Authlogics Active Directory Password Audit

Audit Report Prepared For

Sample

14 June 2018

Authlogics Ltd, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

Report Details

Company	Sample
Domain Analysed	Sample.org
Analysis Date and Time	04/06/2018 12:04:11

Introduction

The following report is compiled from the metrics retrieved by running the Authlogics Password Audit Tool on your domain controllers to analyse the passwords currently in use in your organisation. Below are the findings highlighting the critical and high-risk areas we recommend addressing. Detailed information has been supplied as part of the audit.

Executive Summary

	Count	%	Risk
Accounts audited	15558		
Enabled accounts	8196	52.68	
Enabled accounts with breached passwords	3541	43.2	High
Administrators with breached passwords	34	0.22	Critical
Accounts with breached passwords	7771	49.95	High
Accounts with commonly breached passwords	3449	22.17	Critical
Breached accounts with identifiable information	325	2.09	Medium
Breached accounts with matching passwords	4	0.03	Critical
Accounts with shared passwords	6185	39.75	High
Emails for this domain with breached passwords	79	0.51	Medium

An audit was conducted, and out of the 15558 accounts, 7771 accounts (49.95%) have passwords that have been found in breaches. Of this number, 3541 of the accounts (43.2%) are enabled and 34 (0.22%) belong to your administrators.

The high percentage of accounts using breached passwords is of great concern and requires immediate addressing.

The high number of accounts using commonly breached passwords is of serious concern as these passwords are typically very weak and are easily guessed or brute-forced.

4 user accounts were found to have an exact match of the account name and password which would allow immediate access and compromise of your systems.

We detected a number of email accounts for this domain with breached passwords making these accounts subject to attack.

Compliance Status

NIST Special 800-63b Compliance	Fail
GDPR Best Practice	Fail

In order to pass the compliance and best practice checks for **NIST SP800-63b** and **GDPR** respectively, no accounts in your environment must be using breached passwords.

Recommendation

We recommend that accounts that have been breached are forced to change their passwords to a password that has not been breached by using tools such as Authlogics Password Policy Agent.

For accounts with emails from within this domain that have breached passwords, multi-factor authentication should be applied to these accounts.

Analysis

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.
Analysis Result	**Count**: 34 — **Percentage**: 0.22

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.
Analysis Result	**Count**: 7771 — **Percentage**: 49.95

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.
Analysis Result	**Count**: 3449 — **Percentage**: 22.17

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.
Analysis Result	**Count** / **Percentage** 325 / 2.09

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.
Analysis Result	**Count** / **Percentage** 4 / 0.03

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.
Analysis Result	**Count** / **Percentage** 6185 / 39.75

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 the user's accounts as their accounts are known and therefore it is safe to assume that the account has been hacked or is currently subject to multiple attacks.
Analysis Result	**Count** / **Percentage**: 79 / 0.51

User Metrics

	Count	Percentage
Total Accounts	15558	
Enabled accounts	8196	52.68
Enabled accounts with breached passwords	3541	43.2
Disable accounts	7362	47.32
Expired accounts	0	0
Number of breached disabled accounts	4230	27.19
Number of breached expired accounts	0	0

Background

I.T. security, regulatory compliance and audit controls are topics that no system administrator can ignore, and a great amount of time and expense can be spent protecting environments from a wide variety number of threats.

Passwords are still an integral part of an organisations security profile and will be for the foreseeable future. Sadly, for most systems, a compromise on an individual's password renders all other security controls useless and exposes their systems to all and sundry; irrespective of the expensive and detailed layers of firewalls, honey-pots and detection solutions put in place.

Within an organisation, the most important password to protect is the user's Windows Active Directory password as it is usually the only one a user ever needs and is used to access everything. A compromise on these passwords effectively exposes your environment to breaches.

Regulatory Compliance

Governments around the world are continuously releasing new frameworks for organisations to adhere to with General Data Protection Regulation (GDPR) being one of those designed to protect the data of all EU citizens. Part of this legislation is the enforcement of internal IT Security controls and ensuring that companies are taking all the necessary precautions to secure their IT systems. However, these guidelines tend not to be rather generic and high-level and not prescriptive. A such, organisations need to adhere by adapting to best practice guidelines from standards authorities.

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce and is one of these trusted authorities. In June 2017, this government body released a Special Publication (SP 800-63b) on Digital Identity Guidelines with an area dedicated to passwords do's and don'ts. Their recommendations include increasing passwords to a minimum of 8 characters and have no upper boundary for lengths.

Furthermore, they suggest that passwords include Uppercase and lower-case characters, numeric and special characters that include emoji's and not only the normal "!"£$%&*()". The guidelines also note that password reminders should not be used as they can reveal the real password.

One of the key aspects of this publication is that users should not be allowed to select passwords that have been previously breached from the thousands of hacks perpetrated over the years. For this Authlogics has created a Password Policy Agent (PPA) that processes password change requests and checks user 's passwords to ensure NIST compliance and that passwords haven't been previously breached.

Authlogics Password Policy Agent

Authlogics Password Policy Agent (PPA) has been designed from the ground up to allow organisations to enforce the latest password guidelines, reduce helpdesk calls for password-related problems, and improve productivity with fewer password changes and lockouts. Once installed on Active Directory servers, the software immediately intercepts and analyses password changes as they happen, no matter where they originate from, ensuring compatibility with 3rd party software and helpdesk management systems.

There is no need to install extra software onto workstations. Password Policy Agent is centrally managed and has a small footprint. All password change attempts, both accepted and declined, are logged centrally for auditing and reporting purposes.

Authlogics Password Audit Tool

Authlogics Password Policy Agent does an excellent job of preventing non-NIST compliant passwords entering the system and compromising the environment, however, organisations can still be exposed based on passwords that have been selected prior to the adoption of PPA.

Previously, organisations need to employ highly skilled ethical hackers who would spend hours if not days to access the corporate Active Directory database, use specialised tools to extract the hashed passwords and then, due to the limitations of brute forcing attempt to reverse the hashes to get the clear text passwords to see how many are “weak” and report accordingly. Sadly, this approach, apart from being rather time-consuming and costly, tends to be limited in its scope and cannot determine the number of passwords being used that have been previously breached.

Authlogics Password Audit Tool is a tool designed for security specialists and administrators to ethically hack their Active Directory and generate a comprehensive and consistent report ensuring the password posture of their current environment complies to best-practice and NIST standards.