Password Policies, Mitigation M1027 - Enterprise

Archived: 2026-04-05 15:29:37 UTC

Enterprise T1110 Brute Force

Refer to NIST guidelines when creating password policies.[1]

.001 Password Guessing

Refer to NIST guidelines when creating password policies. [1]

.002 Password Cracking

Refer to NIST guidelines when creating password policies. [1]

.003 Password Spraying

Refer to NIST guidelines when creating password policies. [1]

.004 Credential Stuffing

Refer to NIST guidelines when creating password policies. [1]

Enterprise T1555 Credentials from Password Stores

The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password.

Organizations may consider weighing the risk of storing credentials in password stores and web browsers. If system, software, or web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in improper locations.

.001 Keychain

The password for the user's login keychain can be changed from the user's login password. This increases the complexity for an adversary because they need to know an additional password.

.003 Credentials from Web Browsers

Organizations may consider weighing the risk of storing credentials in web browsers. If web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in web browsers.

.005 Password Managers

Refer to NIST guidelines when creating password policies for master passwords.[1]

Enterprise T1187 Forced Authentication

Use strong passwords to increase the difficulty of credential hashes from being cracked if they are obtained.

Enterprise T1556 Modify Authentication Process

Ensure that `AllowReversiblePasswordEncryption` property is set to disabled unless there are application requirements.[2]

.005 Reversible Encryption

Ensure that `AllowReversiblePasswordEncryption` property is set to disabled unless there are application requirements.[2]

Enterprise T1601 Modify System Image

Refer to NIST guidelines when creating password policies. [1]

.001 Patch System Image

Refer to NIST guidelines when creating password policies. [1]

.002 Downgrade System Image

Refer to NIST guidelines when creating password policies. [1]

Enterprise T1599 Network Boundary Bridging

Refer to NIST guidelines when creating password policies. [1]

.001 Network Address Translation Traversal

Refer to NIST guidelines when creating password policies. [1]

Enterprise T1003 OS Credential Dumping

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.001 LSASS Memory

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.002 Security Account Manager

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.003 NTDS

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.004 LSA Secrets

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.005 Cached Domain Credentials

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.006 DCSync

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.007 Proc Filesystem

Ensure that root accounts have complex, unique passwords across all systems on the network.

.008 /etc/passwd and /etc/shadow

Ensure that root accounts have complex, unique passwords across all systems on the network.

Enterprise T1201 Password Policy Discovery

Ensure only valid password filters are registered. Filter DLLs must be present in Windows installation directory (`C:\Windows\System32\` by default) of a domain controller and/or local computer with a corresponding entry in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages` . [3]

Enterprise T1563 Remote Service Session Hijacking

Set and enforce secure password policies for accounts.

.001 SSH Hijacking

Ensure SSH key pairs have strong passwords and refrain from using key-store technologies such as ssh-agent unless they are properly protected.

Enterprise T1021 Remote Services

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.

.002 SMB/Windows Admin Shares

Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.

Enterprise T1072 Software Deployment Tools

Verify that account credentials that may be used to access deployment systems are unique and not used throughout the enterprise network.

Enterprise T1558 Steal or Forge Kerberos Tickets

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire.[4] Also consider using Group Managed Service Accounts or another third party product such as password vaulting.[4]

.002 Silver Ticket

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire.[4] Also consider using Group Managed Service Accounts or another third party product such as password vaulting.[4]

.003 Kerberoasting

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire.[4] Also consider using Group Managed Service Accounts or another third party product such as password vaulting.[4]

.004 AS-REP Roasting

Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. Also consider using Group Managed Service Accounts or another third party product such as password vaulting. [4]

Enterprise T1552 Unsecured Credentials

Use strong passphrases for private keys to make cracking difficult. Do not store credentials within the Registry. Establish an organizational policy that prohibits password storage in files.

.001 Credentials In Files

Establish an organizational policy that prohibits password storage in files.

.002 Credentials in Registry

Do not store credentials within the Registry.

.004 Private Keys

Use strong passphrases for private keys to make cracking difficult.

Enterprise T1550 Use Alternate Authentication Material

Set and enforce secure password policies for accounts.

.003 Pass the Ticket

Ensure that local administrator accounts have complex, unique passwords.

Enterprise T1078 Valid Accounts

Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.[5] When possible, applications that use SSH keys should be updated periodically and properly secured.

Policies should minimize (if not eliminate) reuse of passwords between different user accounts, especially employees using the same credentials for personal accounts that may not be defended by enterprise security resources.

.001 Default Accounts

Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment. [5]

.002 Domain Accounts

Implement and enforce strong password policies for domain accounts to ensure passwords are complex, unique, and regularly rotated. This reduces the likelihood of password guessing, credential stuffing, and other attack methods that rely on weak or static credentials.

.003 Local Accounts

Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

.004 Cloud Accounts

Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Cloud service providers may track access key age to help audit and identify keys that may need to be rotated.[6]
