

# Defanging the Dog: Attacking Windows Kerberos

---

Matthew Navarro



# General Outline

- Review the Kerberos authentication process.
- Overview of the Kerberos landscape
- Analyze some Kerberos attacks
- Create detections with PowerShell

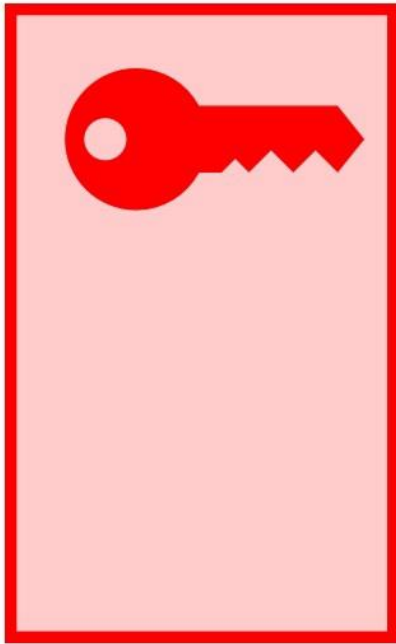
# Kerberos Authentication Process

# 3 Big Key Exchanges

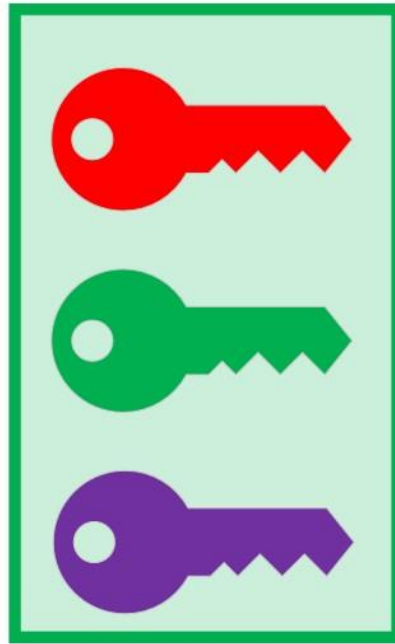
- Client <===> Authentication Server (AS)
- Client <===> Ticket Granting Server (TGS)
- Client <===> Application Server (AP)

# Keys Before Exchanges

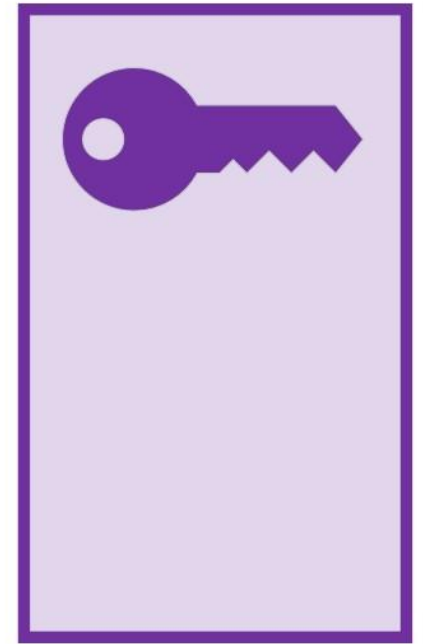
Client



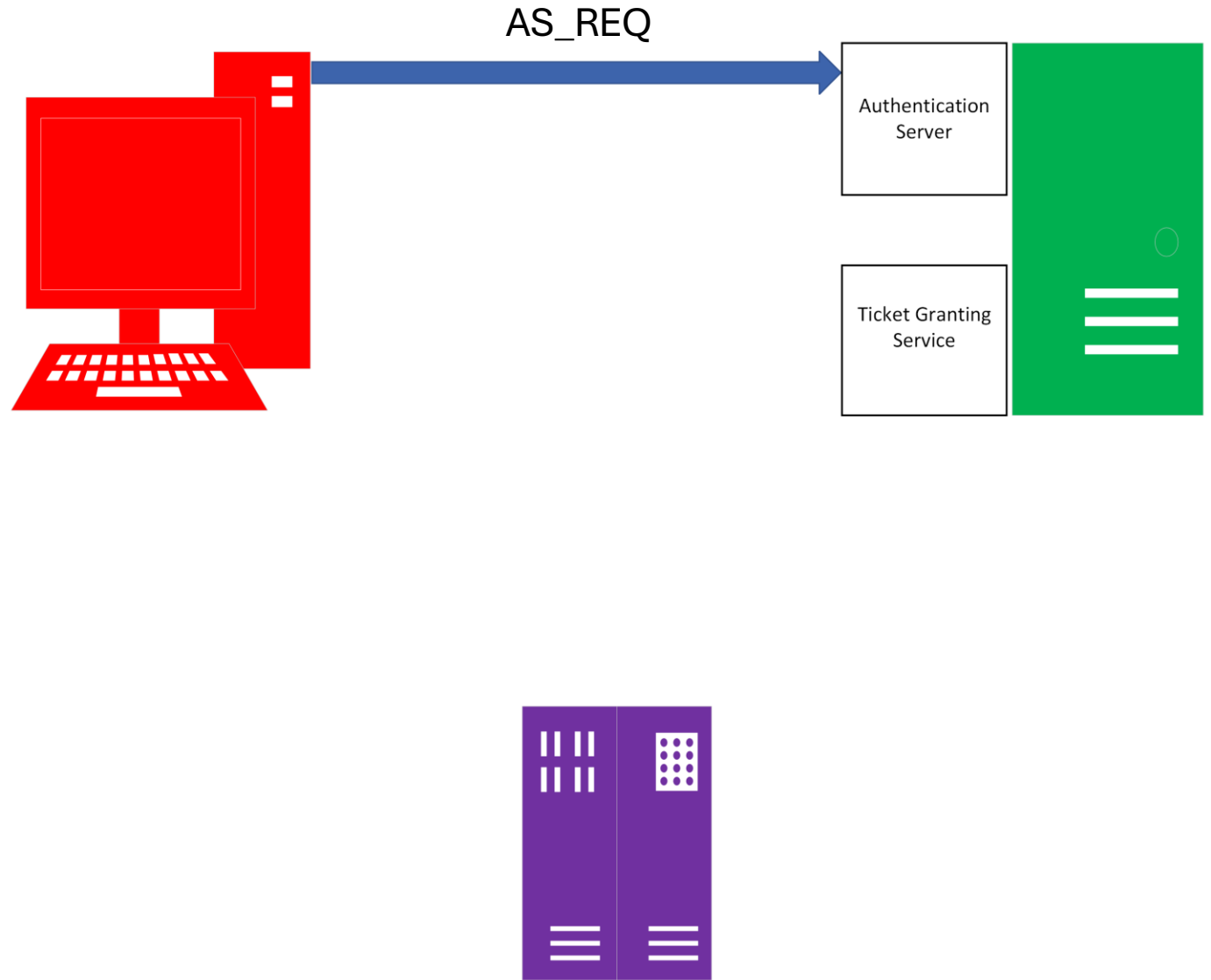
KDC

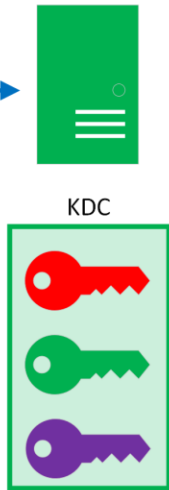
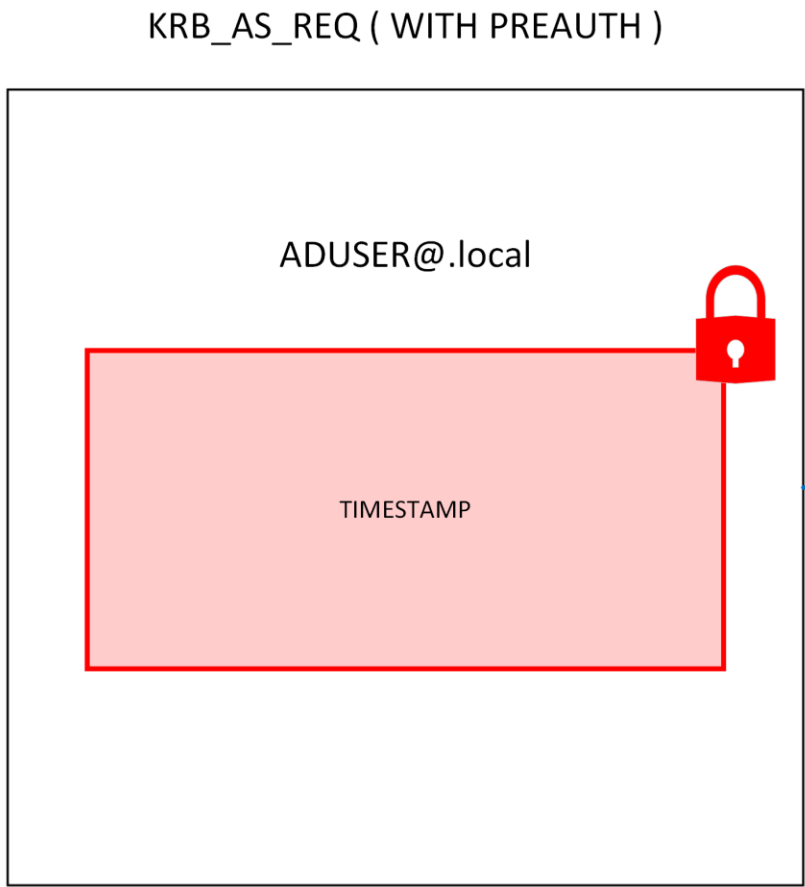
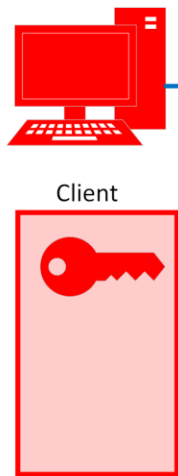


