This document contains confidential information intended for internal use by FakeCorp Industries only. Distribution or disclosure without explicit permission is prohibited.

Client: FakeCorp Industries

Prepared By: Zion Spearman

Report Date: May 31, 2025

Red Team Report: Golden Ticket Attack on fakecorp.com via kerberoasting

## Table of Contents

**Executive Summary…………………………………………………………………………….. 2**

**Overview of the Engagement ……………...……………...…………………………………… 2**

**Objectives and Outcomes …………………………………………………………………...…. 2**

**High-Level Risks Demonstrated …………………………………………………...………...... 3**

**Tools and Methodology………………………………………………………………………… 5**

**Attack Narrative ……………………………………………………………………………...... 7**

**Impact Assessment .…………………………………………………………………………… 20**

**Recommendations …………………………………………………………………………….. 21**

**Conclusion …………………………………………………………………………………...... 22**

**Appendix A: Tools Used ……………………………………………………………………… 22**

**Appendix B: Indicators of Compromise …………………………………………………….. 23**

## Executive Summary

Overview:

This red team lab simulates a targeted Active Directory attack against FakeCorp Industries domain, focusing on the exploitation of Kerberos service ticket vulnerabilities. The Objective was to escalate privileges by extracting service account hashes and forging a Golden Ticket to gain administrative access to the domain

The lab environments contained multiple internal subnets producing a realistic corporate network. An implant beacon was constructed to call back the attacker’s machine on port 4321 every 15 minutes, which caused the operator to gain direct access to the internal admin network.

The attack involved the use of tools such as Metasploit, Kiwi, Remote Desktop Protocol, and command utilities. Skills that were applied include payload generation, antivirus evasion, Kerberoasting, and ticket forging

This report documents steps taken to take control over the environment, highlights tactics used to escalate privileges and proves the creation and usage of a Golden Ticket for the FakeCorp.com domain account.

Engagement Objectives and Outcomes:

* **Objectives**:
  + Extract service account credentials via Kerberoasting
  + Forge and inject a valid Golden Ticket using krbtgt hash data
  + Access high-value systems (e.g., Admin Workstation and Domain Controller)
  + Demonstrate lateral movement, token impersonation, and privilege escalation
* **Outcomes**:
  + Full Domain Administrator access achieved
  + Golden Ticket successfully created and applied
  + Unrestricted access to administrative file shares (\\mainadds\c$) obtained
  + Demonstrated persistence and stealth using forged Kerberos authentication

High-Level Risks Demonstrated

* **Golden Ticket Abuse** – Long-term domain compromise without reauthentication
* **Kerberos Ticket Forging** – Exploiting krbtgt hash to impersonate any domain user
* **Token Impersonation** – Theft of access tokens from privileged processes
* **Lateral Movement** – Stealthy navigation across segmented subnets
* **Defensive Evasion** – AV bypass via payload encoding (x86/shikata\_ga\_nai)

Summary of Success

The red team effectively:

* Compromised the Admin Workstation through a reverse shell
* Escalated privileges to SYSTEM and stole a Domain Admin token
* Extracted the krbtgt hash using DCSync
* Created and injected a Golden Ticket as administrator@fakecorp.com
* Accessed the Domain Controller’s C$ share and retrieved sensitive files (Ex: flag204090.txt)

This engagement simulates a realistic domain compromise scenario and demonstrates the severe risks posed by unmonitored Kerberos abuse and privileged account mismanagement.

Project Summary

This document provides the Red Team Assessment report performed by the operator on targets defined in the lab’s internal network scope. The purpose of this lab was to simulate an Kerberos attack against FakeCorp industries domain in a controlled lab environment. The focus was on privilege escalation using kerberoasting and the creation of a Golden Ticket to gain persistent access to the domain.

Program Objective

The Objective of this assessment was to simulate a real world attack targeting an enterprise Active Directory infrastructure. The lab aimed to assessed the success of layered security controls and privilege management with FakeCorp.com domain. This test replicated a post exploitation phase following initial access through a deployed implant

This assessment allowed for a realistic simulation of attacks that could come about from internal compromise and abuse of Kerberos authentication. Based on the outcome, the operator was able to evaluate:

* Active Directory authentication mechanisms
* Privilege escalation paths
* Golden Ticket attack viability
* Antivirus evasion techniques
* Domain persistence methods
* Remote access post exploitation
* Internal network segmentation and visibility
* Defender detection and response limitation

Scope and Timeframes

Testing and exploitation in a lab environment were performed between May 25, 2025, and May 31, 2025. The scope of this project simulated clients enterprise Active Directory infrastructure cover the following subnets

* 192.168.1.0/24
* 10.10.10.8/29
* 10.10.30.16/28
* 10.10.50.16/28
* 10.10.70.16/28
* 10.10.40.8/29

The goals of this attack were to

* Extract service account hashes via Kerberoasting
* Forge a Golden Ticket impersonating the Domain Administrator
* Use the Golden Ticket to access internal resources
* Maintain persistence through ticket reuse
* Demonstrate command execution and RDP access
* Enumerate network services and systems

Tools Used

The following tools were used to perform enumeration, credential extraction, ticket manipulation, and post exploitation access

