# TTP Detail – T1558.003

## TTP Information

Name: Kerberoasting

Description: Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to [Brute Force](https://attack.mitre.org/techniques/T1110).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015)

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service(Citation: Microsoft Detecting Kerberoasting Feb 2018)).(Citation: Microsoft SPN)(Citation: Microsoft SetSPN)(Citation: SANS Attacking Kerberos Nov 2014)(Citation: Harmj0y Kerberoast Nov 2016)

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).(Citation: Empire InvokeKerberoast Oct 2016)(Citation: AdSecurity Cracking Kerberos Dec 2015) Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline [Brute Force](https://attack.mitre.org/techniques/T1110) attacks that may expose plaintext credentials.(Citation: AdSecurity Cracking Kerberos Dec 2015)(Citation: Empire InvokeKerberoast Oct 2016) (Citation: Harmj0y Kerberoast Nov 2016)

This same behavior could be executed using service tickets captured from network traffic.(Citation: AdSecurity Cracking Kerberos Dec 2015)

Cracked hashes may enable [Persistence](https://attack.mitre.org/tactics/TA0003), [Privilege Escalation](https://attack.mitre.org/tactics/TA0004), and [Lateral Movement](https://attack.mitre.org/tactics/TA0008) via access to [Valid Accounts](https://attack.mitre.org/techniques/T1078).(Citation: SANS Attacking Kerberos Nov 2014)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* Brute Ratel C4
* Empire
* Impacket
* PowerSploit
* Rubeus
* SILENTTRINITY

## APTs (Intrusion Sets)

* FIN7
* Indrik Spider
* Wizard Spider