Kerberoasting Investigation Report

Analyst: Aarush Nepali
Date: July 14, 2025
Environment: Kali Linux, Splunk (local instance)
Log Source: Converted Windows Event Logs (`.evtx` to JSON)
Primary Data Location: `/home/kali/Downloads/Triage/converted/`

Objective

To analyze Windows Security logs for indicators of a **Kerberoasting attack**. Kerberoasting typically involves Event ID 4769, where a Ticket Granting Service (TGS) ticket is requested for a service account with RC4 encryption (e.g., `0x17`, `0x18`).

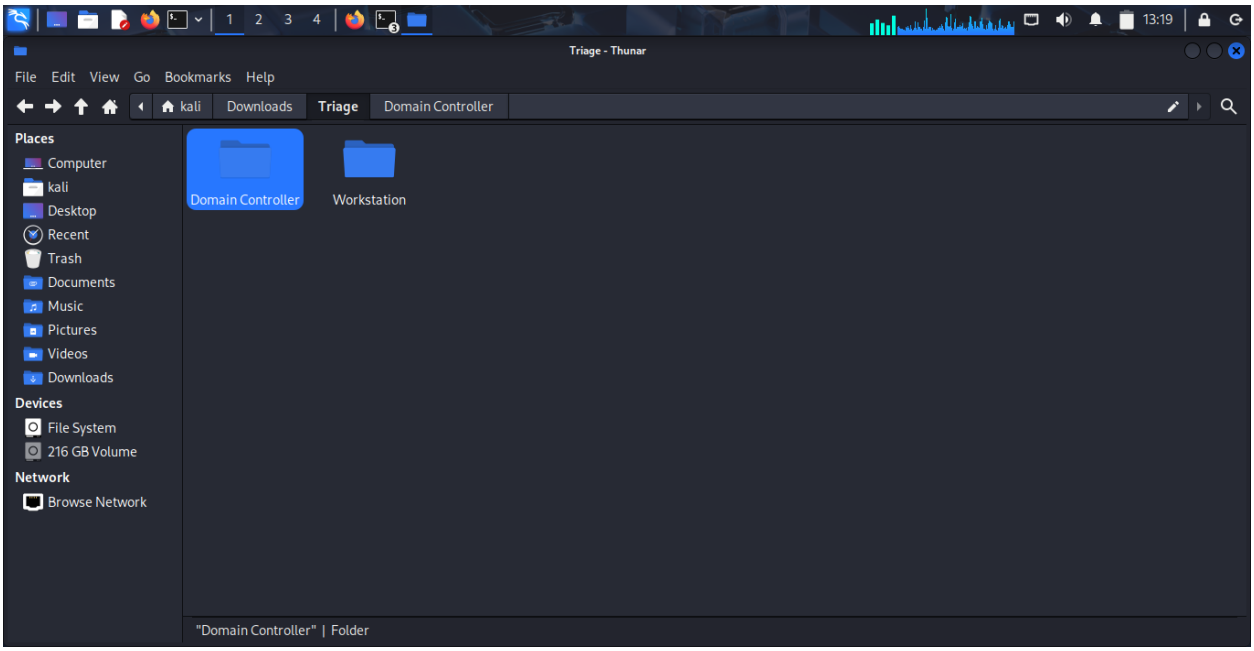
Process Summary

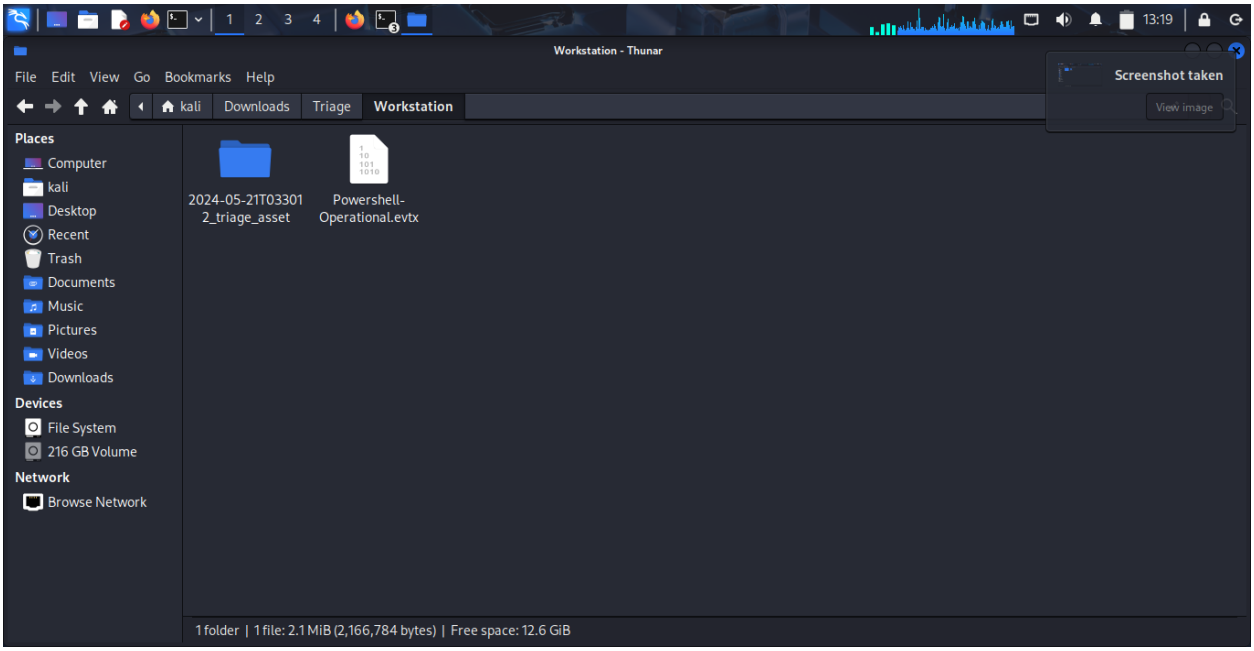
1. Initial Setup and Conversion

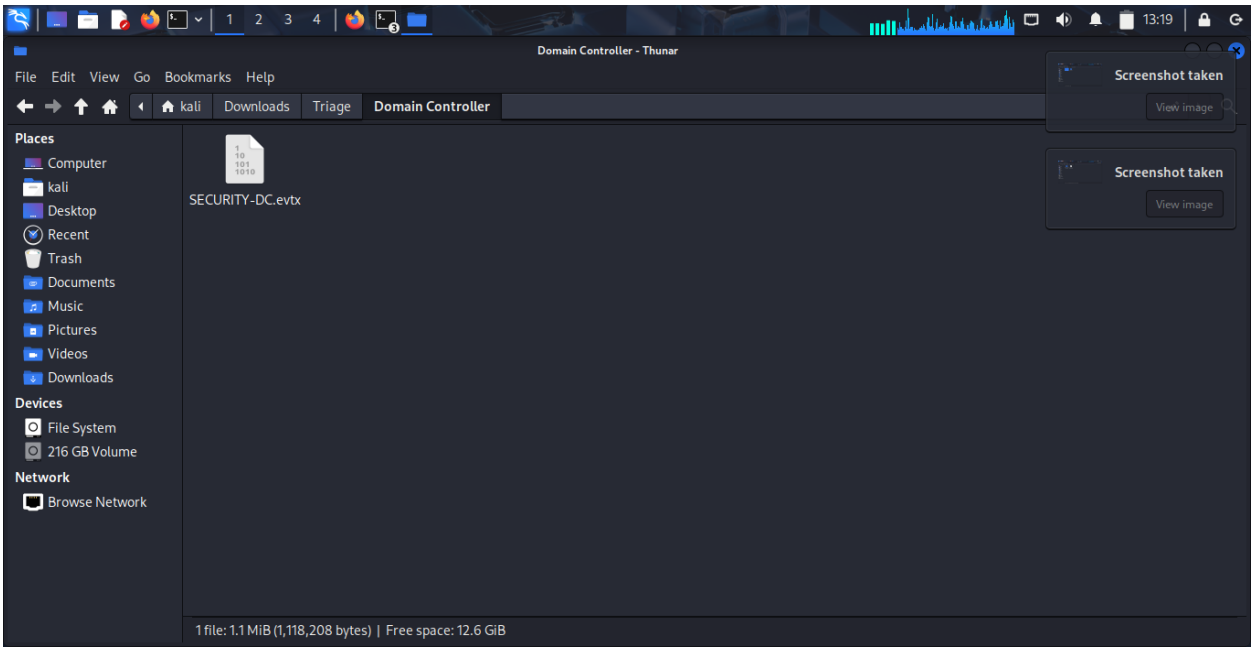
- Original `.evtx` files located in `/home/kali/Downloads/Triage/eventlogs/`
- Converted to JSON using a Python script (via `python-evtx`).
- Converted files saved in: `/home/kali/Downloads/Triage/converted/`

