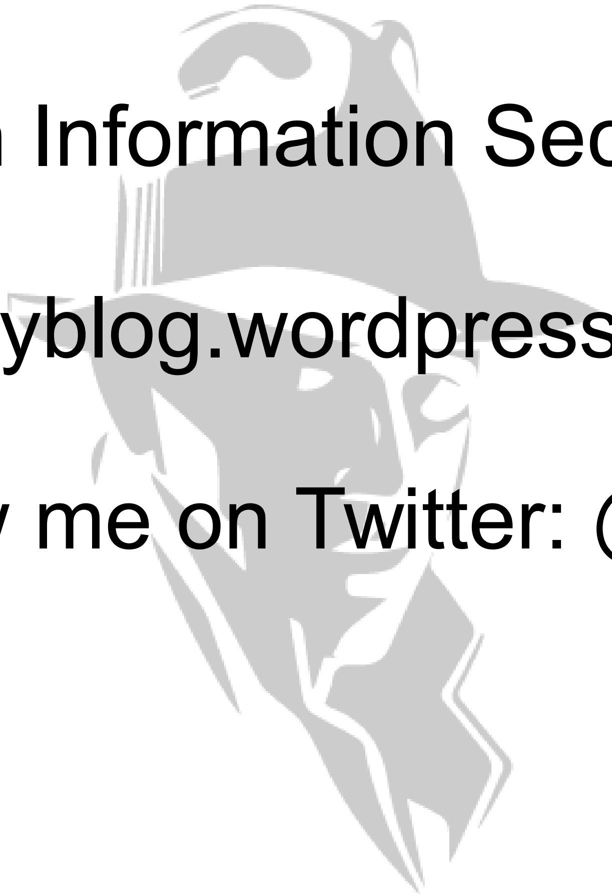
Active Directory Attacks and Detection

HAKON-2017™

Creating Information Security Culture Seriously

#Whoami



- Working as an Information Security Executive
- Blog : www.akijosberryblog.wordpress.com

- You can follow me on Twitter: @AkiJos

Lab Setup

AJLAB.COM:

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

What happens when you log into WorkStation ?

http://www.troll.me/

- Suppose a user has an account and users workstation belong to the domain(AJLAB.COM), the user logs on to the network with Ctrl+Alt+Del which is a SAS(Secure Attention Sequence).

- The workstations Winlogon service switches to logon Desktop and calls the GINA(Graphical Identification and Authentication) Dll collects the user logon information and passes that information to LSA (Local Security Authority) for authentication.

- LSA simply passes the information to SSPI (Security Support Provider Interface).

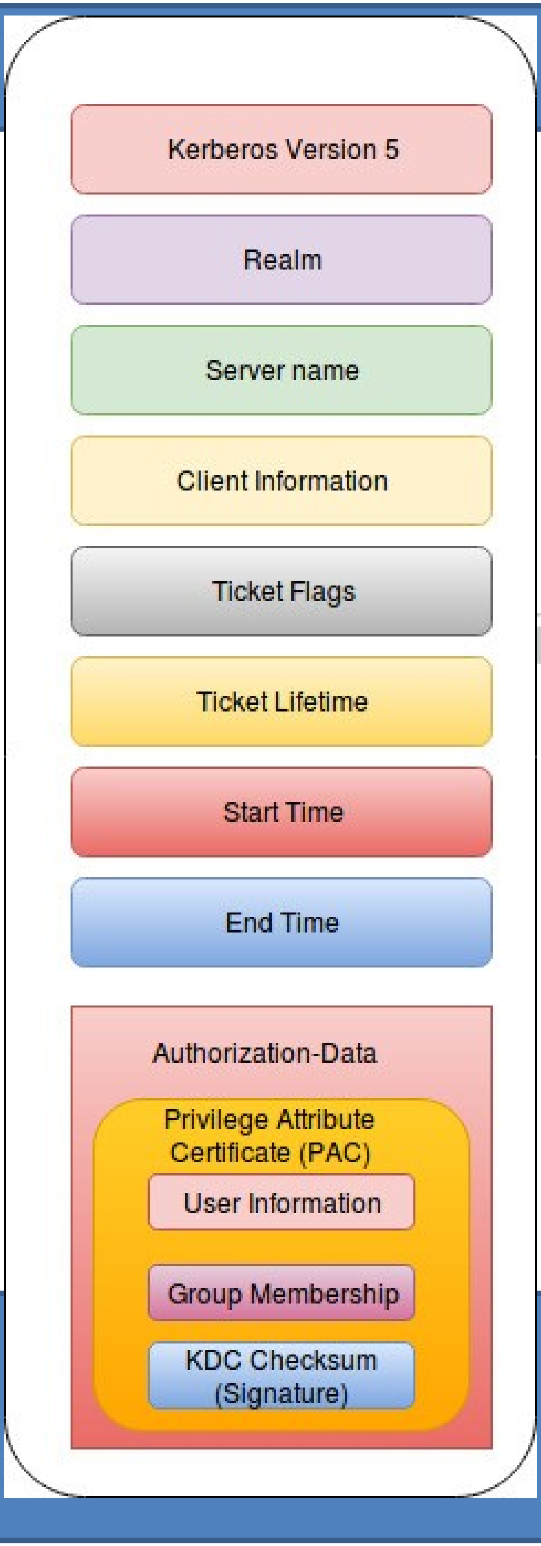
- SSPI calls the Kerberos SSP because Kerberos.dll is the first choice of windows Operating System followed by NTLM,Digest,Schannel and Negotiate.

Kerberos 101

http://3-headed-dog.blogspot.in/

- Kerberos is a bit complex authentication protocol
- Active Directory implements Kerberos version 5 in two components: **Authentication Service** (**AS**) and **Ticket-Granting service** (**TGS**).
- The Authentication Service (AS) is the first contact the client has with Kerberos and is used to lookup the user’s password and create the Ticket Granting Ticket (TGT).
- The AS also creates the session key the user will use for future communication with Kerberos.
- The Ticket Granting Ticket (TGT) is the Kerberos ticket used to obtain Service Ticket. TGT is encrypted using the KDC key and Only a KDC can decrypt and read the ticket.

Kerberos Ticket Contents



Kerberos Version 5

Realm

Server name

Client Information

Ticket Flags

Ticket Lifetime

Start Time

End Time

Authorization-Data

Privilege Attribute Certificate (PAC)

User Information

Group Membership

KDC Checksum (Signature)

https://www.draw.io/

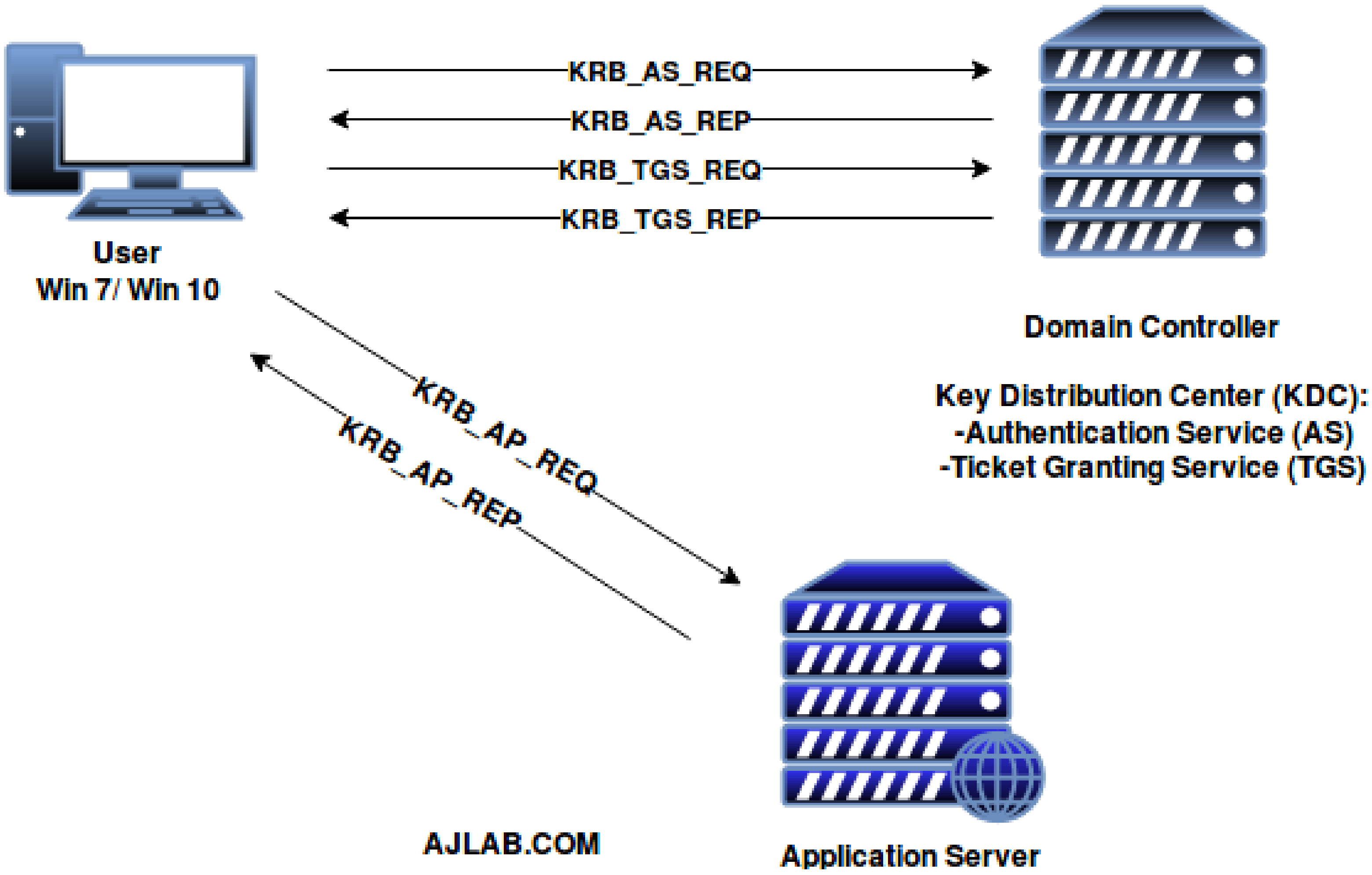
- **Realm** - Name of the realm (domain) that issued the ticket. A KDC can issue tickets only for servers in its own realm, so this is also the name of the server's realm.
- **Client Information** – workstation FQDN & IP address
- **Ticket Flags** – Encryption, ticket type (impersonation, Delegation, etc)
- **Auth Data** – PAC
- **User Info**: User name, user SID, profile info.
- **Group Membership**: Group RIDs
- **PAC Signature**

Kerberos Flags	Description
FORWARDABLE	(TGT only). Tells the ticket-granting service that it can issue a new TGT—based on the presented TGT—with a different network address based on the presented TGT.
RENEWABLE	Applications that need to authenticate again after the ticket expiration time can ask for a ticket to be renewed instead of requesting for a new one.
PRE-AUTHENT	Indicates that the client was authenticated by the KDC before a ticket was issued. This flag usually indicates the presence of an authenticator in the ticket. It can also flag the presence of credentials taken from a smart card logon.
FORWARDED	Indicates either that a TGT has been forwarded or that a ticket was issued from a forwarded TGT.