* Metasploit Framework – Payload creation, implant handler, post exploitation tools
* Kiwi – Forged Golden Tickets, Interacted with Kerberos tickets
* Windows Command Line & PowerShell - Ticket injection, local system commands
* Remote Desktop Protocol – Used to validate access as Domain Administrator
* SOCKS proxy – Enabled pivoting and lateral movement between internal subnets
* Implant Listener – Simulated beacon calling out every 15 minutes on port 4321

Methodologies

The assessment followed a structured red team method aligned with industry standards adversary simulation phases. The key stages were:

1. Initial access and Persistence
   1. Access was stimulated through an implant with a call back to the attacker’s system
2. Enumeration and Reconnaissance
   1. Internal host and domain enumeration were done to find SPN’s, user accounts and domain details for Kerberoasting
3. Kerberoasting Attack Execution
   1. The tickets were extracted in hashed form for offline cracking
4. Golden Ticket Creation
   1. A forged ticket was generated using mikikatz
   2. The ticket was put into the attacker’s session to simulate privilege access
5. Access Validation and Privilege Escalation
   1. Administrative access RDP
   2. Accessed on domain controlled systems
6. Lateral Movement and Persistence
   1. The red team demonstrated unrestricted movements across subnets using the forge Golden Ticket

Findings and Technical Walkthrough

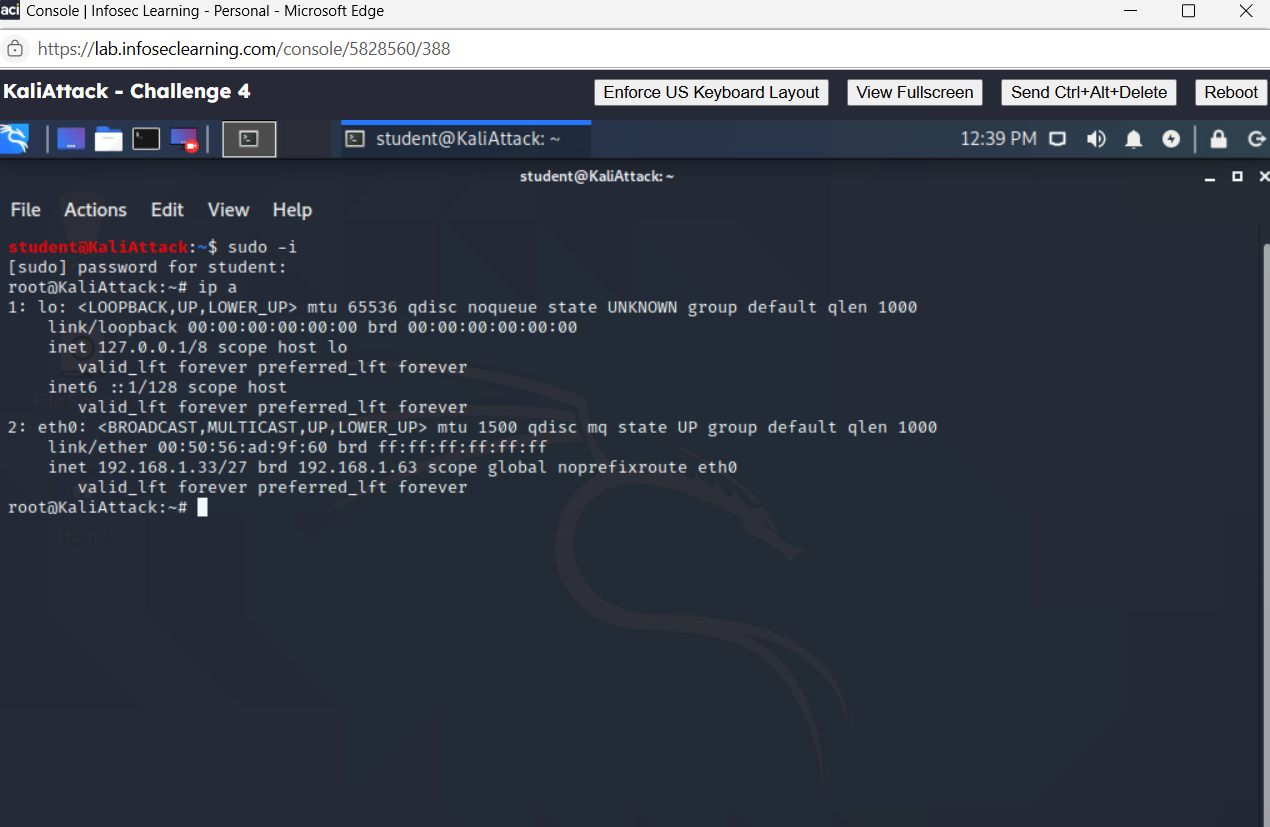
Figure 1: Admin Network Diagram showing key systems targeted during the assessment

A diagram of a computer network

AI-generated content may be incorrect.

* This diagram illustrates the target admin network. The red team’s objective was to pivot through the environment, starting at the Admin Workstation (10.10.40.9), which is centrally connected to critical infrastructure components such as the Main AD Server, File Server, and Backup Server.

Figure 2: Attacker IP confirmed using IP A command (192.168.1.33)



* Before establishing the reverse shell connection, the operator confirmed that the ip address of the Linux system

Figure 3: Metasploit handler catching a reverse shell from the backup server

A screenshot of a computer

AI-generated content may be incorrect.

