Active Directory Password Audit Guide

Online and Offline assesments

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Authlogics, 329, Doncastle Road, Bracknell, Berkshire, RG12 8PE, UK
www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Authlogics may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Authlogics, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2023 Authlogics. All rights reserved.

Table of Contents

Introduction 3

Pre-requisites 3

Requirements 3

Extract Processing 3

Running the Tool 4

Usage 5

Parameters 5

Extraction Modes and Steps 8

Default Extraction Mode 8

Domain Controller Mode 8

Using Multiple Steps to Extract and Process Data 8

Offline Password Breach Extract 9

Manual Extract Process 10

Process 10

Audit Report Result 13

Audit Controls 15

Administrator accounts with passwords that have been breached 15

Accounts with passwords that have been found in previous breaches 15

Accounts with passwords that are commonly breached 15

Breached account passwords with identifiable information 16

Breached accounts with matching emails and passwords 16

Accounts with shared passwords 16

Emails for this domain with breached passwords 17

Introduction

The Authlogics Password Audit Tool is a command-line program that retrieves user accounts from an Active Directory Domain and analyses passwords to identify potential security and compliance issues. The tool is designed specifically so that no sensitive data leaves the corporate network, with all processing done locally on the machine running the audit tool. For more information, please contact Authlogics.

All extracted data is encrypted by default; data files generated from the audit process contain sensitive user information and should be handled accordingly. The tool generates a set of text and CSV report files that contain no sensitive password information.

Authlogics Password Audit Tool includes offline password breach analysis which does not require access to the cloud-hosted Authlogics Password Breach Database and is designed to work fully on-premise.

> ***Note***
> *When running the Password Audit Tool against the on-premise Password Breach Database, no email address analysis will be performed.*

Pre-requisites

The following requirements need to be met for a successful audit.

> ***Note***
> *The Password Audit Tool will attempt to determine whether the pre-requisites requirements are met before the extract process commences.*

Requirements

- A domain-joined machine with access to a Domain Controller.
- Domain Administrator user account permissions for the user running the Password Audit Tool.
- Ability to run Command Prompt with administrator privileges.
- .Net Framework version 4.8 or later on the machine running the Authlogics Password Audit Tool.

Domain Controller Only Extraction Mode

- The Volume Shadow Copy service needs to be running (on by default).
- The Active Directory Management tools need to be installed (installed by default).

Extract Processing

- A valid Authlogics Password Cloud Database or offline API key (provided by Authlogics)
- An Internet connection with HTTPS access to Authlogics Password Breach database for online processing
  `https://passwordsecurityapi.authlogics.com/api/*`
- Access to Offline Breach database for offline processing

- .Net Framework version 4.8 or later

The audit tool will attempt to connect to the internet to process the extract data and will use the system proxy settings if available. If an Internet connection is not available, the data can be extracted from the server and the analysis process can be completed on a separate machine. If the .Net framework 4.8 or later is not available, the required Active Directory files can be manually extracted and processed separately. See Manual Extract Process for details.

Running the Tool

Authlogics Password Audit Tool is a command-line tool that accepts various parameters and will function based on the provided parameters. By default, the tool will perform the following tasks in sequence:

- Verify the requirements listed above
- Perform a full Active Directory Backup
- Extract the relevant user and password information and create an encrypted export file
- Clean-up any data generated by the backup process
- Connect to Authlogics Cloud Password Database and perform user and password analysis
- Generate text reports and output .csv files

Usage

passtool.exe APIKEY [/I *Inputfile*] [/O *Outputfile*] [/D] [/N *DomainName*] [/P *Password*] [/F] [/V] [/DC] [/Offline] [/ADPermissions][/DormantDays *Days*]

