Active Directory Attacks and Detection

#Whoami

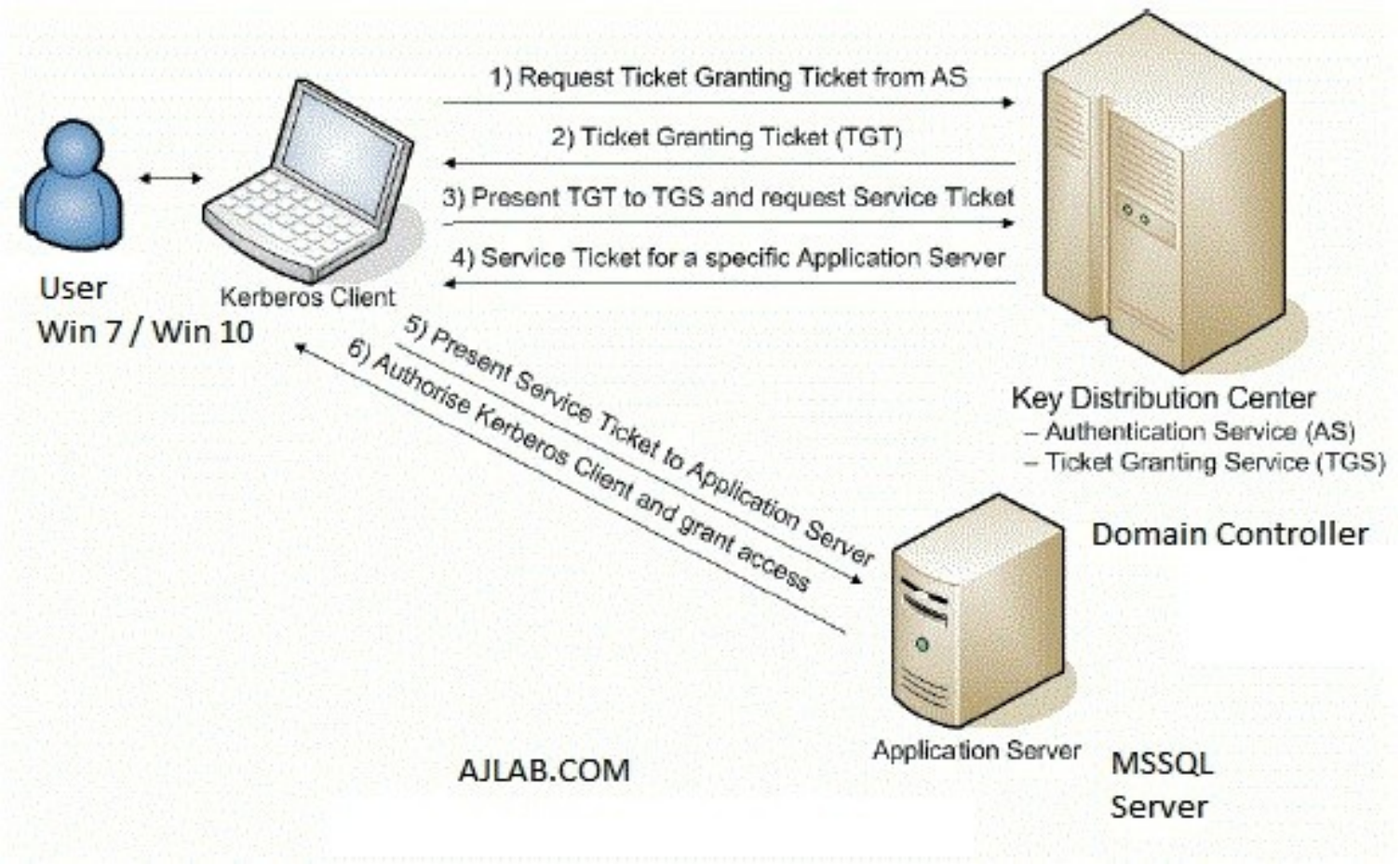
- Working as an Information Security Executive
- Blog : www.akijosberryblog.wordpress.com

- You can follow me on Twitter: @AkiJos

- This talk is Based on Tim Madin’s Derbycon Talk(2014) (Kerberoasting) and Sean Metacalf’s Blackhat(2015) Talk.
- You will learn how to Tame a Three Headed Dog.
- You will learn how to request Kerberos Tickets for no reason.
- How not to create deck like this one :P