Service

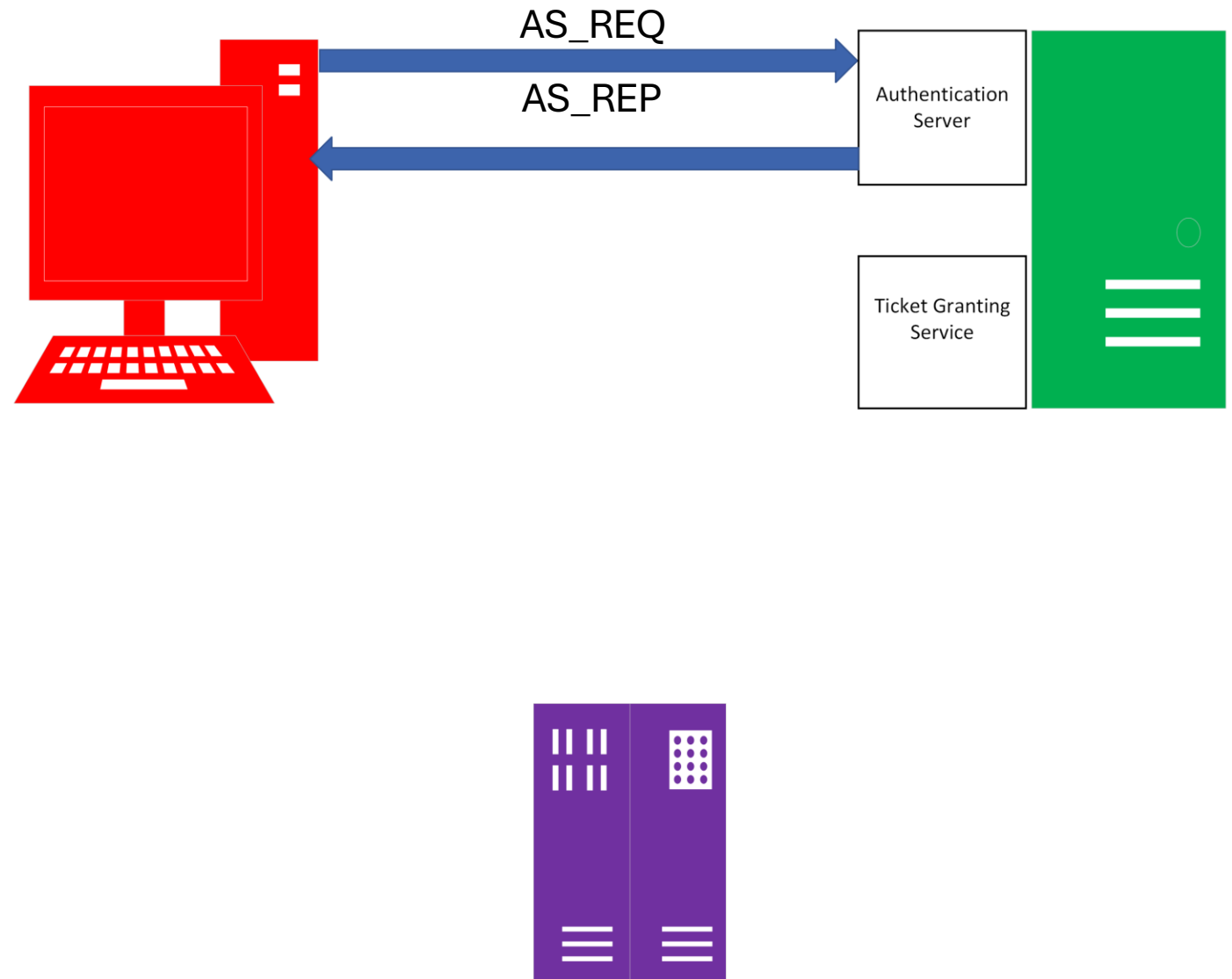


# AS Exchange 1

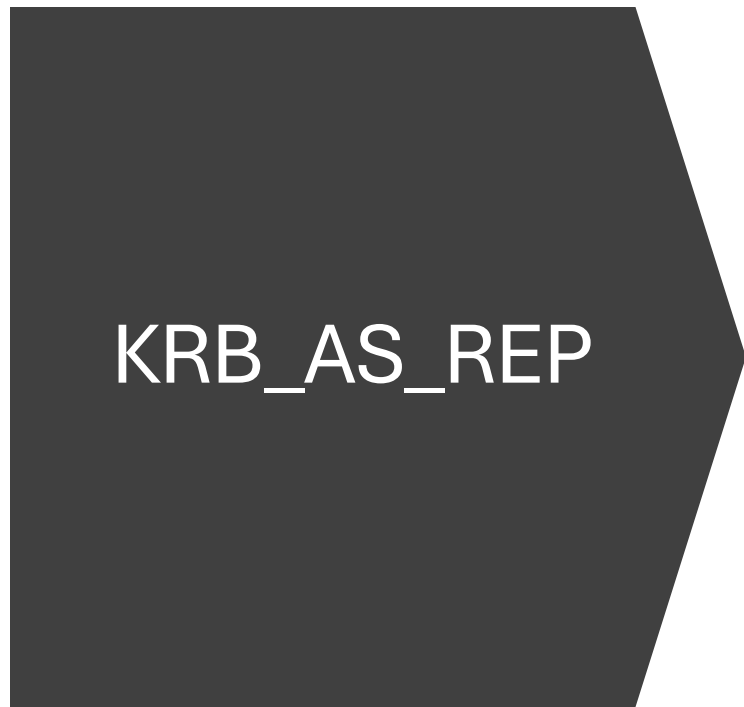




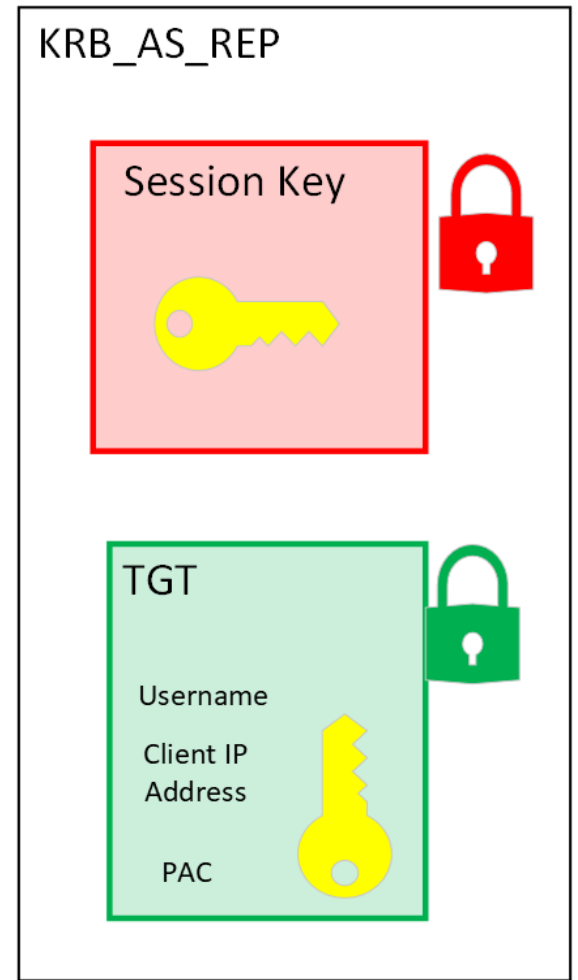
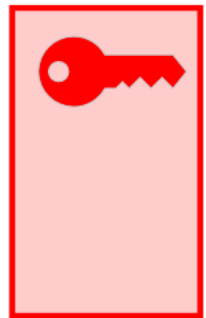
# AS Exchange 2



