Incident Response Playbook: Suspicious Kerberos Activity (Golden/Silver Ticket)

Team AnubisX

Version 1.0
September 18, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a structured approach to detect, analyze, contain, and respond to suspicious Kerberos activity—specifically Golden Ticket and Silver Ticket attacks. These attacks involve forging Kerberos tickets to gain unauthorized, persistent, and often stealthy access to enterprise systems.

1.2 Scope

This playbook applies to Active Directory environments, Kerberos authentication systems, domain controllers, and enterprise endpoints relying on Kerberos for authentication.

2 Overview of Kerberos Ticket Attacks

Golden Ticket and Silver Ticket attacks exploit Kerberos authentication by forging valid tickets. Both allow attackers to authenticate as legitimate users and move laterally undetected, often bypassing traditional security controls.

- **Golden Ticket:** Attackers compromise the KRBTGT account in Active Directory and generate Ticket Granting Tickets (TGTs) that grant domain-wide administrative access.
- **Silver Ticket:** Attackers forge service tickets (TGS) by obtaining a specific service account's password hash, granting access to that particular service.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a Kerberos ticket forgery incident.

- **Roles and Responsibilities:** Define roles (Incident Commander, SOC Analysts, AD Security Engineers, IR Team, Communications Lead).
- **Tools & Resources:** Ensure availability of SIEM, EDR, Kerberos traffic monitoring, AD logs (Event IDs 4768-4776), and memory forensic tools.
- **Training:** Conduct regular blue team exercises simulating Golden/Silver Ticket attacks and remediation steps.
- **Controls:** Harden domain controllers, monitor privileged accounts, enforce least privilege, and enable advanced Kerberos logging and detection rules.

3.2 Phase 2: Identification & Analysis

Goal: To confirm Kerberos ticket forgery activity and determine its scope.

1. **Initial Triage:** Collect alerts from SIEM/EDR, isolate suspected systems, open an official incident ticket, and activate secure communication channels.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

- Abnormal Kerberos Ticket Granting Ticket (TGT) lifetimes (e.g., 10 years).
- Event ID 4769 (Service Ticket Request) with unusual service accounts or from unexpected sources.
- Logon events (Event ID 4624) with inconsistencies between account names and security IDs.
- Service tickets for accounts that do not exist or are disabled.
- High-volume ticket renewal requests (Event ID 4770) at abnormal frequencies.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is based on the type of ticket forged, the scope of compromise, and the criticality of accessed systems.

Level	Description	Example	MTTD	MTTR
Low	Suspicious Kerberos request detected but blocked.	An abnormal ticket lifetime is detected in a log, but no successful logon is achieved.	6-12 hours	24-48 hours
Medium	Limited Silver Ticket use on a non-critical system.	A forged service ticket is used to access a single, non-critical file server.	12-24 hours	2-4 days
High	Silver or Golden Tickets used for lateral movement.	A Golden Ticket is used to access multiple systems, but not domain controllers.	24-48 hours	4-7 days
Critical	Widespread Golden Ticket abuse; full domain compromise.	The KRBTGT account is confirmed compromised, allowing attackers to issue valid TGTs indefinitely.	48 hours	7-14+ days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points.
   - **If True Positive (TP):** Logs confirm forged ticket usage. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander. For Golden Tickets, activate critical incident protocol.
   - **If False Positive (FP):** Anomaly is confirmed benign (e.g., clock skew, misconfigured service). **Action:** Document findings, close the alert, and tune detection rules.
5. **Incident Declaration:** If confirmed, formally declare a Kerberos incident and escalate to leadership, AD Admins, and legal counsel.

3.3 Phase 3: Containment

Goal: To limit attacker access and prevent further lateral movement.

- **Short-Term Containment (Immediate Actions):**
  - Isolate systems where forged tickets were used.
  - Force logoffs for all suspicious user and computer sessions.
  - Disable any accounts confirmed to be compromised.
- **Evidence Preservation:** Acquire memory dumps, Kerberos ticket caches, and relevant logs **before** remediation.

3.4 Phase 4: Eradication

Goal: To remove attacker artifacts and close the exploited vulnerabilities.

- **Root Cause Analysis:** Identify how the initial credentials (KRBTGT or service account hash) were compromised.
- **Credential Reset:** For a Golden Ticket, reset the KRBTGT password **twice**. For a Silver Ticket, reset the compromised service account password. Reset all privileged account passwords.
- **Security Hardening:** Patch domain controllers and other exploited systems. Remove any persistence mechanisms found.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- **System Restoration:** Reintroduce cleaned systems into the environment after clearing all Kerberos ticket caches.
- **Enhanced Monitoring:** Increase monitoring of Kerberos logs, especially for high-value accounts and domain controllers.
- **Validation:** Ensure restored systems are clean and that normal authentication patterns have resumed.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem meeting within two weeks of incident closure.
- **Final Incident Report:** Create a detailed report covering the timeline, root cause, response actions, and costs.
- **Action Plan:** Implement security improvements (e.g., credential protection, improved DC hardening, enhanced Kerberos monitoring).

4 MITRE ATT&CK Framework Mapping

Kerberos Ticket Abuse ATT&CK Mapping

- **Tactic: Credential Access**
  - *T1003.006 – OS Credential Dumping: KRBTGT*
- **Tactic: Persistence**
  - *T1558.001 – Steal or Forge Kerberos Tickets: Golden Ticket*
  - *T1558.002 – Steal or Forge Kerberos Tickets: Silver Ticket*
- **Tactic: Privilege Escalation**
  - *T1558 – Steal or Forge Kerberos Tickets*
- **Tactic: Defense Evasion**
  - *T1078 – Valid Accounts*
- **Tactic: Lateral Movement**
  - *T1550.003 – Use Alternate Authentication Material: Pass the Ticket*