Active Directory Attacks and Detection Part -III

#Whoami

- Working as an Information Security Executive
- Blog : www.akijosberryblog.wordpress.com
- You can follow me on Twitter: @AkiJos

Key Takeaways

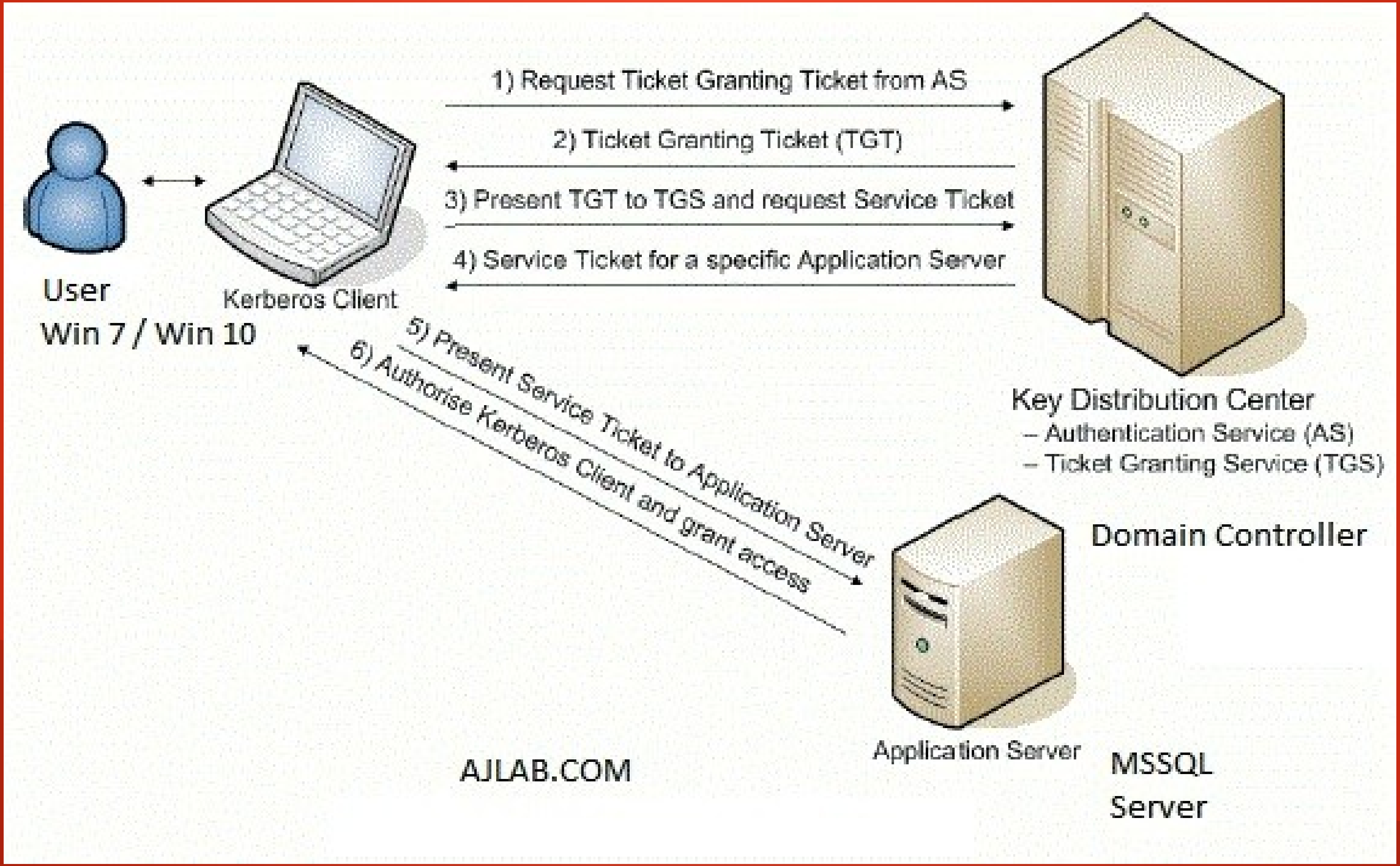
- Abusing S4U2 service
- Creating Golden Tickets & Silver Tickets
- Loading arbitrary DLL on DNS server