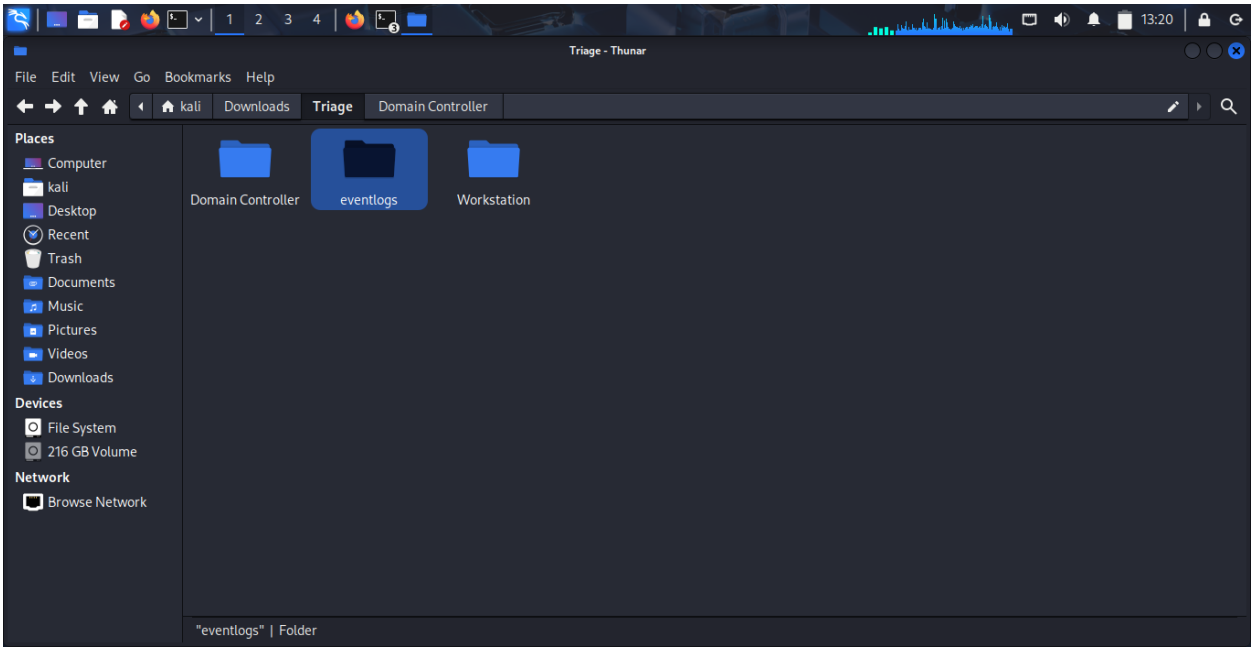
2. Splunk Ingestion

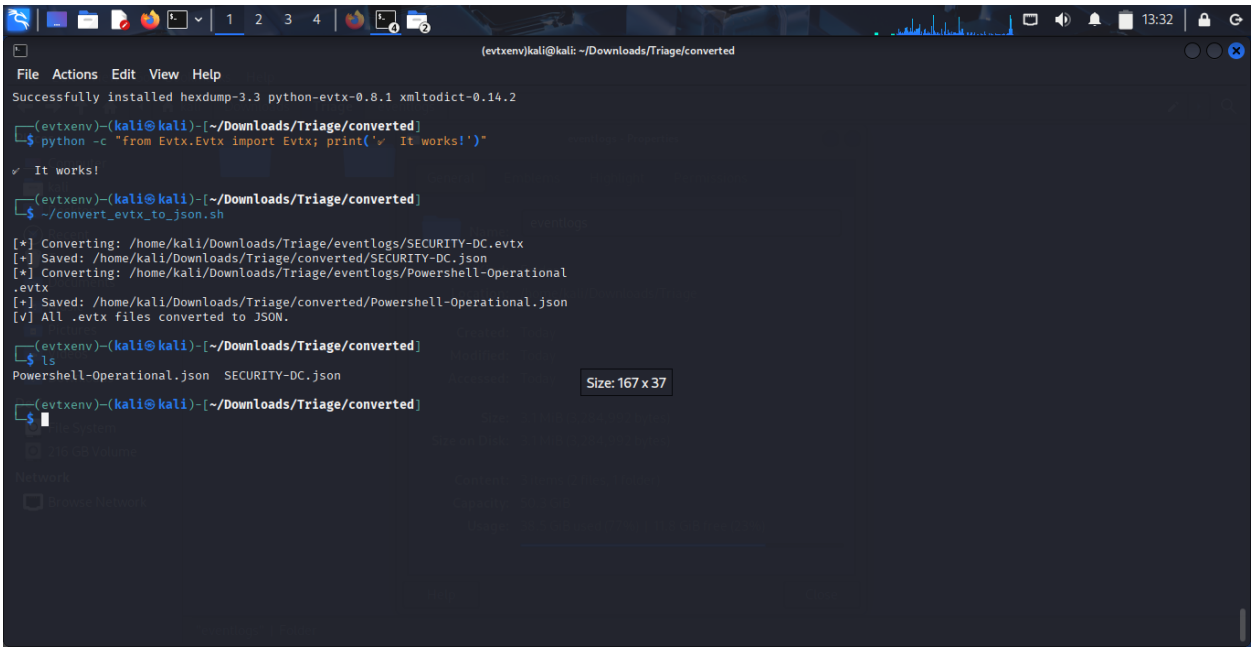
- Files ingested into Splunk under sourcetype: `json-2`
- Total events


1 2 3 4
13:19
Triage - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
Triage
Domain Controller
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
216 GB Volume
Network
Browse Network
Domain Controller
Workstation
"Domain Controller" | Folder


1 2 3 4
13:19
Workstation - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
Triage
Workstation
Screenshot taken
View image
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
216 GB Volume
Network
Browse Network
2024-05-21T033012_triage_asset
Powershell-Operational.evtx
1 folder | 1 file: 2.1 MiB (2,166,784 bytes) | Free space: 12.6 GiB