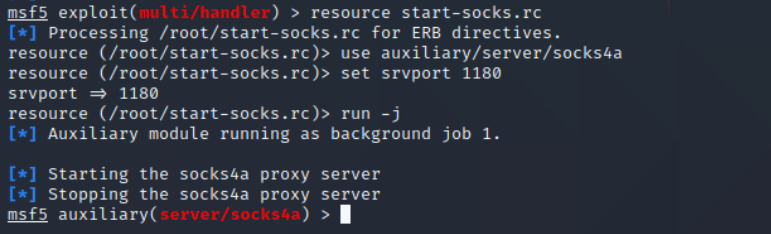
* The engagement began with getting a foothold in the network. The attacker configured a Metasploit multi/handler listener(lport) on port 4321 to receive a reverse Meterpreter shell

Figure 4: Internal route added to access Admin Network (10.10.40.8/29)



* Following gaining a Meterpreter session on the compromised server, the red team configured internal configuring by adding an admin route

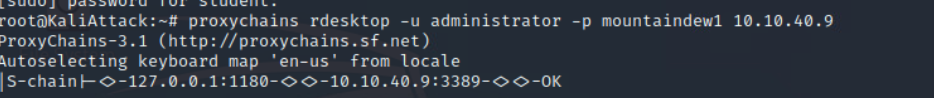
Figure 5: SOCKS4a proxy server running on port 1190 for internal pivioting



* To gain access to internal subnets from the attacker’s machine, a SOCKS4a server was made through Metasploit. This allowed traffic to go through the compromise server. Traffic will be tunneled through the server and into the Admin Subnet

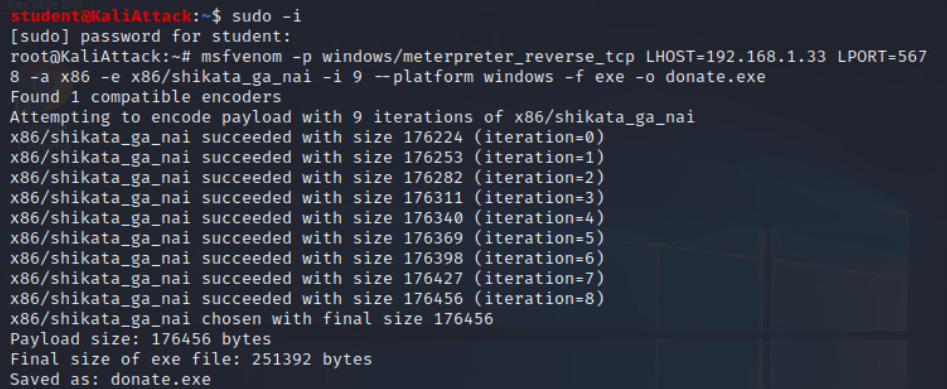
Figure 6: RDP access to Admin Workstation through proxychains and forged credentials

A screenshot of a computer

AI-generated content may be incorrect.

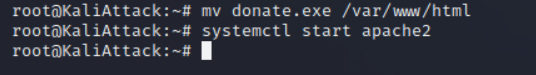
* With the SOCKS4a proxy and the internal route to the Admins Network, the red team launched a RDP session at 10.10.40.9 using forge domain credentials .
* The RDP session successfully routed through the proxy and authenticated credentials linked to the fake Golden Ticket.
* The operator had access to the Admin Workstation, confirming high level privilege escalation.

Figure 7: Obfuscated Meterpreter payload created using x86/shikata\_ga\_nai



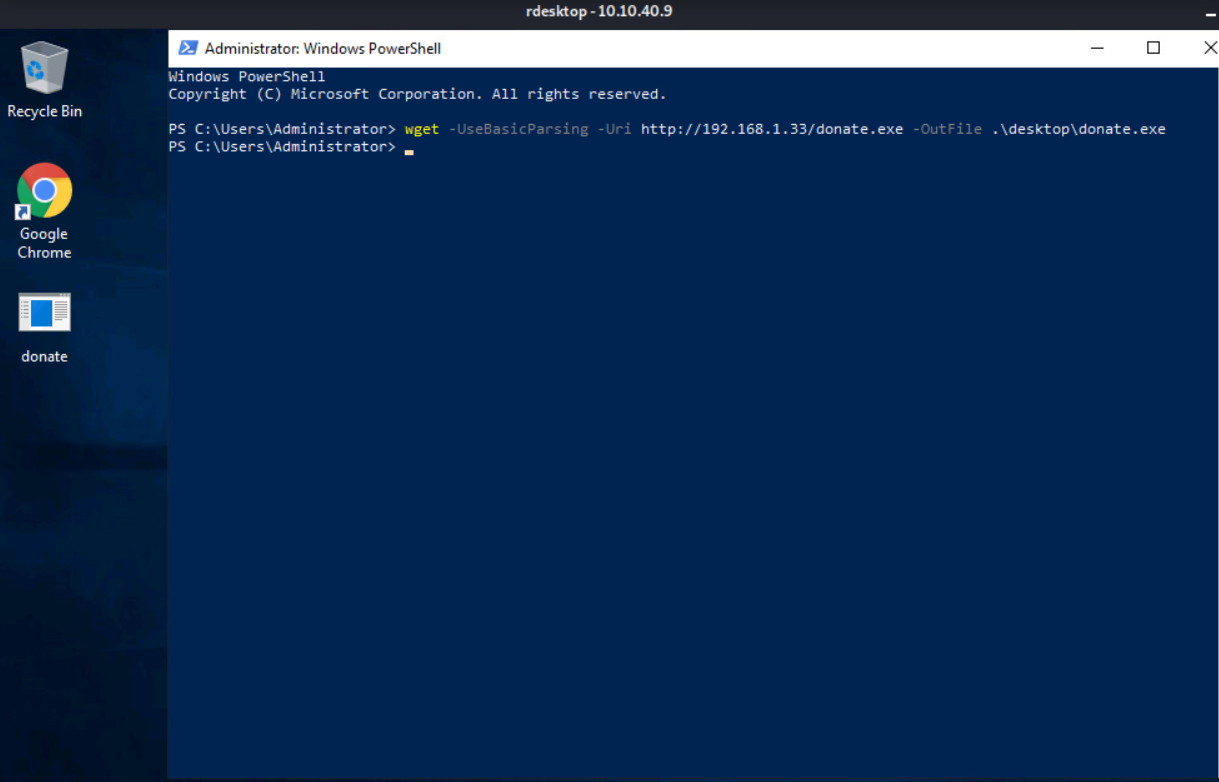
* For remote access on target machine, the red team created a Meterpreter reverse TCP payload using msfvenom. The payload encoded with x86/shikata\_ga\_nai to skip signature based antivirus detection

