2015	7/24/2018	CRITICAL
22130	Barracuda Spam Firewall Default Credentials	Nessus	CGI abuses	8/2/2006	4/11/2022	HIGH
34217	Default Password (000000) for 'admin' on WIP5000 IP Phone	Nessus	Misc.	9/16/2008	8/7/2018	CRITICAL
35649	Trend Micro InterScan Web Security Suite Default Credentials	Nessus	CGI abuses	2/12/2009	1/19/2021	HIGH
86148	Persistent Systems Radia Client Automation Agent	Nessus	Windows	9/25/2015	4/11/2022	CRITICAL



In addition, Tenable Identity Exposure provides the ability to determine if a default administrator account was recently used in the environment, as shown in the image below:

tenable.ad | Active Directory

Indicators of Exposure

Indicator details X

default

Critical

No indicators

High

No indicators

Medium

Recent Use of the Default Administrator Account

Built-in Administrator Account

▲ 4 domains

Low

No indicators

Recent Use of the Default Administrator Account

Severity: Medium

Status: Not compliant

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Built-in administrative accounts should almost never be used (except in very specific cases that rarely happen).

DOCUMENTS

[Securing Active Directory Administrative Groups and Accounts](#)

[Appendix D: Securing Built-In Administrator Accounts in Active Directory](#)

ATTACKER KNOWN TOOLS

No tools listed for this indicator

IMPACTED DOMAINS



User Access Controls

Strong authentication mechanisms help validate that accounts are being used by the authorized user to read, create, modify, or delete data in accordance with business needs. The [Center for Internet Security \(CIS\)](#) provides [benchmarks](#) for a large number Operating System platforms and applications. [Tenable Research](#) writes [audit files](#) for these benchmarks to help organizations quickly determine their alignment with the CIS recommendations. The benchmarks include guidance on access controls for both non-privileged and privileged accounts.



User Accounts

Non-privileged user accounts require strong access controls to prevent attackers from gaining local access to the network. Attackers often target user accounts to exploit weaknesses in the local network and escalate privileges. Security teams can use the [Tenable Audits Search Page](#) to find audit files for their Operating System platforms, which check for common compliance requirements such as “Lock Workstations after Inactivity” and other issues.

The screenshot displays the Tenable Audits File Search interface. On the left is a sidebar with navigation links: Newest, Updated, Search Audit Files (highlighted), Search Items, References, Authorities, Documentation, and Download All Audit Files. The main header shows the Tenable logo and 'Audits' with a 'Settings' dropdown. Below the header, the breadcrumb 'Audits / File Search' is visible. The main section is titled 'File Search' and contains a search bar with 'Red Hat' entered. To the right of the search bar are buttons for 'Add Filter' and 'Relevance'. Below the search bar are navigation buttons: '<< Previous', 'Page 1 of 1 • 29 Total', and 'Next >>'. A table lists the search results with columns: Name, Plugin, Revision, and Updated.

Name	Plugin	Revision	Updated
BSI-100-2 Red Hat Linux 2005	Unix	1.6	4/25/2022
PCI DSS 2.0/3.0 - Red Hat Linux	Unix	1.53	4/25/2022
CIS Red Hat EL8 Workstation L2 v2.0.0	Unix	1.11	7/5/2023
CIS Red Hat EL7 Workstation L2 v3.1.1	Unix	1.8	7/5/2023

Active Directory accounts can be configured to escape global password renewal policies. Accounts set up in this manner can be used indefinitely without ever changing their password. Tenable recommends reviewing user and administrator accounts to ensure they are not configured to have this attribute.

The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be used to identify issues with user accounts in an organization’s Active Directory environment:

- Accounts with Never Expiring Passwords
- Application of Weak Password Policies on Users
- Dangerous Kerberos Delegation
- Account that Might Have an Empty Password



- AdminCount Attribute Set on Standard Users
- User Account Using Old Password
- Kerberos Configuration on User Account



Privileged Accounts

Most compliance standards and frameworks require privileged users to have a non-privileged account for standard user activities, such as web browsing or reading emails. Tenable Nessus and Tenable Identity Exposure provide the tools to identify settings for root and admin accounts.

