# TTP Detail – T1212

## TTP Information

Name: Exploitation for Credential Access

Description: Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.

Credentialing and authentication mechanisms may be targeted for exploitation by adversaries as a means to gain access to useful credentials or circumvent the process to gain authenticated access to systems. One example of this is `MS14-068`, which targets Kerberos and can be used to forge Kerberos tickets using domain user permissions.(Citation: Technet MS14-068)(Citation: ADSecurity Detecting Forged Tickets) Another example of this is replay attacks, in which the adversary intercepts data packets sent between parties and then later replays these packets. If services don't properly validate authentication requests, these replayed packets may allow an adversary to impersonate one of the parties and gain unauthorized access or privileges.(Citation: Bugcrowd Replay Attack)(Citation: Comparitech Replay Attack)(Citation: Microsoft Midnight Blizzard Replay Attack)

Such exploitation has been demonstrated in cloud environments as well. For example, adversaries have exploited vulnerabilities in public cloud infrastructure that allowed for unintended authentication token creation and renewal.(Citation: Storm-0558 techniques for unauthorized email access)

Exploitation for credential access may also result in Privilege Escalation depending on the process targeted or credentials obtained.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access