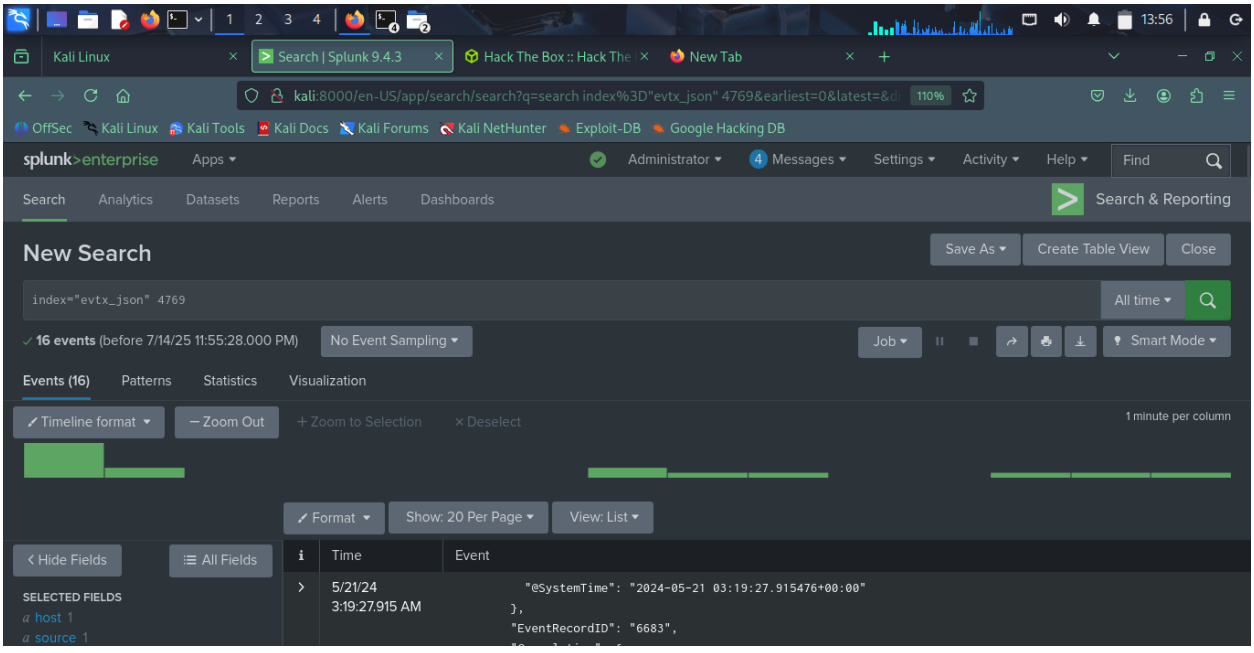

13:19
Domain Controller - Thunar
File Edit View Go Bookmarks Help
kali Downloads Triage Domain Controller
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
216 GB Volume
Network
Browse Network
SECURITY-DC.evtx
Screenshot taken
View image
Screenshot taken
View image
1 file: 1.1 MiB (1,118,208 bytes) | Free space: 12.6 GiB

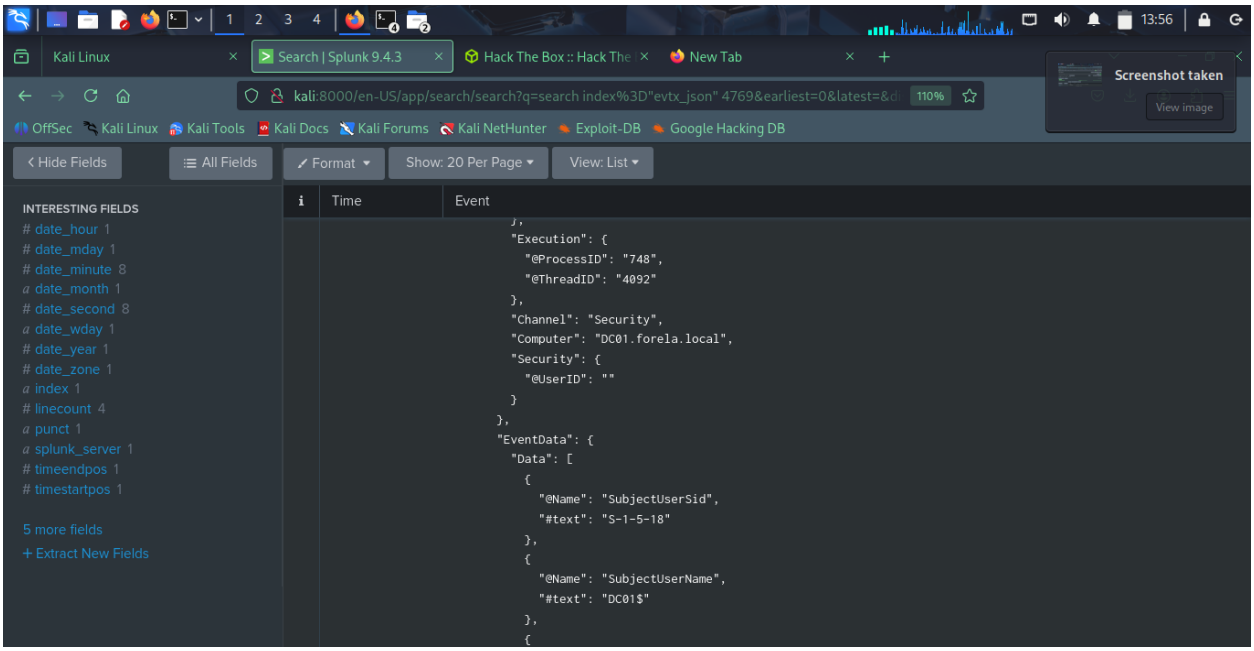

13:20
Triage - Thunar
File Edit View Go Bookmarks Help
kali Downloads Triage Domain Controller
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
216 GB Volume
Network
Browse Network
Domain Controller
eventlogs
Workstation
"eventlogs" | Folder

