ENZOIC

SUMMARY REPORT

ENZOIC *for* ACTIVE DIRECTORY LITE

Password Audit Results

ACTIVE DIRECTORY

PASSWORD AUDIT RESULTS

ENZOIC

Executive Summary

Below are the results of your Enzoic for Active Directory Lite password audit. Enzoic scans for credentials related issues in your Active Directory that could pose a risk to your organization. By leveraging its industry-leading, up-to-the-minute database of billions of compromised credentials, Enzoic ensures you have the most accurate and comprehensive picture of the password security of your Active Directory.

Scan Results

8/28/2024

enzoic-josh.local | 1,001 users — **HEALTHY**

Accounts with Compromised Passwords	0	HIGH RISK
These passwords have been exposed in breaches and may have specifically been compromised alongside one of your user’s information, thus making them a prime target for attackers.		
Accounts with No Passwords	0	HIGH RISK
Active accounts with no password could potentially be logged into by anyone without restrictions.		
Accounts with Weak Passwords	0	MEDIUM RISK
Weak passwords pose a risk for credential spraying attacks and could easily be cracked if an attacker is able to extract password hashes from the Active Directory.		
Accounts Sharing Passwords	0	MEDIUM RISK
Sharing passwords between accounts is poor security practice and could indicate a password is being socialized amongst users, increasing the risk of exposure.		
Stale Accounts	1,000	LOW RISK
Stale user accounts in Active Directory have not been logged into in the last 6 months. They are a security risk since they could be used by an attacker or a former employee.		

NEXT STEPS

ACCOUNTS WITH COMPROMISED PASSWORDS

HOW TO FIX: Ensuring that all users with compromised passwords update to a secure password will mitigate your organization’s risk from exposed or vulnerable credentials. In Active Directory Users and Computers, you can right-click a user with a vulnerable password then select Properties. Click the Account tab, navigate to Account Options and check the box next to “User must change password at next logon”. Scans should be performed regularly to ensure the updated passwords are not compromised.

ACCOUNTS WITH NO PASSWORDS

HOW TO FIX: In the Active Directory Module for Powershell, the following command will require a user account to have a password: `Net user <username> /passwordreq:yes`

ACCOUNTS WITH WEAK PASSWORDS

HOW TO FIX: Ensuring that all users with weak passwords update to a secure password will mitigate your organization’s risk of compromise. In Active Directory Users and Computers, you can right-click the user with a vulnerable password then click Properties. Click the Account tab, navigate to Account Options and check the box next to ”User must change password at next logon”. This will prompt the user to update their password.

ACCOUNT SHARING PASSWORDS

HOW TO FIX: It is recommended that all users with a shared password update to a secure password. In Active Directory Users and Computers, you can right-click the user with a shared password then click Properties. Click the Account tab, navigate to Account Options and check the box next to ”User must change password at next logon”. Scans should be performed regularly to ensure the updated passwords are not weak.

STALE ACCOUNTS

HOW TO FIX: Deleting inactive accounts will prevent these accounts from posing a security risk to your environment. Microsoft recommends disabling user accounts before deleting them to ensure there are no issues. You can disable and delete accounts by right-clicking on a user in Active Directory Users and Computers.

ENZOIC

Enzoic for Active Directory allows for real-time blocking of unsafe passwords at setup and then automatically provides continuous monitoring of those same passwords to ensure they don’t become vulnerable later. This ongoing protection is essential because a password that was safe yesterday may not be secure today. By continuously monitoring for compromised credentials, organizations can stop enforcing periodic password resets, meaning that users only need to change their password if it is compromised. This efficiency reduces IT help desk costs and improves security because users will choose better passwords if they don’t have to change them frequently. Enzoic indexes newly compromised passwords daily, so your organization is immediately protected. We source our data from the public Internet, Dark Web, and private sources. It is updated continuously by proprietary automated processes and human threat intelligence to ensure your accounts and PII stay secure.