Lab Setup

AJLAB.COM:

- 2 Domain Controller – Win 2008 & Win 2012 r2
- 1 MSSQL Server – Running on Win2012 r2
- 1 Windows 2012 r2 Server
- Win7,Win10 – Workstation Machines
- PFSense used as gateway(Just in Case Internet is required)

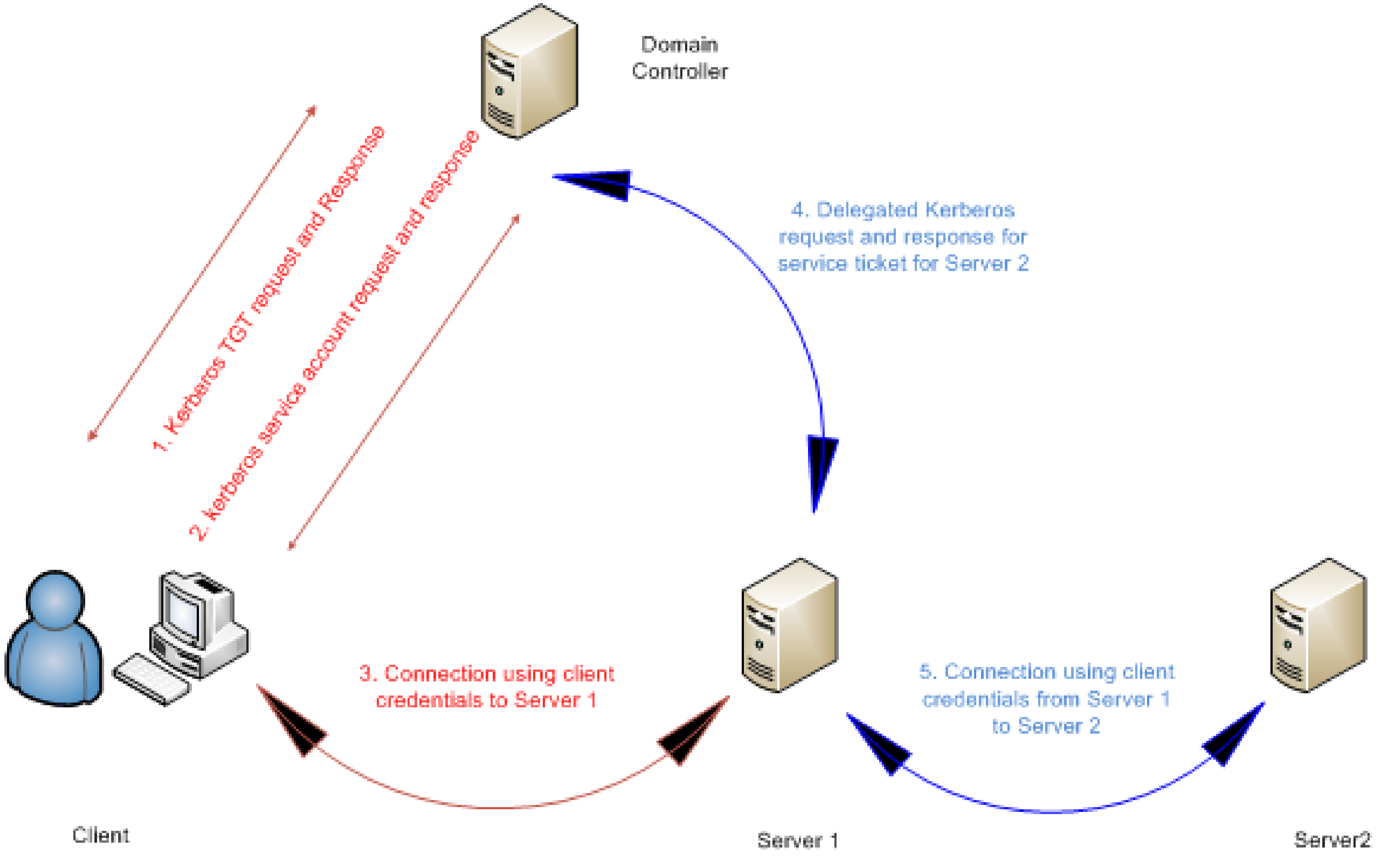
Kerberos Ticket Process Overview


1) Request Ticket Granting Ticket from AS
2) Ticket Granting Ticket (TGT)
3) Present TGT to TGS and request Service Ticket
4) Service Ticket for a specific Application Server
User
Win 7 / Win 10
Kerberos Client
5) Present Service Ticket to Application Server
6) Authorise Kerberos Client and grant access
Key Distribution Center
– Authentication Service (AS)
– Ticket Granting Service (TGS)
Domain Controller
Application Server
MSSQL
Server
AJLAB.COM