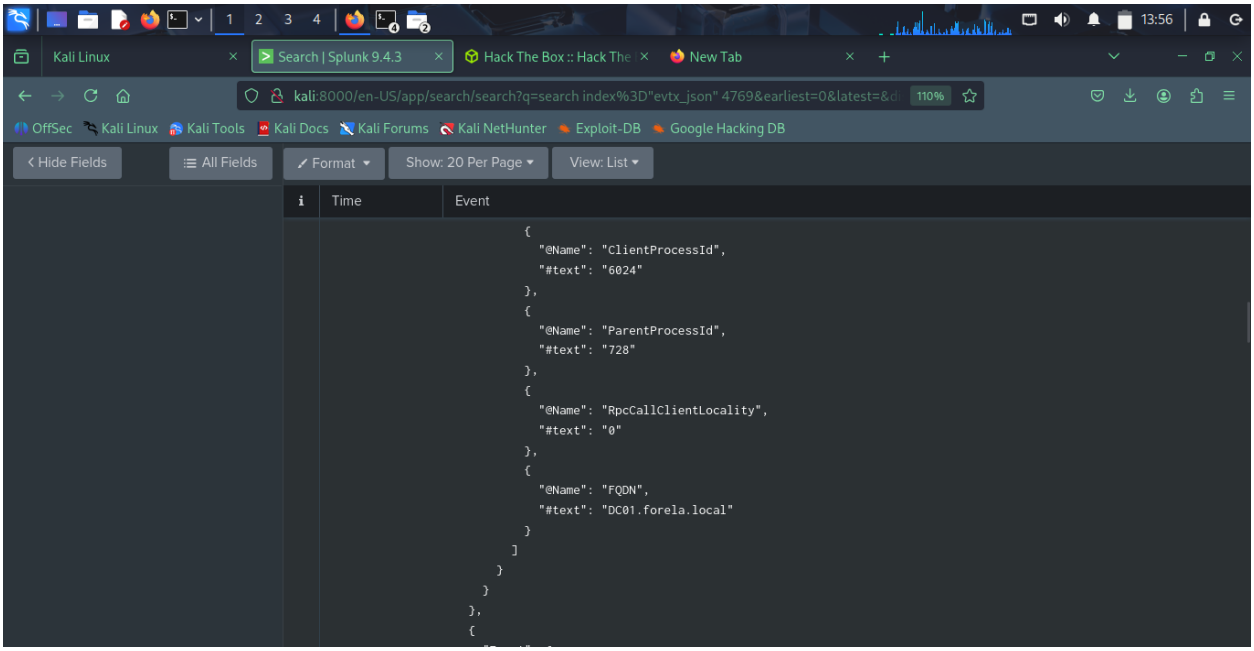


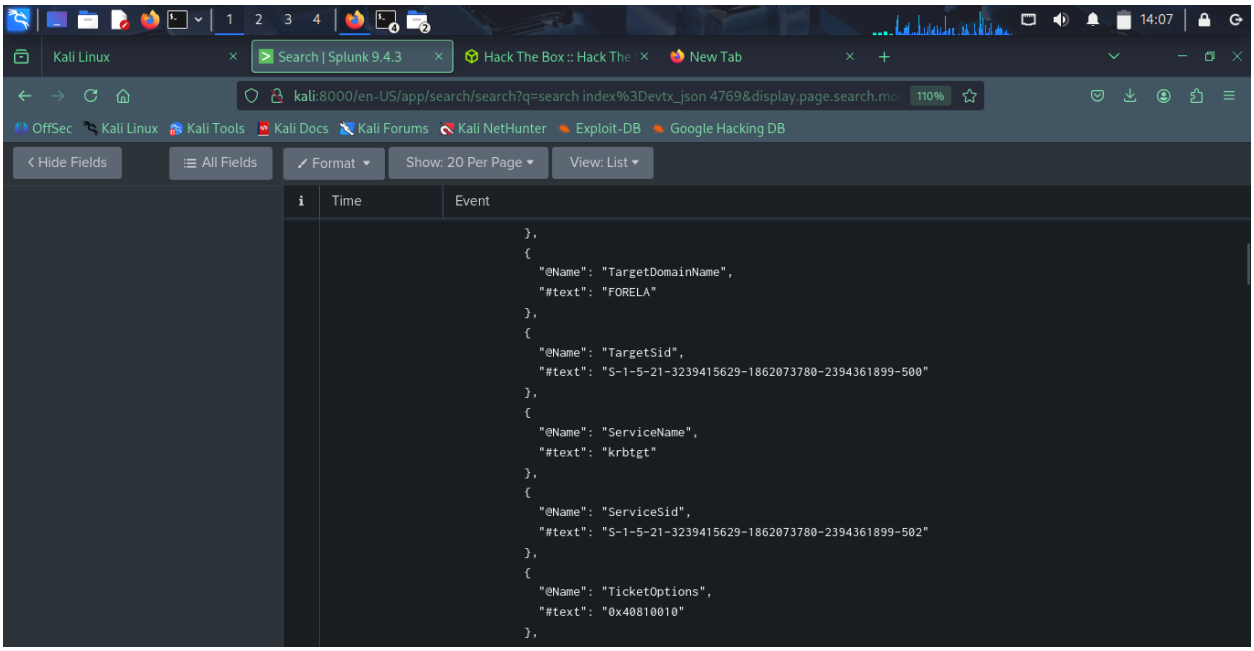
3. Search Methodology for Kerberoasting

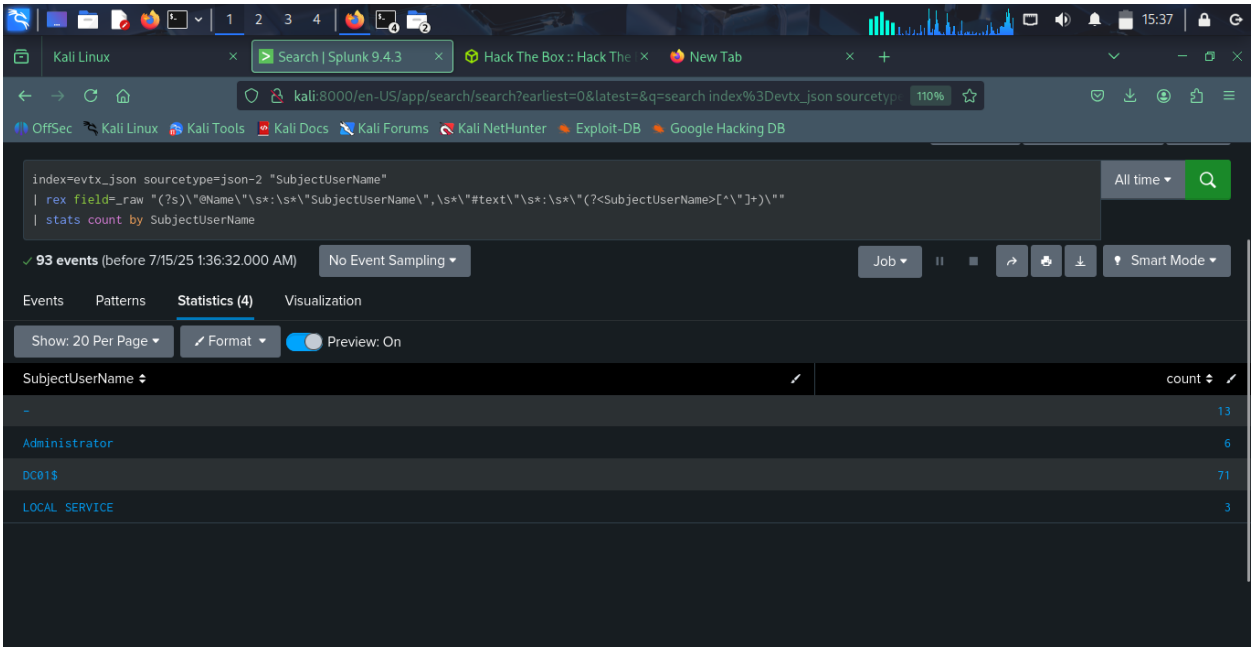
- Targeted Event ID: **4769** (TGS requests)
- Fields of interest:
  - `ServiceName`
  - `TicketEncryptionType`
  - `TargetUserName`