* Some of the well known Flags

Kerberos Ticket Process

Overview



Key Distribution Center (KDC):
-Authentication Service (AS)
-Ticket Granting Service (TGS)

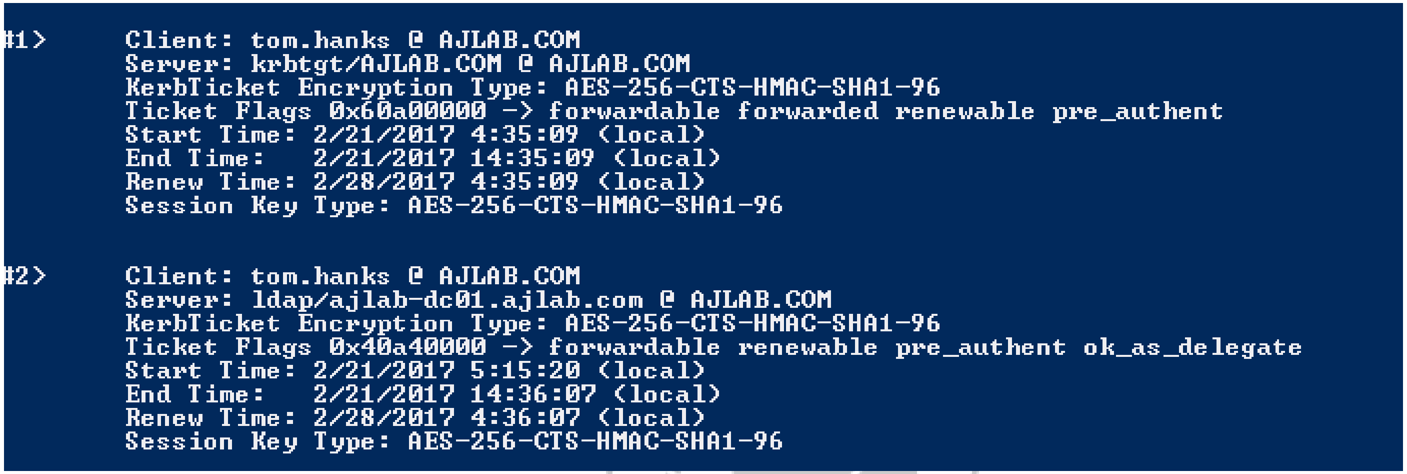
AJLAB.COM

https://www.draw.io/

- **KRB_AS_REQ**: The client contacts the Key Distribution Center's authentication service for a short-lived ticket (a message containing the client's identity and—for Windows clients—SIDs) called a **Ticket-Granting Ticket** (**TGT**). The Domain Controller (**KDC**) checks user information (logon restrictions, group membership, etc) and creates Ticket-Granting Ticket (TGT).
- **KRB_AS_REP**:The TGT is encrypted, signed, & delivered to the user (AS-REP). Only the Kerberos service (**KRBTGT**) in the domain can open and read TGT data.
- **KRB_TGS_REQ**:The User presents the TGT to the DC when requesting a **Ticket Granting Service** (**TGS**) ticket. The DC opens the TGT & validates PAC checksum – If the DC can open the ticket & the checksum check out, TGT is valid. The data in the TGT is effectively copied to create the TGS ticket.

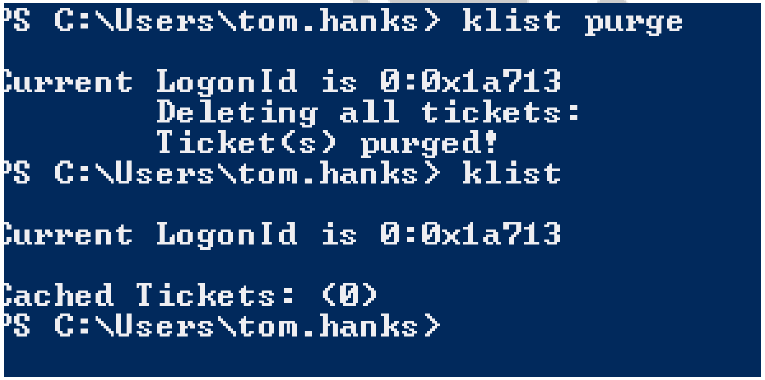
- **KRB_TGS_REP**:The TGS is encrypted using the target service accounts NTLM password hash and sent to the user.
- **KRB_AP_REQ**:The user connects to the server hosting the service on the appropriate port & presents the TGS (AP-REQ). The service opens the TGS ticket using its NTLM password hash.
- **KRB_AP_REP**(Optional): If mutual authentication is requested, the target server will take the client computer's timestamp from the authenticator, encrypt it with the session key the TGS provided for client-target server messages, and send it to the client.

- To check the list of cached Kerberos Tickets use the command : klist



```
#1>     Client: tom.hanks @ AJLAB.COM
        Server: krbtgt/AJLAB.COM @ AJLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent
        Start Time: 2/21/2017 4:35:09 (local)
        End Time:   2/21/2017 14:35:09 (local)
        Renew Time: 2/28/2017 4:35:09 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96


#2>     Client: tom.hanks @ AJLAB.COM
        Server: ldap/ajlab-dc01.ajlab.com @ AJLAB.COM
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
        Start Time: 2/21/2017 5:15:20 (local)
        End Time:   2/21/2017 14:36:07 (local)
        Renew Time: 2/28/2017 4:36:07 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

- To purge Kerberos Tickets use the command: Klist purge

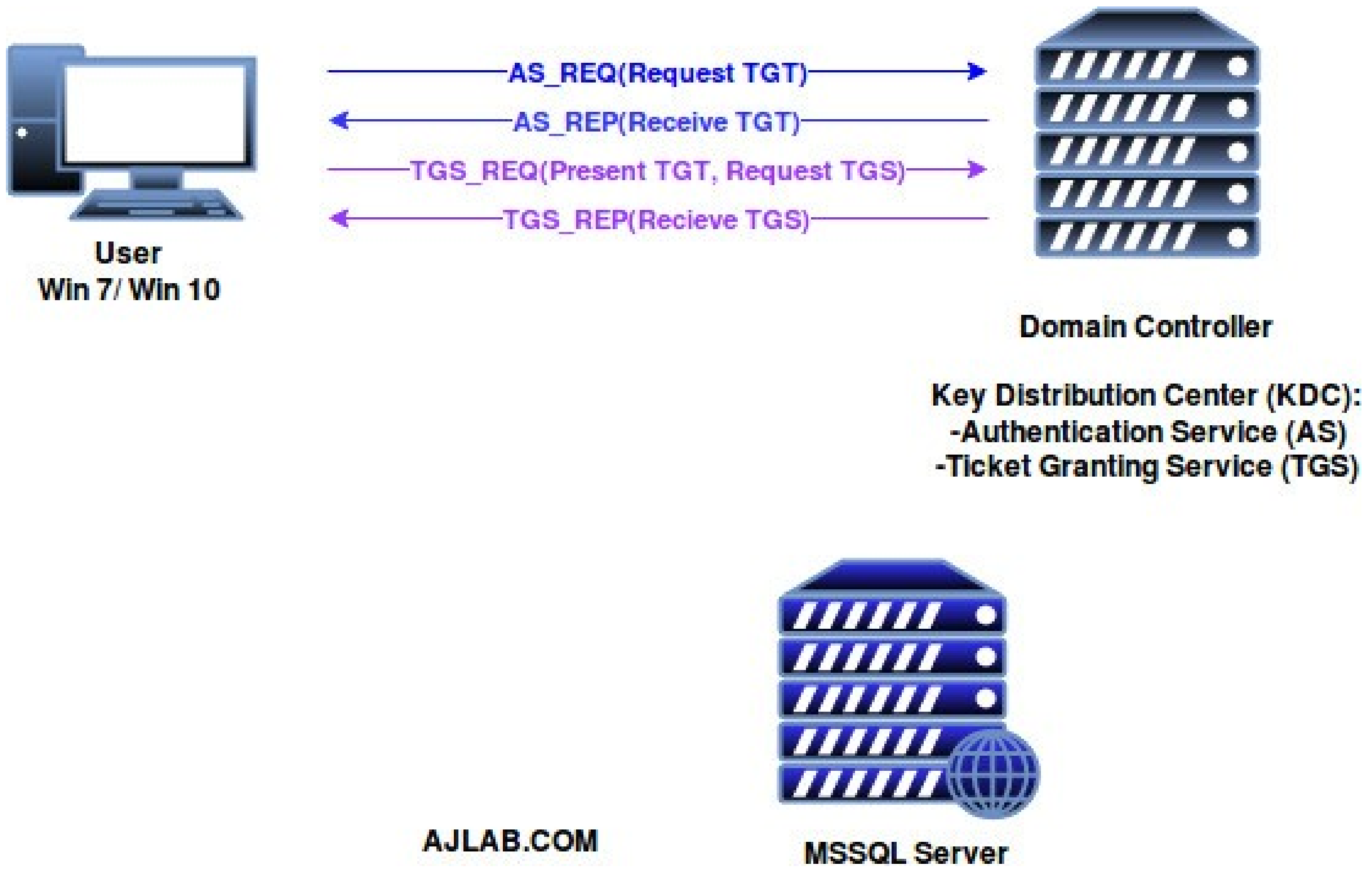


```
PS C:\Users\tom.hanks> klist purge

Current LogonId is 0:0x1a713
        Deleting all tickets:
        Ticket(s) purged!
PS C:\Users\tom.hanks> klist