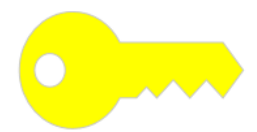




Key Database



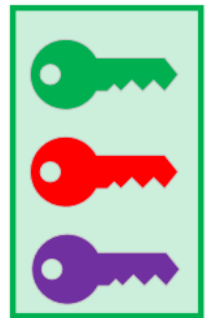
Session Key



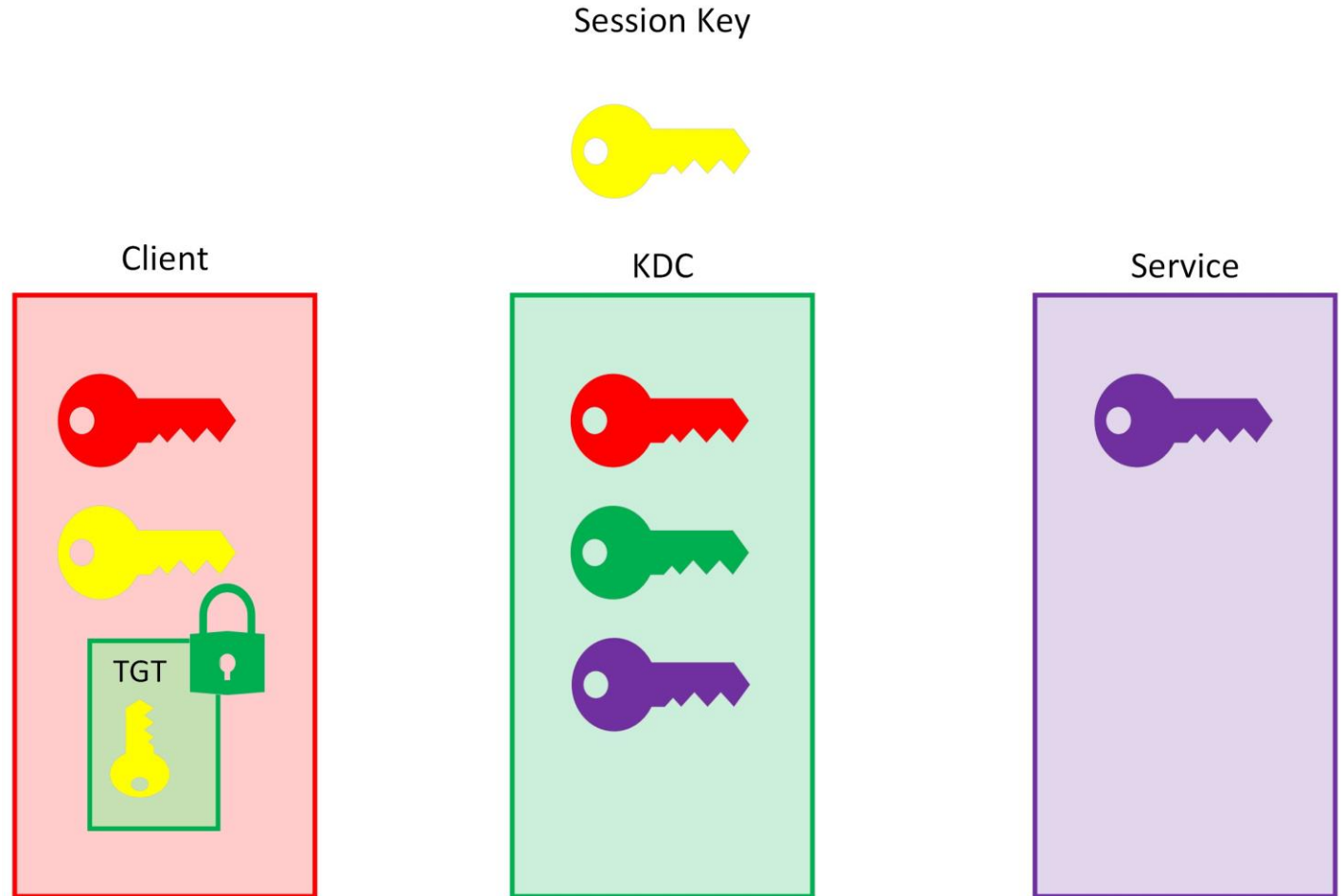
KDC



Key Database



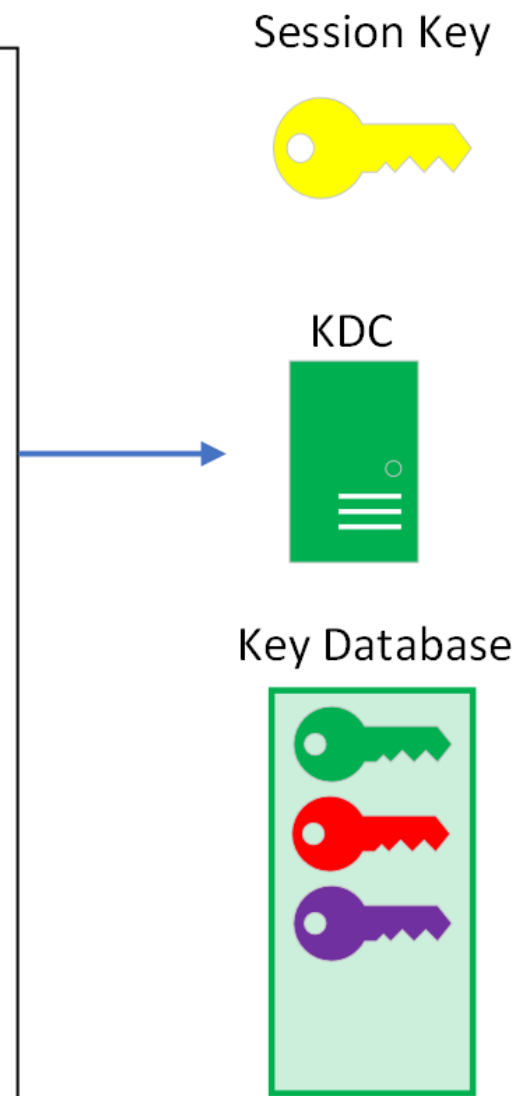
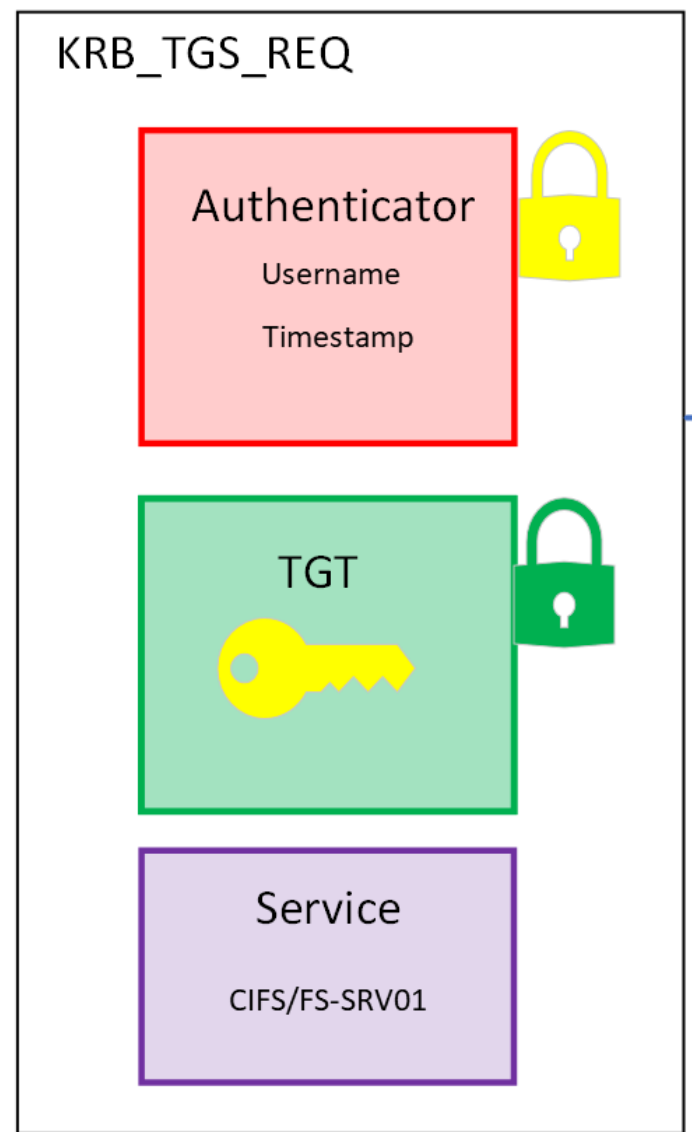
# Keys After Authentication Service Exchange