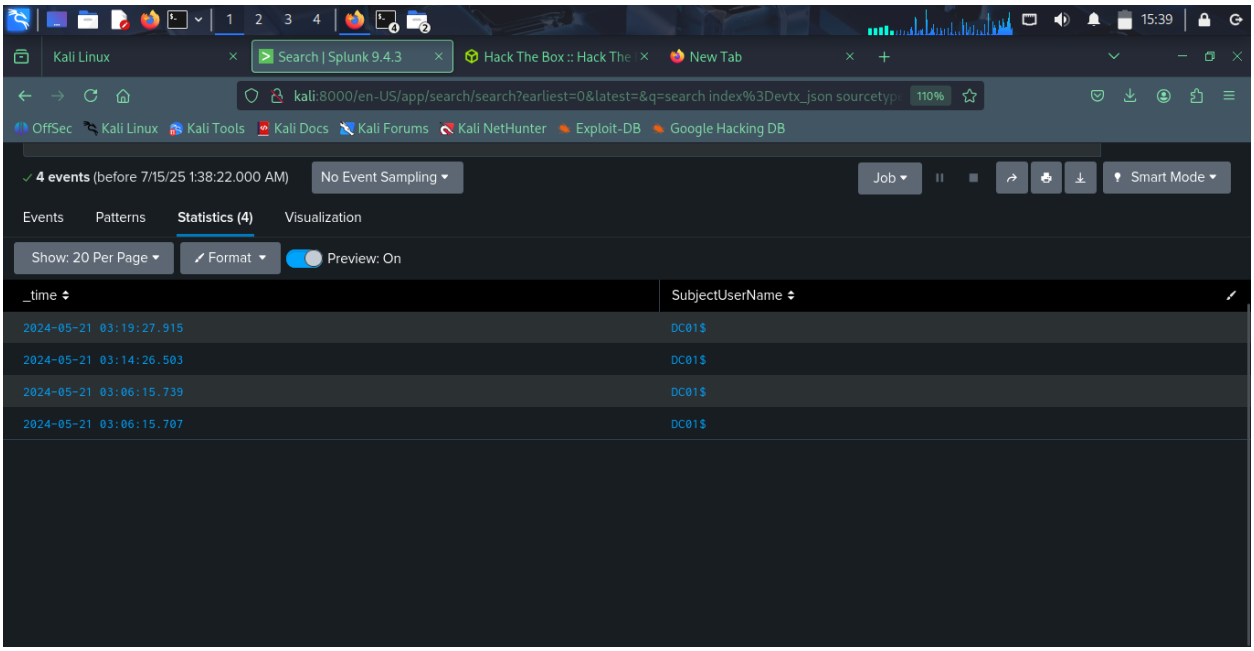


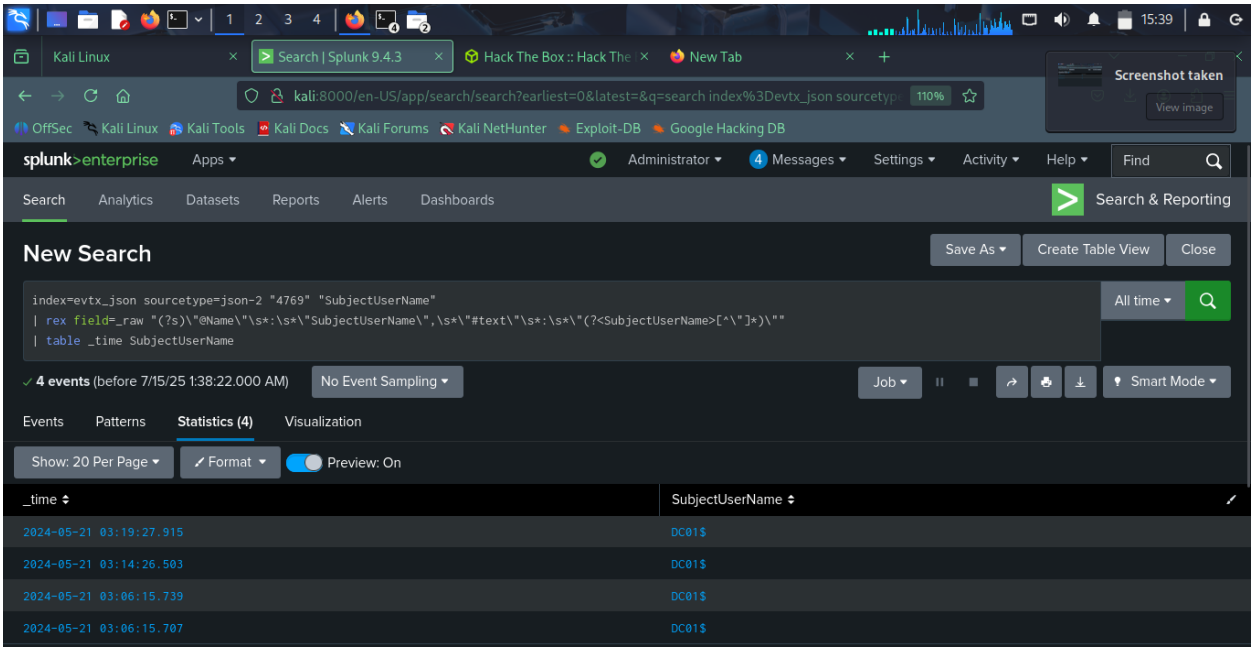

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
13:56
kali:8000/en-US/app/search/search?q=search index%3D"evtx_json" 4769&earliest=0&latest=&
110%
Screenshot taken
View image
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 8
a date_month 1
date_second 8
a date_wday 1
date_year 1
date_zone 1
a index 1
linecount 4
a punct 1
a splunk_server 1
timeendpos 1
timestartpos 1
5 more fields
+ Extract New Fields
Time
Event
},
"Execution": {
"@ProcessID": "748",
"@ThreadID": "4092"
},
"Channel": "Security",
"Computer": "DC01.forela.local",
"Security": {
"@UserID": ""
}
},
"EventData": {
"Data": [
{
"@Name": "SubjectUserSid",
"#text": "S-1-5-18"
},
{
"@Name": "SubjectUserName",
"#text": "DC01$"
},
{

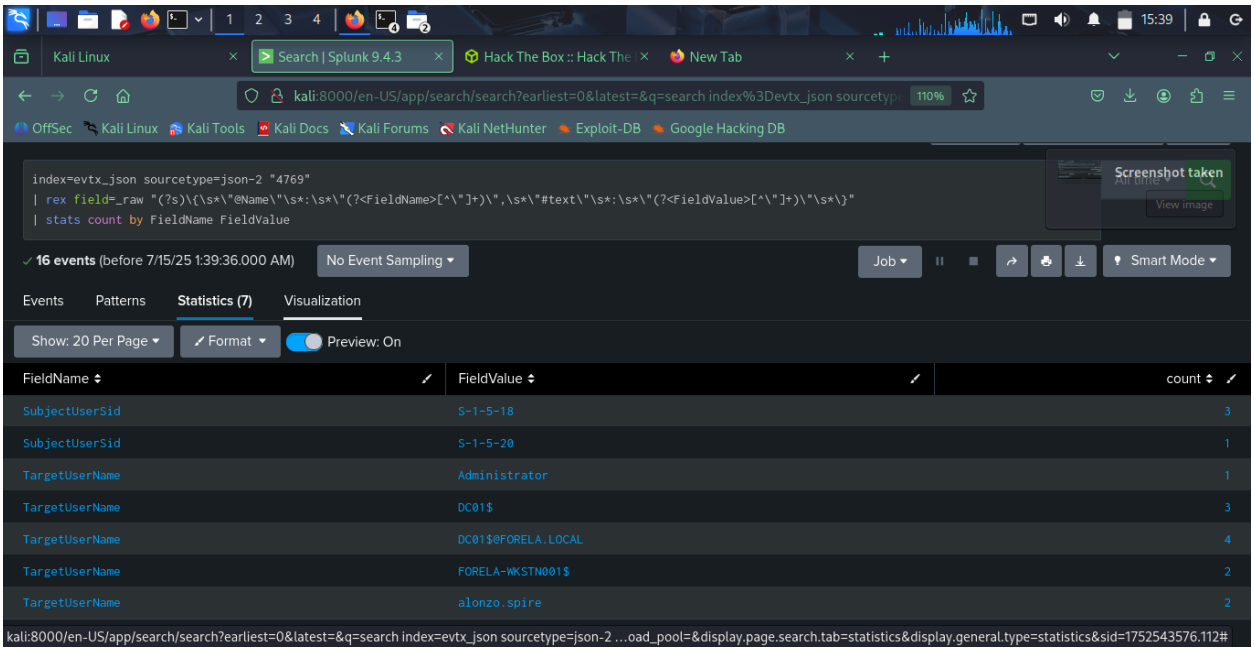

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
13:56
kali:8000/en-US/app/search/search?q=search index%3D"evtx_json" 4769&earliest=0&latest=&
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
{
"@Name": "ClientProcessId",
"#text": "6024"
},
{
"@Name": "ParentProcessId",
"#text": "728"
},
{
"@Name": "RpcCallClientLocality",
"#text": "0"
},
{
"@Name": "FQDN",
"#text": "DC01.forela.local"
}
]
}
}
},
{

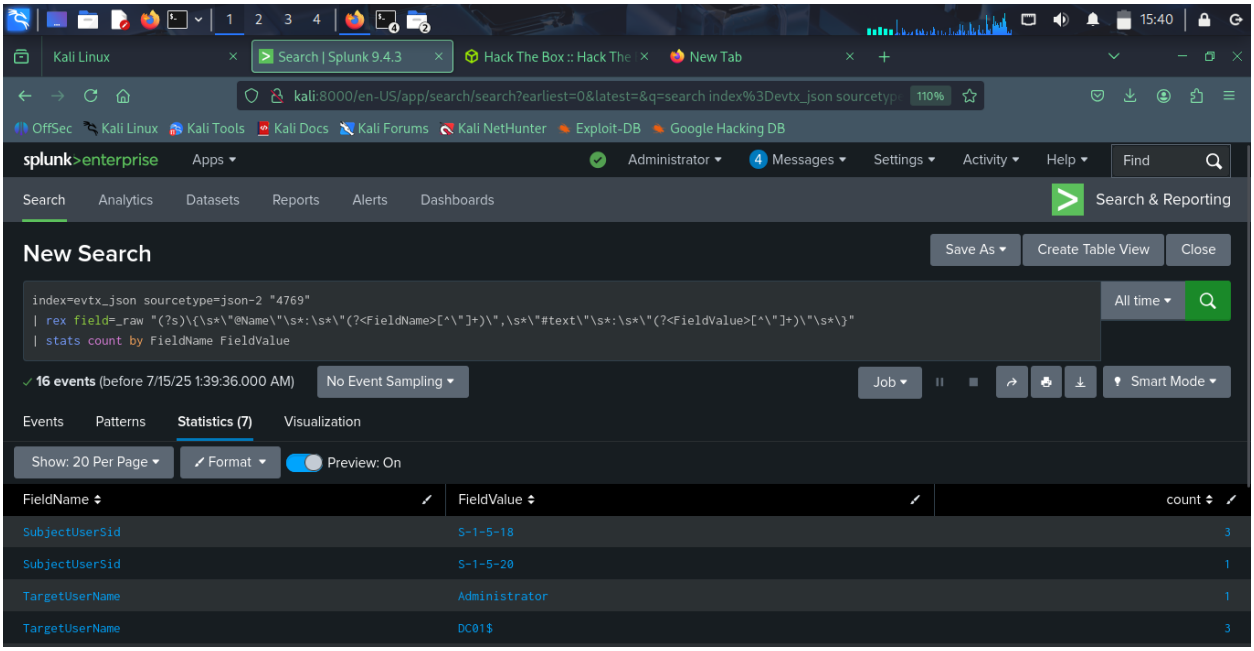

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?q=search index%3Devtx_json 4769&display.page.search.mo
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Hide Fields
All Fields
Format
Show: 20 Per Page
View: List
Time
Event
},
{
"@Name": "TargetDomainName",
"#text": "FORELA"
},
{
"@Name": "TargetSid",
"#text": "S-1-5-21-3239415629-1862073780-2394361899-500"
},
{
"@Name": "ServiceName",
"#text": "krbtgt"
},
{
"@Name": "ServiceSid",
"#text": "S-1-5-21-3239415629-1862073780-2394361899-502"
},
{
"@Name": "TicketOptions",
"#text": "0x40810010"
},