Parameters

Parameter	Name	Description
APIKEY		Provide the Authlogics supplied API Key. An API Key is always required unless running the tool using the Validate option.
?	Help	Provides help on the parameters available
O	Output File	Save the extraction data to a hashes data file. Use this option when the machine extracting active directory data does not have access to the internet, directly or through a proxy. Analysis and reporting can take place on a separate machine providing the same API keys are used. If no filename is specified with the **/O** parameter, a file called ***extract.dat*** will be created.
I	Input File	Specify the name of the extraction output file, or system files to be processed. Use this option when the /O option has been performed and the contents are available for analysis and a machine with an internet connection, or when data has been manually extracted. If no filename is specified with the **/I** parameter, the tool will try to import a file called ***extract.dat***.
D	Debug	Enable enhanced diagnostic mode for debugging purposes.
N	Domain Name	Specify the domain name from Active Directory used to report domain breaches. This option is typically used when the AD domain name does not match the organisation's email address notation i.e. *acme.local* vs *acme.com*. This parameter will report the email addresses for the specified domain found in the Authlogics Password Breach Database.
P	Password	Specify password used in encryption/decryption of input and output files instead of using the API key.
F	Full hashes	Send full password hashes to Authlogics online servers; turning off partial K-Anonymity.
V	Validate	Validate only. Use this option to run the verification step only. This can be useful to ensure the environment is configured correctly before a full audit is run.
DC	Domain Controller Only Extraction	Execute Authlogics Password Audit data using a domain-controller based alternate extract method (default method for version 1.x). This can only be performed by a Domain Administrator on a Domain Controller. When executing the solution in domain controller mode, the Windows Volume Shadow Copy service needs to be running and the Active Directory Management tools need to be installed locally.

Offline	Offline Mode	Prevent Authlogics Password Audit Tool from accessing the internet and processing any data online. Running in Offline mode will limit what is reported on as sections like password breaches and identifiable email analyses require Internet access for processing. **NOTE**: A special offline API key is required to run Password Audit Tool in Offline mode. Please contact Authlogics for an Offline API key.
OU	Organisational Unit	Limit the audit to report on users that are a member of the specified Active Directory Organisational Unit only. Accounts that are not a member of the specified Organisational Unit will be ignored.
Active	Active Users Only	Limit the audit to report on Active accounts only. Disabled and Expired accounts will be ignored.
Admin	Administrator Accounts Only	Limit the audit to report on Administrator and elevated privileged accounts only. Non-administrator Active Directory accounts will be ignored.
B	Blacklist	Enable the Blacklist file mode which allows an administrator to specify a custom set of passwords to report against. When enabled, create a *Blacklist.txt* file in the same directory as the Audit tool executable and then enter the passwords (in clear text) to report against.
DCServerName	Domain Controller Server Name	Override the auto-detection of a Domain Controller and specify the Domain Controller to run the tool against.
ADPermissions	Active Directory Domain Permissions	Extract and report on Advanced Security Settings for the root domain.
DormantDays	Number of days since last-logon	Set the number of days elapsed for an account not to have logged in to be deemed to be a dormant account. If no number is specified, then any account not logged in within the last 90 days will be deemed to be a dormant account. Setting this value to 0 will turn off this analysis.
ExcludeBreachedEmails	Exclude breached email analysis	Limit the analysis to exclude the analysis of matched breached email addresses.
OfflineBreachedDBPath	Perform on-premise password breach analysis	Specify the location of the offline password breach database. When not specified, the current folder will be applied. Offline parameter must be selected for this option to be enabled.
VerboseUserDetails	Extract and report on extended user details	Enable detailed user extraction and reporting. VerboseUserDetails parameter must be selected for this parameter to be enabled. NOTE: This option is not available for offline extracts.

VerboseUserDetails

When the Authlogics Password Audit Tool is run using the **VerboseUserDetails** parameter, the following additional data is extracted and listed in the CSV files.

- fullName
- username
- isAdministrator
- isDomainAdmin
- isEnterpriseAdmin
- isDisabled
- isExpired
- isBreached
- passwordNeverExpires
- passwordNotRequired
- lastLogon
- passwordLastChanged
- samaccountname
- displayName
- distinguishedName (CNs are ";" delimetered)
- enabled
- name
- canonicalName
- LMHashPasswordExists
- DefaultPassword
- PreAuthNotRequired
- AESKeyMissing
- UseDESKeyOnly
- AdminDelegated
- KerberosRoasting
- emails

Extraction Modes and Steps

Authlogics Password Audit Tool can be executed using two different data extraction modes, on either any machine joined to the domain, or directly on a Domain Controller if required.