Using the Plugin Name filter on the [Plugins Search](#) page enables analysts to search for plugins with terms that identify privileged accounts such as “root,” “admin,” or “privileged,” as shown below:

Start typing or add a filter... Filters (1) Relevance

Plugin Name (Active) Clear All

Search by Plugin Name

Page 1 of 4 • 169 Total Next >>

ID	Name	Product	Family	Published	Updated	Severity
11255	Default Password (root) for 'root' Account	Nessus	Default Unix Accounts	2/20/2003	4/11/2022	CRITICAL
9526	Webmin Default Configuration 'root' Logon	Nessus Network Monitor	CGI	8/25/2016	5/18/2018	INFO
1817	Debian proftpd root Privilege Escalation	Nessus Network Monitor	FTP Servers	8/20/2004	3/6/2019	HIGH

The following [Indicators of Exposure](#) (IoE) in Tenable Identity Exposure can be used to identify Active Directory settings for privileged accounts:

- Mapped Certificates on Accounts
- Ensure SDProp Consistency
- Native Administrative Group Members
- Privileged Accounts Running Kerberos Services
- Potential Clear-Text Password
- Protected Users Group not Used
- Logon Restrictions for Privileged Users
- Local Administrative Account Overview Management



Dormant Accounts

User accounts that have not been accessed in more than a year provide an opportunity for attackers to leverage compromised credentials and perform brute-force attacks. Nessus plugins 10915 or 10899 Microsoft Windows - Local Users Information: User Has Never Logged In displays a list of Windows accounts where the user has never logged in. The Sleeping Accounts Indicator of Exposure in Tenable Identity Exposure detects accounts that have not been accessed in over a year.