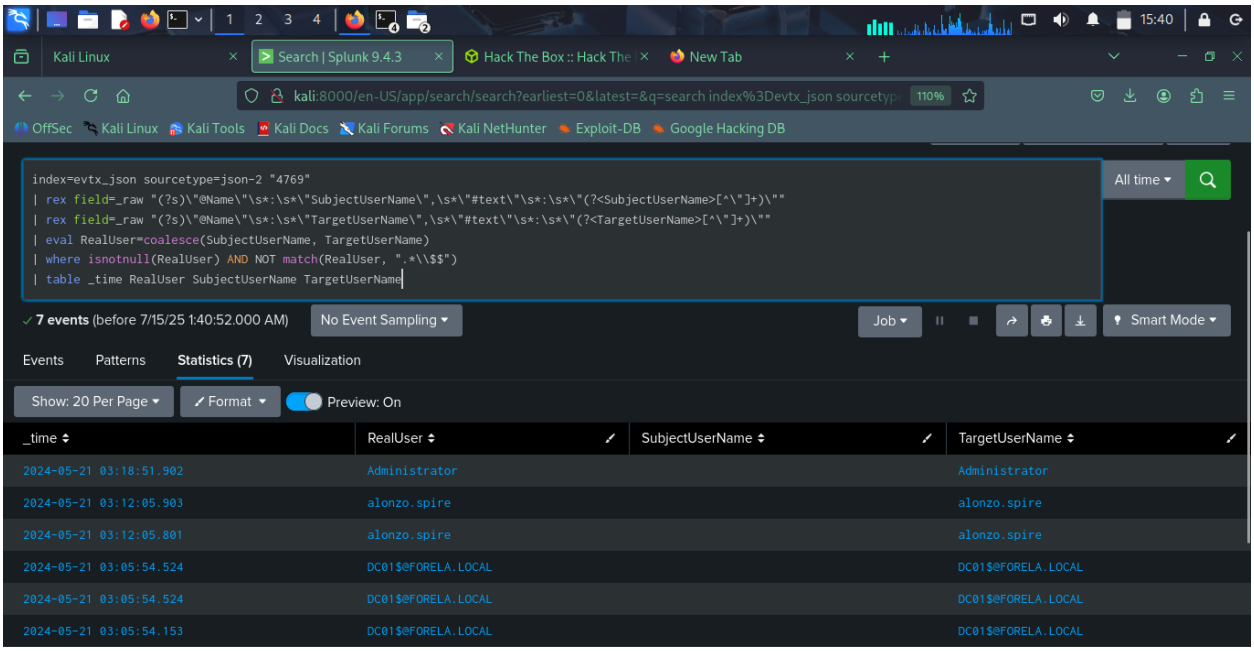

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
index=evtx_json sourcetype=json-2 "SubjectUserName"
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"SubjectUserName\",\s*\"#text\"\s*:\s*\"(?<SubjectUserName>[^\"]+)\""
| stats count by SubjectUserName
All time
93 events (before 7/15/25 1:36:32.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (4)
Visualization
Show: 20 Per Page
Format
Preview: On
SubjectUserName
count
-
13
Administrator
6
DC01$
71
LOCAL SERVICE
3

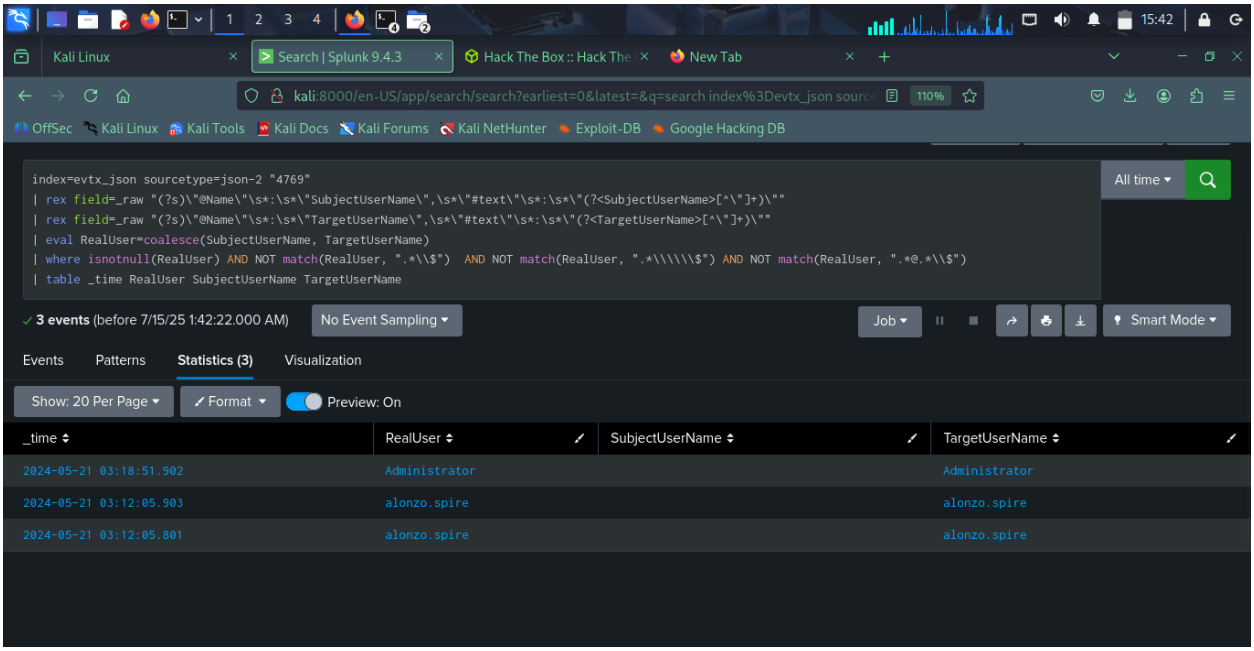

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
4 events (before 7/15/25 1:38:22.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (4)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
SubjectUserName
2024-05-21 03:19:27.915
DC01$
2024-05-21 03:14:26.503
DC01$
2024-05-21 03:06:15.739
DC01$
2024-05-21 03:06:15.707
DC01$