If the machine has an active Internet connection, then the extract and analysis is performed in a single step. If the machine does not have an Internet connection, then the processing of the data will need to occur on a machine with an internet connection providing access to the Authlogics Password Breach Database. Both extraction modes can be used to create output files, although this option is usually only required when data extraction occurs using the Domain Controller extraction mode.

Default Extraction Mode

Authlogics Password Audit Tool will utilise the context of the user running the Command Prompt. If you are logged onto a domain-joined machine using a non-Domain Admin account, we recommend you either logoff and then logon with a Domain Admin/Enterprise Admin account or open a Command Prompt using '*Run as different user …. Using a domain account.*'

The tool will then auto-detect the domain name and closest Domain Controller which are both needed for the extract process.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY
```

Wherever possible, Authlogics tries to remove temporary files and folders on completion, however, this may not always be the case. In these cases, we recommend that you manually remove the temporary files left behind.

Domain Controller Mode

If a domain-joined machine cannot remotely access the data on a Domain Controller, it may be necessary to extract, and optionally process, the information directly on a Domain Controller, using a different underlying method for extracting account information from Active Directory.

As per the default extraction method, we recommend you either logoff and then logon with a Domain Admin/Enterprise Admin account or open a Command Prompt using '*Run as different user …. Using a domain account.*' and run the executable using the */DC* command-line switch.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /DC
```

Using Multiple Steps to Extract and Process Data

When the machine used to extract account information from Active Directory does not have Internet access, the required extract file can be copied onto any Windows computer with Internet access and then processed separately.

To do this, first execute the Authlogics Password Audit Tool as normal using either the default or domain controller extraction method, additionally adding the **/O** (Output mode) command-line parameter. Copy the encrypted output file to a machine with internet access and then use the **/I** (Input) parameter using the same API key in both processes.

If no file name is specified, then the filename will be called ***extract.dat.*** If a name is provided, the file name can be any name you wish except ***ntds.dit,*** which is reserved for manual extracts.

```
C:\Authlogics\PasswordAudit\Server\>passtool.exe APIKEY /O AcmeDomain1.dat
```

In the example above, a file called “AcmeDomain1.dat” will be created in the same folder as the executable. Copy this file to a machine with Internet access for processing.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /I AcmeDomain1.dat
```

Offline Password Breach Extract

The following commands extract the Active Directory user’s password information locally for and process the breach password database from a local on-premise Password Breach Database and does not connect to the cloud for analysis.

By default, the tool will attempt to locate the on-premise Password Breach database in the current executing folder “Breach Database” sub-folder . This folder structure can be overridden using the /OfflineBreachDBPath parameter.

Execute passtool.exe using the **/Offline** and **/OfflineBreachDBPath** parameters.

The example below extracts the Password Audit Tool where the Breach Database folder resides in C:\Authlogics\Breach Database

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /Offline /OfflineBreachDBPath “C:\Authlogics”
```

Manual Extract Process

The following commands extract the Active Directory user's password information locally for offline/remote processing purposes. The manual extraction should only be used when no other option is available. This will perform a full Active Directory database backup and will provide the raw data files which can be processed on a separate machine. The files contain sensitive user information and should be handled accordingly.

> ***Note***
> *This is not the recommended method and should only be used when other methods are not available.*