S4U2 Pwnage

I just want to talk to ServerC.
ServerA
I can take a message to ServerC.
ServerB
Server who?
ServerC

https://msdnshared.blob.core.windows.net/media/2016/08/image828.png



Domain Controller

1. Kerberos TGT request and Response

2. kerberos service account request and response

4. Delegated Kerberos request and response for service ticket for Server 2

3. Connection using client credentials to Server 1

5. Connection using client credentials from Server 1 to Server 2

Client

Server 1

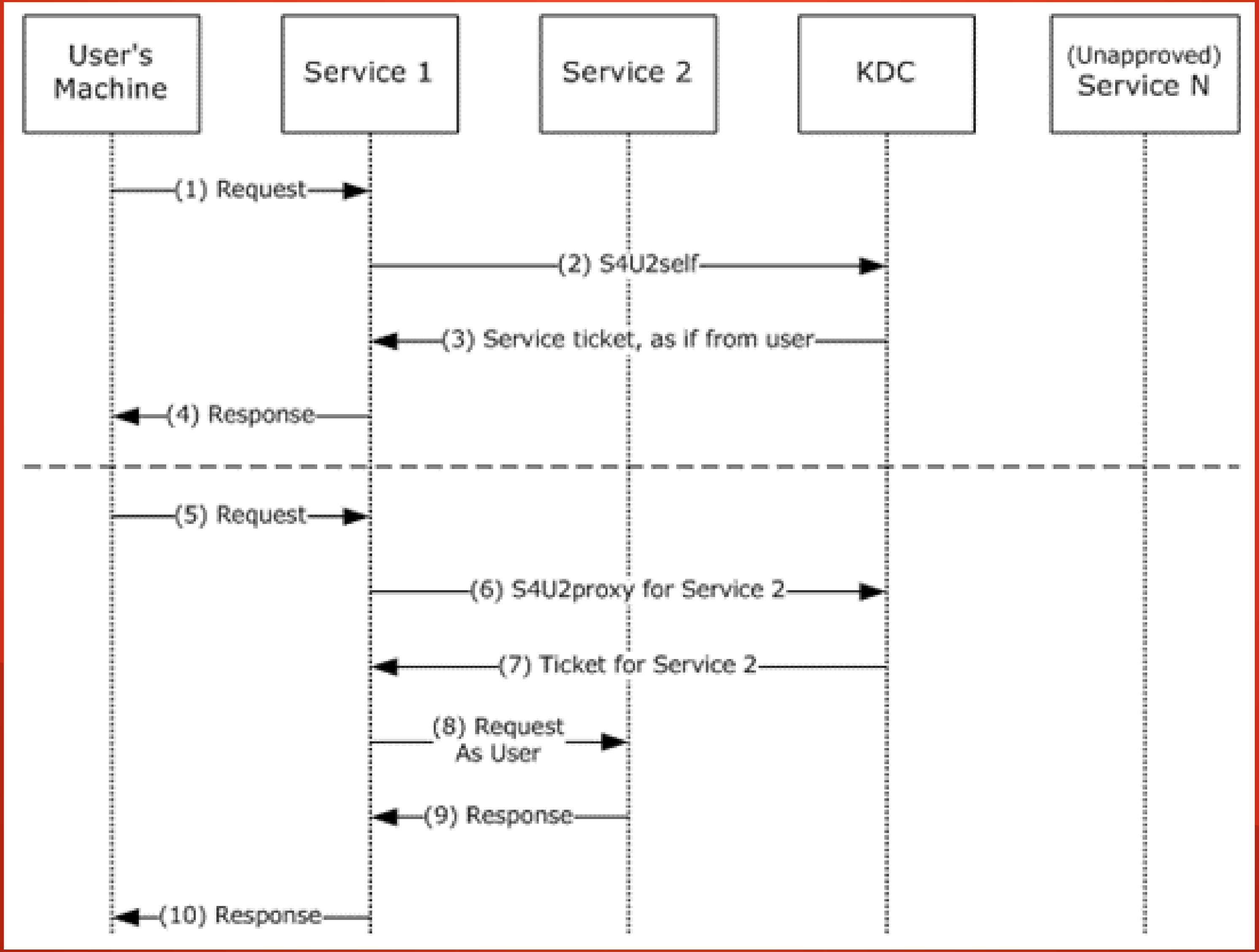
Server2

Kerberos Double Hop

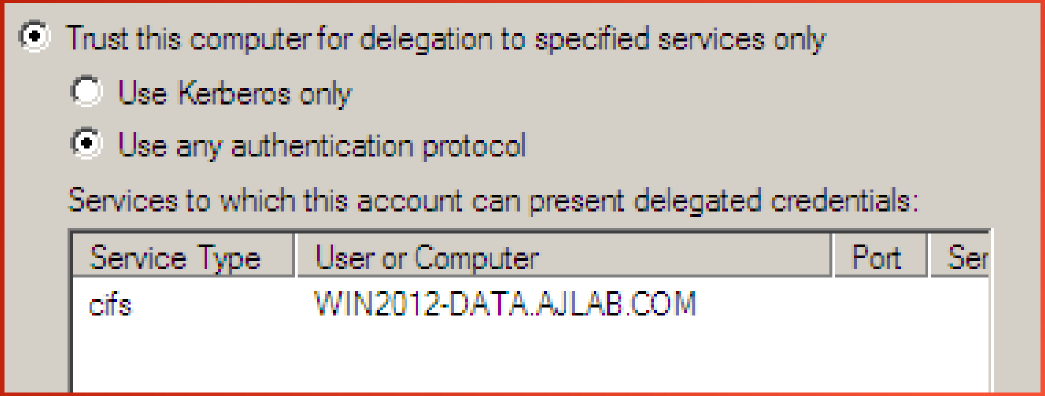
- Constrained Delegation is a way to limit what services a particular machine/account can access while impersonating other users.
- S4U2Self and S4u2Proxy are protocol extensions for Kerberos which will enable protocol transitions.
- S4U2Self extension is intended to be used when the user authenticates to the service in some way other than kerberos.

- S4U2Self extension allows a service to obtain a service ticket to itself on behalf of a user and it can be either obtained by using PA-FOR-USER (contains user data and user realm) or PA_S4U_ X509_USER (Contains the Users Certificate).
- S4U2Proxy extension provides a service that obtains a service ticket to another service on behalf of a user.
- S4U2Proxy requires the service ticket to the first service has the Forwardable flag set, This ticket can be obtained through S4U2Self protocol exchange.

S4U2self and S4U2proxy



https://msdn.microsoft.com/en-us/library/cc246080.aspx



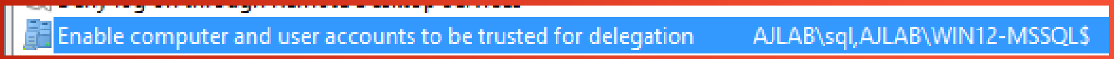
● Trust this computer for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Ser
cifs	WIN2012-DATA.AJLAB.COM		



Enable computer and user accounts to be trusted for delegation   AJLAB\sql,AJLAB\WIN12-MSSQL$

- Computer account configured with constrained delegation.
- Along with this User Right Assignment setting “Enable computer and user accounts to be trusted for delegation” also needs to be configured.