Current LogonId is 0:0x1a713

Cached Tickets: (0)
PS C:\Users\tom.hanks>
```

https://makeameme.org/

Kerberoasting

Cracking Service accounts with Kerberoasting


AS_REQ(Request TGT)
AS_REP(Receive TGT)
TGS_REQ(Present TGT, Request TGS)
TGS_REP(Recieve TGS)
User
Win 7/ Win 10
Domain Controller
Key Distribution Center (KDC):
-Authentication Service (AS)
-Ticket Granting Service (TGS)
AJLAB.COM
MSSQL Server

- We will start with SPN scanning to identify service accounts

  cmd : **setspn -T <<domain>> -Q */***

- The output would be in the following form:

  <Service Class>/<Host>:<Port>

  MSSQLSvc/WIN12SQL.AJLAB.COM:1433

- After identifying the target, we will use PowerShell to request the service ticket for this Service Principal Name (SPN):

  Cmd: **Add-Type -AssemblyName System.IdentityModel**

  Cmd: **New-object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList ‘<<SPN Name>>’**

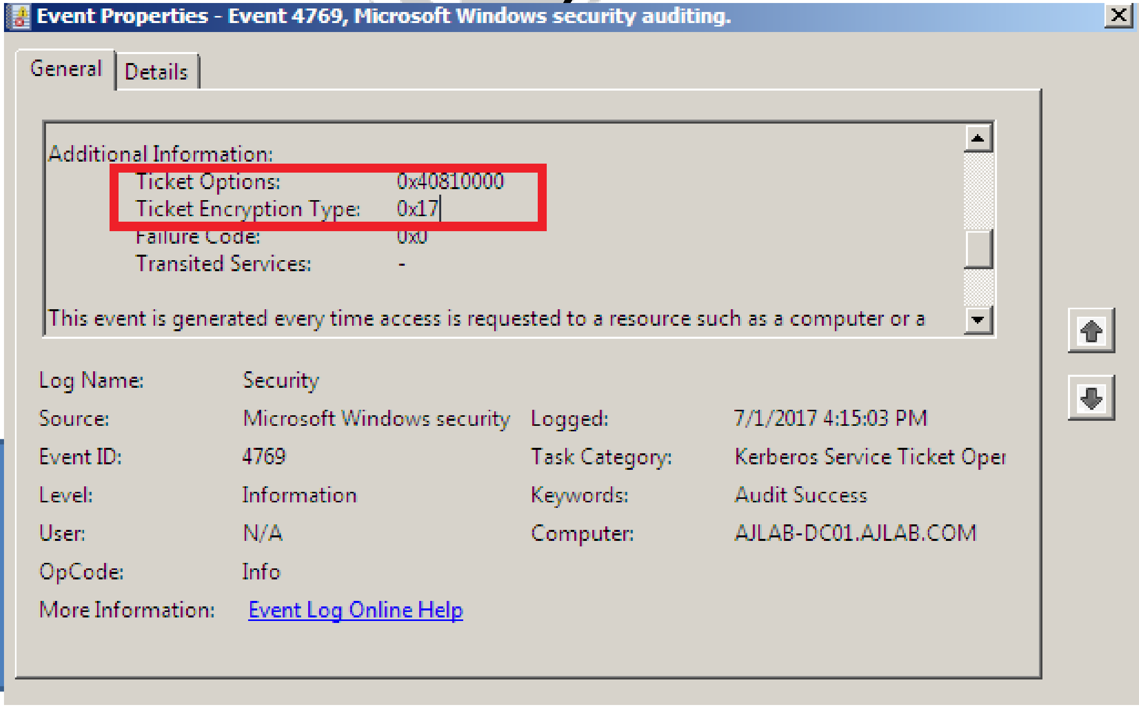
- A service ticket (**RC4 KerbEnc Format**) will be returned and stored in memory of the system.

- Once the ticket is received by the client, we can use Mimikatz (or other) to export all Kerberos tickets in the user’s memory space.
- After exporting the service ticket, we will copy the ticket to our attacker machine (Kali Linux).
- Depending on our wordlist file, we may be able to crack the service account’s password associated with the ticket (file).
- Cracking service account is a particular successful approach because their passwords rarely change and most of the service accounts are Domain Admins.
- We will Crack TGS offline, No Traffic is sent to the Target server and no elevated rights required.

Demo Time

Detection:

- It is very difficult to detect, Event ID which would interest us is 4769: A kerberos Service Ticket was requested (look for Ticket Encryption type 0x17 or 0x18).



Event Properties - Event 4769, Microsoft Windows security auditing.

```
Additional Information:
        Ticket Options:            0x40810000
        Ticket Encryption Type:    0x17
        Failure Code:              0x0
        Transited Services:        -

This event is generated every time access is requested to a resource such as a computer or a
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/1/2017 4:15:03 PM
Event ID:	4769	Task Category:	Kerberos Service Ticket Oper
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	AJLAB-DC01.AJLAB.COM
OpCode:	Info		
More Information:	Event Log Online Help		

- Create Service account honeypot and detect any service ticket requested for the honeypot.

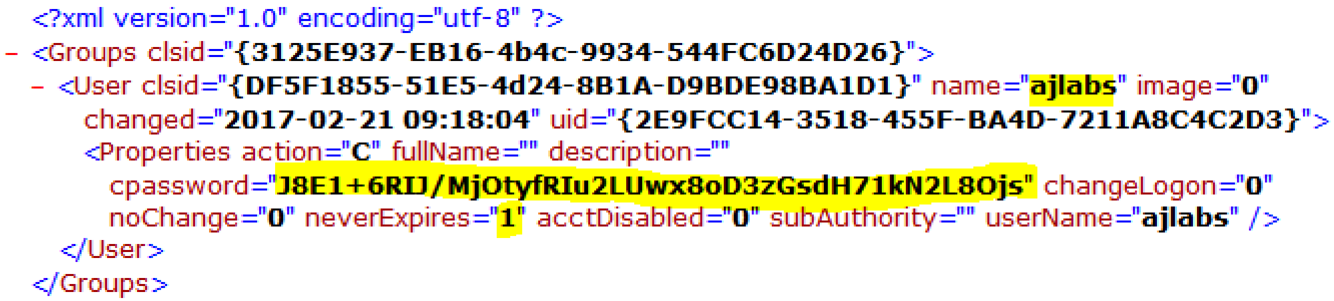
Mitigation:

- Service Account passwords >25 characters
- Use (Group) Managed Service Accounts.

Credential Storage in Groups.xml

- SYSVOL is the domain-wide share in Active Directory to which all authenticated users have read access. SYSVOL contains logon scripts, group policy data, and other domain-wide data which needs to be available anywhere there is a Domain Controller (since SYSVOL is automatically synchronized and shared among all Domain Controllers).
- All domain Group Policies are stored here:

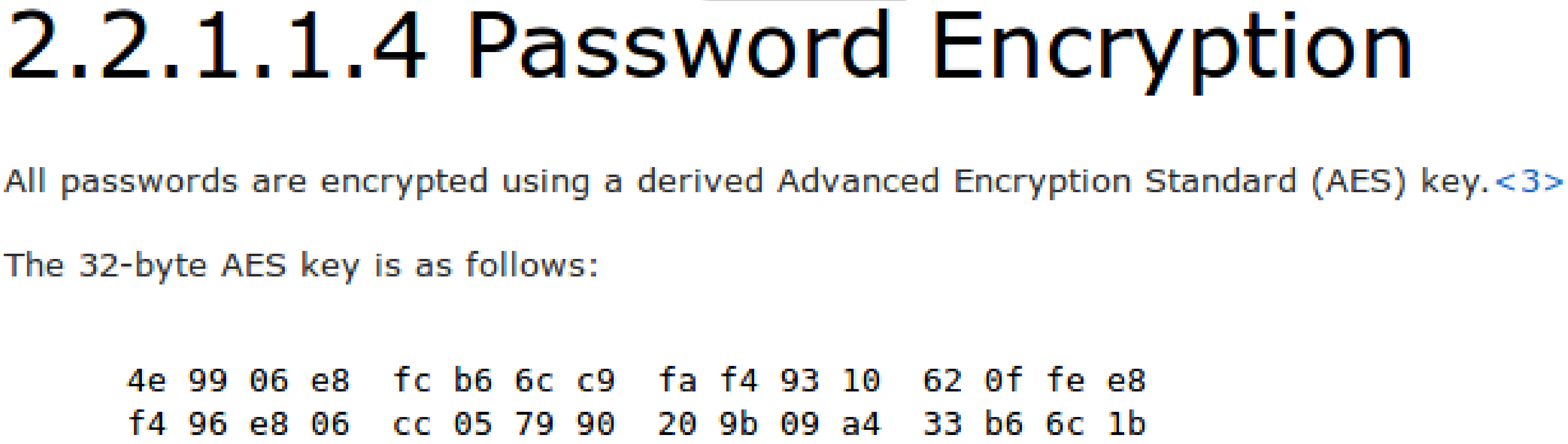
  \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\



```
  <?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="ajlabs" image="0"
      changed="2017-02-21 09:18:04" uid="{2E9FCC14-3518-455F-BA4D-7211A8C4C2D3}">
      <Properties action="C" fullName="" description=""
        cpassword="J8E1+6RIJ/MjOtyfRIu2LUwx8oD3zGsdH71kN2L8Ojs" changeLogon="0"
        noChange="0" neverExpires="1" acctDisabled="0" subAuthority="" userName="ajlabs" />
    </User>
  </Groups>
```

- When a new GPP is created, there’s an associated XML file (groups.xml) created in SYSVOL with the relevant configuration data and if there is a password provided, it is AES-256 bit encrypted which is a good news.

- Because Microsoft has published key on MSDN....