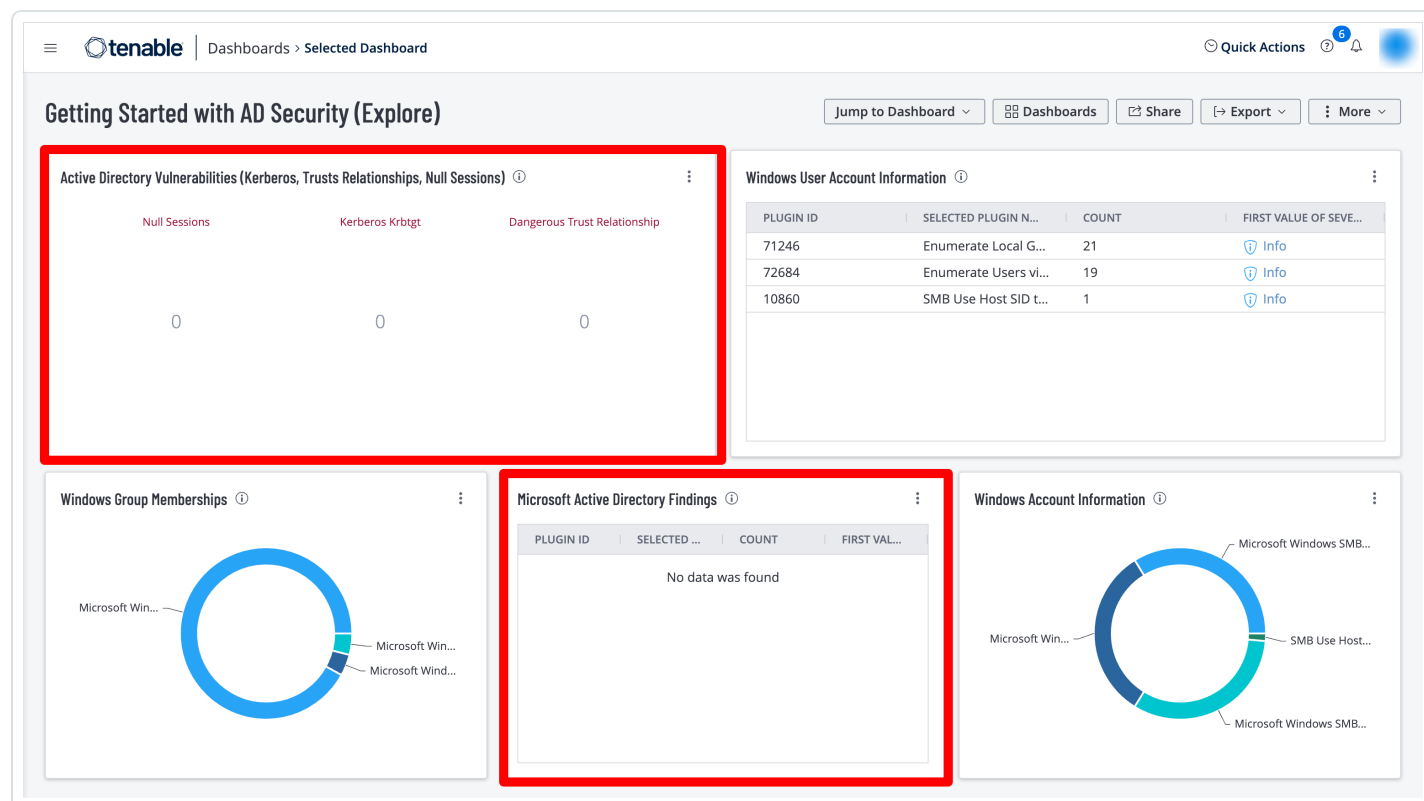


Active Directory Settings

The [Getting Started with AD Security](#) Tenable Vulnerability Management dashboard uses output derived from a set of plugins that are part of the Tenable Active Directory Starter Scan Template to help organizations determine the security posture of their Active Directory Servers using the following widgets:

Active Directory Vulnerabilities (Kerberos, Trusts Relationships, Null Sessions) – This widget uses plugins 150488, 150484, and 150486 to list a total count of findings for assets that were identified with the Active Directory vulnerabilities plugins directly related to Kerberos, Trusts Relationships, and Null Sessions.

Microsoft Active Directory Findings – This widget displays a vulnerability summary for assets that contain any vulnerabilities related to Active Directory. The application CPE filter is used to cross reference Tenable plugins that contain “active_directory”, including those from the AD Starter Scan.



These widgets leverage the following Tenable Nessus plugins:

- 150480 AD Starter Scan - Kerberoasting



- 150484 AD Starter Scan - Kerberos Krbtgt
- 150486 AD Starter Scan - Dangerous Trust Relationship
- 150481 AD Starter Scan - Weak Kerberos encryption
- 150488 AD Starter Scan - Null sessions
- 150489 AD Starter Scan - Blank passwords
- 150485 AD Starter Scan - Unconstrained delegation
- 150482 AD Starter Scan - Kerberos Pre-authentication Validation
- 150483 AD Starter Scan - Non-Expiring Account Password
- 150487 AD Starter Scan - Primary Group ID integrity



Domain Controllers

Organizations can leverage the following Nessus plugins in Tenable Vulnerability Management to identify security issues in Domain Controllers:

- 10413 - Microsoft Windows SMB Registry: Remote PDC/BDC Detection

Organizations can leverage the following Nessus plugins in Tenable Security Center to identify security issues in Domain Controllers:

- 44871 - WMI Windows Feature Enumeration With Vuln Text = Active Directory Domain Services
- 10456 - Microsoft Windows SMB Service Enumeration With Vuln Text = Active Directory Domain Services [NTDS]
- 44401 - Microsoft Windows SMB Service Config Enumeration With Vuln Text = Display name : Active Directory Domain Services