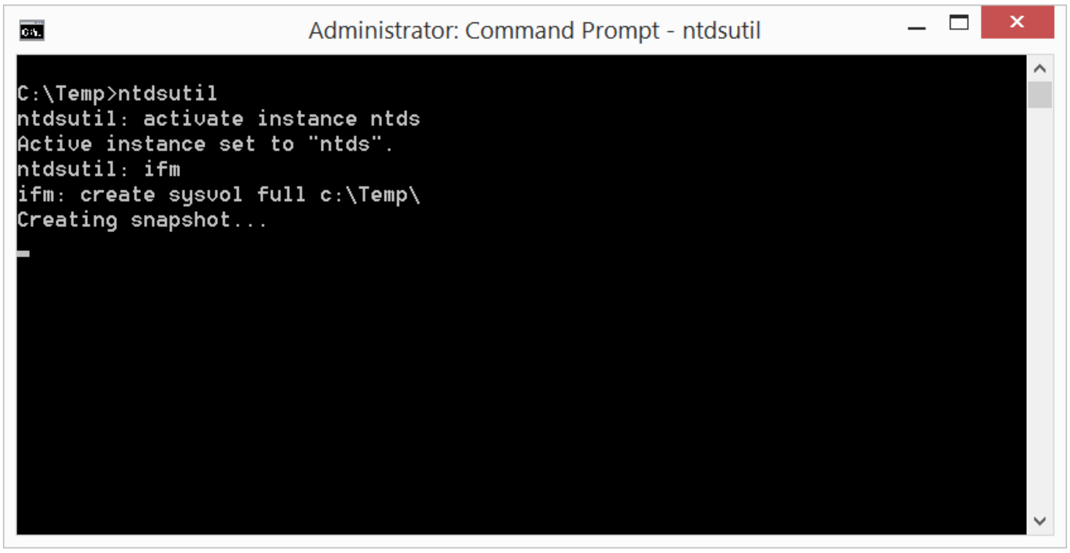
These steps can ONLY be performed by a Domain Administrator on a Domain Controller with:

- The Volume Shadow Copy service needs to be running (on by default)
- The Active Directory Management tools need to be installed on the DC (installed by default)

The Manual Process utilises the inbuilt Microsoft Active Directory command-line tool *NTDSUtil.exe.*

Process

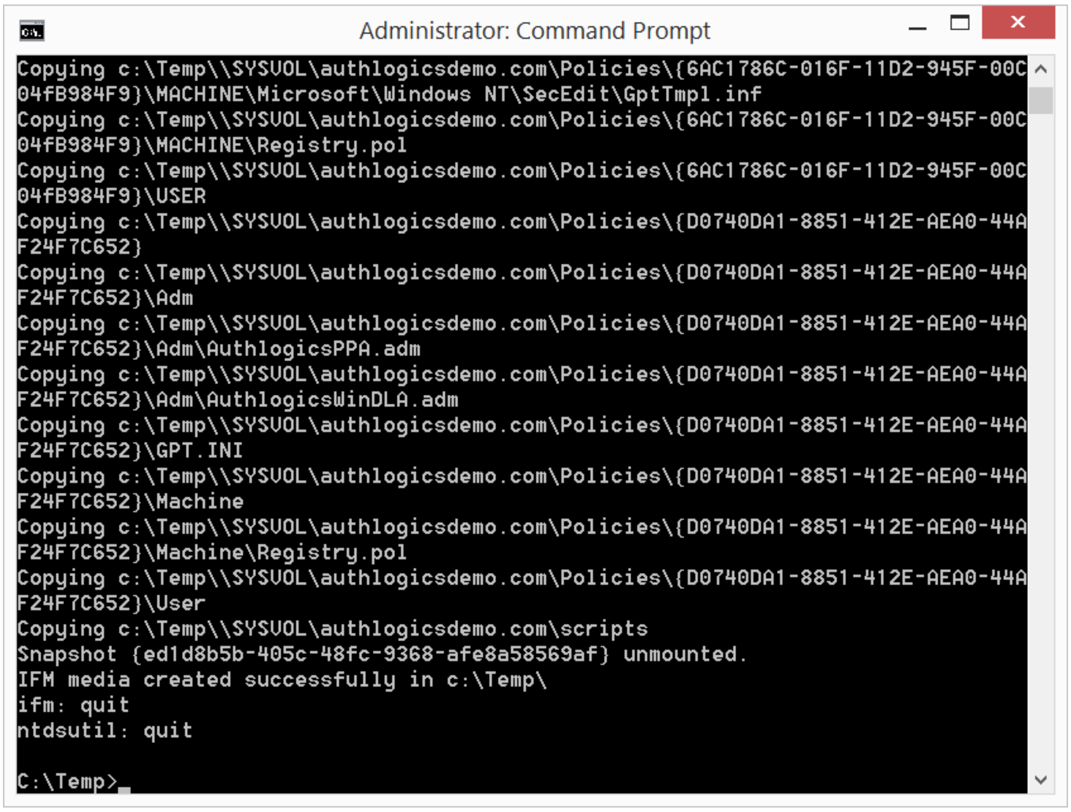
1. Open an administrative command prompt on a Domain Controller within the targeted domain using a Domain Administrator account.
2. Create a Temporary folder on the server. Ensure that the folder is empty. E.g. C:\Temp
3. Change directory to the temp folder
4. Type the following commands:
    - *ntdsutil*
    - *activate instance ntds*
    - *ifm*
    - *create sysvol full C:\Temp\*



```
C:\Temp>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create sysvol full c:\Temp\
Creating snapshot...
```