Figure 8: donate.exe payload delivered to Admin Workstation through PowerShell



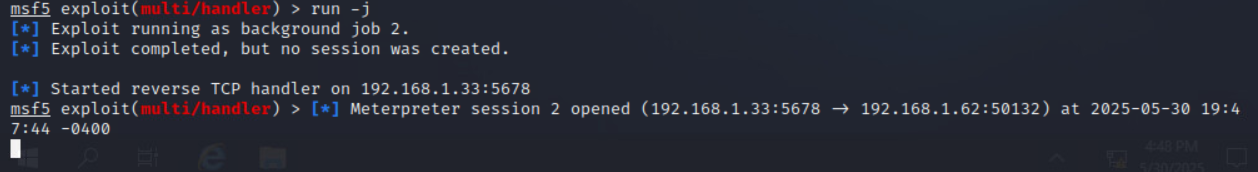
* After Generating the donate.exe payload, the red team started the Apache 2 service on attacking machine, making it engage with HTTP

Figure 9: Second Meterpreter session opened from Admin Workstation



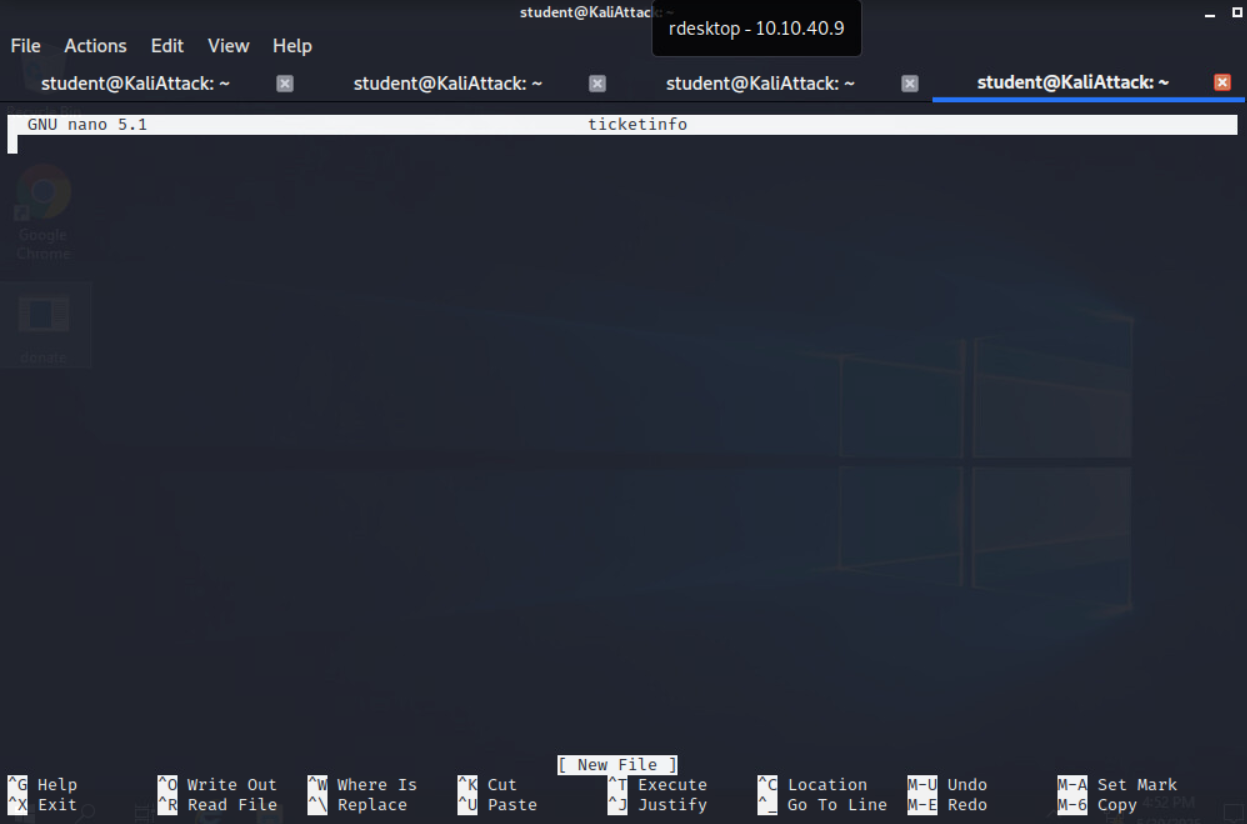
* The red team used PowerShell’s wget command to send donate.exe payload to the Admin Workstation (10.10.40.9). This technique is a way of how malware might be produced and sent out to a compromised system by a threat