2.2.1.1.4 Password Encryption

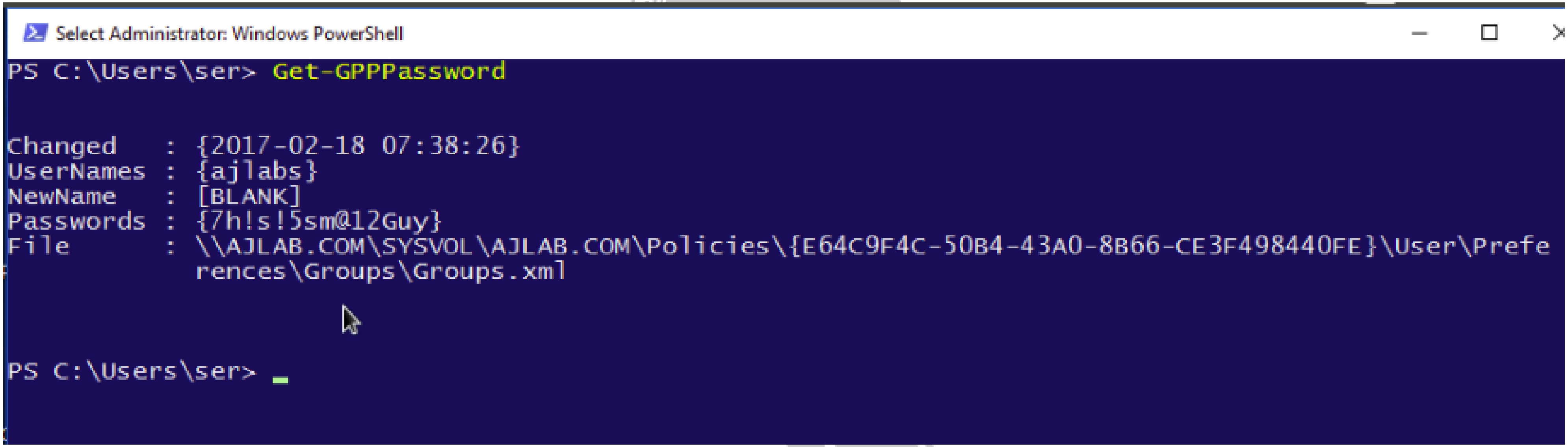
All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
    4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
    f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Ref: https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx

Demo Time

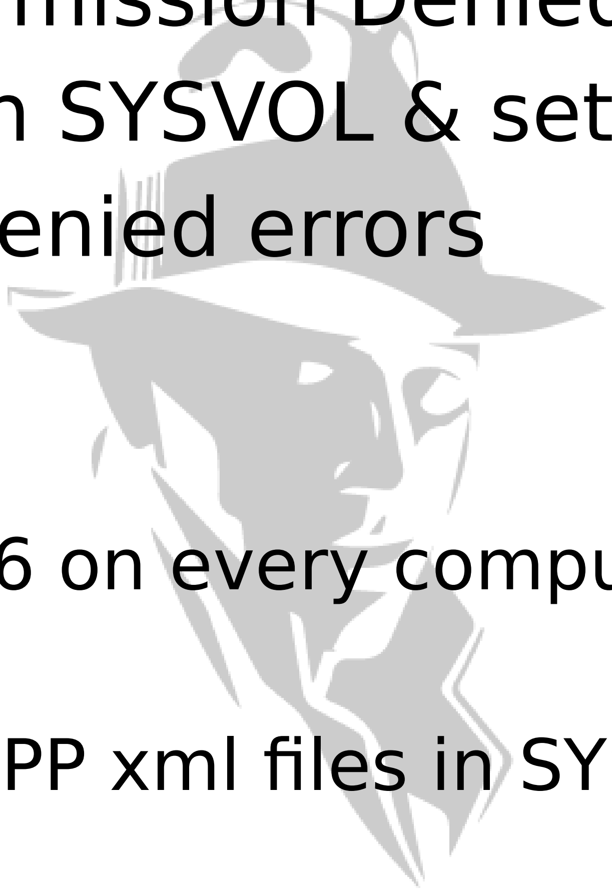


```
PS C:\Users\ser> Get-GPPPassword


Changed    : {2017-02-18 07:38:26}
UserNames  : {ajlabs}
NewName    : [BLANK]
Passwords  : {7h!s!5sm@12Guy}
File       : \\AJLAB.COM\SYSVOL\AJLAB.COM\Policies\{E64C9F4C-50B4-43A0-8B66-CE3F498440FE}\User\Prefe
             rences\Groups\Groups.xml



PS C:\Users\ser> _
```

* After Importing Powersploit Module use the above cmd

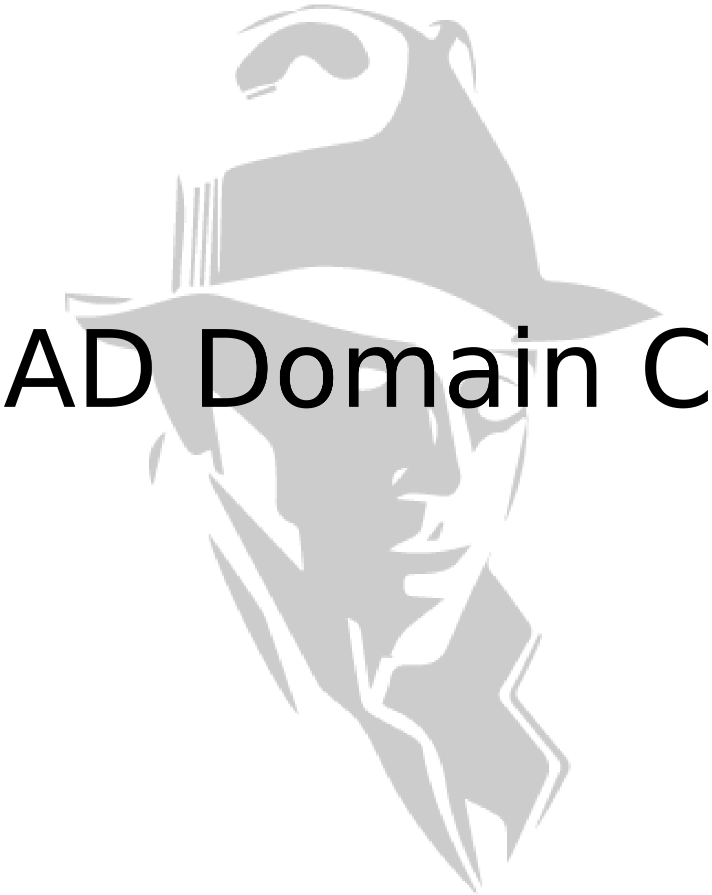
Detection:

- Create XML Permission Denied Checks
- Place xml file in SYSVOL & set Everyone:Deny
- Audit Access Denied errors



Mitigation:

- Install KB2962486 on every computer used to manage GPOs.
- Delete existing GPP xml files in SYSVOL containing passwords.



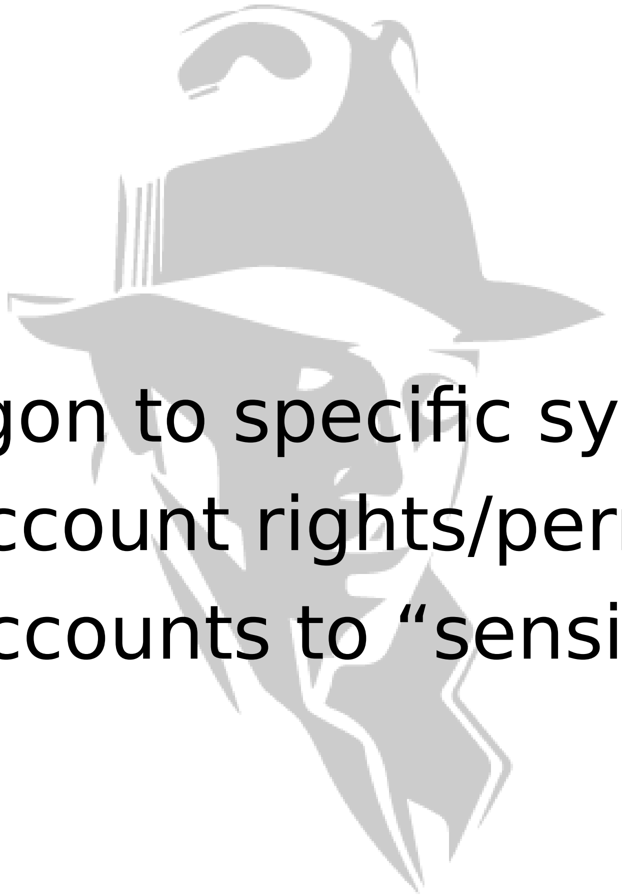
Dumping AD Domain Credentials

- The Active Directory database (ntds.dit) contains all information about all objects in the Active Directory domain. Data in this database is replicated to all Domain Controllers in the domain. This file also contains password hashes for all domain user and computer accounts.
- NTDSUtil is the command utility for natively working with the AD DB (ntds.dit) & enables IFM set creation for DCPromo. IFM is used with DCPromo to “Install From Media” so the server being promoted doesn’t need to copy domain data over the network from another DC. The IFM set is a copy of the NTDS.dit file created in this instance.
- The safest way of extracting NTDS.dit file and SYSTEM Registry file is using the NTDS util command(Which will be shown later in the Demo and it can also be achieved by vssadmin.exe).
- Next step would be extracting the Hashes from NTDS file and cracking those hashes.