S4U2 Pwnage

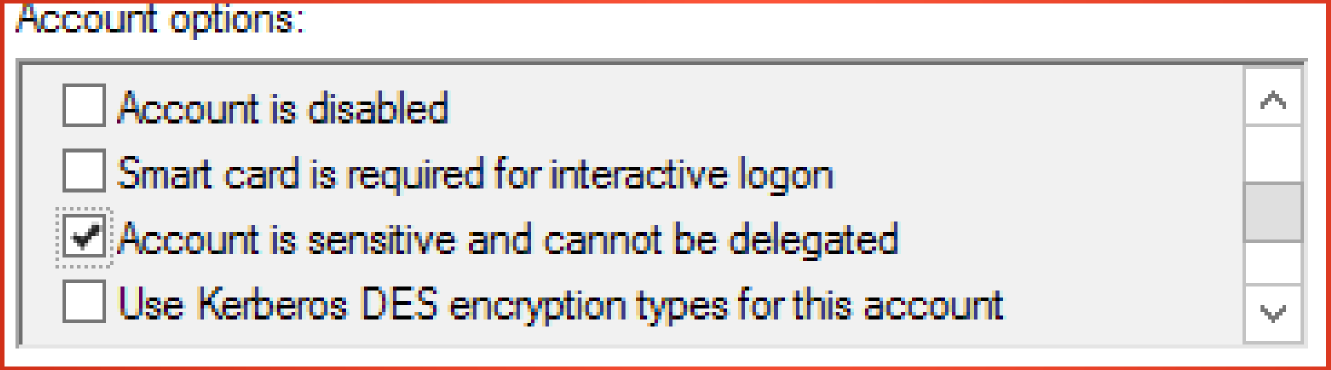
- We will first find the machines which has msDS-AllowedToDelegateTo and TrustedToAuthForDelegation(T2A4D):
- import-module activedirectory
- get-ADComputer -Filter {(TrustedToAuthForDelegation -eq $True) -AND (PrimaryGroupID -eq 515)} -Properties TrustedToAuthForDelegation,ServicePrincipalName,msDS-AllowedToDelegateTo
- We will be using computer account for authentication and Kekeo tool will be used for abusing S4U.

Demo Time

S4U2 Pwnage

Blue Team Response

- Use Kerberos Constrained Delegation.
- Limit the exposure of services configured for delegation.
- Configure the user account to “Account is Sensitive and cannot be Delegated”.



Account options:

- □ Account is disabled
- □ Smart card is required for interactive logon
- ☑ Account is sensitive and cannot be delegated
- □ Use Kerberos DES encryption types for this account

- The “protected users” group available starting windows 2012 R2 domain function level also mitigates against this issue, since delegation is not allowed for accounts in this group.