Figure 10: Showing a successful connection back from the Admin Workstation



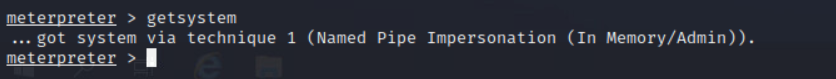
* After accessing a payload on the admin workstation, the Metasploit handler on the attacker machine received a successful connection back establishing a Meterpreter session.

Figure 11: Ticket forging information staged in nano



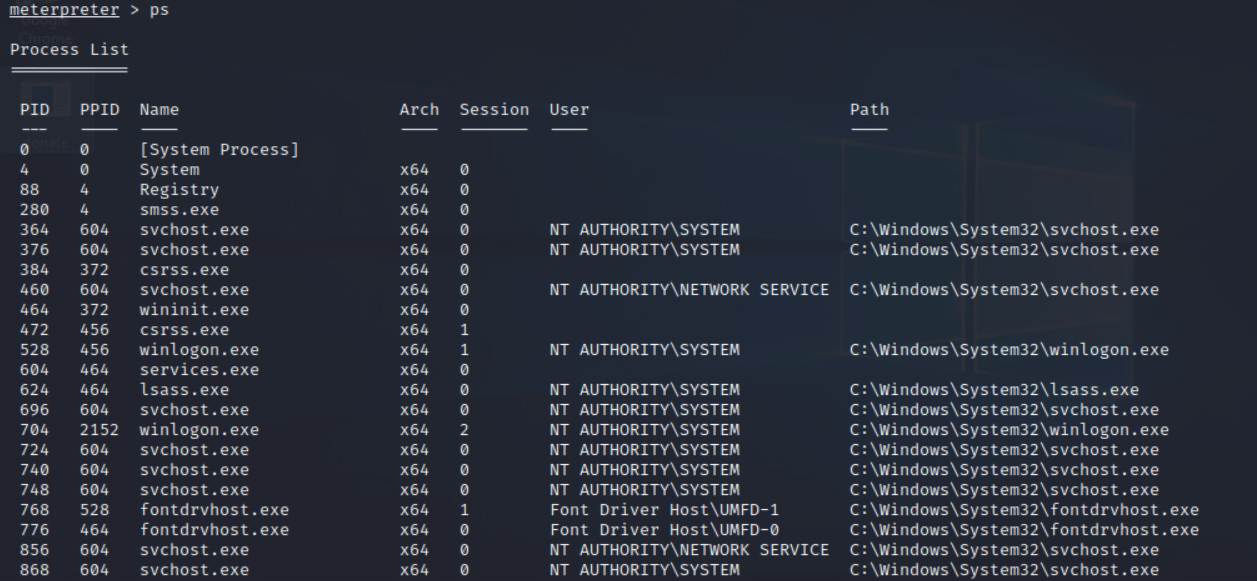
* The operator used nano on the admin workstation to document key information like target user, domain name and SID. All this information will be required later to forge the Golden Ticket

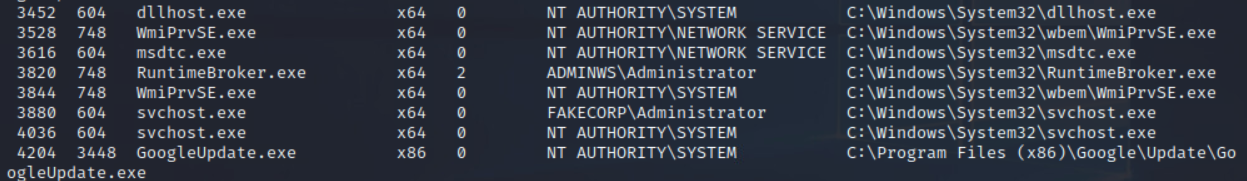
Figure 12: SYSTEM privileges obtained through Named Pipe Impersonation



* To gain full system privileges from the host, the red team executed the getsystem command. This is a major step for taking sensitive data and stealing tokens.

