

Hunting Kerberoasting in AD

Created by : Anas Abdelrahman

**Linkedin :
[http://www.linkedin.com/in/anas-
abdelrahman-80030b226](http://www.linkedin.com/in/anas-abdelrahman-80030b226)**

بسم الله الرحمن الرحيم الحمد لله رب العالمين، والصلاة والسلام على أشرف الأنبياء والمرسلين، نبينا محمد وعلى آله وصحبه أجمعين، ومن تبعهم بإحسان إلى يوم الدين وبعد :

Introduction

Kerberoasting is an attack to steal service account hashes by requesting then cracking them offline for lateral movement or TGS tickets, privilege escalation

Kerberoasting Attack Steps

1-Authenticate & Get TGT :

Attacker logs in as a valid domain user and requests a TGT (Ticket-Granting Ticket) from the KDC

2-Request Service Ticket (TGS) :

Uses that TGT to request a TGS (Service Ticket) for a service account with an SPN

3-Extract Encrypted TGS :

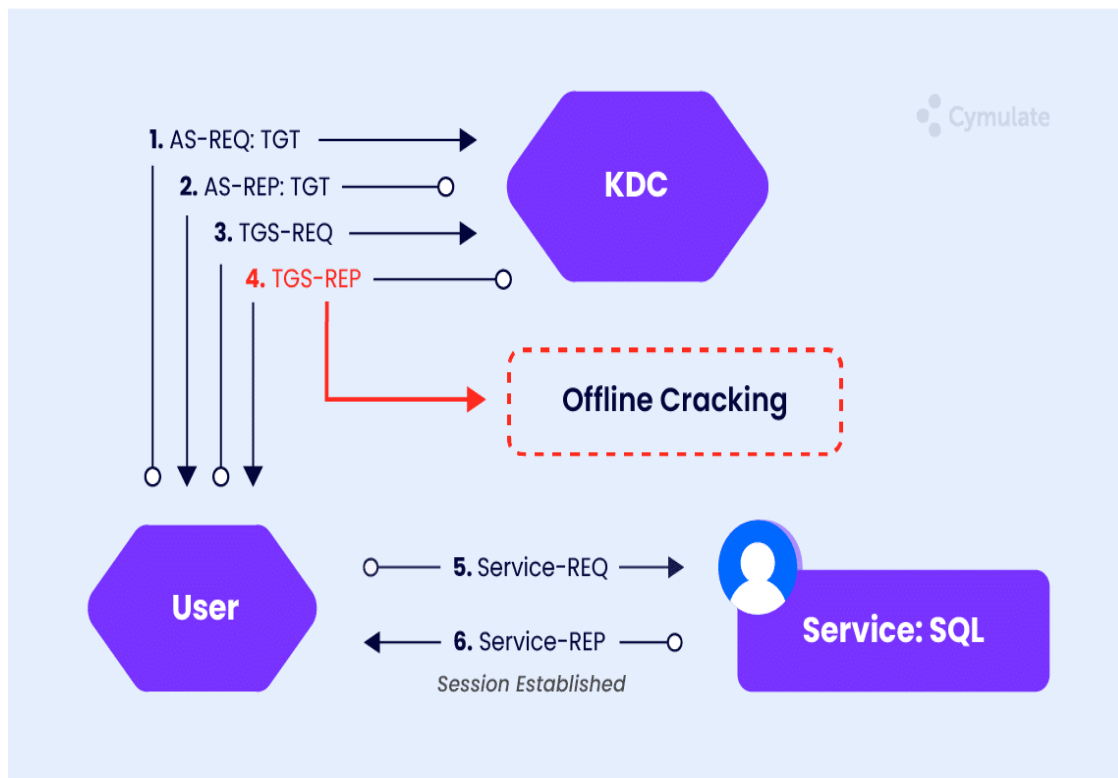
.Pulls the encrypted service ticket (TGS) from memory

4-Offline Brute-Force :

Cracks the TGS encryption offline to recover the service account's password

5-Use Cracked Credentials :

