CAPEC-645: Use of Captured Tickets (Pass The Ticket) (Version 3.9)

Archived: 2026-04-05 18:04:26 UTC

Description

An adversary uses stolen Kerberos tickets to access systems/resources that leverage the Kerberos authentication protocol. The Kerberos authentication protocol centers around a ticketing system which is used to request/grant access to services and to then access the requested services. An adversary can obtain any one of these tickets (e.g. Service Ticket, Ticket Granting Ticket, Silver Ticket, or Golden Ticket) to authenticate to a system/resource without needing the account's credentials. Depending on the ticket obtained, the adversary may be able to access a particular resource or generate TGTs for any account within an Active Directory Domain.

Likelihood Of Attack

Typical Severity

Relationships

This table shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

This table shows the views that this attack pattern belongs to and top level categories within that view.

Prerequisites

The adversary needs physical access to the victim system.
The use of a third-party credential harvesting tool.

Skills Required

[Level: Low] Determine if Kerberos authentication is used on the server.
[Level: High] The adversary uses a third-party tool to obtain the necessary tickets to execute the attack.

Consequences

This table specifies different individual consequences associated with the attack pattern. The Scope identifies the security property that is violated, while the Impact describes the negative technical impact that arises if an adversary succeeds in their attack. The Likelihood provides information about how likely the specific consequence is expected to be seen relative to the other consequences in the list. For example, there may be high likelihood that a pattern will be used to achieve a certain impact, but a low likelihood that it will be exploited to achieve a different impact.

Scope	Impact	Likelihood
Integrity	Gain Privileges	

Mitigations

Reset the built-in KRBTGT account password twice to invalidate the existence of any current Golden Tickets and any tickets derived from them.
Monitor system and domain logs for abnormal access.

Example Instances

Bronze Butler (also known as Tick), has been shown to leverage forged Kerberos Ticket Granting Tickets (TGTs) and Ticket Granting Service (TGS) tickets to maintain administrative access on a number of systems. [REF-584]

Taxonomy Mappings

CAPEC mappings to ATT&CK techniques leverage an inheritance model to streamline and minimize direct CAPEC/ATT&CK mappings. Inheritance of a mapping is indicated by text stating that the parent CAPEC has relevant ATT&CK mappings. Note that the ATT&CK Enterprise Framework does not use an inheritance model as part of the mapping to CAPEC.

Relevant to the ATT&CK taxonomy mapping (also see parent)

Entry ID	Entry Name
1550.003	Use Alternate Authentication Material:Pass The Ticket

References

Content History

Submissions

Submission Date	Submitter	Organization
2018-07-31 (Version 2.12)	CAPEC Content Team	
Modifications		
Modification Date	**Modifier**	**Organization**
2020-07-30 (Version 3.3)	CAPEC Content Team	The MITRE Corporation
	Updated Description, Example_Instances, References, Related_Attack_Patterns, Related_Weaknesses, Taxonomy_Mappings	

More information is available — Please select a different filter.

Source: https://capec.mitre.org/data/definitions/645.html