**Password Spray**

1. Mapping

* MITRE ATT&CK Tactic ID: T1110 – Brute Forcing
* CAPEC Parent ID: 112 – Brute Force
* CAPEC Child: 49 – Password Brute Force

|  |  |
| --- | --- |
| **CWE ID** | **NIST SP800-53** |
| 521 – Weak Password | IA-5(1)(A), IA-5(4) |
| 262 – No Password Aging | IA-5(1)(D) |
| 263 – Long Password Aging | IA-5(1)(D) |
| 257 – Recoverable Passwords | IA-5(1)(C) |
| 693 – Protection Mechanism Failure | IA-5 |

1. Related Controls

|  |  |
| --- | --- |
| **Control ID** | **Control Requirement** |
| IA-5(1)(A) | Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type] |
| IA-5(4) | The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements]. |
| IA-5(1)(D) | Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; |
| IA-5(1)(D) | Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; |
| IA-5(1)(C) | Stores and transmits only cryptographically-protected passwords; |
| IA-5 | Overall Authentication Management |

1. Narrative Information

|  |  |
| --- | --- |
| **Source** | **Value** |
| MITRE ATT&CK  Description ID: T1110 | Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.  [Credential Dumping](https://attack.mitre.org/techniques/T1003) is used to obtain password hashes, this may only get an adversary so far when [Pass the Hash](https://attack.mitre.org/techniques/T1075) is not an option. Techniques to systematically guess the passwords used to compute hashes are available, or the adversary may use a pre-computed rainbow table to crack hashes. Cracking hashes is usually done on adversary-controlled systems outside of the target network. [[1]](https://en.wikipedia.org/wiki/Password_cracking)  Adversaries may attempt to brute force logins without knowledge of passwords or hashes during an operation either with zero knowledge or by attempting a list of known or possible passwords. This is a riskier option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. [[2]](https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf)  A related technique called password spraying uses one password (e.g. 'Password01'), or a small list of passwords, that matches the complexity policy of the domain and may be a commonly used password. Logins are attempted with that password and many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [[3]](http://www.blackhillsinfosec.com/?p=4645)  Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:   * SSH (22/TCP) * Telnet (23/TCP) * FTP (21/TCP) * NetBIOS / SMB / Samba (139/TCP & 445/TCP) * LDAP (389/TCP) * Kerberos (88/TCP) * RDP / Terminal Services (3389/TCP) * HTTP/HTTP Management Services (80/TCP & 443/TCP) * MSSQL (1433/TCP) * Oracle (1521/TCP) * MySQL (3306/TCP) * VNC (5900/TCP)   In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625. |
| CAPEC Description ID: 49 | In this attack, the adversary tries every possible value for a password until they succeed. A brute force attack, if feasible computationally, will always be successful because it will essentially go through all possible passwords given the alphabet used (lower case letters, upper case letters, numbers, symbols, etc.) and the maximum length of the password. A system will be particularly vulnerable to this type of an attack if it does not have a proper enforcement mechanism in place to ensure that passwords selected by users are strong passwords that comply with an adequate password policy. In practice a pure brute force attack on passwords is rarely used, unless the password is suspected to be weak. Other password cracking methods exist that are far more effective (e.g. dictionary attacks, rainbow tables, etc.). Knowing the password policy on the system can make a brute force attack more efficient. For instance, if the policy states that all passwords must be of a certain level, there is no need to check smaller candidates. |

1. Attack Information

|  |  |  |
| --- | --- | --- |
| **Source** | **Phase** | **Value** |
| ATT&CK ID: T1110 | Credential Access | Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment. |
| CAPEC ID: 49 | Explore | Determine application's/system's password policy: Determine the password policies of the target application/system.   1. Determine minimum and maximum allowed password lengths. 2. Determine format of allowed passwords (whether they are required or allowed to contain numbers, special characters, etc.). 3. Determine account lockout policy (a strict account lockout policy will prevent brute force attacks |
| CAPEC ID: 49 | Exploit | Brute force password: Given the finite space of possible passwords dictated by the password policy determined in the previous step, try all possible passwords for a known user ID until application/system grants access.   1. Manually or automatically enter all possible passwords through the application/system's interface. In most systems, start with the shortest and simplest possible passwords, because most users tend to select such passwords if allowed to do so. 2. Perform an offline dictionary attack or a rainbow table attack against a known password hash. |