Logs in or moves laterally using the recovered password for privilege escalation



How to Hunt for Kerberoasting

1- Filter for Suspicious STs :

- Check for TGS Requests (Event ID 4769)
- ServiceName should not be krbtgt
- Look for user accounts making multiple ST requests
- Filter out ServiceName ending with \$ → these are computer accounts (not Kerberoastable)

2- Key Indicators

- Unusual volume of TGS requests in a short time
- TGS requests using RC4-HMAC encryption (TicketEncryptionType 0x17) attackers prefer weak encryption for easier cracking
- Source IPs making mass SPN requests

3- Cross-Check

- Correlate with PowerShell logs (Event ID 4104) look for enumeration tools

Examples: PowerView, Rubeus, Impacket scripts

4- Validate

- Check for brute force behavior
 - Many STs → same account → short timeframe → suspicious
- Compare with normal baselines (what's normal for your domain)

5- Enrichment

- Host logs → what user ran the query
- Network logs → unusual traffic
- Prefetch / Sysmon → suspicious tools run

Tools

Rubeus → ticket requests, ticket extraction, and offline cracking prep

<https://github.com/GhostPack/Rubeus>

Impacket → Python toolkit with GetUserSPNs.py for enumerating SPNs and requesting service tickets

<https://github.com/fortra/impacket>

PowerView.ps1 → Part of PowerSploit. Used to enumerate domain objects including SPNs

<https://github.com/PowerShellMafia/PowerSploit>

Invoke-Kerberoast → PowerShell script that automates SPN hunting and ticket extraction

https://github.com/EmpireProject/Empire/blob/master/data/module_source/credentials/Invoke-Kerberoast.ps1

Cracking Tools → To brute-force the dumped hashes offline, like:

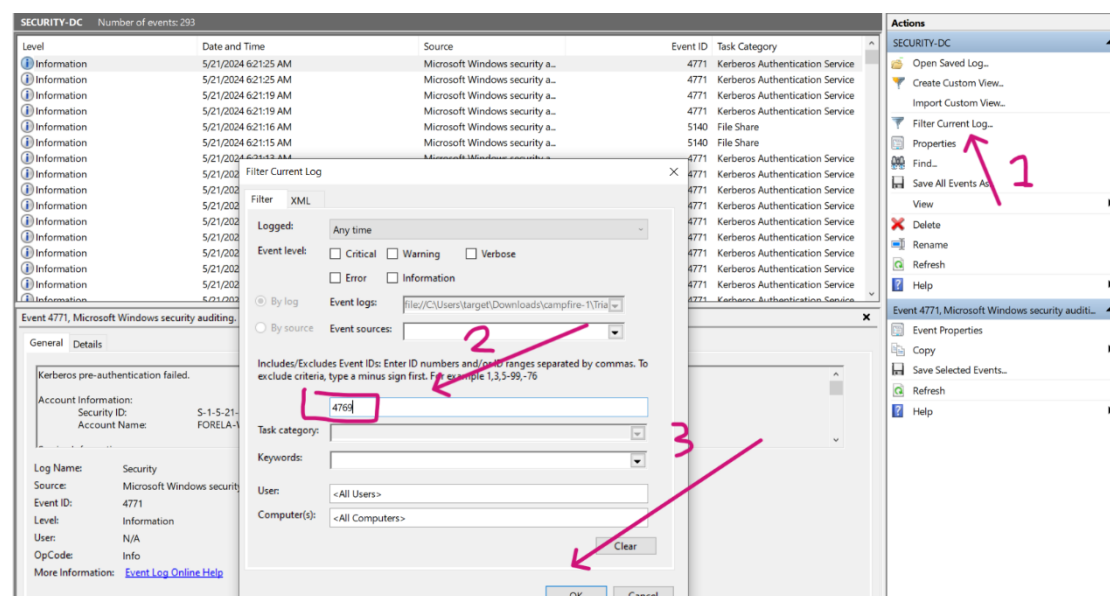
Hashcat <https://hashcat.net/hashcat/> John the Ripper