Wait for the process to complete then quit the *ntdsutil* operation

- *quit*
- *quit*



```
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{6AC1786C-016F-11D2-945F-00C
04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{6AC1786C-016F-11D2-945F-00C
04fB984F9}\MACHINE\Registry.pol
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{6AC1786C-016F-11D2-945F-00C
04fB984F9}\USER
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\Adm
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\Adm\AuthlogicsPPA.adm
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\Adm\AuthlogicsWinDLA.adm
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\GPT.INI
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\Machine
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\Machine\Registry.pol
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\Policies\{D0740DA1-8851-412E-AEA0-44A
F24F7C652}\User
Copying c:\Temp\\SYSVOL\authlogicsdemo.com\scripts
Snapshot {ed1d8b5b-405c-48fc-9368-afe8a58569af} unmounted.
IFM media created successfully in c:\Temp\
ifm: quit
ntdsutil: quit

C:\Temp>_
```

On completion, the following folders will remain in the extract folder:

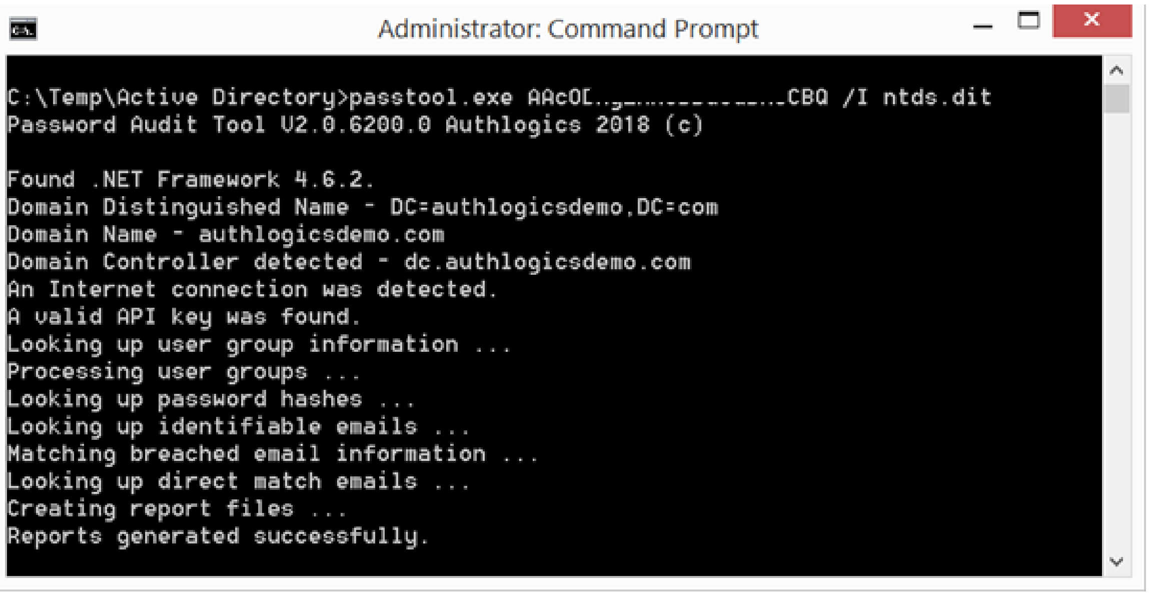
- Active Directory
- Registry
- SYSVOL

To process and analyse the contents, copy **"\Active Directory\NTDS.dit"** and **"Registry\SYSTEM"** files to a temporary folder on a machine with the pre-requisites noted above. Copy the **passtool.exe** file to the same folder.