Demo Time

Detection:

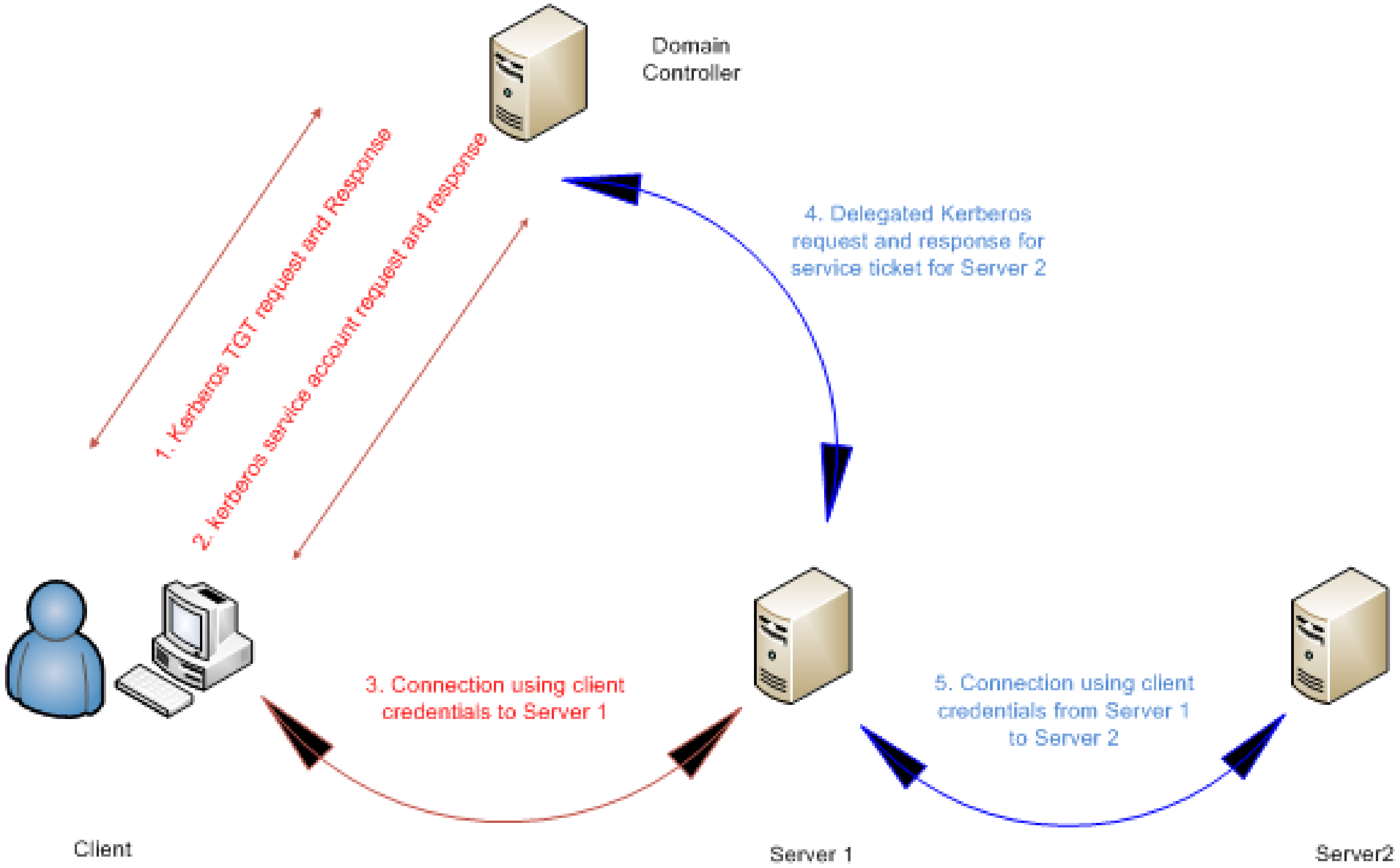
- Difficult :(



Mitigation:

- Admins only logon to specific systems.
- Limit Service Account rights/permissions.
- Set all admin accounts to “sensitive & cannot be delegated”.

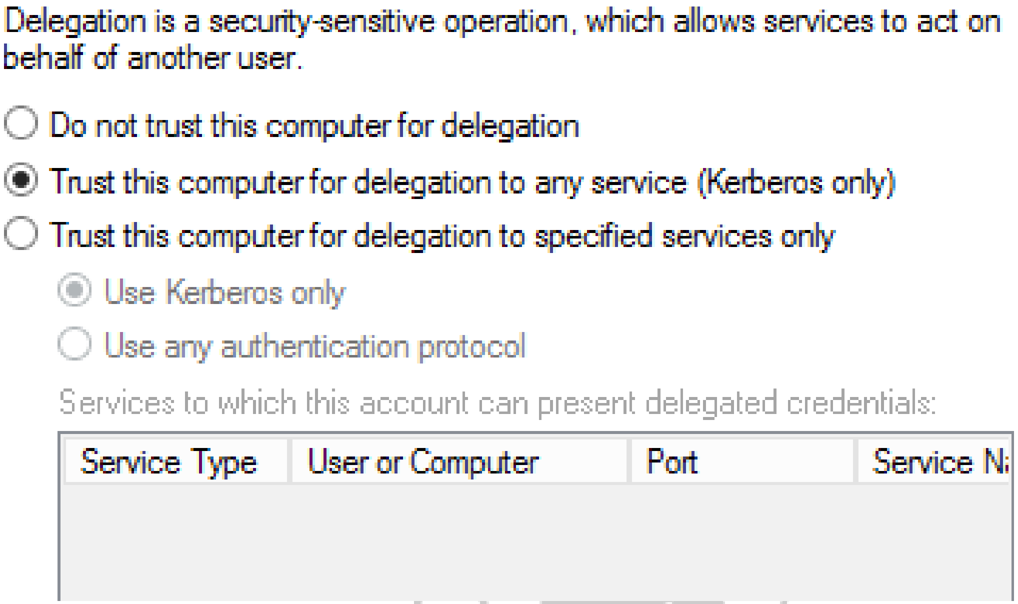
Exploitating Kerberos Unconstrained Delegation


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

https://blogs.technet.microsoft.com/askds/2008/06/13/understanding-kerberos-double-hop/

- Kerberos Double Hop is a term used to describe method of maintaining the client’s Kerberos authentication credentials over two or more connections.
- When kerberos Unconstrained Delegation is used on the server hosting the service specified in SPN, the DC places the users TGT into the service Ticket (TGS).
- When the user’s service ticket (TGS) is provided to the server for server access, the server opens the TGS and places the user’s TGT into LSASS for later use.
- The Application server can impersonate the user without limitation.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

● Use Kerberos only

○ Use any authentication protocol

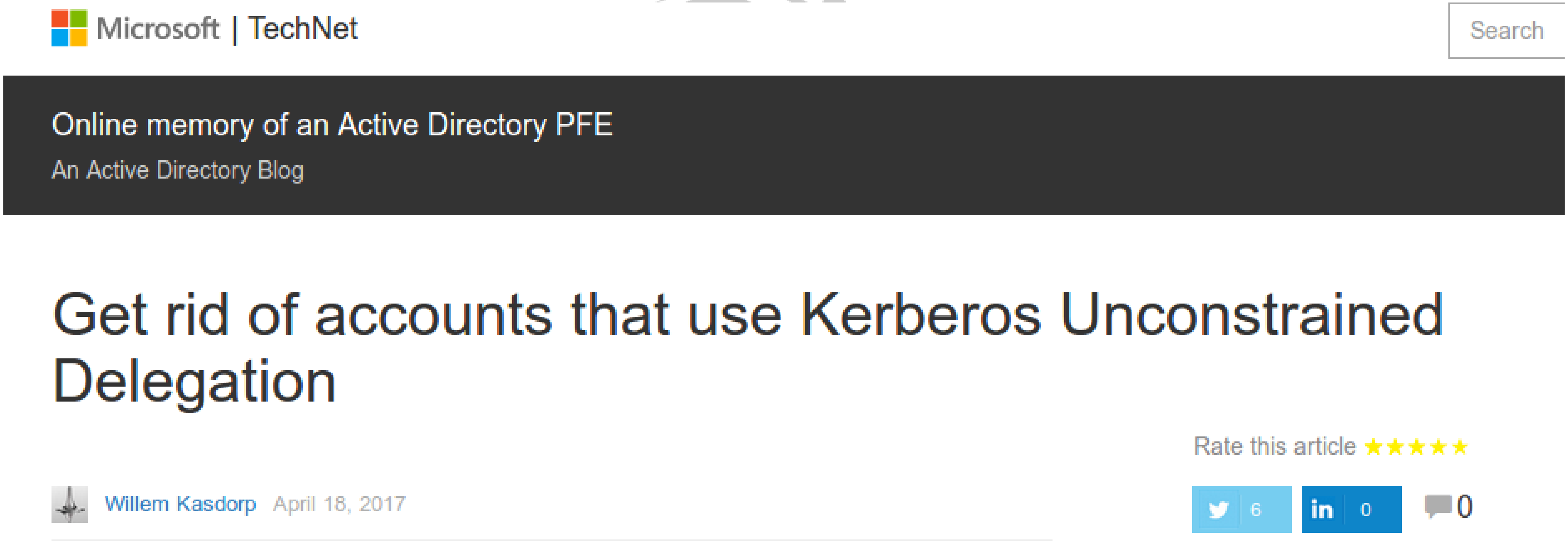
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N:

- Powershell cmdlet to discover Unconstrained Delegation:
  - Import-Module activedirectory
  - Get-Adcomputer -Filter {(TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515) } -Properties TrustedForDelegation,SevicePrincipalName,Description

Demo Time

Microsoft’s Blog Post



Microsoft | TechNet

Search

Online memory of an Active Directory PFE

An Active Directory Blog

Get rid of accounts that use Kerberos Unconstrained Delegation

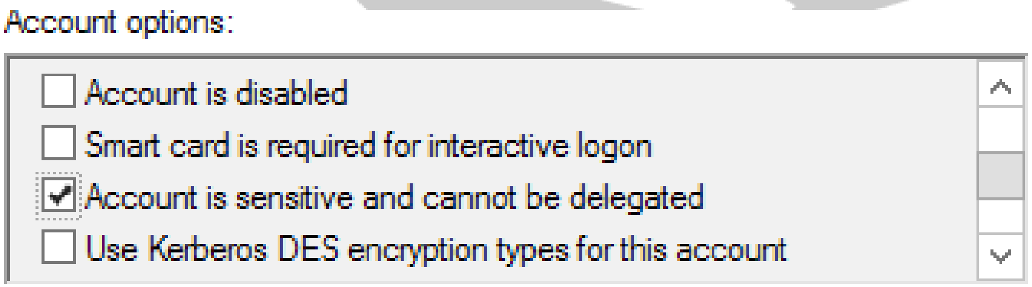
Rate this article ★★★★★

Willem Kasdorp April 18, 2017

https://blogs.technet.microsoft.com/389thoughts/2017/04/18/get-rid-of-accounts-that-use-kerberos-unconstrained-delegation/

Mitigation:

- Configure servers which requires delegation as Constrained Delegation.
- Disable Delegation for admin accounts.
- Configure all elevated administrator accounts to be “Account is Sensitive and cannot be Delegated”.