The following [Indicators of Exposure](#) (IoE) in Tenable Identity Exposure can be used to identify exposures in Domain Controllers:

- Unsecured Configuration of Netlogon Protocol (Critical)
- Domain Controllers Managed by Illegitimate Users (Critical)
- Insufficient Hardening Against Ransomware (Medium)
- Domain without Computer-Hardening GPOs (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:

Indicators of Exposure

Search: net X Show all indicators ☐ No 4/4 domains >

Critical

- Unsecured Configuration of Netlogon Protocol** (CVE-2020-1472 ("Zerologon")) affects Netlogon protocol and allows elevation of privilege. **4 domains** Complexity
- Mapped Certificates on Accounts** Ensures that privileged objects do not have any mapped certificate assigned to them. **demo** Complexity
- Domain Controllers Managed by Illegitimate Users** Some domain controllers can be managed by non-administrative users due to dangerous access rights. **2 domains** Complexity
- Verify Sensitive GPO Objects and Files Permissions** Ensures that the permissions assigned to GPO objects and files linked to sensitive containers, such as the domain controllers or OU, are appropriate and secure. **2 domains** Complexity
- ADCS Dangerous Misconfigurations** List dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI). **demo** Complexity
- Verify Permissions Related to AAD Connect Accounts** Ensure the permissions set on AAD Connect accounts are sane. **demo** Complexity
- Root Objects Permissions Allowing DCSync-Like Attacks** Checks for unsafe permissions on root objects that may enable unauthorized users to steal authentication credentials. **demo** Complexity
- Dangerous Kerberos Delegation** Checks for unauthorized Kerberos delegation, and ensures protection for privileged users against it. **4 domains** Complexity
- Ensure SDProp Consistency** Control that the adminSDHolder object is in a clean state. **2 domains** Complexity

Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:

Indicators of Exposure | Indicator details X

Search: net

Unsecured Configuration of Netlogon Protocol **Critical** **Not compliant** Latest detection: 15:28:58, 2023-04-17

Information | Vulnerability details | Deviant objects | Recommendations

EXECUTIVE SUMMARY

The vulnerability described by CVE-2020-1472 ("Zerologon") allows an unauthenticated attacker to connect to a domain controller to obtain domain administrator access.

IMPACTED DOMAINS

DOCUMENTS

- CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
- How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472
- [MS-NRPC]: Netlogon Remote Protocol
- [Blog] Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)

ATTACKER KNOWN TOOLS

- CVE-2020-1472 POC
Dirk-jan Mollema
- Mimikatz - LsaDump Zerologon
Benjamin Delpy