[/https://www.openwall.com/john](https://www.openwall.com/john)

Lets Practice

We have evtx File From Dc , and we want to analyze it To Hunt Kerberoasting attack

We download it from here : [HackTheBox](#)



SECURITY-DC Number of events: 293

Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:

- Account Name: DC015@FORELA.LOCAL
- Account Domain: FORELA.LOCAL
- Logon GUID: {8adc4d32-b1dc-937f-efec-0bda6b606c42}

Service Information:

- Service Name: DC015
- Service ID: S-1-5-21-3239415629-1862073780-2394361899-1000

Network Information:

- Client Address: ::1
- Client Port: 0

Additional Information:

- Ticket Options: 0x40810000
- Ticket Encryption Type: 0x12
- Failure Code: 0x0

This is the first event , and this is not Kerberoasting

- account name ending with \$
- service name ending with \$
- encryption type not weak encryption

SECURITY-DC Number of events: 293

Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:

- Account Name: DC015@FORELA.LOCAL
- Account Domain: FORELA.LOCAL
- Logon GUID: {8adc4d32-b1dc-937f-efec-0bda6b606c42}

Service Information:

- Service Name: krbtgt
- Service ID: S-1-5-21-3239415629-1862073780-2394361899-502

Network Information:

- Client Address: ::1
- Client Port: 0

Additional Information:

- Ticket Options: 0x60810010
- Ticket Encryption Type: 0x12
- Failure Code: 0x0

Same

SECURITY-DC Number of events: 293

Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:18:51 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:18:09 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:15:12 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:13:02 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:

- Account Name: alonzo.spire@FORELA.LOCAL
- Account Domain: FORELA.LOCAL
- Logon GUID: {59f3b9b1-65ed-a449-5ac0-8ea1f68478ee}

Service Information:

- Service Name: MSSQLService
- Service ID: S-1-5-21-3239415629-1862073780-2394361899-105

Network Information:

- Client Address: ::ffff:172.17.79.129
- Client Port: 58107

Additional Information:

- Ticket Options: 0x40800000
- Ticket Encryption Type: 0x17
- Failure Code: 0x0

0x17 → RC4
account name → \$ not
also service name

- This is Kerberoasting pattern [5/21/2024 6:18:09 AM]
- if we search with this ip (172.17.79.129) we can find more TGS Request with short periode
- remember the time

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:06:15 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:06:15 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:05:54 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:
Account Name: alonzo.spire@FORELA.LOCAL
Account Domain: FORELA.LOCAL
Logon GUID: {afc77729-012f-9e47-0026-cd4fe0c4f367}

Service Information:
Service Name: FORELA-WKSTN001\$
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1106

Network Information:
Client Address: ::ffff:172.17.79.129
Client Port: 57641

SECURITY-DC Number of events: 293

Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:15:12 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:13:02 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:
Account Name: alonzo.spire@FORELA.LOCAL
Account Domain: FORELA.LOCAL
Logon GUID: {afc77729-012f-9e47-0026-cd4fe0c4f367}

Service Information:
Service Name: DC01\$
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1000

Network Information:
Client Address: ::ffff:172.17.79.129
Client Port: 57648

SECURITY-DC Number of events: 293

Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16

Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:15:12 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:13:02 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:
Account Name: alonzo.spire@FORELA.LOCAL
Account Domain: FORELA.LOCAL
Logon GUID: {1ed76799-8ef3-2892-5747-89a4562533a5}

Service Information:
Service Name: DC01\$
Service ID: S-1-5-21-3239415629-1862073780-2394361899-1000

Network Information:
Client Address: ::ffff:172.17.79.129
Client Port: 57822

SECURITY-DC Number of events: 293				
Filtered: Log: file://C:\Users\target\Downloads\campfire-1\Triage\event\SECURITY-DC.evtx; Source: ; Event ID: 4769. Number of events: 16				
Level	Date and Time	Source	Event ID	Task Category
Information	5/21/2024 6:18:09 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:15:12 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:13:02 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...
Information	5/21/2024 6:12:05 AM	Microsoft Windows security a...	4769	Kerberos Service Ticket Operati...

