# TTP Detail – T1201

## TTP Information

Name: Password Policy Discovery

Description: Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment. Password policies are a way to enforce complex passwords that are difficult to guess or crack through [Brute Force](https://attack.mitre.org/techniques/T1110). This information may help the adversary to create a list of common passwords and launch dictionary and/or brute force attacks which adheres to the policy (e.g. if the minimum password length should be 8, then not trying passwords such as 'pass123'; not checking for more than 3-4 passwords per account if the lockout is set to 6 as to not lock out accounts).

Password policies can be set and discovered on Windows, Linux, and macOS systems via various command shell utilities such as <code>net accounts (/domain)</code>, <code>Get-ADDefaultDomainPasswordPolicy</code>, <code>chage -l <username></code>, <code>cat /etc/pam.d/common-password</code>, and <code>pwpolicy getaccountpolicies</code> (Citation: Superuser Linux Password Policies) (Citation: Jamf User Password Policies). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to discover password policy information (e.g. <code>show aaa</code>, <code>show aaa common-criteria policy all</code>).(Citation: US-CERT-TA18-106A)

Password policies can be discovered in cloud environments using available APIs such as <code>GetAccountPasswordPolicy</code> in AWS (Citation: AWS GetPasswordPolicy).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Kwampirs

## Tools

* CrackMapExec
* Net
* PoshC2

## APTs (Intrusion Sets)

* Chimera
* OilRig
* Turla