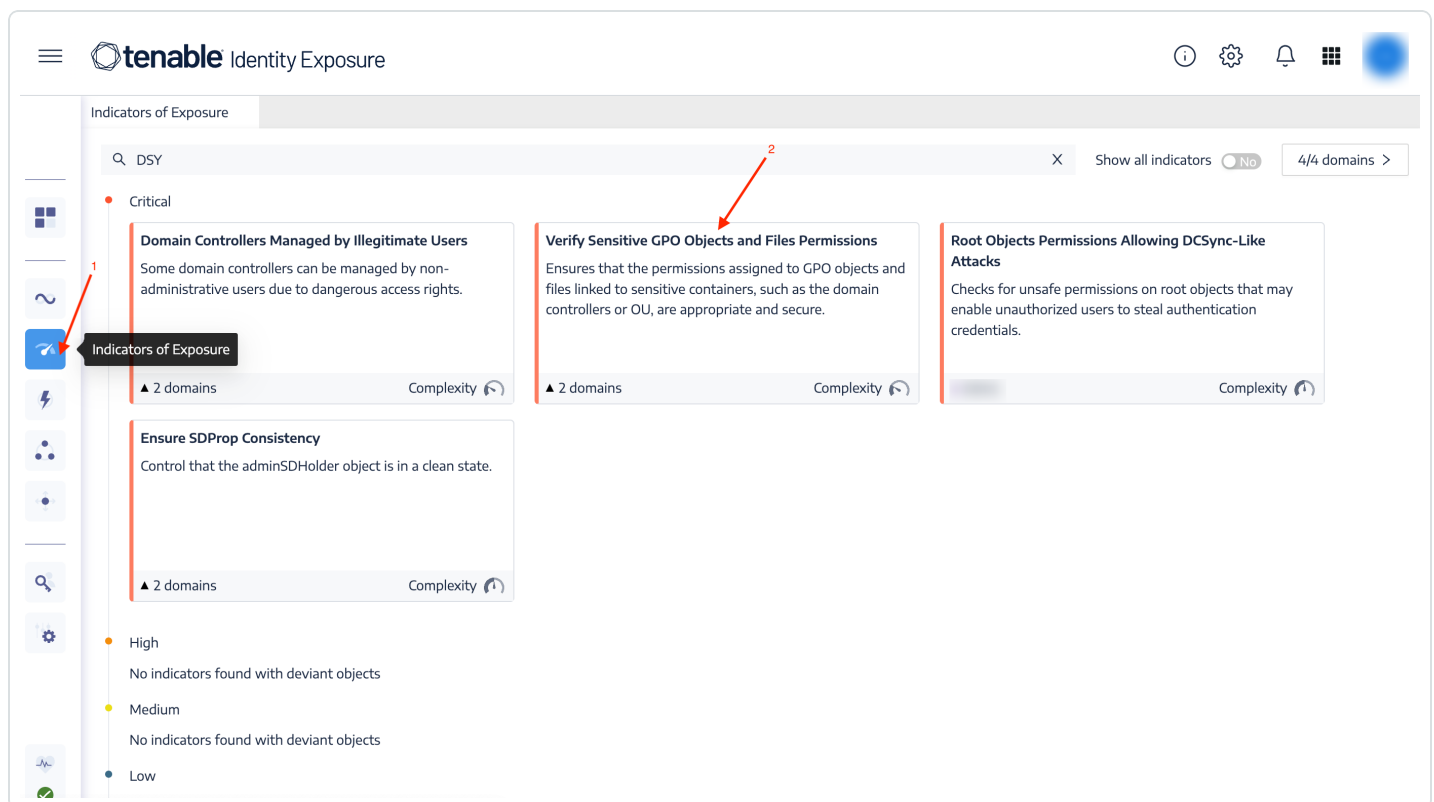


Group and File Permissions

The following Indicators of Exposure (IoE) in Tenable Identity Exposure can be leveraged to determine exposures in group and file permissions:

- Verify Sensitive GPO Objects and File Permissions (Critical)
- User Primary Group (Critical)
- Verify Permissions Related to AAD (Azure Active Directory) Connect Accounts (Critical)
- Root Objects Permissions Allowing DCSync-Like Attacks (Critical)
- Users Allowed to Join Computers to the Domain (Medium)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Indicators of Exposure

Indicator details X

DSY

Critical

Domain

Some c

admini

2 do

Ensured

Contro

2 do

Verify Sensitive GPO Objects and Files Permissions

Critical

Not compliant

16:38:02, 2023-05-08

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Group Policy Objects (GPOs) configure Windows systems and perform tasks at a high level of privileges. However, only legitimate administrative accounts should manage GPOs linked to sensitive containers, such as the ones containing administrators or domain controllers.

IMPACTED DOMAINS

DOCUMENTS

Group Policy Object reference

ATTACKER KNOWN TOOLS

No tools listed for this indicator



Cryptographic Controls

Applications and servers often support SSL/TLS key exchanges that are cryptographically weaker than recommended. Key exchanges must be recommended by IANA and provide at least 224 bits of security, which translates to a minimum key size of 2048 bits for Diffie Hellman and RSA key exchanges. Nessus has over 1000 plugins that identify vulnerabilities with SSH/OpenSSH, and other cipher suites.