Event 4769, Microsoft Windows security auditing.	
General	Details
A Kerberos service ticket was requested. Account Information: Account Name: alonzo.spire@FORELA.LOCAL Account Domain: FORELA.LOCAL Logon GUID: (59f3b9b1-65ed-a449-5ac0-8ea1f68478ee) Service Information: Service Name: MSSQLService Service ID: S-1-5-21-3239415629-1862073780-2394361899-1105 Network Information: Client Address: ::ffff:172.17.79.129 Client Port: 58107	

Analyzing Powershell events :

Powershell-Operational_1 Number of events: 42				
Level	Date and Time	Source	Event ID	Task Category
Warning	5/21/2024 6:16:32 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	5/21/2024 6:16:32 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Information	5/21/2024 6:16:30 AM	PowerShell (Microsoft-Windo...	40962	PowerShell Console Startup
Information	5/21/2024 6:16:30 AM	PowerShell (Microsoft-Windo...	53504	PowerShell Named Pipe IPC
Information	5/21/2024 6:16:29 AM	PowerShell (Microsoft-Windo...	40961	PowerShell Console Startup

Event 4104, PowerShell (Microsoft-Windows-PowerShell)	
General	Details
Creating Scriptblock text (1 of 20): #requires -version 2 <# PowerSploit File: PowerView.ps1 Author: Will Schroeder (@harmj0y) License: BSD 3-Clause Required Dependencies: None Optional Dependencies: None	

- **Script block logging [4104]** : Record the processing of commands, script blocks, functions, and scripts whether invoked interactively, or through automation

- **Script Block Logging**: This is the raw, deobfuscated script supplied through the command line or wrapped in a function, script, workflow

Analyzing prefetch file

Prefetch files are great artifacts for forensic investigators trying to analyze applications that have been run on a system. Windows creates a prefetch file when an application is run from a particular location for the very first time. This is used to help speed up the loading of applications. For investigators, these files contain some valuable data on a user's application history on a computer

using WinPrefetchView tool

UNEXPIREVESE.TUP.EXE...	7/11/2025 4:53:53 AM	3/21/2024 6:18:09 AM	36,106	UNEXPIREVESE.TUP.EXE	\\VOLUME{01d951602330db46-52233816}\PROGRAM FILES\WINNLSOFT\UNEXPIREVESE.TUP.EXE
OPENWITH.EXE-8B50...	7/11/2025 4:53:53 AM	5/3/2023 4:33:01 PM	35,704	OPENWITH.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\OPENWITH.EXE
PHPSTORM-2023.1.1.E...	7/11/2025 4:53:53 AM	5/2/2023 5:38:28 PM	30,889	PHPSTORM-2023.1.1.EXE	\\VOLUME{01d951602330db46-52233816}\USERS\SIMON\STARK\DOWNLOADS\PHPSTORM-2023.1.1.EXE
POWERPNT.EXE-7ABD...	7/11/2025 4:53:53 AM	5/2/2023 6:01:40 PM	65,004	POWERPNT.EXE	\\VOLUME{01d951602330db46-52233816}\PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\POWERPNT.EXE
POWERSHELL.EXE-CA...	7/11/2025 4:53:53 AM	5/21/2024 6:16:39 AM	32,954	POWERSHELL.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
POWERSHELL_ISE.EXE...	7/11/2025 4:53:53 AM	3/19/2024 7:08:10 AM	62,437	POWERSHELL_ISE.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL_ISE.EXE
PSEXEC64.EXE-BE2659...	7/11/2025 4:53:53 AM	9/7/2023 3:05:28 PM	3,961	PSEXEC64.EXE	\\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\DOWNLOADS\PSTOOLS\PSEXEC64.EXE
REGEDIT.EXE-DAB9D6...	7/11/2025 4:53:53 AM	3/26/2024 10:35:03 PM	8,172	REGEDIT.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\REGEDIT.EXE
RUBEUS.EXE-679234...	7/11/2025 4:53:53 AM	5/21/2024 6:18:09 AM	17,769	RUBEUS.EXE	\\VOLUME{01d951602330db46-52233816}\USERS\ALONZO.SPIRE\DOWNLOADS\RUBEUS.EXE
RUNDLL32.EXE-1C52D...	7/11/2025 4:53:53 AM	5/21/2024 6:12:05 AM	4,225	RUNDLL32.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
RUNDLL32.EXE-27E52...	7/11/2025 4:53:53 AM	4/26/2024 1:17:24 PM	2,764	RUNDLL32.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
RUNDLL32.EXE-41CF3...	7/11/2025 4:53:53 AM	6/12/2023 9:52:19 AM	12,357	RUNDLL32.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
RUNDLL32.EXE-75313...	7/11/2025 4:53:53 AM	5/21/2024 6:28:21 AM	3,307	RUNDLL32.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
RUNDLL32.EXE-C0159...	7/11/2025 4:53:53 AM	4/26/2024 1:17:26 PM	3,206	RUNDLL32.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE
RUNONCE.EXE-FB4EF...	7/11/2025 4:53:53 AM	3/26/2024 10:34:55 PM	13,668	RUNONCE.EXE	\\VOLUME{01d951602330db46-52233816}\WINDOWS\SYSTEM32\RUNDLL32.EXE

