# TTP Detail – T1110.001

## TTP Information

Name: Password Guessing

Description: Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwords to attempt access to accounts. Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism. An adversary may guess login credentials without prior knowledge of system or environment passwords during an operation by using a list of common passwords. Password guessing may or may not take into account the target's policies on password complexity or use policies that may lock accounts out after a number of failed attempts.

Guessing passwords can be a risky option because it could cause numerous authentication failures and account lockouts, depending on the organization's login failure policies. (Citation: Cylance Cleaver)

Typically, management services over commonly used ports are used when guessing passwords. 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)
\* SNMP (161/UDP and 162/TCP/UDP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.(Citation: US-CERT TA18-068A 2018). Further, adversaries may abuse network device interfaces (such as `wlanAPI`) to brute force accessible wifi-router(s) via wireless authentication protocols.(Citation: Trend Micro Emotet 2020)

In default environments, LDAP and Kerberos connection attempts are less likely to trigger events over SMB, which creates Windows "logon failure" event ID 4625.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* China Chopper
* Emotet
* HermeticWizard
* Lucifer
* P.A.S. Webshell
* Pony
* SpeakUp
* Xbash

## Tools

* CrackMapExec

## APTs (Intrusion Sets)

* APT28
* APT29