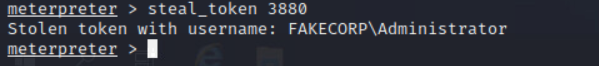
Figure 13: Svchost.exe (PID: 3880) running as the domain Administrator has the token





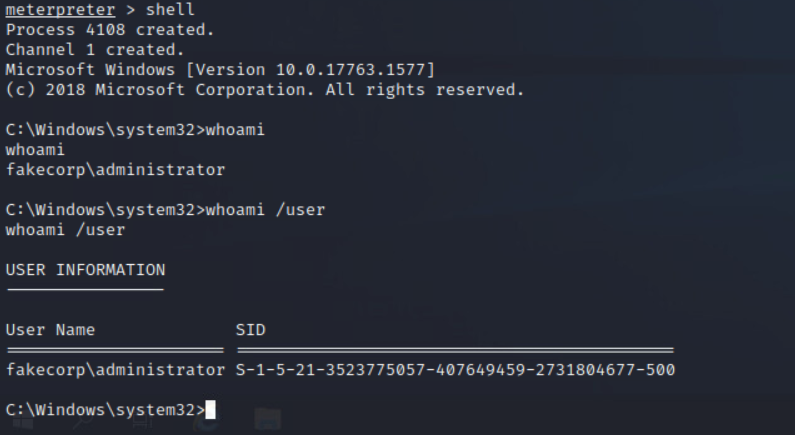
* Using the PS command, the red team looked at the process and found PID 3880, which was owned by fakecorp\administrator

Figure 14: Domain Administrator token successfully stolen from PID 3880



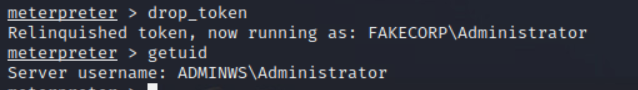
* The red team used the Meterpreter command steal token on PID 3880. Previously identified as running under the FAKECORP\Administrator context. The red team impersonation succeeded, and they adopted the privileges of the Domain Administrator

Figure 15: Token impersonation validated through whoami and SID check



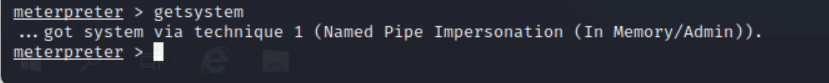
* The red team used whoamI command to run a shell from Meterpreter session. The red team verified that the token impersonation was a success

Figure 16: Token dropped; session returned to local admin



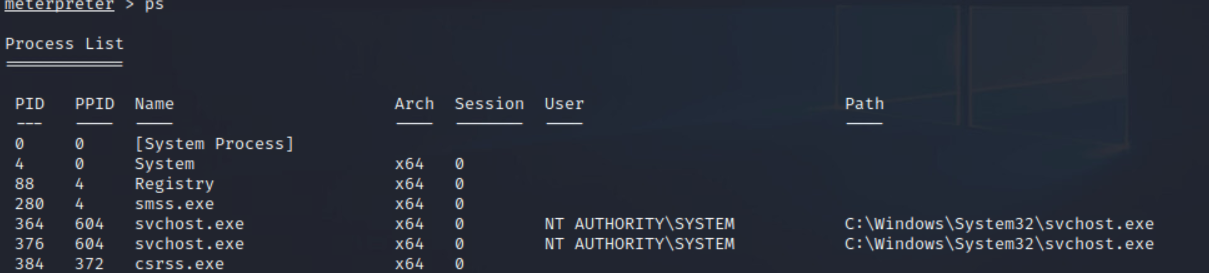
* Once the objectives were completed, the red team released the impersonated token. They were done using Meterpreter and returned to a local administrator

Figure 17: Pulled up system privileges through getsystem



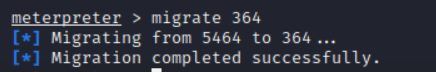
* System privileges gained using Named Pipe Impersonation

Figure 18: Meterpreter showing available SYSTEM process



* Meterpreter process listing showing available SYSTEM processes such as svchost.exe (PID 364)

Figure 19: Meterpreter session migrated to PID 364



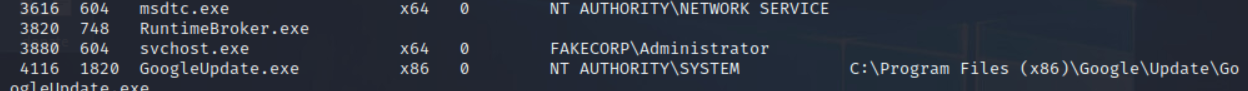
* Session migrated into 364 PID to maintain stability under system privileges

Figure 20: Kiwi loaded for Kerberos ticket manipulation



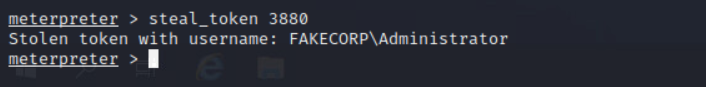
* With full SYSTEM privileges and a stable session, the red team loaded the kiwi **module**, a powerful post-exploitation framework used for credential and ticket manipulation.
* The use of Kiwi enabled the red team to:
  + Interact with Kerberos tickets
  + Extract cleartext passwords and hashes
  + Perform pass the ticket hashes
  + Forge a Golden Ticket to maintain persistent domain access

Figure 21: Red team obtained FAKECORP at PID 3880



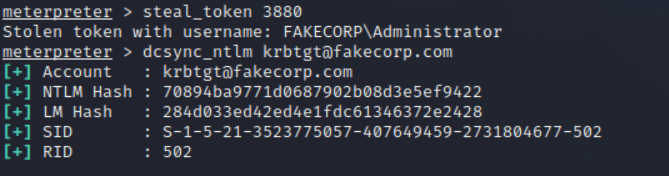
* Once the red team obtained fakecorp\Administrator access, a DC Sync attack was conducted to extract the krbtgt account hash. This enabled Golden Ticket creation and long-term impersonation of a domain administrator.