* Protected Users group applies to windows 8.1 and 2012 R2 server

Golden Ticket

WONKA

GOLDEN TICKET

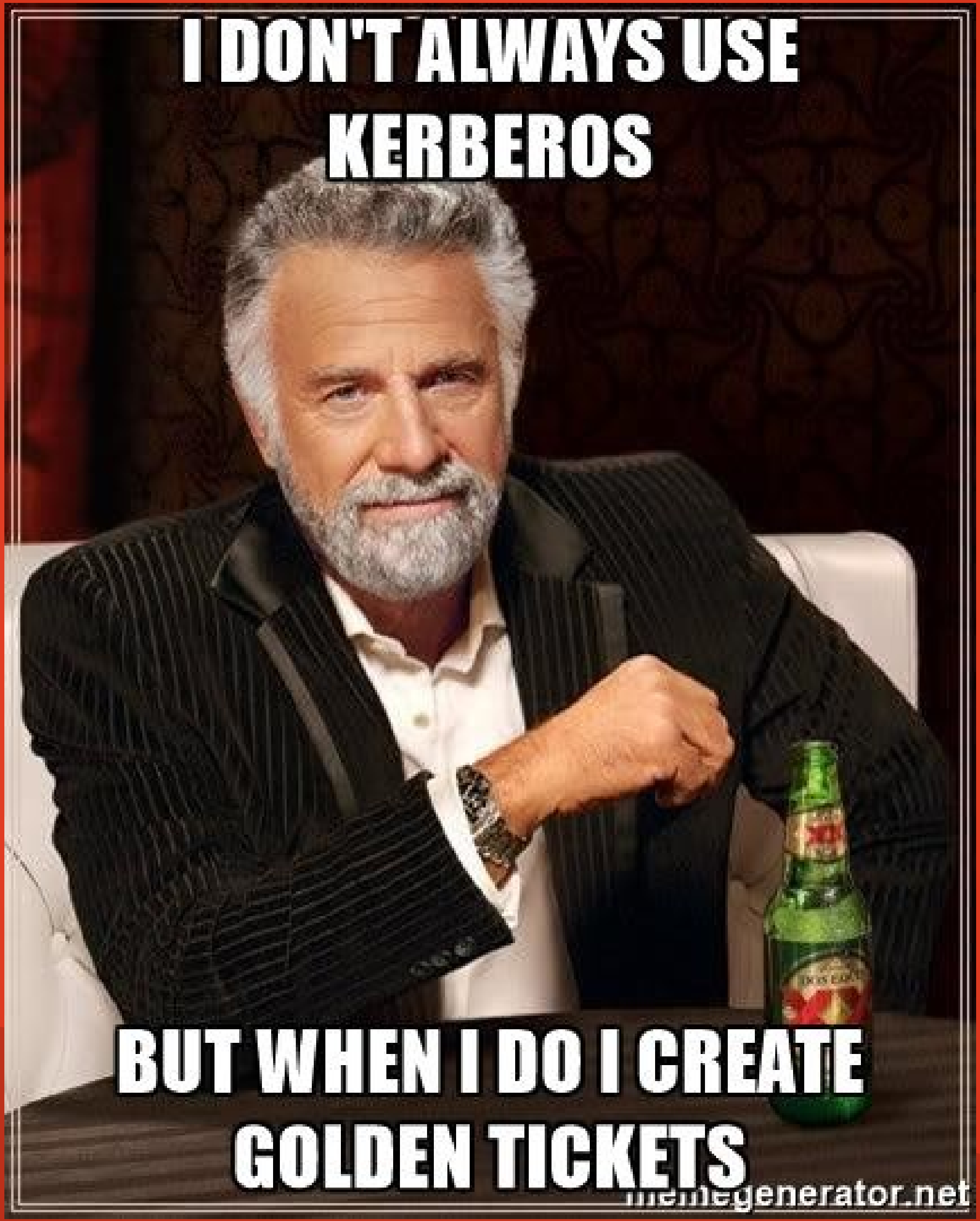
DATE	TIME	PLACE
FEB. 1	10 A.M. (SHARP)	FRONT GATES

THIS GOLDEN TICKET ENSURES ADMITTANCE.

- Golden Ticket is forged Ticket Granting Ticket (TGT).
- The KRBTGT account is used to encrypt and sign all kerberos ticket within the domain.
- KRBTGT account password hash can be extracted using DCSYNC or from the NTDS.DIT file (or any other ways).
- Golden ticket can be used to impersonate any user in the domain.
- The best part of golden ticket is you can create an golden TGT ticket for a user which does not even exist in the domain.
- By default the Golden ticket lifetime using mimikatz module is 10 years (It can be customized using /startoffset, /endin, /renewmax).

https://makeameme.org

- The Microsoft Kerberos validates a TGT’s PAC only after the ticket is 20 minutes old.
- Some of the Key Things to Remember:
  - Maximum LifeTime of Service Ticket (TGS): Default is **600 minutes**
  - Maximum LifeTime of User Ticket(TGT): Default is **10 Hours**
  - Maximum LifeTime of User Ticket Renewal (TGT Renewal): Default is **7 Days**
  - Well known RID’s :
  - **513**- Domain User, **512** - Domain Admin, **518** - Schema Admin, **519** - Enterprise Admin, **520** - Group Policy Creator Owner, **502** - KRBTGT Account


I DON'T ALWAYS USE KERBEROS
BUT WHEN I DO I CREATE GOLDEN TICKETS
memegenerator.net