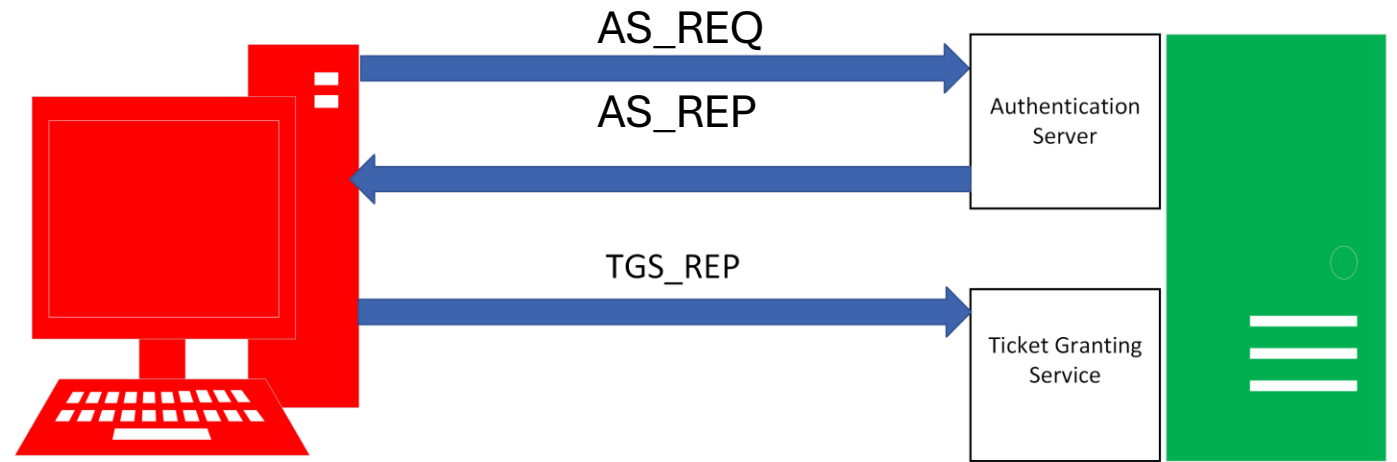
# The Authentication Server drops out

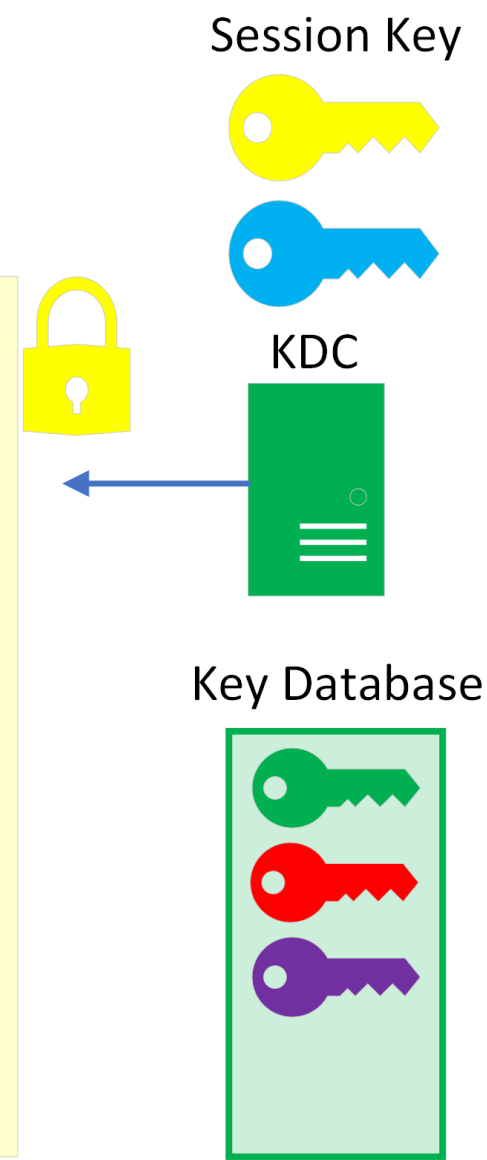
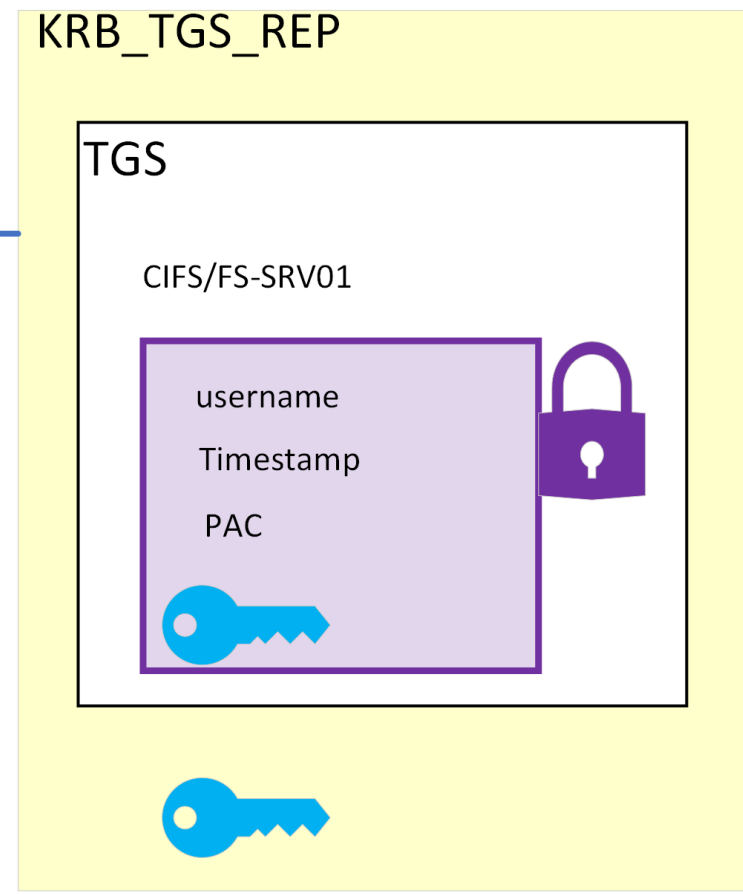
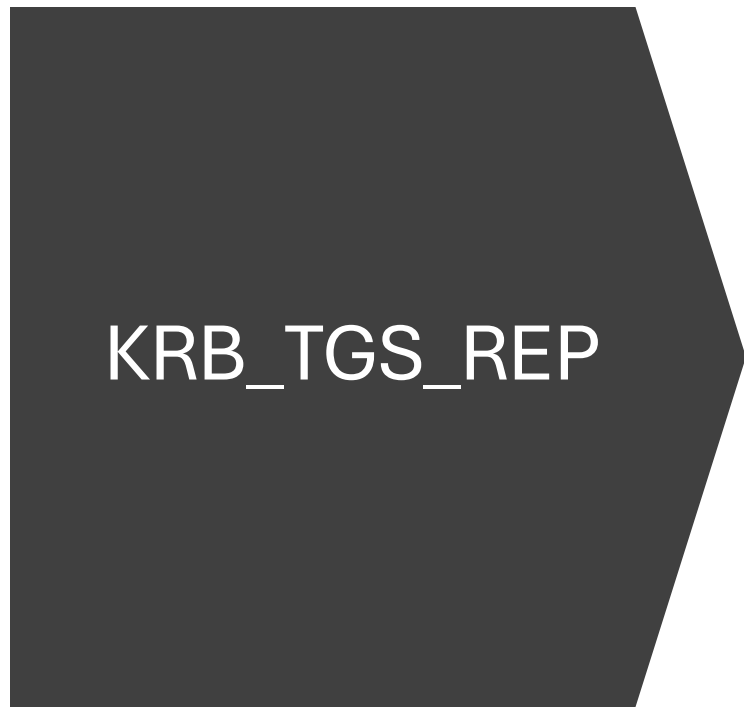
- Client has been authenticated as a user in the domain.
- Client can now begin its request for services.
- TGT will be recycled until it expires.