> ***Note***
> *As the process is manual, the residual files will not auto-clean and therefore should be deleted manually once the analysis has been processed.*

Execute passtool.exe using the **/I** option specifying the **ntds.dit** file.

```
C:\Authlogics\PasswordAudit\>passtool.exe APIKEY /I ntds.dit
```



```
C:\Temp\Active Directory>passtool.exe AAcOL[redacted]CBQ /I ntds.dit
Password Audit Tool V2.0.6200.0 Authlogics 2018 (c)

Found .NET Framework 4.6.2.
Domain Distinguished Name - DC=authlogicsdemo,DC=com
Domain Name - authlogicsdemo.com
Domain Controller detected - dc.authlogicsdemo.com
An Internet connection was detected.
A valid API key was found.
Looking up user group information ...
Processing user groups ...
Looking up password hashes ...
Looking up identifiable emails ...
Matching breached email information ...
Looking up direct match emails ...
Creating report files ...
Reports generated successfully.
```

Audit Report Result

When the analysis has been completed, the audit report will be created in a folder dated with the processing date and contains the following text and comma-separated files:

Filename	Extension	Reported Offline	Description
Summary-report	Txt	No	Consolidated summary of the analysis.
Detail-report	Txt	Yes	Detail listing of accounts matching criteria of analysis control.
Ad-principal-permissions	Txt	Yes	Lists the advanced security permissions for the root domain. Extracted using ADPermissions parameter.
Aeskeymissing-accounts	Csv	Yes	Lists all AD accounts where weak encryption algorithms like DES or RC4 can be used during authentication of accounts as these accounts are missing Kerberos AES Keys. Extracted using VerboseUserDetails parameter.
Aeskeymissing-admin-accounts	Csv	Yes	Lists all Administrator AD accounts where weak encryption algorithms like DES or RC4 can be used during authentication of accounts as these accounts are missing Kerberos AES Keys. Extracted using VerboseUserDetails parameter.
Blankpwd-accounts	Csv	Yes	Lists all accounts that have a blank password
Blankpwd-admin-accounts	Csv	Yes	Lists all Administrator accounts that have a blank password
Breached	Csv	No	Lists all the AD accounts with breached passwords
Breached-administrators	Csv	No	Lists all the administrator AD accounts with breached passwords.
Breached-common	Csv	No	Lists all the AD accounts with commonly breached passwords i.e. these accounts have been breached thousands of times and therefore are deemed to be common.
Breached-identifiable	Csv	No	Lists all the AD accounts with breached passwords which can be traced to social media and other breaches based on breached password in use.
Breached-matching	Csv	No	Lists all the AD accounts with breached passwords which match the local domain name. ie. the username/email address and password are breached and can be used to authenticate to the domain.
Defaultpwds-accounts	Csv	Yes	Lists all the AD accounts where the password is set to the default password (logon username). Extracted using VerboseUserDetails parameter.
Defaultpwds-admin-accounts	Csv	Yes	Lists all the administrator AD accounts where the password is set to the default password (logon username). Extracted using VerboseUserDetails parameter.
Deskeyonly-accounts	Csv	Yes	Lists all the AD accounts using DES as the block cipher for encryption and susceptible for brute force attacks. Extracted using VerboseUserDetails parameter.