Lab Setup

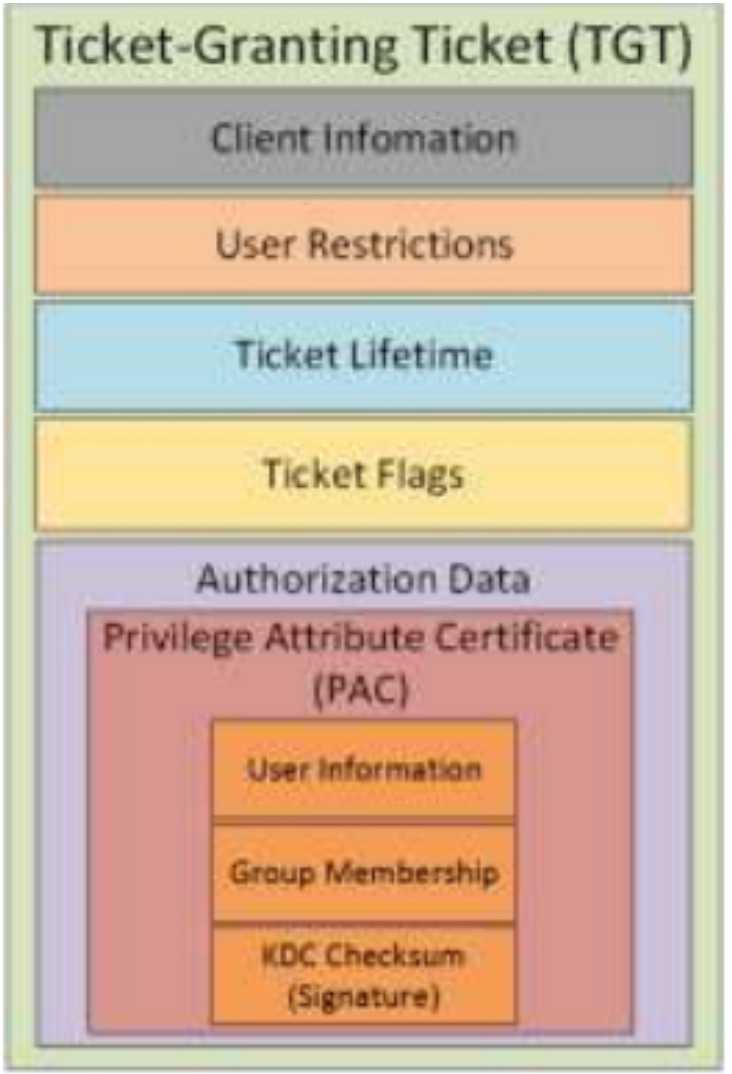
- AJLAB.COM:
- 2 Domain Controller – Win 2008 & Win 2012 r2
- 1 MSSQL Server – Running on Win2012 r2
- Win7,Win10 – Workstation Machines
- PFSense used as gateway(Just in Case Internet is required)


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
5) Present Service Ticket to Application Server
6) Authorise Kerberos Client and grant access
User
Win 7 / Win 10
Kerberos Client
Key Distribution Center
– Authentication Service (AS)
– Ticket Granting Service (TGS)
Domain Controller
Application Server
MSSQL
Server
AJLAB.COM