KRB\_TGS\_REQ

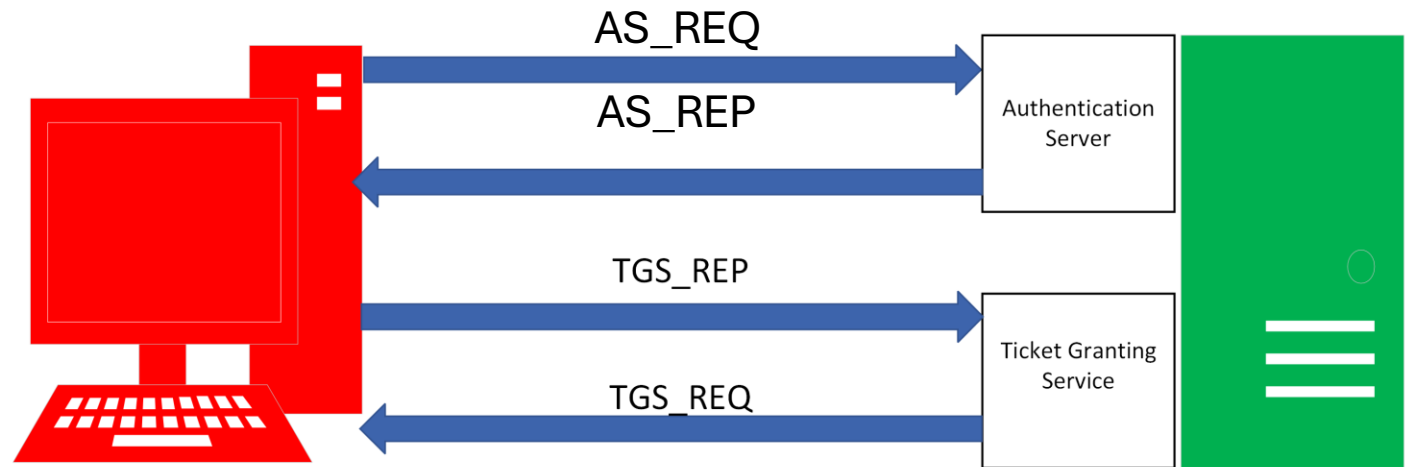


# TGS Exchange 1

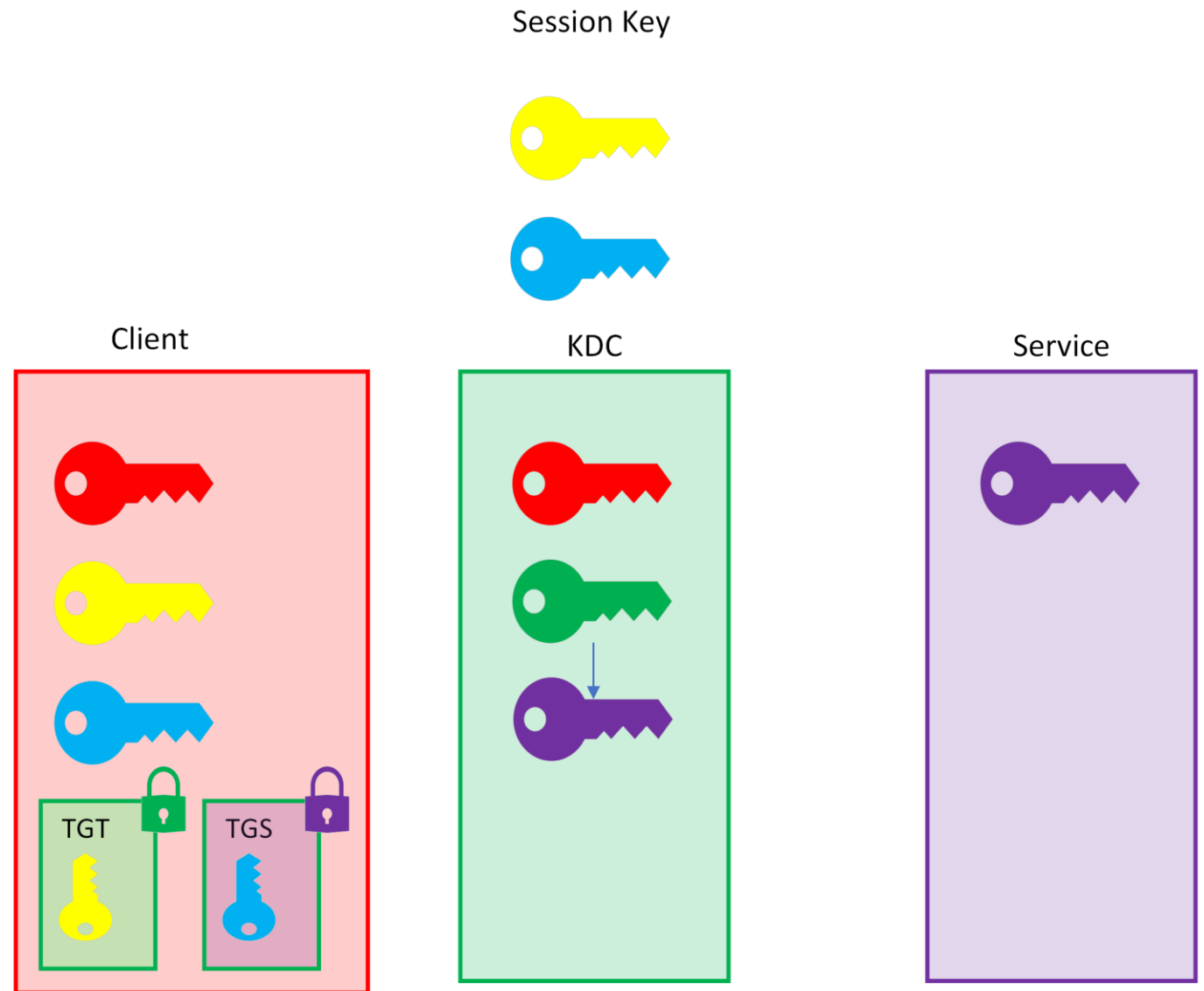




## TGS Exchange 2

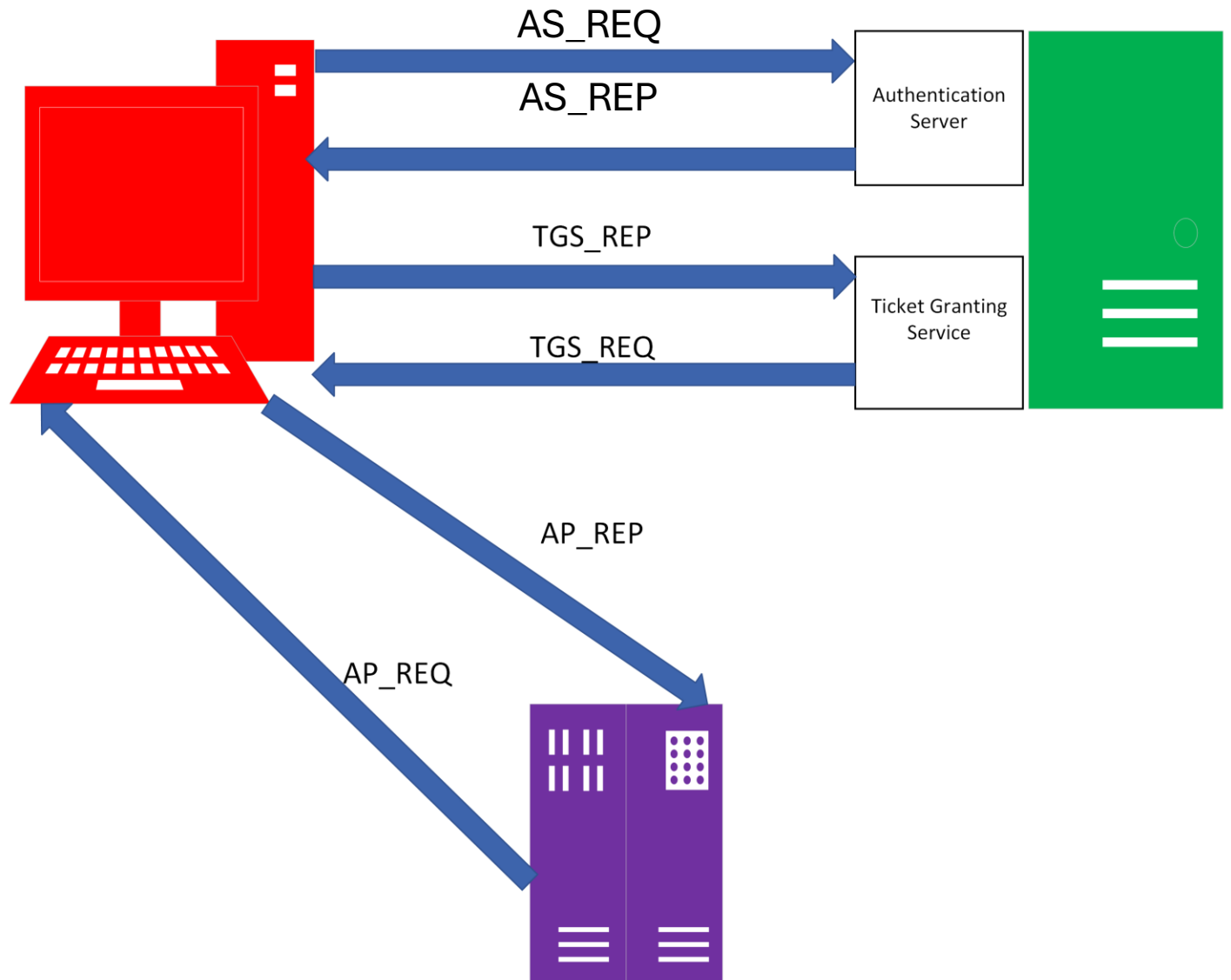


# Keys After TGS Exchange

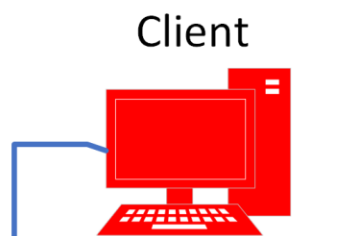




# AP Exchange 1

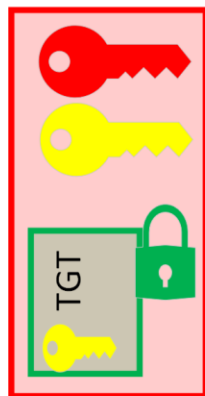


KRB\_AP\_REQ



Client

Key Database



KRB\_AP\_REQ

TGS

CIFS/FS-SRV01

username  
Timestamp  
PAC



Authenticator

username  
