Credential Exposure Evaluation Overview

Table of Contents

Executive Summary 3
Technical Overview 4
Collection Package Components 4
High-Level Collection Workflow 4
Environment Validation 4
Encrypted credential material collection 4
Active Directory Enumeration 5
Microsoft Entra ID Collection 5
Packaging and Archive Creation 5
Secure Transfer by the Customer 5
Security and Operational Considerations 5
Customer Review and Transparency 5

Executive Summary

Scapien's Credential Exposure Evaluation is designed to help organizations identify weak, reused, and high-risk passwords within Active Directory and Microsoft Entra ID environments. The assessment is intended to provide organizations with:

- Visibility into credential exposure risk
- Identification of cracked or crackable credentials
- Prioritized remediation guidance
- Executive and technical reporting
- Improved credential security posture

The assessment provides actionable insight into credential-related risk that may expose the organization to unauthorized access, privilege escalation, ransomware, and other identity-based attacks.

The assessment is performed using encrypted password hashes extracted from Active Directory. No plain text passwords are collected, transmitted, or stored during the collection process.

To maintain transparency and customer control, the collection activities are performed directly by the customer within their own environment using PowerShell scripts provided by Scapien. The scripts are fully readable. We recommend that appropriate security, infrastructure, or audit teams review these scripts prior to execution.

The collection package performs the following functions:

- Extracts encrypted password hash data from Active Directory using standard Microsoft-supported administrative mechanisms
- Collects Active Directory inventory and password policy information
- Optionally collects Microsoft Entra ID (Azure AD) reporting and configuration data
- Packages the collected data into a compressed archive for secure transfer to Scapien

The scripts operate in a read-only manner. No passwords, policies, accounts, or Active Directory objects are modified.

Because the Active Directory credential database is locked while Active Directory is running, the collection process temporarily creates a Volume Shadow Copy snapshot of the Domain Controller to safely access the NTDS database files. This is a standard administrative mechanism commonly used for backup and recovery operations.

Customers retain full visibility and control throughout the engagement, including the ability to inspect the scripts, review the collected files, and control the transfer process.

Technical Overview

Following is a technical overview of the PowerShell scripts included in collection package. The scripts are intended solely for controlled assessment data collection. The scripts do not

- Collect plain text passwords
- Modify Active Directory objects
- Change passwords
- Alter Group Policy
- Create persistence mechanisms
- Install permanent software or services
- Automatically transmit data without customer action

Collection Package Components

The collection package contains the following PowerShell scripts together with customer instructions guide. The scripts work together to perform the assessment data collection.

Script	Purpose
Invoke-ScapienPackage.ps1	Main orchestration script that coordinates the full collection workflow
Invoke-ADEnumAuditPlus.ps1	Performs detailed Active Directory enumeration and reporting
Invoke-ADEnumAuditSafe.ps1	Lightweight enumeration option for restricted environments
Get-EntraIDReport.ps1	Collects Microsoft Entra ID reporting and configuration data

The scripts are standard PowerShell source files and are not obfuscated.

High-Level Collection Workflow

The collection package contains several PowerShell scripts together with customer instructions guide. The scripts work together to perform the assessment data collection.

The collection process consists of the following stages:

1. Environment validation
2. Encrypted credential material collection
3. Active Directory enumeration
4. Optional Microsoft Entra ID collection
5. Packaging and archive creation
6. Secure transfer by the customer

Environment Validation

The main orchestration script performs several validation checks before collection begins, to reduce the likelihood of incomplete collection or operational disruption. These include:

- Confirming the script is running with administrative privileges
- Verifying the system is a Domain Controller
- Checking required PowerShell modules
- Verifying sufficient disk space
- Creating temporary working directories

Encrypted credential material collection

Active Directory stores password data within the NTDS.dit database in encrypted hash form. This database is locked while Active Directory is running. The script creates a temporary Volume Shadow Copy snapshot of the Domain Controller to facilitate extraction. The script uses standard Microsoft administrative and backup mechanisms.

If all snapshot-based methods fail, the script will offer an offline extraction option that temporarily stops Active Directory services on the selected Domain Controller and executes this option with explicit customer confirmation.

Active Directory Enumeration

The enumeration scripts collect Active Directory inventory and configuration data used to contextualize password risk. The enumeration data includes

- User enumeration: User information such as username, display name, account status (enabled / disabled), password age etc.
- Group enumeration: Group information such as group names, group types and scope, and membership counts.
- Computer enumeration: Computer information such as hostname, operating system, last logon timestamp, etc.
- Password policy enumeration: Password policy details such as default domain policy, fine-grained password policies, and Kerberos related settings.
- Trust enumeration: Domain and forest trust relationships

Microsoft Entra ID Collection

If enabled by the customer, the package optionally collects Microsoft Entra ID reporting information which may include user inventory, group inventory, sign-in activity, licensing status etc.

The Entra collection does not retrieve cloud password hashes. In hybrid environments, password hash analysis is performed using the on-premises NTDS database.

Packaging and Archive Creation

After collection is completed, the orchestration script organizes the extracted files, generates collection and manifest information, and compresses the output into a timestamped archive. The packaging process is performed locally on the customer-controlled system.

Secure Transfer by the Customer

After the archive is created, the customer is responsible for transferring the package to Scapien using approved secure transfer methods. The orchestration script provides an option for the customer to transfer the package via SFTP, should the customer choose to do so. Alternately, the customer may encrypt the archive and share it with Scapien via a secure file sharing platform or email.

The script does not automatically exfiltrate or transmit data without customer approval.

Security and Operational Considerations

Because the scripts interact with backup-related Windows functionality, security monitoring products may generate alerts related to:

- Volume Shadow Copy creation
- NTDS database access
- Registry hive export operations

Customers are advised to notify SOC, MDR, or EDR monitoring teams prior to execution.

Customer Review and Transparency

Customers are encouraged to:

- Review the scripts before execution
- Monitor execution in real time
- Inspect generated files prior to transfer
- Execute the scripts only during approved maintenance windows