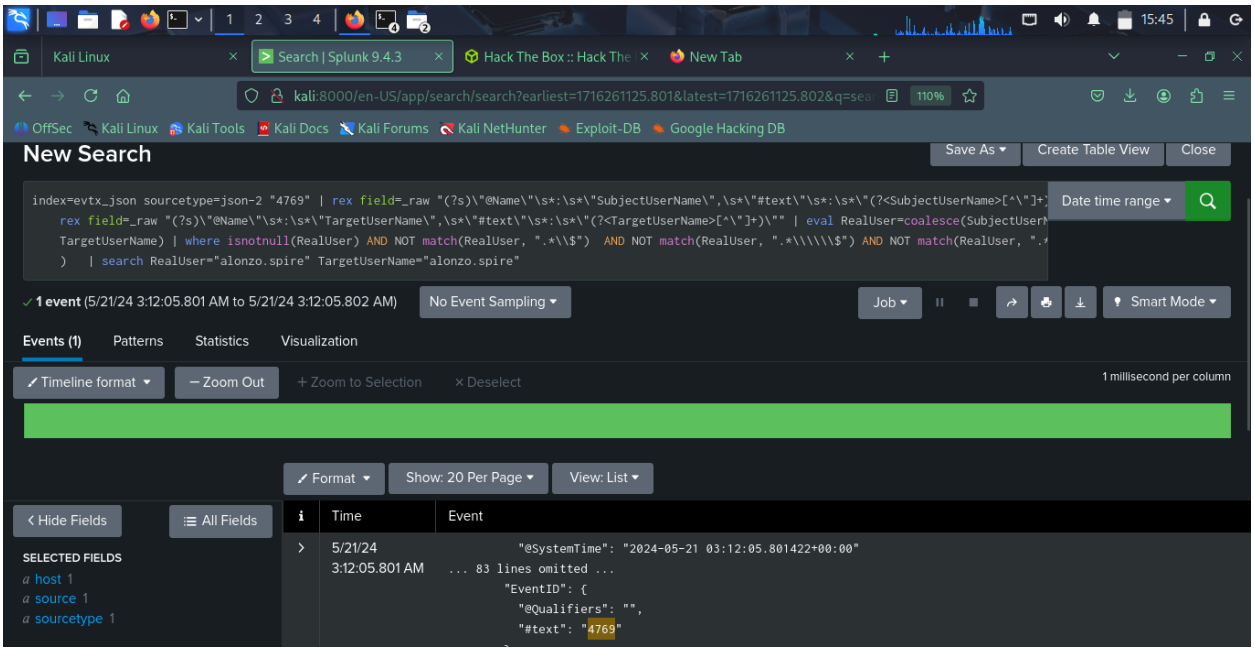

Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
Screenshot taken
View image
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=evtx_json sourcetype=json-2 "4769" "SubjectUserName"
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"SubjectUserName\",\s*\"#text\"\s*:\s*\"(?<SubjectUserName>[^\"]*)\""
| table _time SubjectUserName
All time
4 events (before 7/15/25 1:38:22.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (4)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
SubjectUserName
2024-05-21 03:19:27.915
DC01$
2024-05-21 03:14:26.503
DC01$
2024-05-21 03:06:15.739
DC01$
2024-05-21 03:06:15.707
DC01$

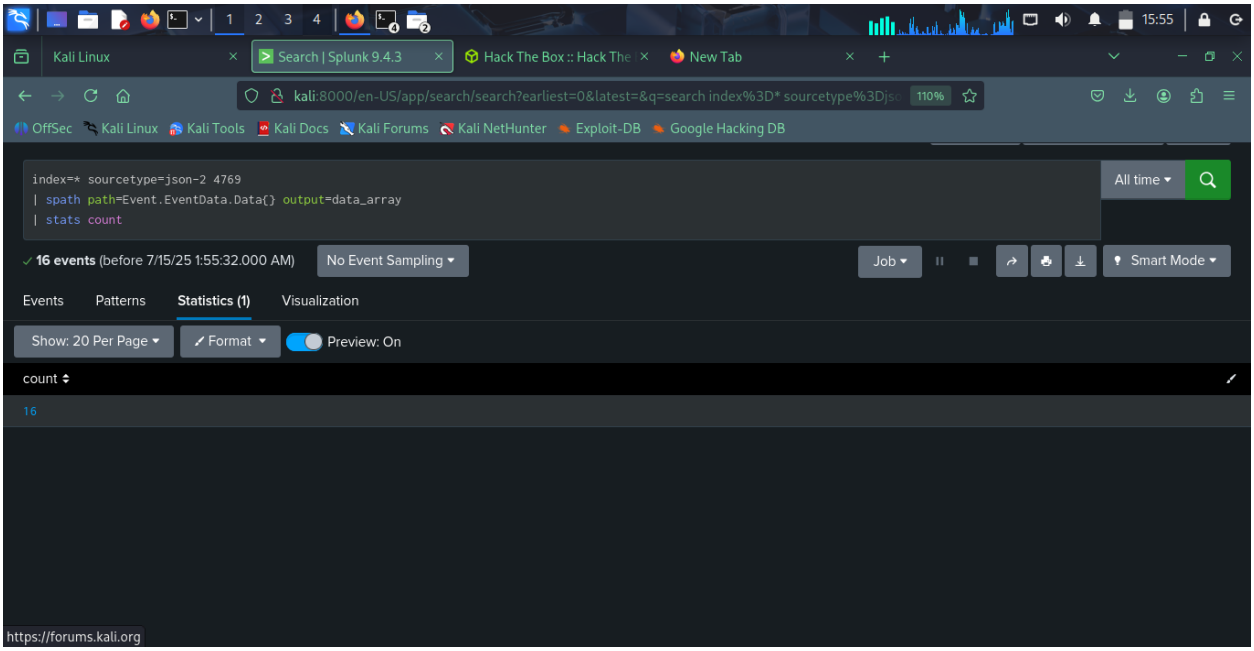

15:39
Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
index=evtx_json sourcetype=json-2 "4769"
| rex field=_raw "(?s)\{\s*\"@Name\"\s*:\s*\"(?<FieldName>[^\"]+)\",\s*\"#text\"\s*:\s*\"(?<FieldValue>[^\"]+)\"\s*\}"
| stats count by FieldName FieldValue
Screenshot taken
View image
16 events (before 7/15/25 1:39:36.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (7)
Visualization
Show: 20 Per Page
Format
Preview: On
FieldName
FieldValue
count
SubjectUserSid
S-1-5-18
3
SubjectUserSid
S-1-5-20
1
TargetUserName
Administrator
1
TargetUserName
DC01$
3
TargetUserName
DC01$@FORELA.LOCAL
4
TargetUserName
FORELA-WKSTN001$
2
TargetUserName
alonzo.spire
2
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index=evtx_json sourcetype=json-2 ...oad_pool=&display.page.search.tab=statistics&display.general.type=statistics&sid=1752543576.112#

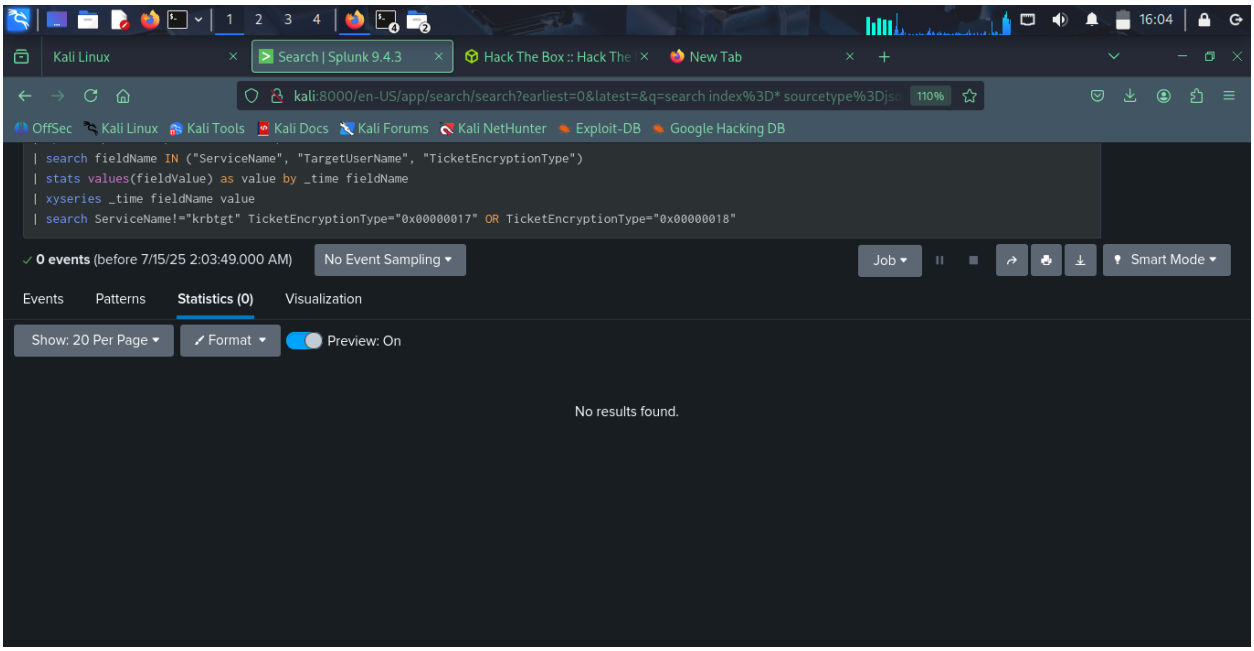

15:40
Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
splunk>enterprise
Apps
Administrator
4 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=evtx_json sourcetype=json-2 "4769"
| rex field=_raw "(?s)\{\s*\"@Name\"\s*:\s*\"(?<FieldName>[^\"]+)\",\s*\"#text\"\s*:\s*\"(?<FieldValue>[^\"]+)\"\s*\}"
| stats count by FieldName FieldValue
All time
16 events (before 7/15/25 1:39:36.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (7)
Visualization
Show: 20 Per Page
Format
Preview: On
FieldName
FieldValue
count
SubjectUserSid
S-1-5-18
3
SubjectUserSid
S-1-5-20
1
TargetUserName
Administrator
1
TargetUserName
DC01$
3