Deskeyonly-admin-accounts	Csv	Yes	Lists all the administrator AD accounts using DES as the block cipher for encryption and susceptible for brute force attacks. Extracted using VerboseUserDetails parameter.
Domain-breaches	Csv	No	Lists all the email address in the Authlogics Password Breach Database matching the domain name.
Dormant-accounts	Csv	Yes	Lists all accounts that have not logged on for the period of days specified by the /DormantDays parameter. The default is 90 days.
Dormant-admin-accounts	Csv	Yes	Lists all administrator accounts that have not logged on for the period of days specified by the /DormantDays parameter. The default is 90 days.
Lmhashpwdexists-accounts	Csv	Yes	Lists all the AD accounts with passwords stored in LM Hash form. Extracted using VerboseUserDetails parameter.
Lmhashpwdexists-admin-accounts	Csv	Yes	Lists all the administrator AD accounts with passwords stored in LM Hash form. Extracted using VerboseUserDetails parameter.
Never-logged-on-accounts	Csv	Yes	Lists all accounts that have never logged on.
Preauthnotreqd-accounts	Csv	Yes	Lists all the AD accounts with where pre-authentication has been disabled. Extracted using VerboseUserDetails parameter.
Preauthnotreqd-admin-accounts	Csv	Yes	Lists all the administrator AD accounts with where pre-authentication has been disabled. Extracted using VerboseUserDetails parameter.
Servicedelegatable-admin-accounts	Csv	Yes	Lists all the administrator AD accounts which can be delegated as a service. Extracted using VerboseUserDetails parameter.
Shared-passwords	Csv	Yes	Lists the partial hash of the shared passwords and accounts that share those passwords.
Shared-passwords-administrators	Csv	Yes	Lists the partial hash of the shared passwords and accounts that share those passwords with administrator accounts.
Blacklist-passwords	Csv	Yes	Lists the partial hash of the passwords and administrator accounts that match the passwords specified in the custom Blacklist.txt file.
Blacklist-passwords-administrators	Csv	Yes	Lists the partial hash of the passwords and accounts that match the passwords specified in the custom Blacklist.txt file.
Summary	Csv	No	As with Summary-report txt file in CSV format.

Audit Controls

Administrator accounts with passwords that have been breached

Risk Severity	Critical
Description	The Administrator accounts that have a password that has appeared in at least one public breach and also are members of one or more of the following Active Directory Groups: Administrators, Domain Admins, Enterprise Admins. Because these accounts have elevated privileges, the passwords should be changed to one that does not appear in a breach.
Remediation	Force the users to change their passwords to a NIST compliant password.

Accounts with passwords that have been found in previous breaches

Risk Severity	High
Description	User accounts with passwords that have been found in any breach. The password does not need to be related to the user in any way, just that this password was found in a breach somewhere at least once. This is a key part of the NIST 800-63 password guidelines, meaning this password should be changed to one that has not appeared in a breach to comply with these guidelines.
Remediation	Force the users to change their passwords to a NIST compliant password.

Accounts with passwords that are commonly breached

Risk Severity	Critical
Description	User accounts with passwords that appear often in breaches (usually more than 100 times). This means that the password is often found in breaches and would mean it could appear in a list of common passwords bad actors would use to try gain access to an account. Because these passwords are commonly breached, these passwords should be reset and users should choose a password that has not been breached.
Remediation	Force the users to change their passwords to a NIST compliant password.

Breached account passwords with identifiable information

Risk Severity	High
Description	These users have passwords that have been breached and list those with identifiable information, such as email addresses, that could allow bad actors to tie information in this password breach back to the user, allowing them to gain access to their account. The email address does not have to belong to a specific domain, the account details are used to look at full or partial matches for any email address information that could be used to identify the user. Each user password in the list should be immediately changed to a non-breached password if there is a suspicion that the email information supplied could identify the user account and allow a bad actor to gain access.
Remediation	Force the users to change their passwords to a NIST compliant password.

Breached accounts with matching emails and passwords

Risk Severity	Critical
Description	Lists users with breached passwords and email addresses that are tied directly to the active directory domain or to the domain supplied to the tool. Because both the identifying information as well as the passwords in the list match a known breach these accounts are highly likely to be compromised. These passwords for these accounts should be changed immediately to a secure, compliant password.
Remediation	Force user to change their passwords and apply multi-factor authentication to their account as they have been compromised and that their details are known.

Accounts with shared passwords

Risk Severity	High
Description	List of users by password hash that share the same password. Shared passwords can be used to compromise multiple accounts and may be against local password policies or indicate that default passwords have not been changed.
Remediation	Force user to change their passwords and ensure that users with multiple accounts (Administrative, standard, system and test accounts) do not re-use this password across accounts.

Emails for this domain with breached passwords

Risk Severity	High
Description	List of all emails found in password breaches for the active directory domain or to the domain supplied to the tool. This list provides a good indication of the amount of user account information available for use by bad actors. It does not indicate that any of these accounts have passwords that have been breached, however, these accounts are at higher risk of being involved in a breach as they are publicly associated with this domain.
Remediation	Apply multi-factor authentication to these accounts as their credentials have been compromised and the account may already have been hacked or is currently subject to attacks.