timestamp



FS-SRV01 Key Database



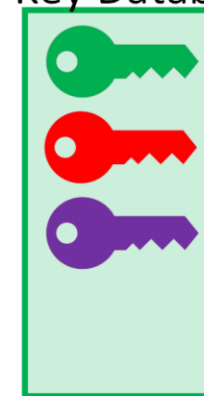
Session Key



KDC



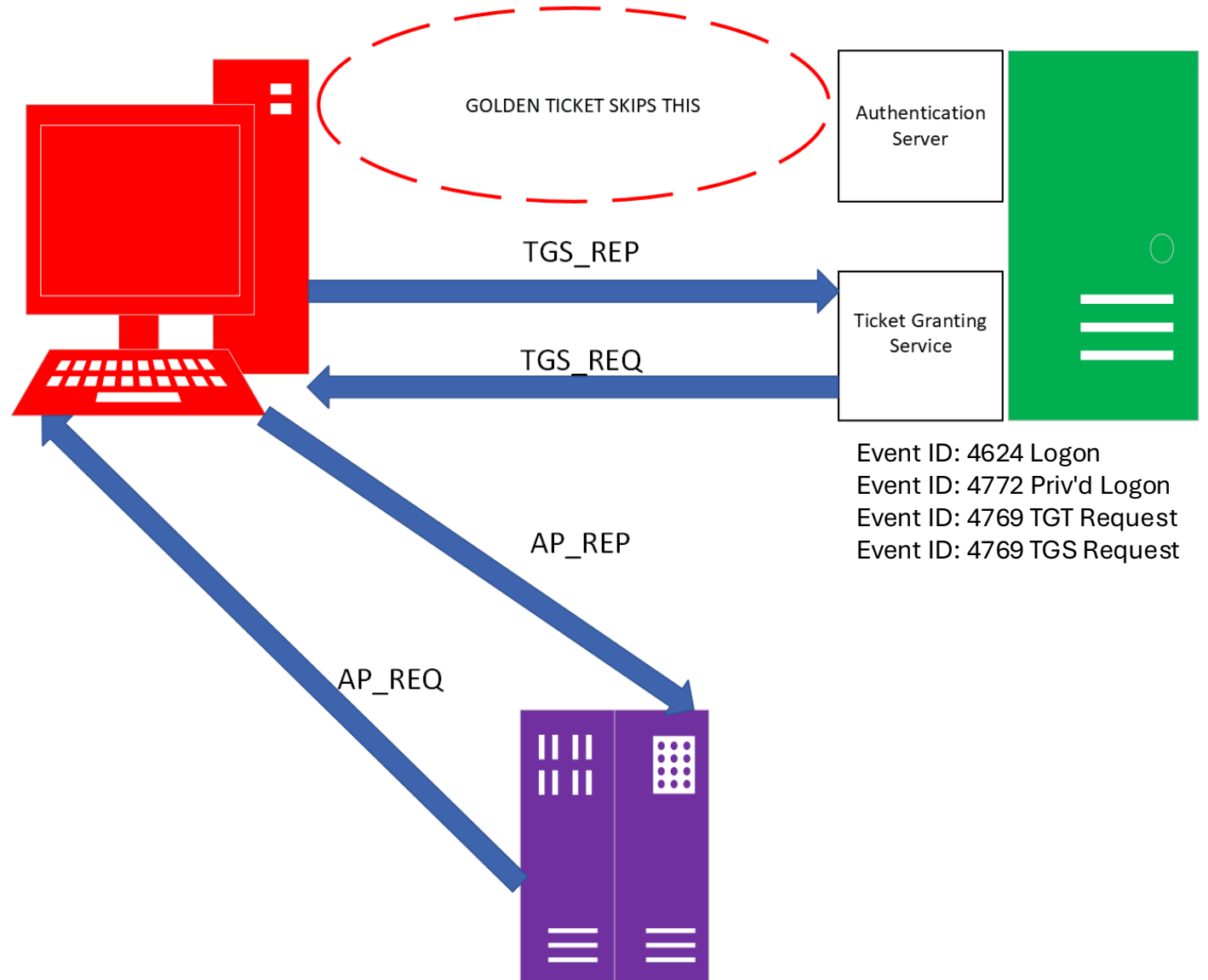
Key Database



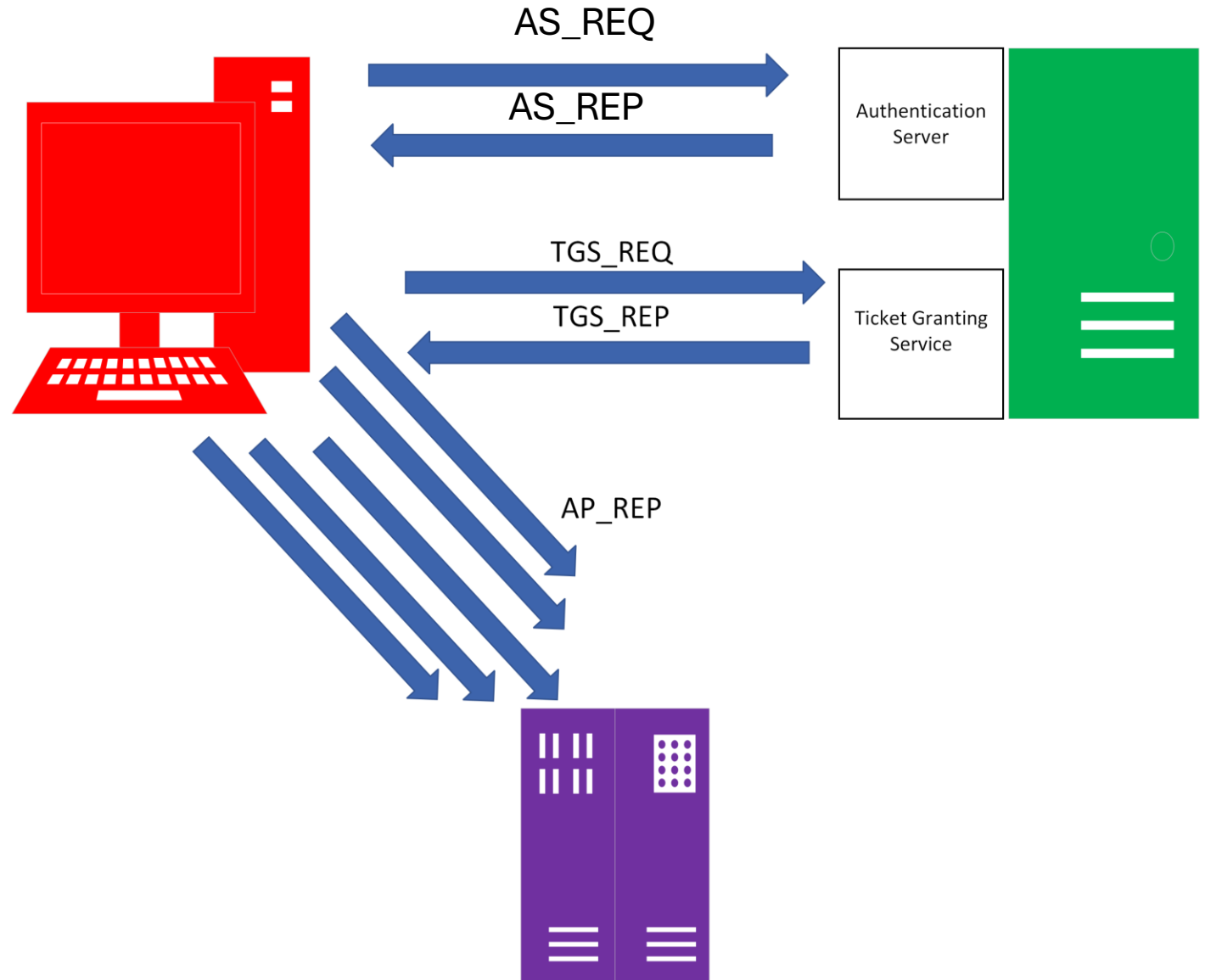
# Some famous Kerberos attacks

- AS-REP Roasting (PrivEsc)
- AS-REQ Spamming / Bruteforce (Enumeration/PrivEsc)
- Kerberoasting (PrivEsc) <===
- Golden Ticket (Persistence) <===
- Silver Ticket (Persistence) <===
- Delegation Attacks (PrivEsc)