Filename	Full Path	Device Path	Index
SMFT		\\VOLUME{01d951602330db46-52233816}	28
19.043.0304[1].JSON		\\VOLUME{01d951602330db46-52233816}	633
21.220.1024[1].JSON		\\VOLUME{01d951602330db46-52233816}	590
5475CB191E478C3937...		\\VOLUME{01d951602330db46-52233816}	402
5A2A7058CF8D1E56C...		\\VOLUME{01d951602330db46-52233816}	592
6BADA8974A10C48D6...		\\VOLUME{01d951602330db46-52233816}	205
6BADA8974A10C48D6...		\\VOLUME{01d951602330db46-52233816}	206
7423F88C7F265F0DEF...		\\VOLUME{01d951602330db46-52233816}	219
7423F88C7F265F0DEF...		\\VOLUME{01d951602330db46-52233816}	220
80237EE4964FC9C409...		\\VOLUME{01d951602330db46-52233816}	588

Hunting With Custom Script

```
(kali@Anas404)-[~/Desktop/scripts/kerbroastor]
$ python kerbroast_detector.py SECURITY-DC.evtx

Total TGS requests found: 16
RC4 Kerberoasting Tickets (0x17) found: 1

+-----+-----+-----+-----+-----+
| Time | IP | Account | Service | Encryption |
+-----+-----+-----+-----+-----+
| 2024-05-21 03:18:09.459681+00:00 | ::ffff:172.17.79.129 | alonzo.spire@FORELA.LOCAL | MSSQLService | 0x00000017 |
+-----+-----+-----+-----+-----+

IP Request Counts:
::1 -> 12 requests
::ffff:172.17.79.129 -> 4 requests

Services requested with RC4 Encryption:
MSSQLService -> 1 requests

(kali@Anas404)-[~/Desktop/scripts/kerbroastor]
```

Same Result

kerberoasting behaviour

account name : alonzo.spire -

service name : MSSQLService -

client address : 172.17.79.129 -

time : 5/21/2024 6:18:09 AM -

TicketEncryptionType : 0x17 -

more TGS Request <-- 172.17.79.129 -

tool : C:\Users\Alonzo.spire\Downloads\Rubeus.exe

enumeration

tool : PowerView.ps1 -

time : 5/21/2024 6:16:32 AM -
from 4104 : Script Block logging -

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>
](<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia>

سبحانك اللهم وبحمدك أشهد أن لا إله إلا أنت أستغفرك وأتوب إليك