# TTP Detail – T1558

## TTP Information

Name: Steal or Forge Kerberos Tickets

Description: Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as “realms”, there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access.

On Windows, the built-in <code>klist</code> utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

## APTs (Intrusion Sets)

* Akira