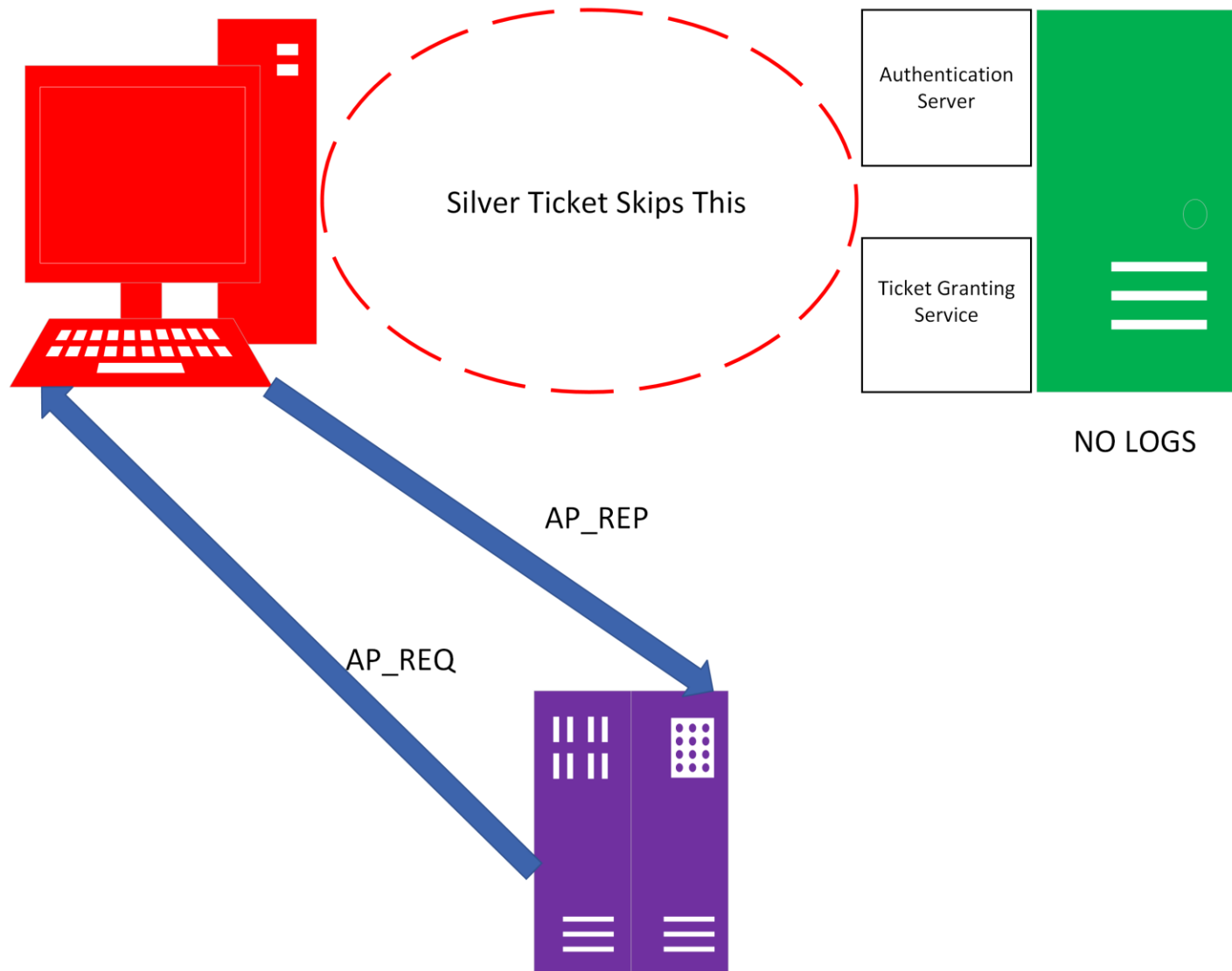
# Golden Ticket



# Kerberoasting

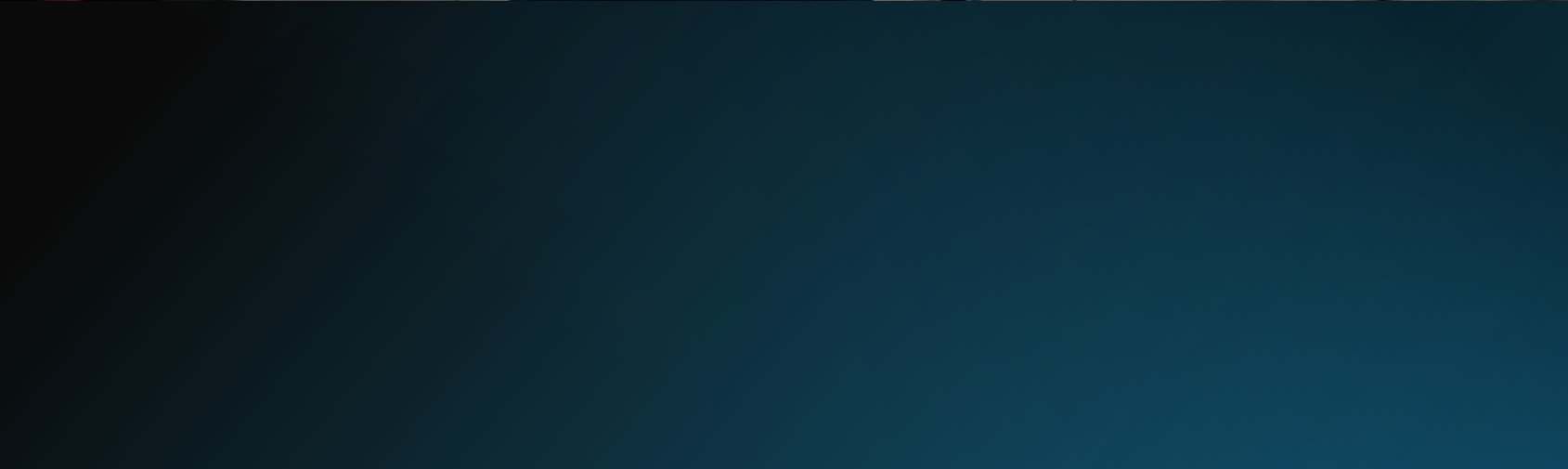


# Silver Ticket



# Writing Detections







# BrokeBoyz Cyber Kit™



- We may not have the resources to create static IOC's
- Let's make some Behavior detections

# BrokeBoyz Cyber Kit™: Catching Golden Tickets

Behaviors we will focus on:

- Missing Auth Flow
- LOW PRIVs making 4672



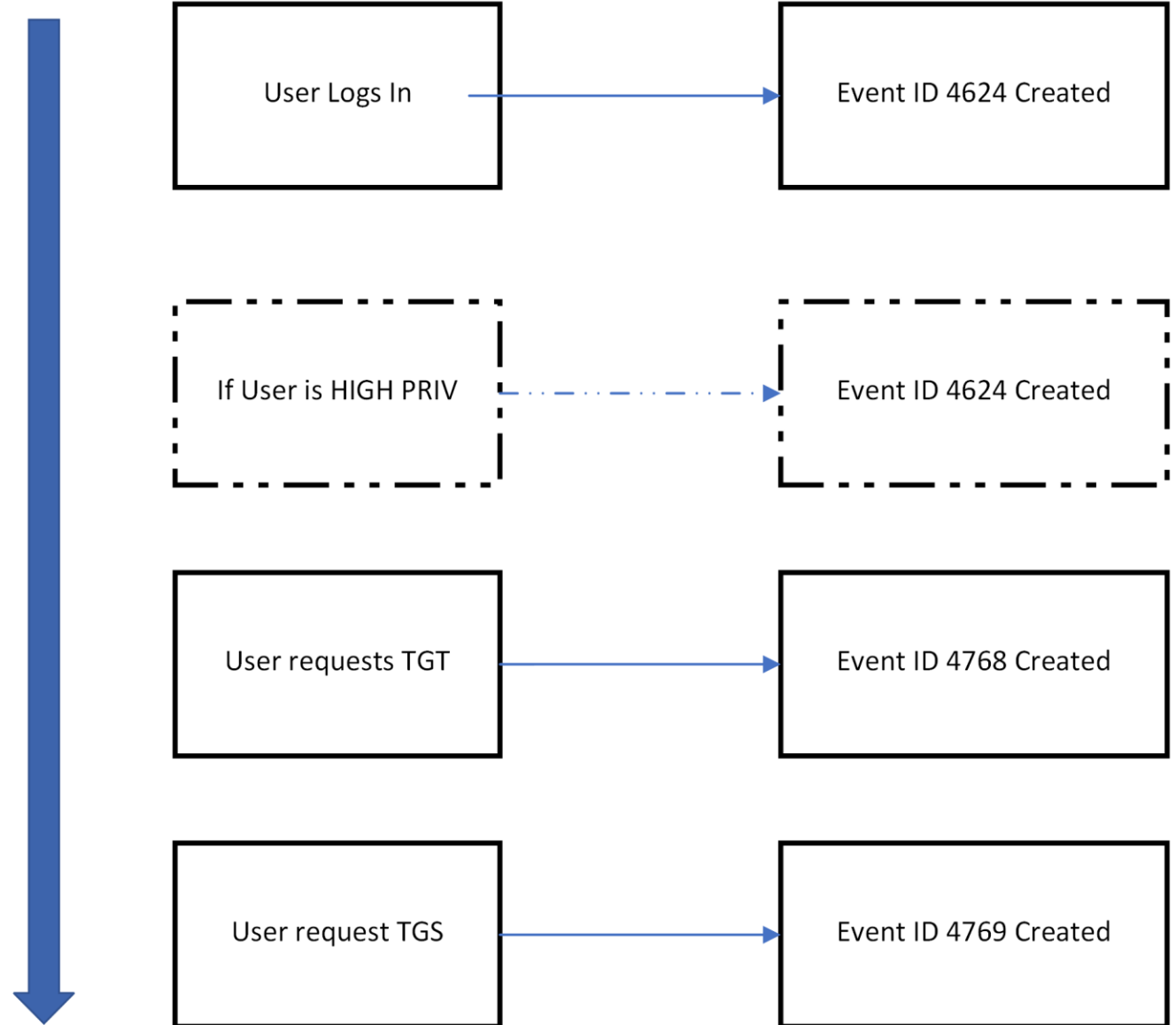
# Catching Golden Tickets: Missing Auth Flow

Event	4624 Logon
Event	4672 Special Logon (HIGH PRIV ACCOUNTS)
Event	4768 TGT request
Event	4769 TGS request