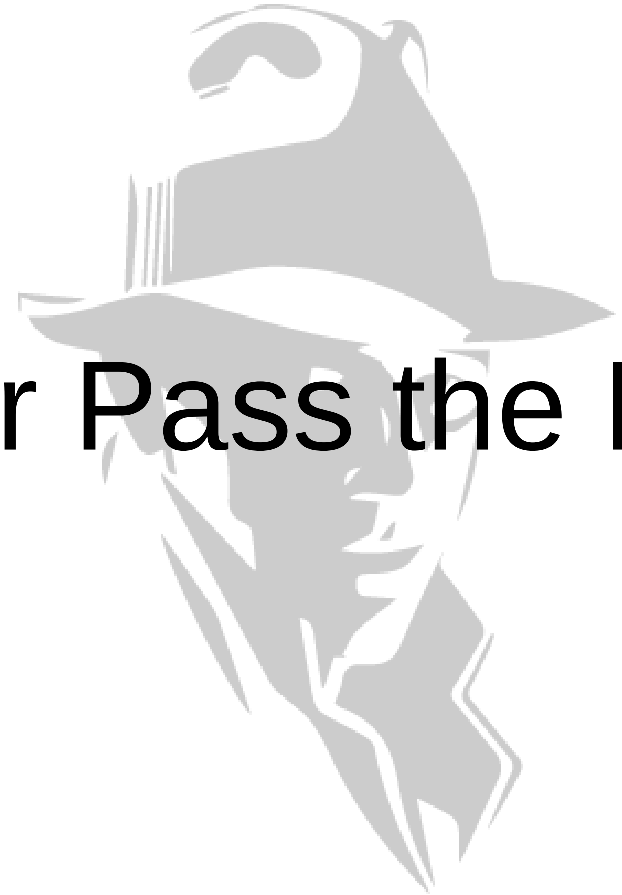
Account options:

- □ 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

Over Pass the Hash



What is Pass the Hash (PTH) ?

Pass the Hash is a Technique that allows the attacker to authenticate to remote server or service using NTLM Hash. Hash is valid until user changes the password.

What is Pass the Ticket (PTT) ?

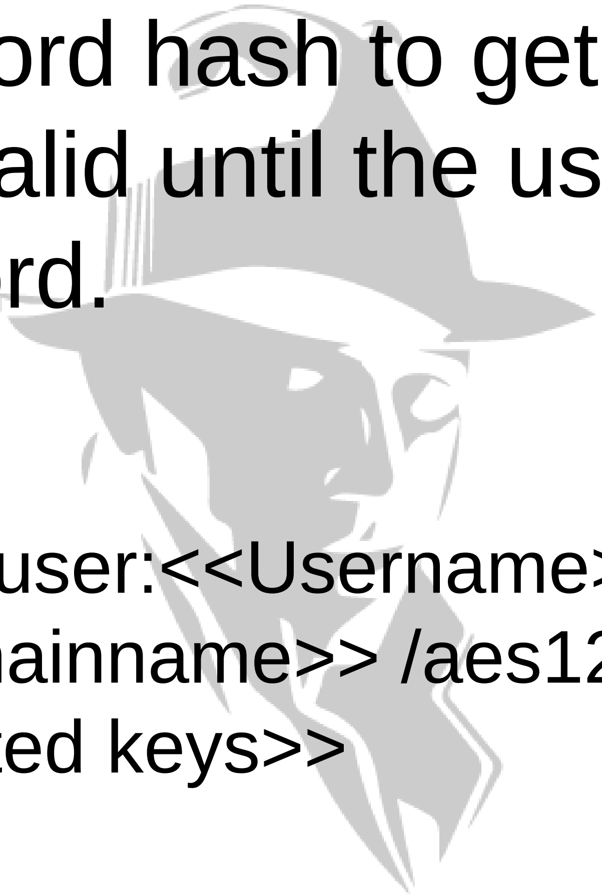
Pass the Ticket involves grabbing the existing kerberos ticket and using it to impersonate a user. Ticket is valid until ticket lifetime expires (Default is 7 days)

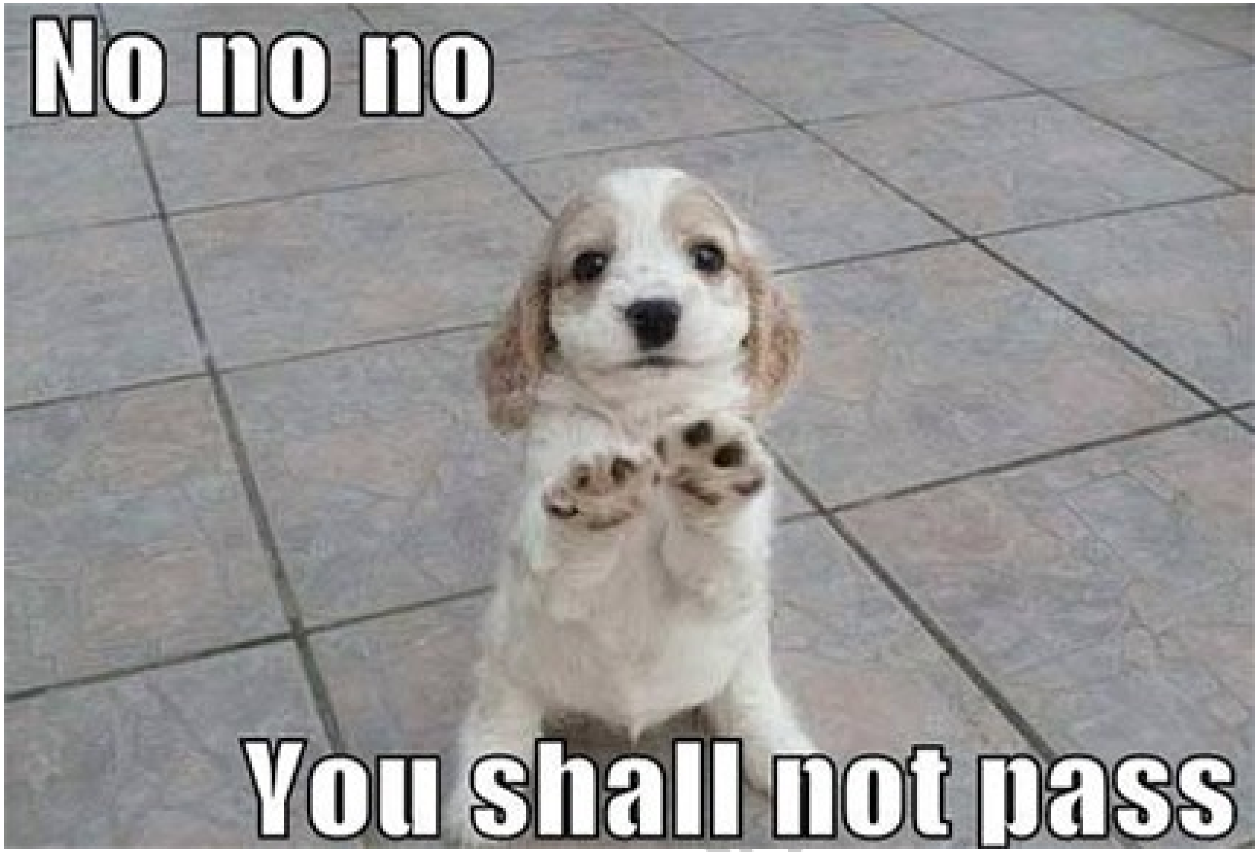
Over pass the Hash

- Over Pass the Hash involves using an acquired password hash to get a kerberos ticket. Hash is valid until the user changes the account password.

- Mimikatz cmd:

```
 kerberos::pth /user:<<Username>>
/domain:<<domainname>> /aes128 or /aes256 or
/ntlm:<<encrypted keys>>
```





http://www.ifunny.com/pictures/no-no-no-you-shall-not-pass/

Demo Time

Detection:

- Microsoft Advanced Threat Analytics(ATA)

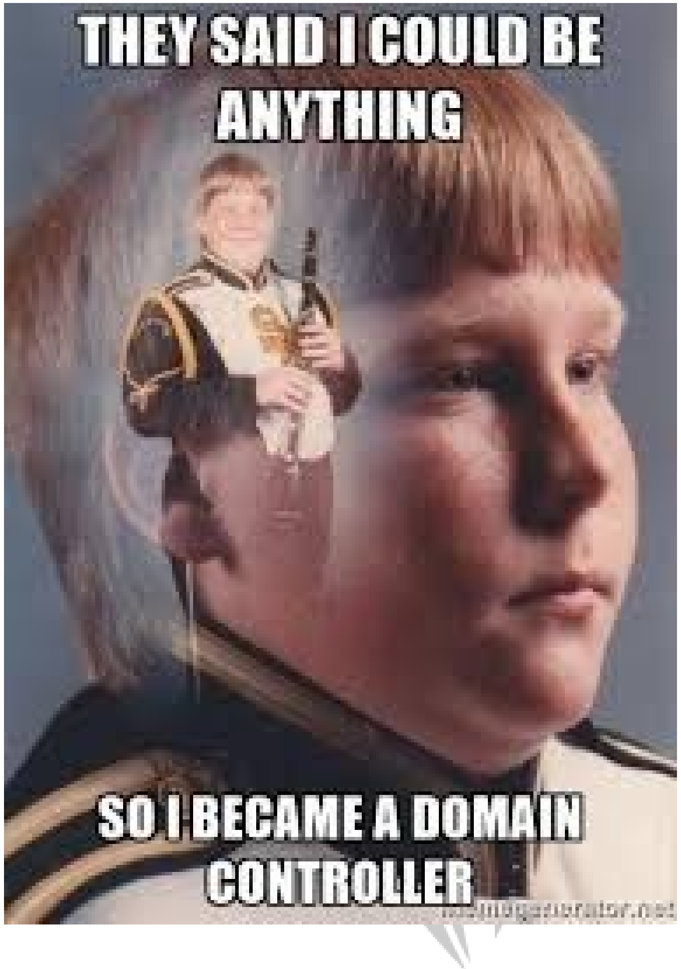
Mitigation:

- Admins only logon to specific systems
- Local administrator account management for every computer in active directory product like Microsoft LAPS(Local Administrator Password Solution) can be helpful.