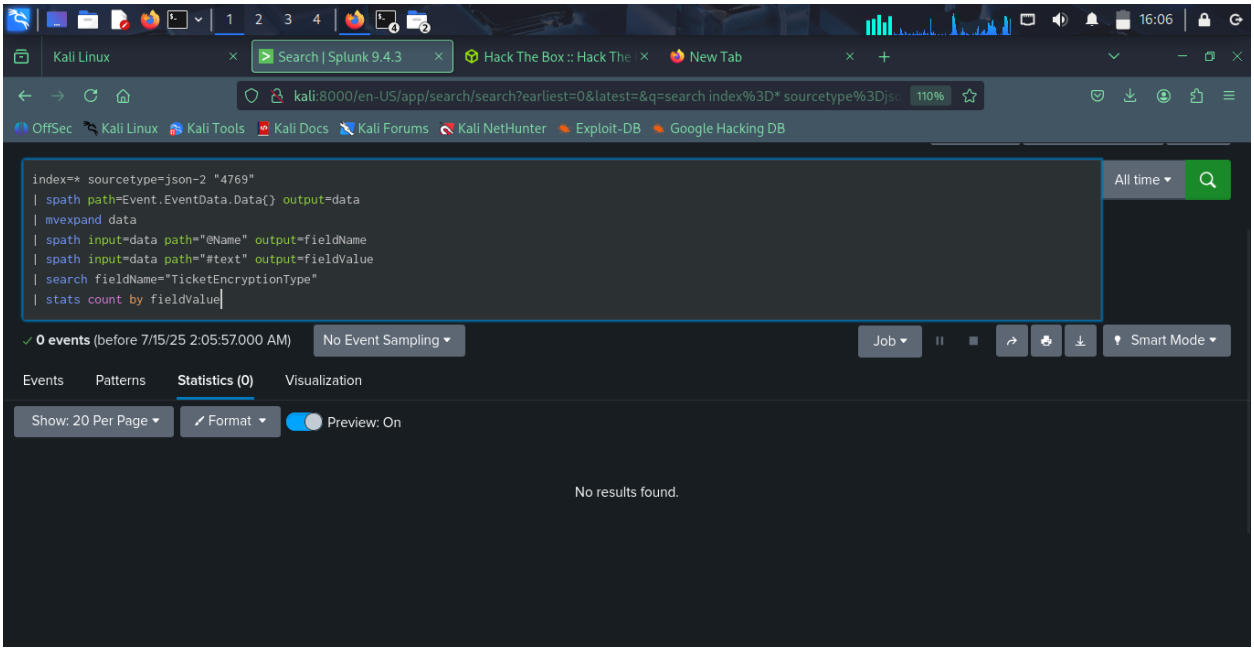

15:40
Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourcetyp
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
index=evtx_json sourcetype=json-2 "4769"
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"SubjectUserName\",\s*\"#text\"\s*:\s*\"(?<SubjectUserName>[^\"]+)\""
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"TargetUserName\",\s*\"#text\"\s*:\s*\"(?<TargetUserName>[^\"]+)\""
| eval RealUser=coalesce(SubjectUserName, TargetUserName)
| where isnotnull(RealUser) AND NOT match(RealUser, ".*\\$")
| table _time RealUser SubjectUserName TargetUserName
All time
7 events (before 7/15/25 1:40:52.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (7)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
RealUser
SubjectUserName
TargetUserName
2024-05-21 03:18:51.902
Administrator
Administrator
2024-05-21 03:12:05.903
alonzo.spire
alonzo.spire
2024-05-21 03:12:05.801
alonzo.spire
alonzo.spire
2024-05-21 03:05:54.524
DC01$@FORELA.LOCAL
DC01$@FORELA.LOCAL
2024-05-21 03:05:54.524
DC01$@FORELA.LOCAL
DC01$@FORELA.LOCAL
2024-05-21 03:05:54.153
DC01$@FORELA.LOCAL
DC01$@FORELA.LOCAL


15:42
Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3Devtx_json sourc
110%
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
index=evtx_json sourcetype=json-2 "4769"
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"SubjectUserName\",\s*\"#text\"\s*:\s*\"(?<SubjectUserName>[^\"]+)\""
| rex field=_raw "(?s)\"@Name\"\s*:\s*\"TargetUserName\",\s*\"#text\"\s*:\s*\"(?<TargetUserName>[^\"]+)\""
| eval RealUser=coalesce(SubjectUserName, TargetUserName)
| where isnotnull(RealUser) AND NOT match(RealUser, ".*\\$") AND NOT match(RealUser, ".*\\\\$") AND NOT match(RealUser, ".*@.*\\$")
| table _time RealUser SubjectUserName TargetUserName
All time
3 events (before 7/15/25 1:42:22.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (3)
Visualization
Show: 20 Per Page
Format
Preview: On
_time
RealUser
SubjectUserName
TargetUserName
2024-05-21 03:18:51.902
Administrator
Administrator
2024-05-21 03:12:05.903
alonzo.spire
alonzo.spire
2024-05-21 03:12:05.801
alonzo.spire
alonzo.spire


Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=1716261125.801&latest=1716261125.802&q=sea
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
New Search
Save As
Create Table View
Close
index=evtx_json sourcetype=json-2 "4769" | rex field=_raw "(?s)\"@Name\"\s*:\s*\"SubjectUserName\",\s*\"#text\"\s*:\s*\"(?<SubjectUserName>[^\"]+)
rex field=_raw "(?s)\"@Name\"\s*:\s*\"TargetUserName\",\s*\"#text\"\s*:\s*\"(?<TargetUserName>[^\"]+)\"" | eval RealUser=coalesce(SubjectUserN
TargetUserName) | where isnotnull(RealUser) AND NOT match(RealUser, ".*\\$") AND NOT match(RealUser, ".*\\\\\\$") AND NOT match(RealUser, ".*
) | search RealUser="alonzo.spire" TargetUserName="alonzo.spire"
Date time range
1 event (5/21/24 3:12:05.801 AM to 5/21/24 3:12:05.802 AM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
Time
Event
5/21/24
3:12:05.801 AM
"@SystemTime": "2024-05-21 03:12:05.801422+00:00"
... 83 lines omitted ...
"EventID": {
"@Qualifiers": "",
"#text": "4769"


Kali Linux
Search | Splunk 9.4.3
Hack The Box :: Hack The
New Tab
kali:8000/en-US/app/search/search?earliest=0&latest=&q=search index%3D* sourcetype%3Djs
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
index=* sourcetype=json-2 4769
| spath path=Event.EventData.Data{} output=data_array
| stats count
All time
16 events (before 7/15/25 1:55:32.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
Show: 20 Per Page
Format
Preview: On
count
16
https://forums.kali.org





Findings

1. Event ID 4769 Results

- A total of **16 events** were identified with Event ID 4769.
- All events had `ServiceName="krbtgt"` (indicating standard TGS requests for the Kerberos Ticket Granting Ticket service).
- **No events** used `TicketEncryptionType=0x00000017` or `0x00000018`, which are indicative of RC4 encryption vulnerable to Kerberoasting.

2. Accounts Involved

- Accounts observed in `TargetUserName`:
  - `Administrator`
  - `alonzo.spire`
  - `DC01$@FORELA.LOCAL`
- Notably, no suspicious service accounts (like `svc_*`) were targeted.

3. IP Address Analysis

- Some TGS requests came from loopback (`::1`) and local internal IP (`::ffff:172.17.79.129`).
- These are not suspicious in isolation within lab/test environments.

Conclusion

After detailed analysis of Event ID 4769 logs and related fields:

> **No evidence of a Kerberoasting attack was found in the dataset.**

All service ticket requests observed were for `krbtgt`, using AES encryption types (e.g., `0x12`). There were no abnormal service names or RC4 encryption patterns.

Recommendations

- If testing Kerberoasting detection, ingest known simulated attack data.
- Consider enabling detection rules that alert on:
  - `ServiceName != krbtgt`
  - `TicketEncryptionType IN (0x17, 0x18)`
- Maintain robust audit log ingestion from Domain Controllers.