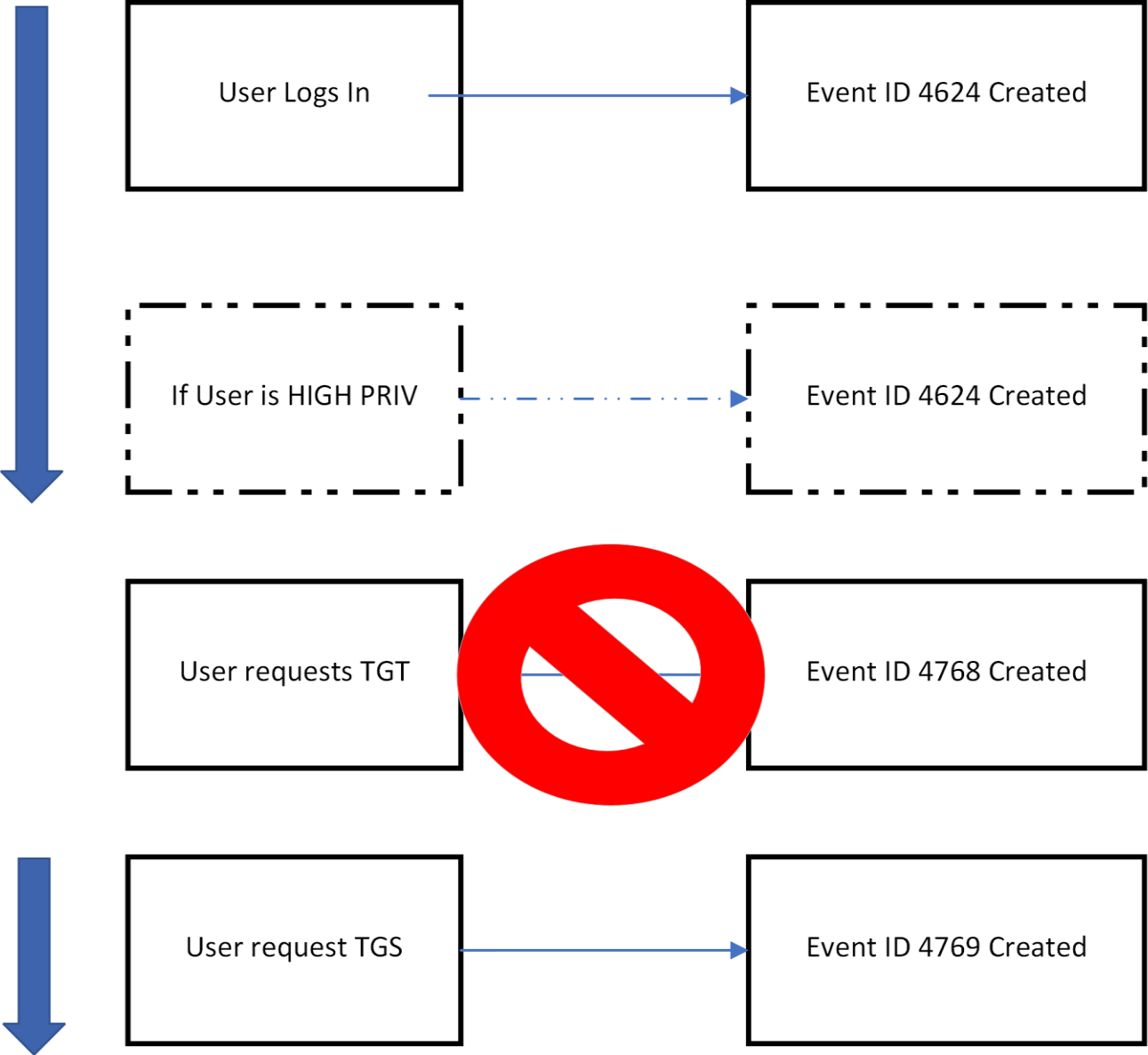
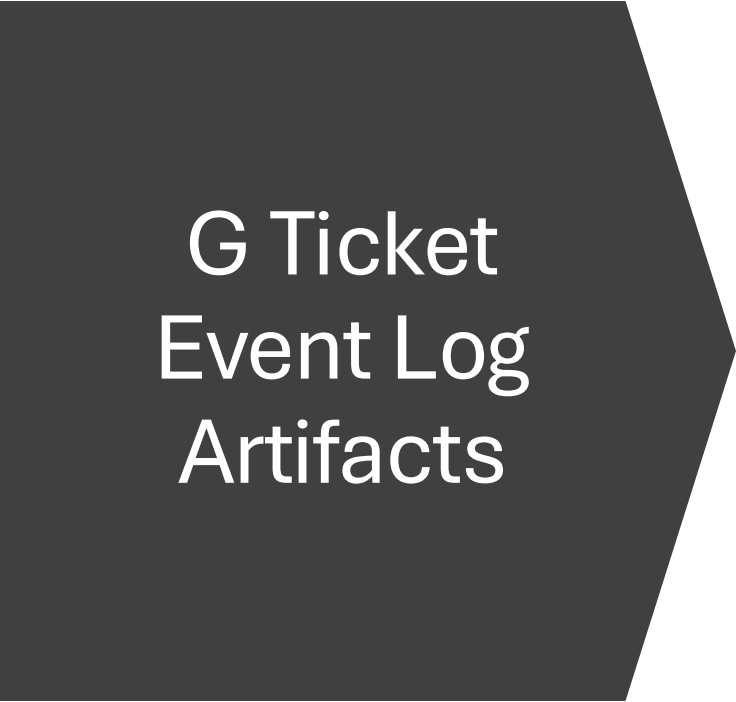


## NORMAL TRAFFIC FLOW

Normal  
Event Log  
Artifacts



GOLDEN TICKET TRAFFIC FLOW



# BrokeBoyz Cyber Kit™: Catching Kerberoasting

Behaviors we will focus on:

- Encryption downgrade ( Default AES-256 Server 2016+ )
- HIGH amounts of TGS request
- ~~Chad from Sales making TGS request to prod SQL SRVs~~



# Catching Kerberoasting : Encryption Downgrade

Event Properties - Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:

Account Name:	dadmin@CONTOSO.LOCAL
Account Domain:	CONTOSO.LOCAL
Logon GUID:	{f85c455e-c66e-205c-6b39-f6c60a7fe453}

Service Information:

Service Name:	WIN2008R2\$
Service ID:	CONTOSO\WIN2008R2\$

Network Information:

Client Address:	::ffff:10.0.0.12
Client Port:	49272

Additional Information:

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

This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested.

This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket.

Ticket options, encryption types, and failure codes are defined in RFC 4120.

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4769  
Level: Information  
User: N/A

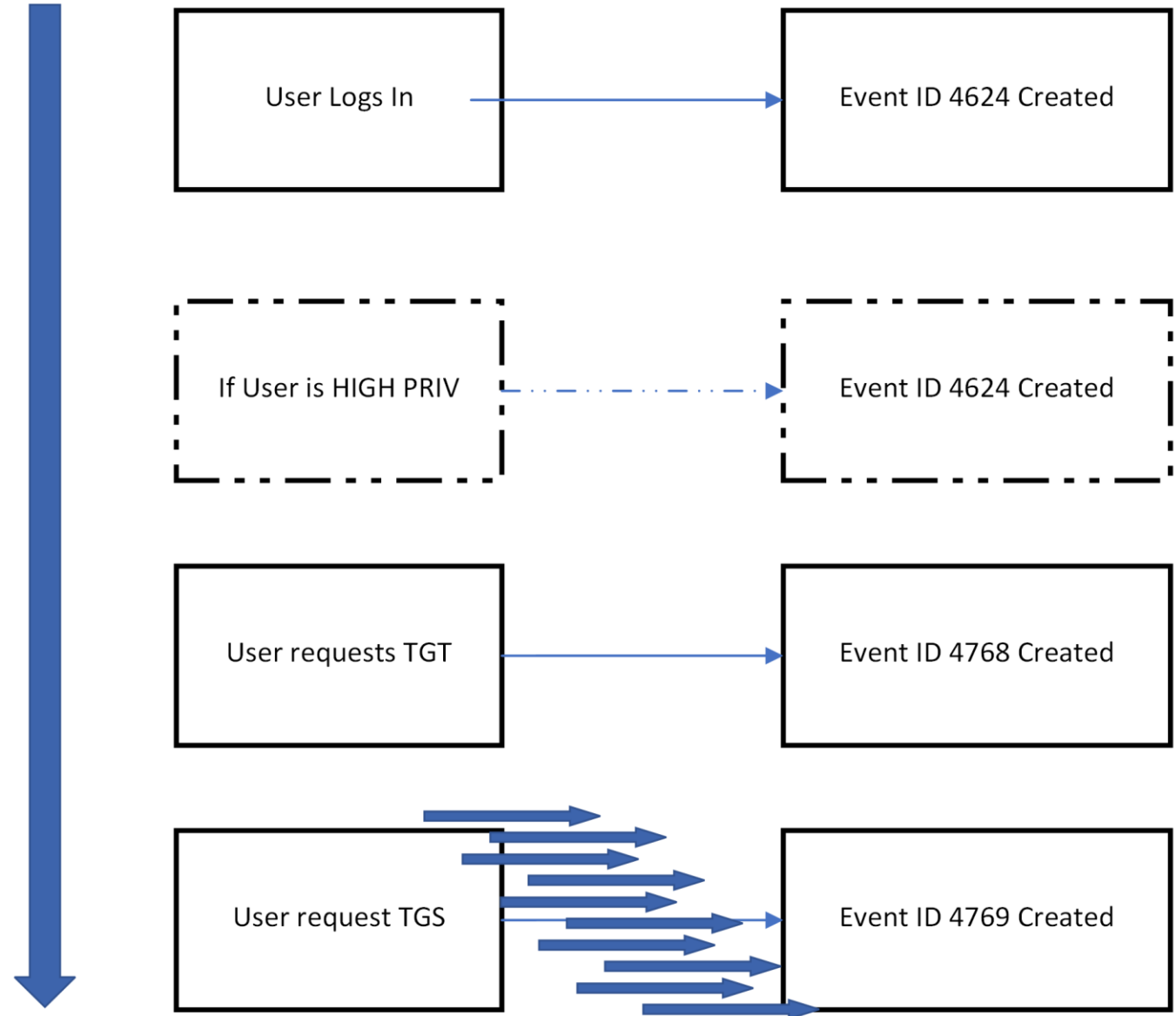
Logged: 8/7/2015 11:13:46 AM  
Task Category: Kerberos Service Ticket Operations  
Keywords: Audit Success  
Computer: DC01.contoso.local

```
<Level>0</Level>
<Task>14337</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2015-08-07T18:13:46.043256100Z" />
<EventRecordID>166746</EventRecordID>
<Correlation />
<Execution ProcessID="520" ThreadID="1496" />
<Channel>Security</Channel>
<Computer>DC01.contoso.local</Computer>
<Security />
</System>
- <EventData>
  <Data Name="TargetUserName">dadmin@CONTOSO.LOCAL</Data>
  <Data Name="TargetDomainName">CONTOSO.LOCAL</Data>
  <Data Name="ServiceName">WIN2008R2$</Data>
  <Data Name="ServiceSid">S-1-5-21-3457937927-2839227994-823803824-2102</Data>
  <Data Name="TicketOptions">0x40810000</Data>
  <Data Name="TicketEncryptionType">0x12</Data>
  <Data Name="IpAddress">::ffff:10.0.0.12</Data>
  <Data Name="IpPort">49272</Data>
  <Data Name="Status">0x0</Data>
  <Data Name="LogonGuid">{F85C455E-C66E-205C-6B39-F6C60A7FE453}</Data>
  <Data Name="TransmittedServices">-</Data>
</EventData>
</Event>
```



## KERBEROASTING TRAFFIC FLOW

Catching  
Kerberoasting:  
High TGS  
Request





# Big thanks to

---

Johannes Pangrestu: [Johannes Pangrestu, MBA | LinkedIn](#)

Daniel Jimenez: [Daniel López Jiménez | LinkedIn](#)