Figure 22: Token stolen with username FakeCorp



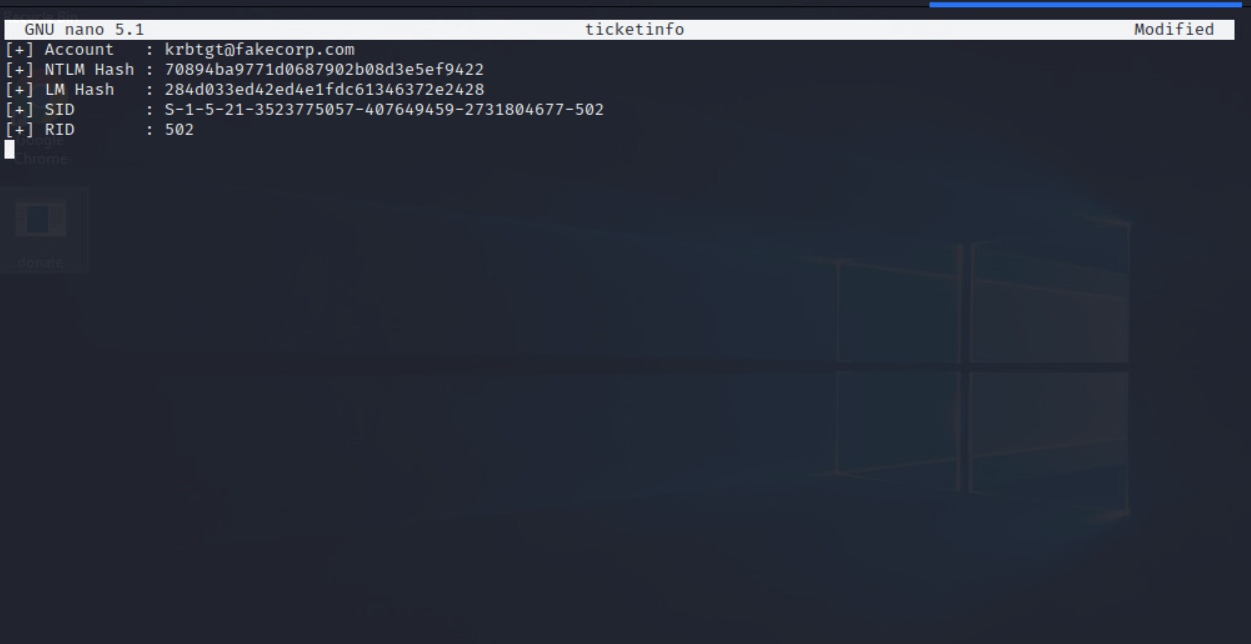
* Token stolen from svchost.exe running as fakecorp\administrator

Figure 23: DCSync attack retrieving krbtgt NTLM and domain SID



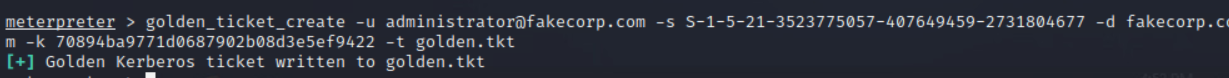
* This command obtain the domain SID and RID for the service account along with the NTLM and LM hashes. In order to obtain long termed domain persistence, these values are required

Figure 24: Krbtgt hash and SID documented for Golden Ticket creation



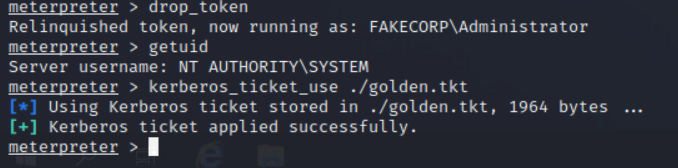
* This screenshot shows the attacker saving the credentials from the DC sync attack into nano

Figure 25: Golden Ticket created for Administrator@fakecorp.com



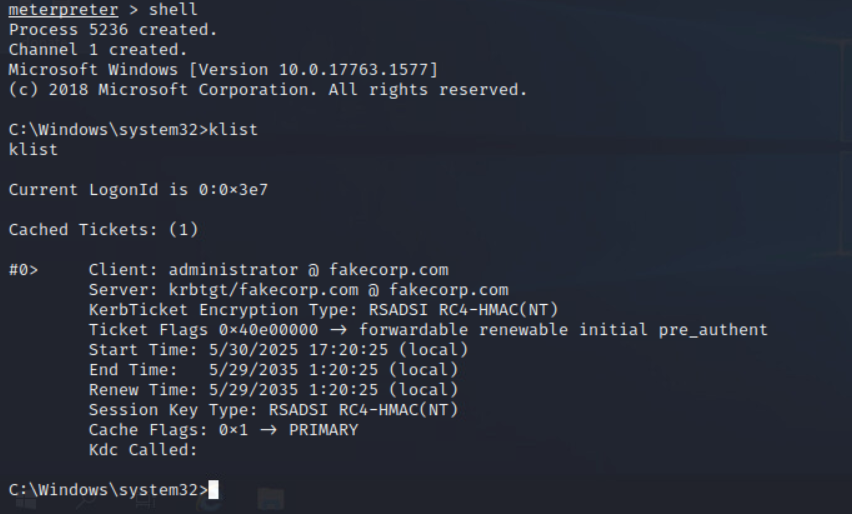
* A golden ticket was created for the domain name fakecorp.com. The ticket was saved as golden.tkt and was created by impersonating administrator@fakecorp.com. Without having to reauthenticate against the Domain Controller, this exploit grants unrestricted privileged access to the domain.