1. Detection/Mitigation

|  |  |
| --- | --- |
| **Source** | **Value** |
| MITRE ATT&CK  Detection ID: T1110 | Monitor authentication logs for system and application login failures of [[Valid Accounts](https://attack.mitre.org/techniques/T1078)]. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.  Refer to NIST guidelines when creating passwords [[NIST 800-63B](https://pages.nist.gov/800-63-3/sp800-63b.html)].  Also monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. |
| MITRE ATT&CK Mitigation ID: T1110 | Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Use multifactor authentication. Follow best practices for mitigating access [[Valid Accounts](https://attack.mitre.org/techniques/T1078)]. |
| CAPEC Mitigation ID: 49 | Implement a password throttling mechanism. This mechanism should consider both the IP address and the log in name of the user. Put together a strong password policy and make sure that all user created passwords comply with it. Alternatively, automatically generate strong passwords for users. Passwords need to be recycled to prevent aging, that is occasionally, a new password must be chosen. |
| CAPEC Indicators ID: 49 | Many incorrect login attempts are detected by the system. |
| CWE Potential Mitigations ID: 521 | PHASE: Architecture and Design - DESCRIPTION: Enforce usage of strong passwords. A password strength policy should contain the following attributes: Minimum and maximum length; Require mixed character sets (alpha, numeric, special, mixed case); Do not contain user name; Expiration; No password reuse.  PHASE: Architecture and Design - DESCRIPTION: Authentication mechanisms should always require sufficiently complex passwords and require that they be periodically changed. |
| CWE Potential Mitigation ID: 262 | PHASE: Architecture and Design - DESCRIPTION: Ensure that password aging is limited so that there is a defined maximum age for passwords and so that the user is notified several times leading up to the password expiration. |
| CWE Potential Mitigation ID: 257 | PHASE: Architecture and Design - DESCRIPTION: Use strong, non-reversible encryption to protect stored passwords. |

1. Risk Factors

|  |  |  |
| --- | --- | --- |
| **Source** | **Factor** | **Value** |
| CAPEC ID: 49 | Likelihood | Medium |
| CAPEC ID: 49 | Severity (Impact) | High |
| CAPEC ID: 49 | Skill Required (Likelihood) | SKILL: A brute force attack is very straightforward. A variety of password cracking tools are widely available.  LEVEL: Low |
| CAPEC ID: 49 | Consequences (Impact) | SCOPE: Confidentiality  SCOPE: Access Control  SCOPE: Authorization  TECHNICAL IMPACT: Gain Privileges |

1. Attack Information

|  |  |  |
| --- | --- | --- |
| **Source** | **Phase** | **Value** |
| ATT&CK ID: T1110 | Credential Access | Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment. |
| CAPEC ID: 49 | Explore | Determine application's/system's password policy: Determine the password policies of the target application/system.   1. Determine minimum and maximum allowed password lengths. 2. Determine format of allowed passwords (whether they are required or allowed to contain numbers, special characters, etc.). 3. Determine account lockout policy (a strict account lockout policy will prevent brute force attacks |
| CAPEC ID: 49 | Exploit | Brute force password: Given the finite space of possible passwords dictated by the password policy determined in the previous step, try all possible passwords for a known user ID until application/system grants access.   1. Manually or automatically enter all possible passwords through the application/system's interface. In most systems, start with the shortest and simplest possible passwords, because most users tend to select such passwords if allowed to do so. 2. Perform an offline dictionary attack or a rainbow table attack against a known password hash. |