Tenable Identity Exposure has the following Indicators of Exposure to evaluate cryptographic controls:

- ADCS (Active Directory Certificate Services) Dangerous Misconfigurations (Critical)
- Use of Weak Cryptography Algorithms into Active Directory PKI (Critical)
- Reversible Passwords (Medium)
- Vulnerable Credential Roaming Related Attributes (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:



Indicators of Exposure

Q Crypto

Critical

Use of Weak Cryptography Algorithms in Active Directory PKI

Identifies weak cryptographic algorithms used in root certificates deployed on an internal Active Directory PKI.

Indicators of Exposure

Complexity

High

No indicators found with deviant objects

Medium

No indicators found with deviant objects

Low

No indicators found with deviant objects

Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Indicators of Exposure

Indicator details

X

Search

Crypto

Critical

Use of Weak Cryptography Algorithms in Active Directory PKI

Identified

certific

▲ dem

High

No indic

Medium

No indic

Low

No indic

Use of Weak Cryptography Algorithms in Active Directory PKI

Identified

certific

▲ dem

High

No indic

Medium

No indic

Low

No indic

Name

Use of Weak Cryptography Algorithms in Active Directory PKI

Severity

Critical

Status

Not compliant

Latest detection

15:30:21, 2023-04-17

Information

Vulnerability details

Deviant objects

Recommendations

EXECUTIVE SUMMARY

Active Directory instances use a public key infrastructure (PKI) for authentication purposes. The various cryptographic algorithms require correct configuration.

IMPACTED DOMAINS

DOCUMENTS

Block Cipher Techniques

ATTACKER KNOWN TOOLS

No tools listed for this indicator



Maintenance

Every structure – physical or virtual – requires maintenance to maintain structural integrity over time. Even the most hardened infrastructure is subject to degradation with regular use. Tenable Security Center, Tenable Vulnerability Management and Tenable Identity Exposure provide comprehensive monitoring to detect drift from the desired state.

Administrator and user activity over time degrades security controls, if the system is not maintained properly. Regular scanning of the environment using the Nessus audit files identifies drift in security controls.

The following [Indicators of Exposure](#) (IoE) in Tenable Identity Exposure can be used to identify maintenance issues in Active Directory:

- Computers Running an Obsolete OS (High)
- Disabled Accounts in Privileged Groups (Low)
- Unlinked, Disabled or Orphan GPO (Low)

Step 1: From the Indicators of Exposure tab in Identity Management, search for the above listed IoEs in the search field as shown below:

Q Obsolete

No indicators found with deviant objects

Computers Running an Obsolete OS

Indicators of Exposure Identifies obsolete systems that Microsoft no longer support and which increase the infrastructure vulnerability.

Complexity 

No indicators found with deviant objects

No indicators found with deviant objects

Step 2: Click on one of the displayed tiles to drill down into more details, as shown below:



Learn More

Tenable Resources

- [Getting Started with Tenable Identity Exposure](#)
- [Getting Started with Active Directory](#)
- [Tenable Plugins Page](#)
- [Tenable Indicators of Attack](#)
- [Tenable Indicators of Exposure](#)

External Resources

- [Center for Internet Security \(CIS\)](#)
- [Microsoft: Monitoring Active Directory for Signs of Compromise](#)
- [Microsoft: Securing Active Directory Administrative Groups and Accounts](#)
- [Microsoft: Azure AD Connect: Accounts and Permissions](#)
- [Microsoft: Privileged Accounts and Groups in Active Directory](#)
- [Microsoft: Reducing the Active Directory Attack Surface \(Privileged Accounts and Groups in Active Directory\)](#)
- [Microsoft: Securing Privileged Access](#)
- [Microsoft: Who Can Add Workstation to the Domain](#)
- [MITRE ATT&CK: Steal or Forge Kerberos Tickets: Kerberoasting](#)