Figure 26: Forged ticket injected and accepted into the session



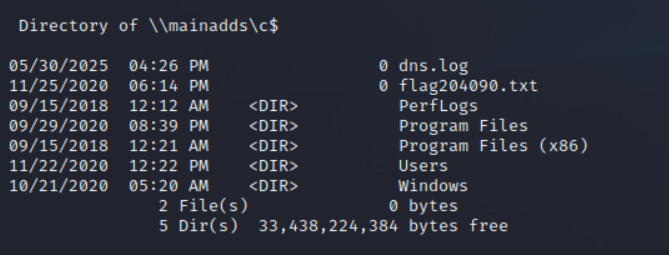
* The Kerberos ticket command was used to load the forged Kerberos ticket. After the ticket was successfully submitted, administrator@fakecorp.com was granted permanent access to the domain without requiring additional Domain Controller verification.

Figure 27: klist confirms Golden Ticket is active and valid



* A legitimate Kerberos ticket cached for administrator@fakecorp.com is displayed by the klist command. It is confirmed that the forged Golden Ticket was successfully applied for and accepted by the system by the existence of the krbtgt/fakecorp.com ticket with a long validity (10 years). Persistent domain-level access is thus granted.

Figure 28: Domain Controller C$ share accessed using Golden Ticket, sensitive data confirmed



* The red team gained access to the domain controller's administrative C$ share by using the falsified Kerberos Golden Ticket. Sensitive files like flag204090.txt and dns.log are there to confirm unfettered, high-level access, illustrating the consequences of full domain penetration and Golden Ticket abuse.

Impact Assessment

The red team successfully executed a Golden Ticket attack, resulting in unrestricted, persistent access to the FakeCorp domain. The following impacts were observed:

* Privilege Escalation: The attacker gained full Domain Administrator privileges using forged Kerberos tickets.
* Persistence: The attacker was able to maintain indefinite access without reauthentication through the use of a Golden Ticket.
* Lateral Movement: Compromised systems were used to pivot through segmented subnets undetected.
* Credential Theft: Domain credentials, including krbtgt NTLM/LM hashes, were exfiltrated via a DCSync attack.
* Defensive Evasion: Antivirus solutions were bypassed using payload encoding and stealthy execution techniques.
* Resource Access: Access was obtained to critical infrastructure including the Admin Workstation, Domain Controller, and network file shares (C$ share).
* Operational Risk: The simulated compromise demonstrates real-world potential for catastrophic damage, including data theft, service disruption, and long-term backdoor access.

Recommendations

To defend against similar attacks in real-world environments, the following mitigation strategies are advised:

1. Restrict Privileged Account Usage
   * Avoid using Domain Administrator accounts for everyday tasks.
   * Use tiered admin accounts and Just-in-Time (JIT) administration.
2. Monitor and Protect KRBTGT Account
   * Reset the KRBTGT password twice after suspected compromise.
   * Monitor for unusual replication requests from non-DC systems (DCSync detection).
3. Implement Detection for Golden Ticket Attacks
   * Monitor klist output and detect anomalies in Kerberos ticket lifetime (e.g., unusually long validity).
   * Audit Kerberos TGT and TGS requests with SIEM tools.
4. Enhance Network Segmentation
   * Limit access between internal subnets.
   * Deploy firewalls and isolate sensitive resources (e.g., Domain Controllers).
5. Harden Endpoint Security
   * Use EDR/XDR solutions to detect post-exploitation tools like Mimikatz.
   * Disable unnecessary services (e.g., PowerShell remoting if not needed).
6. Logging and Alerting
   * Enable advanced logging (e.g., 4662, 4672, 4768–4776) and forward to SIEM.
   * Monitor for creation/use of service tickets (Kerberoasting activity).

Conclusion

This red team lab successfully showed a full domain compromise through a Kerberoasting attack against FakeCorp Industries Active Directory infrastructure. Beginning with an starting footprint through an implant on the backup server, the operator leveraged Meterpreter, DCSync, and Kerberos ticket forging to rise privileges and take over the identity of the domain administrator

The use of a Golden Ticket allowed persistent and secretive access to critical internal systems with full administrative control. This attack scenario showed real world risks associated with weak service account protections, insufficient network segmentation and the lack of detection sources for abnormal Kerberos ticket activity

All objectives of the engagement were met, including:

* Establishing command and control within the admin network
* Extracting domain level credentials
* Forging a functional Golden Ticket
* Accessing the C$ share of the domain controller

The findings emphasize the importance of hardening Active Directory configurations, implementing robust monitoring, and routinely rotating sensitive account credentials.

Appendices

Appendix A: Tools Used

* Metasploit Framework
* Kiwi / Mimikatz
* PowerShell / CMD
* Apache2 (Payload hosting)
* rdesktop / RDP
* nano (for note-taking and SID/hash logging)

Appendix B: Key Indicators of Compromise (IOCs)

* Reverse shell listener on port 4321
* donate.exe payload transfer via HTTP (PowerShell wget)
* NTLM/LM hashes of krbtgt account
* Golden ticket file golden.tkt