https://memegenerator.net/

Demo Time

Golden Ticket

Blue Team Response

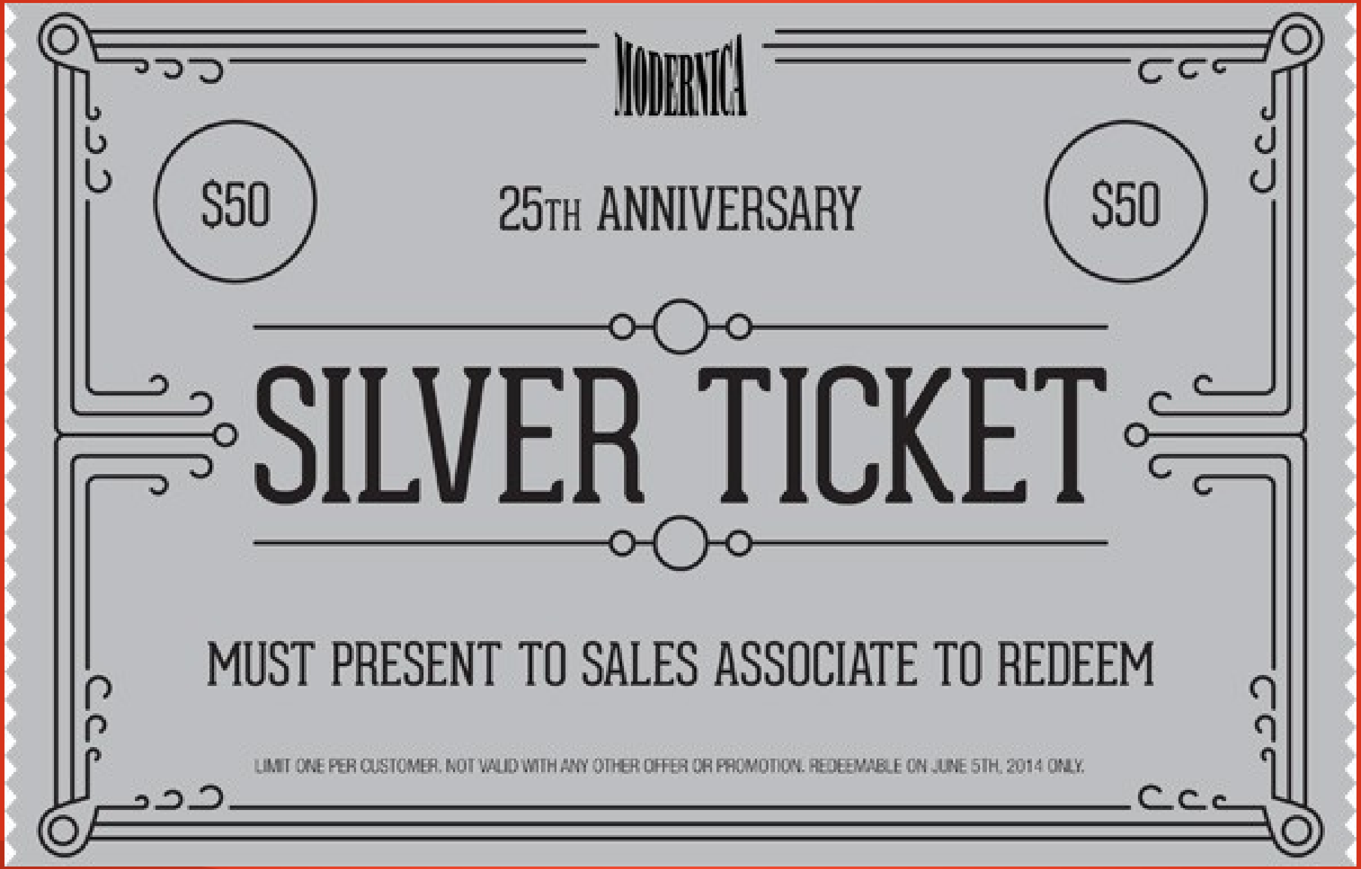
- Consider chaning KRBTGT account password (2x) once a year.

Detection:

- Microsoft Advanced Threat Analytics(ATA)
- Javelin Networks AD Protect/Assessment

- In your recent engangement, you’ve dumped the NTDS.DIT file on Friday evening and on monday morning to your surprise you find the hashes are no more working :(
- The Corporate AD Team had changed user, admin and service account passwords.

So WHAT NEXT ?????