Abusing Directory Replication Service

- The DCSYNC feature in Mimikatz impersonates as a domain controller and requests password data from the targeted domain controller.
- Special rights are required to run DCSYNC. Any members of administrators, Domain Admin or Enterprise Admin as well as Domain controller computer accounts should be able to pull password data.
- The DCSYNC first discovers domain controller in specific domain and then it requests the domain controller to replicate the user credential via GetNCChanges (Abusing MS-DRSR)
- Mimikatz cmd:

```
lsadump::dcsync /domain:<<Domain Name>> /user:<<Username>>
```


THEY SAID I COULD BE ANYTHING
SO I BECAME A DOMAIN CONTROLLER
memegenerator.net

https://memegenerator.net/

Demo Time

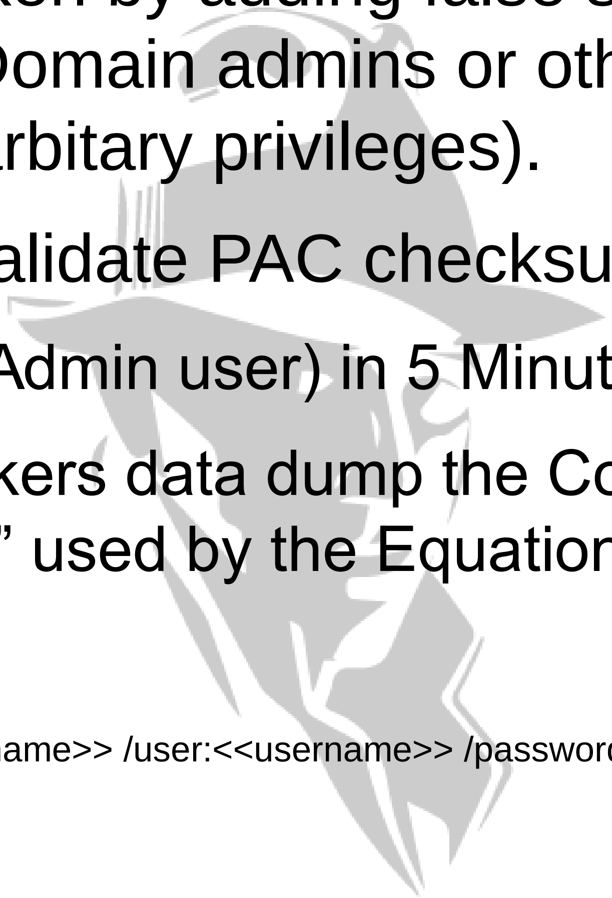
Detection:

- Microsoft Advanced Threat Analytics(ATA)

•Identify all Domain Controller IP addresses and add to “Replication Allow List” in IDS.

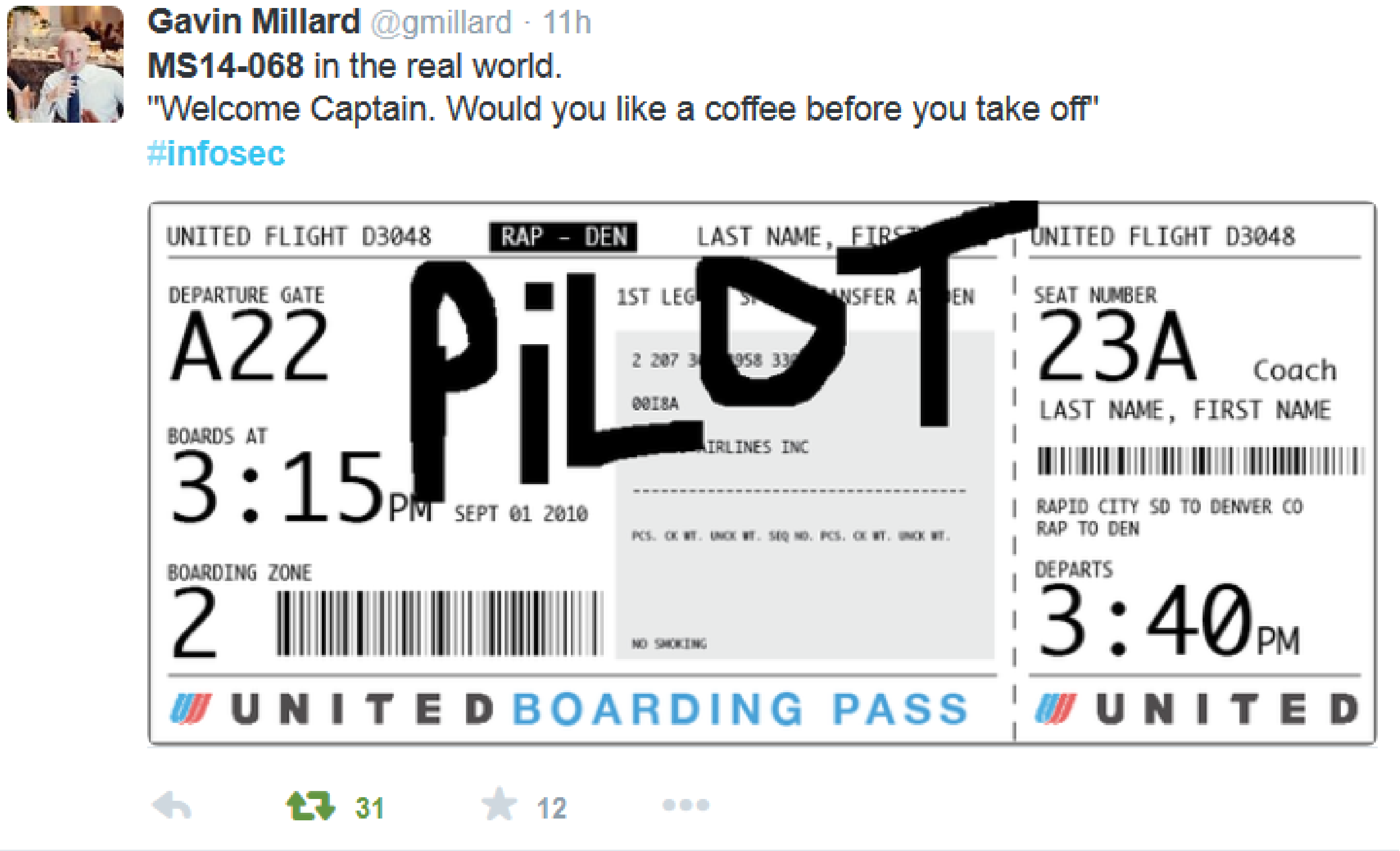
•Configure IDS to trigger if DSGetNCChanges request originates from the IP not on the “Replication Allow List”.

MS14-068: Microsoft Kerberos Vulnerability



- The vulnerability enables an attacker by modifying a valid domain user logon token by adding false statement that the user is a member of Domain admins or other sensitive groups (Forging a PAC with arbitary privileges).
- DC didn’t correctly validate PAC checksum.
- Zero to Hero(Domain Admin user) in 5 Minutes.
- From the Shadow Brokers data dump the Code name for MS14-068 is “ESKIMOROLL” used by the Equation Group.
- Kekeo cmd:

```
ms14068.exe /domain:<<domain name>> /user:<<username>> /password:<<pwd>> /ptt
```



Gavin Millard @gmillard · 11h

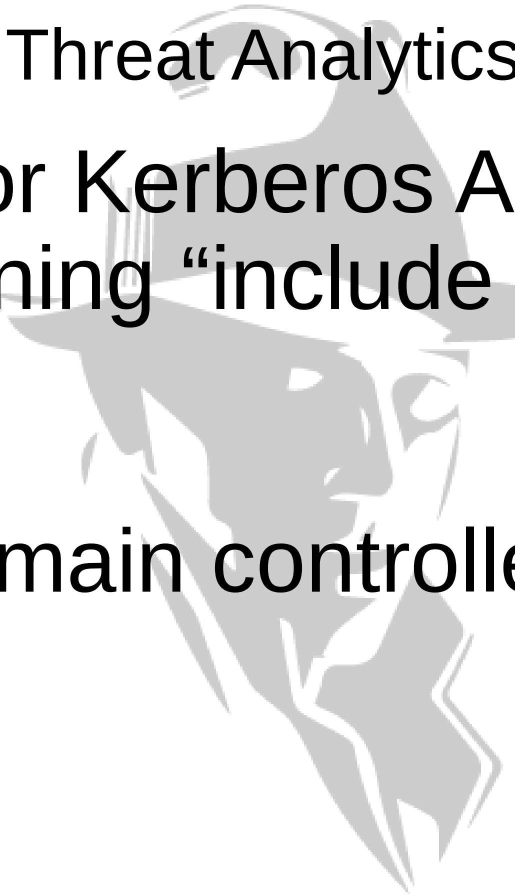
MS14-068 in the real world.
"Welcome Captain. Would you like a coffee before you take off"
#infosec

https://twitter.com/gmillard/status/535061077374296064

Demo Time

Detection:

- Microsoft Advanced Threat Analytics(ATA)
- IDS Signature for Kerberos AS-REQ and TGS-REQ both containing “include PAC: False”



Mitigation:

- Patch all the Domain controllers with KB3011780

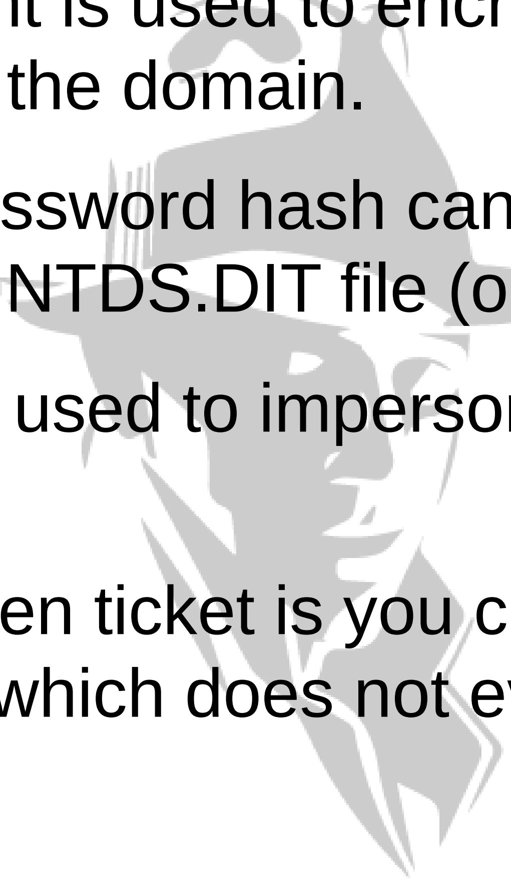
WONKA

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.



