Weak Passwords (version 1.0)

**Cloud Service Label: IaaS, PaaS, SaaS**

Description

Adversaries may be able to exploit weak passwords to gain initial access. When user accounts utilize weak, or reused passwords, it runs the risk of adversaries gaining access, once access is gained, they can continue on in their attack. The adversary may have the ability to change user credentials locking the user out, collect data, maintain persistence, escalate privileges, and move laterally. The level of access, and ability for adversary to complete these tasks, is dependent on the permissions the user of the exploited password holds.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| SYNACKTIV’s Azure AD Introduction to Red Teaming | This Introduction to Red Teaming outlines how an adversary can utilize weak passwords and harvested emails to gain initial access to a system. From there it is explained how an adversary may be able to move laterally and maintain persistence. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| [Account Segmentation](https://attack.mitre.org/mitigations/M1030) | | Consider separating different resources under different administrative domains so that credential compromise does not put all assets in danger. In the case of Azure, multiple subscriptions can be created with different administrators that can only access resources within the subscription. The subscriptions can still belong under the same Azure account for overall accounting and administration/policy. |
| [Multi-factor Authentication](https://attack.mitre.org/mitigations/M1032) | | Use multi-factor authentication for user and privileged accounts. Do not manage Cloud portals from machines that perform user email and web browsing tasks. All users should be required to utilize two factor authentication. |
|  | AWS | This can be enforced by first creating a policy that would prohibit actions except those that allow a user to change their password or manage 2FA, then attaching a policy to a group that includes all user accounts where they can be allowed all access if they sign in with 2FA. Once these actions are completed it should be tested to verify the access is given correctly. To see full details on how to complete this view AWS documentation at: **https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\_users-self-manage-mfa-and-creds.html.** |
|  | Azure | This can be done by creating a MFA registration policy. It can than be assigned to all users (with the ability to exclude some if need be, but is not recommended). Make sure once the policy is created and added to users that it is then being enforced, once enforced it should be tested for verification. To see full details on how to complete this view Azure documentation at: **https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy.** |
|  | GCP | This can be done by first enabling it on the current account being used by admin to assign the roles, then enable two factor on an instance by instance or project by project basis, then assigning the requirements based on IAM roles and applying it to all users. To see full details on how to complete this view Azure documentation at: **https://cloud.google.com/compute/docs/oslogin/setup-two-factor-authentication.** |
| [Privileged Account Management](https://attack.mitre.org/mitigations/M1026) | | Do not allow subscription-level administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems. |
|  | AWS | To manage the access that privileged accounts have on the AWS cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account the IAM limited administrator would be used. This is done by creating a policy that gives a user admin rights, but disallows the other actions using the AWS command line interface. This is outlined at: [**https://aws.amazon.com/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/**](https://aws.amazon.com/blogs/security/how-to-create-a-limited-iam-administrator-by-using-managed-policies/)**.** |
|  | Azure | To manage the access that privilege accounts have on the Azure cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account the specific administrative needs can be picked from a number of options available (Azure DevOps Administrator, Billing Administrator, Cloud Application Administrator, etc.) These different options can be edited to fit the needs and limit the basic access. This is outlined at: [**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles)**.** |
|  | GCP | To manage the access that privilege accounts have on the Azure cloud system to only allow administrators to perform administrative tasks on such accounts can be accomplished utilizing limited IAM administrator accounts. To configure this the administrator would have two accounts; one would have administrative rights and no basic access while the other account has basic access with no administrative rights. To limit the administrative account pre-defined administrator accounts can be used (mobile admin, Google voice admin, help desk admin, etc.). These accounts can be used with their pre-defined settings, or modified depending on specific use cases. These can limit access to basic functionality needed. This is outlined at: [**https://support.google.com/a/answer/2405986?hl=en**](https://support.google.com/a/answer/2405986?hl=en)**.** |
| Strong Password Policies | | Strong password policies in place, as well as training, so users are aware passwords should not be reused from previous accounts. |
|  | AWS | Good password practices can be enforced in AWS via the console, AWS CLI, and AWS API. These configurations are for IAM accounts only and have a range of different characteristics that can be enforced. For instance minimum password length, require a range of characters (lowercase, uppercase, number, and non alphanumeric ), allow users to change their own password, password expiration, prevent password reuse, and require administrator reset after password expiration. All details on how to configure these enforcement policies with all three management systems can be found here: **https://docs.aws.amazon.com/IAM/latest/UserGuide/id\_credentials\_passwords\_account-policy.html.** |
|  | Azure | Good password practices can be enforced in Azure only with managed domains created using the resource manager deployment. By default these accounts have some policies enforced including amount of lockout duration, allowed number of logon attempts, Reset failed logon attempts count after 30 minutes, and lifetime of password. Other policies that can be changed are minimum password length and the ability to enforce the concept of ‘passwords must meet complexity requirements’. These configurations can be accomplished by accessing the Active Directory Administrative Center under administrative tools, then editing the rules under the settings for the Password Settings Container. Full details on how to accomplish this can be found here: **https://docs.microsoft.com/en-us/azure/active-directory-domain-services/password-policy.** |

Detection

Collect events that correlate with changes to account objects on systems and the domain, such as event ID 4738. Monitor for modification of accounts in correlation with other suspicious activity. Changes may occur at unusual times or from unusual systems. Especially flag events where the subject and target accounts differ or that include additional flags such as changing a password.

Use of credentials may also occur at unusual times or to unusual systems or services and may correlate with other suspicious activity. Azure displays all sign-ins to AD under the Active Directory blade.

References

1. https://www.synacktiv.com/posts/pentest/azure-ad-introduction-for-red-teamers.html. Accessed May 14, 2020.