MODERNICA

$50

25TH ANNIVERSARY

$50

SILVER TICKET

MUST PRESENT TO SALES ASSOCIATE TO REDEEM

LIMIT ONE PER CUSTOMER. NOT VALID WITH ANY OTHER OFFER OR PROMOTION. REDEEMABLE ON JUNE 5TH, 2014 ONLY.

http://archive.blog.modernica.net/contests-treasure-hunts-factory-sale/

Silver Ticket

- Silver Ticket is Forged Ticket Granting Service (TGS) Ticket.
- A Silver Ticket is encrypted/signed by the service account (Computer Account or Service Account).
- No AS-REQ/AS-REP,TGS-REQ/TGS-REP and no traffic sent to the Domain Controller.
- We will be using the hash of computer account to generate a silver ticket and access the services running on the target machine.
- Some of the Important service Ticket types are:
  - File Share - CIFS
  - Scheduled Tasks - HOST
  - WMI - HOST,RPCSS
  - PS Remoting - HOST, HTTP,WSMAN
  - WinRM - HTTP, WSMAN

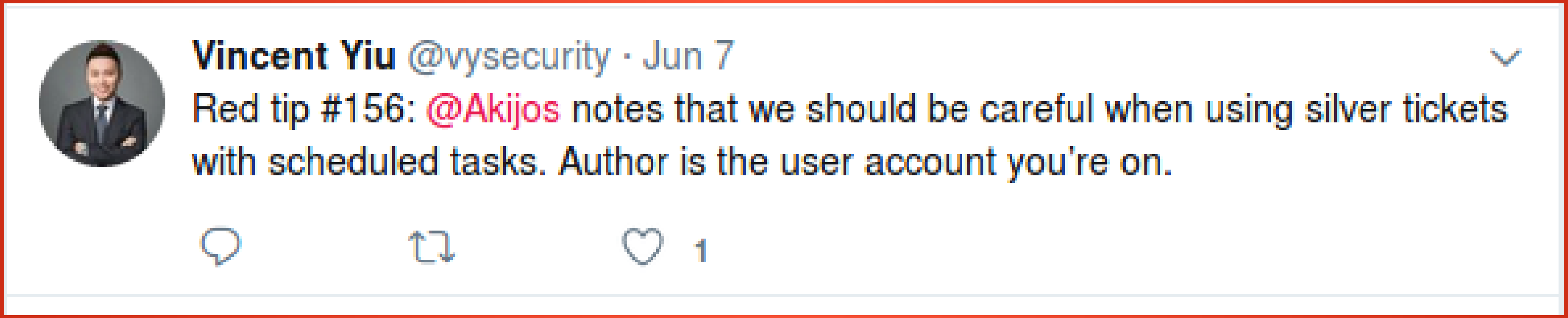
Demo Time

Silver Ticket

http://memes.com/

Blue Team Response

- If the Attacker has created a schedule task with the silver ticket, Author is the user account from which the attacker had created a silver ticket.



Vincent Yiu @vysecurity · Jun 7

Red tip #156: @Akijos notes that we should be careful when using silver tickets with scheduled tasks. Author is the user account you're on.

Blue Team Response

- Include computer account password change as a part of domain-wide password change scenario.

  Detection:

  - ~~Microsoft Advanced Threat Analytics(ATA)~~
  - ~~Javelin Networks AD Protect/Assessment~~

DNSAdmin To DC Compromise

- This was an awesome find by Shay Ber, Kudos to him.
- A Windows feature abuse where the user being a member of DNSAdmins group allowing to load arbitrary DLL.
- Domain Controller’s are by default DNS Servers and needs to be reachable across the domain.
- We will be using dnscmd.exe to load the DLL.
- To enable the dnscmd.exe command, the feature of DNS Server Tools needs to be enabled. The dnscmd command to load the dll looks like:
  - dnscmd << DNS Server Name >> /config /serverlevelplugindll << path of dll >>
- The only caveat is that the DNS service needs a restart.

Demo Time

DNSAdmin To DC Compromise

Blue Team Response

- DNS Server log EventID 550 for Failure log in loading or initialize plug- in dll.
- DNS Server log EventID 770 for Success log in loading or initialize plug- in dll.
- Monitor any changes in the Registry Hive:

  HKLM:\SYSTEM\CurrentControlSet\services\DNS\Parameters\ServerLevelPluginDll

References

- adsecurity.org
- blog.gentilkiwi.com
- blog.harmj0y.net
- labofapenetrationtester.com
- msdn.microsoft.com
- labs.mwrinfosecurity.com/blog/trust-years-to-earn-seconds-to-break/
- medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
- Google.com (everything else)

Thank You