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:

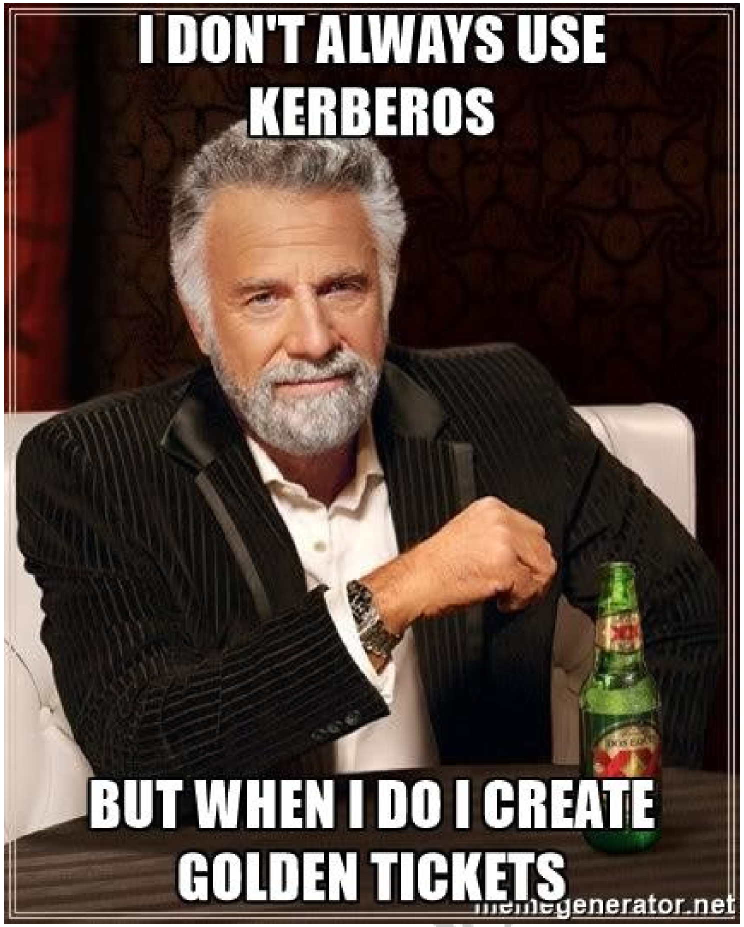
  Maximum LifeTime of Service Ticket (TGS): Default is **600 minutes**

  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 :

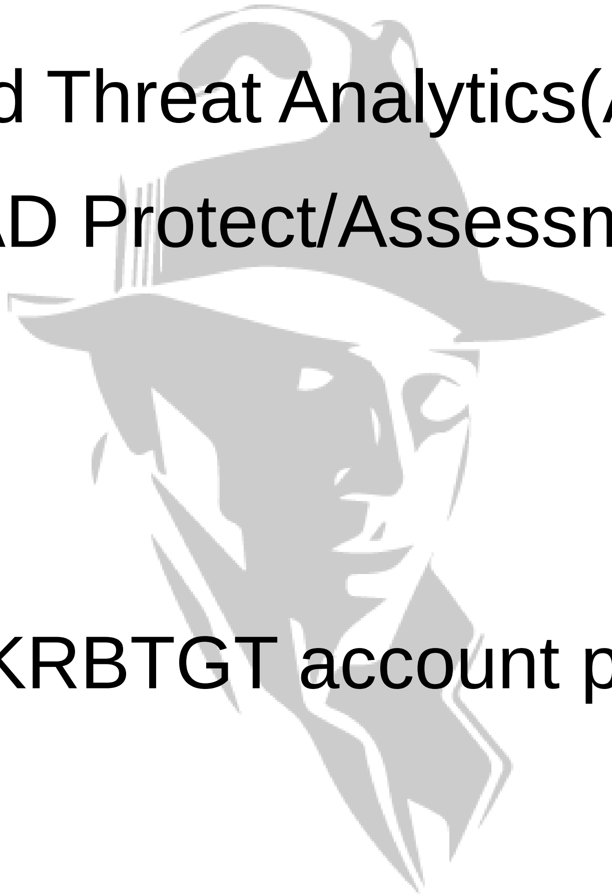
513- Domain User, **512** - Domain Admin, **518** - Schema Admin, **519** - Enterprise Admin, **520** - Group Policy Creator Owner, **502** - KRBTGT Account


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

https://memegenerator.net/

Demo Time

Detection:



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

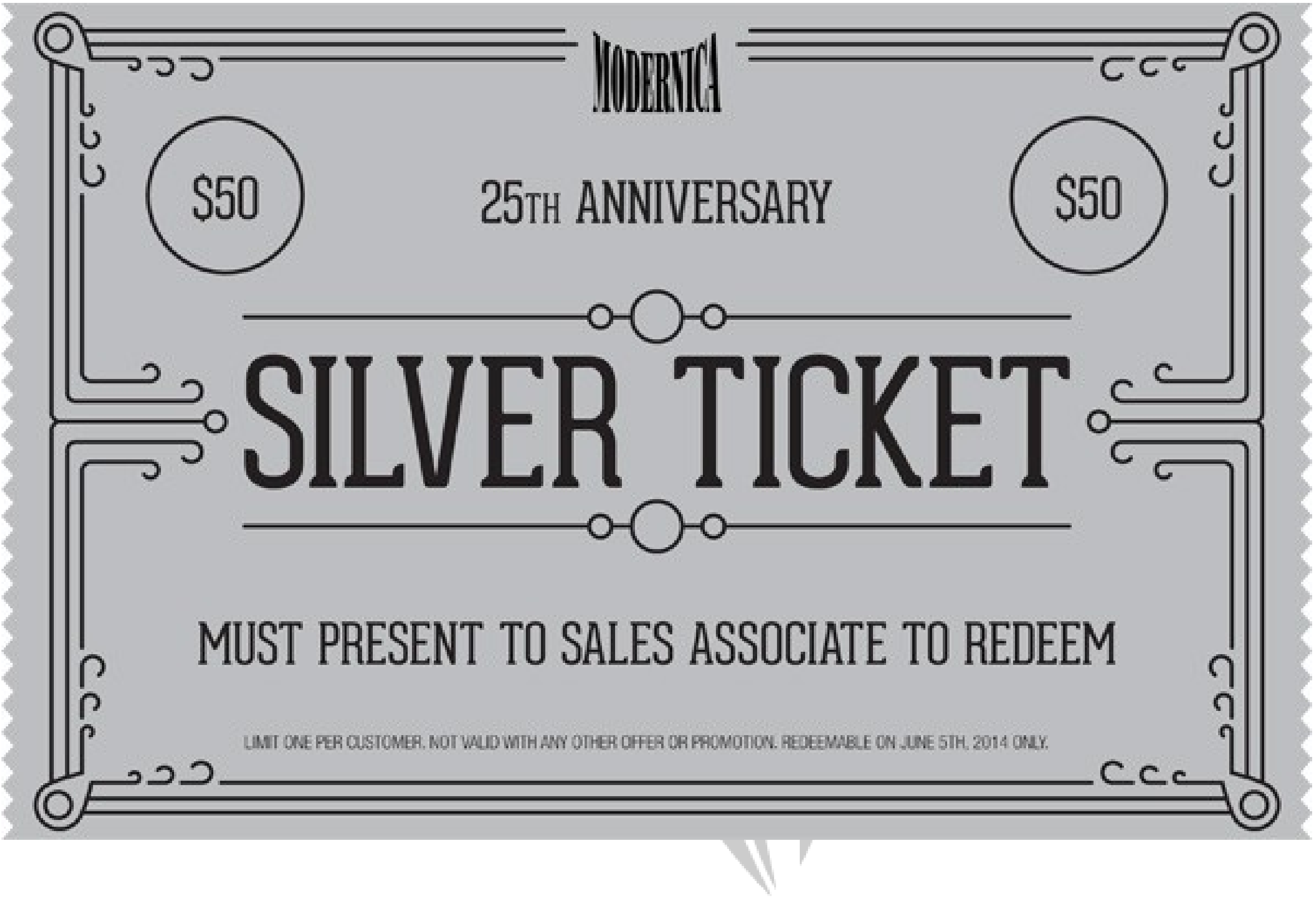
Mitigation:

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

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/

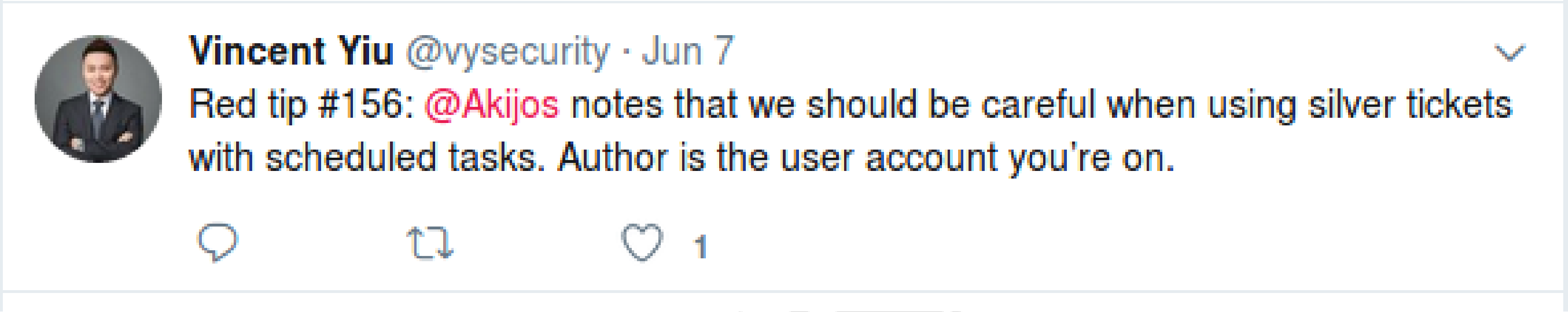
- Silver Ticket is Forged Ticket Granting Service (TGS) Ticket.
- A Silver Ticket is encrypted/signed by the service account (Computer Account or Service Account).
- No AS-REQ/AS-REP,TGS-REQ/TGS-REP and no traffic sent to the Domain Controller.
- We will be using the hash of computer account to generate 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

http://memes.com/

Detection:

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.

Detection :

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

Mitigation:

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

References

- adsecurity.org
- blog.gentilkiwi.com
- blog.harmj0y.net
- labofapenetrationtester.com
- technet.microsoft.com/en-us/library/cc772815(v=ws.10).aspx
- msdn.microsoft.com
- Google.com (everything else)

Thank You

Twitter: @AkiJos
Blog: akijosberryblog.wordpress.com

HAKON-2017™
Creating Information Security Culture Seriously