Kerberos 101

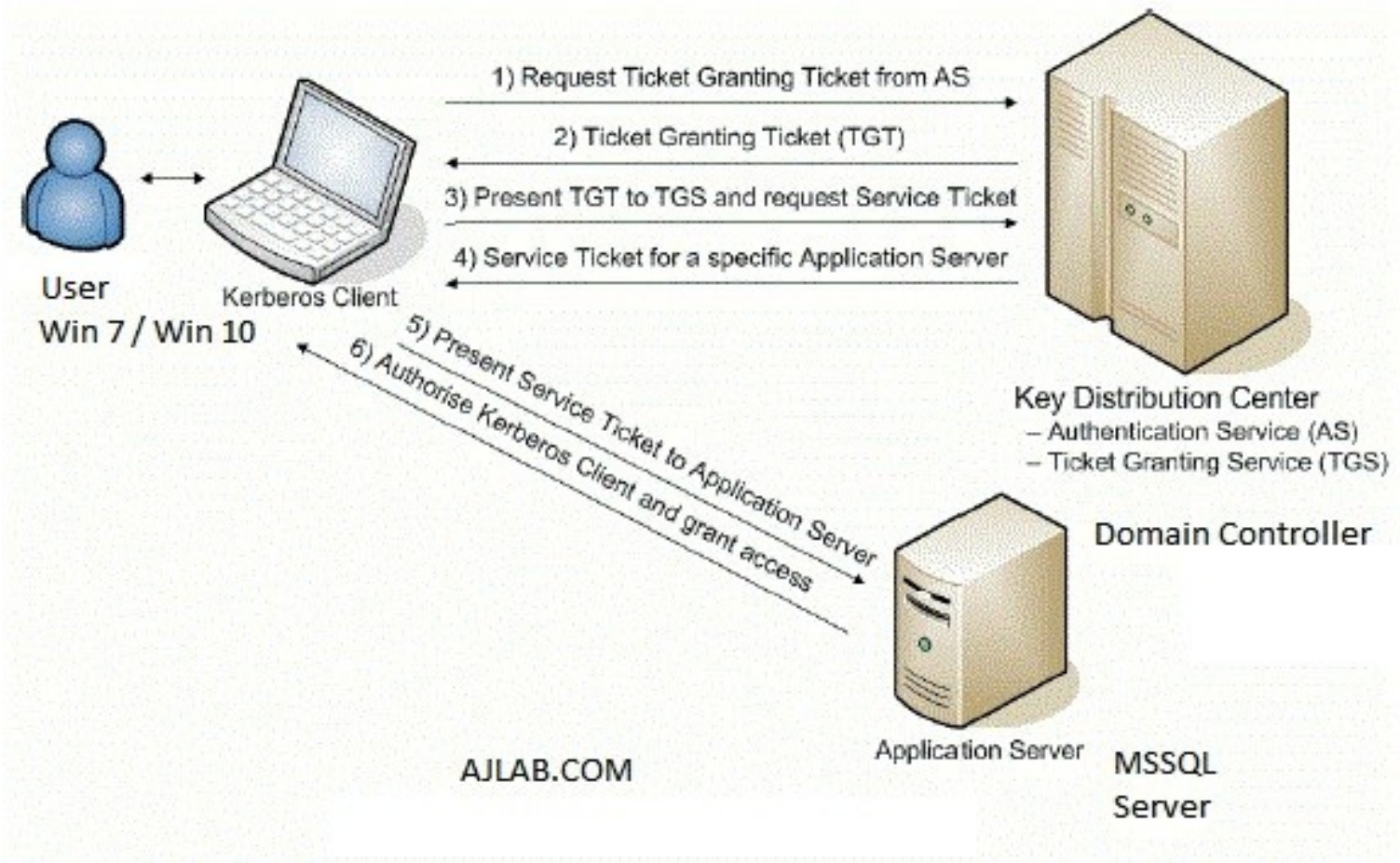
- Kerberos is a bit complex authentication protocol
- Active Directory implements Kerberos version 5 in two components: the Authentication service and the Ticket-granting service.
- The Authentication Service (AS) is the first contact the client has with Kerberos and is used to lookup the user's password 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 for the Ticket Granting Service (runs on the KDC) and is encrypted using the KDC key. Only a KDC can decrypt and read the ticket.

Kerberos Ticket Format



- Client information – workstation FQDN & IP address
- User Restrictions – logon schedule, workstation restrictions, etc.
- Domain Kerberos Policy - Ticket Lifetime (Default: 10 hour lifetime & 7 day max)
- Ticket Flags – Encryption, ticket type (impersonation, can it be delegated, etc)
- Auth Data – PAC
  - User Info: User name, user SID, profile info..
  - Group Membership: Group RIDs
  - PAC Signature
  - A TGS has a server component & user component.

Kerberos Ticket Process Overview



Kerberos Flags

- Renewable Ticket: 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.
- Forwarded Tickets: Applications or users can request a new ticket to the KDC, based on a previously obtained ticket with the forwardable flag set. This option of the Kerberos protocol is what makes it possible to implement single-sign-on (SSO) using Kerberos. Based on the obtainment of a single ticket, a user could request access to all services.
- OK-AS-DELEGATE: The KDC MUST set the OK-AS-DELEGATE flag if the service account is trusted for delegation.

- 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>
```


SAY KERBEROS
ONE MORE TIME
memegenerator.net

Attacker Goals (Red Team)

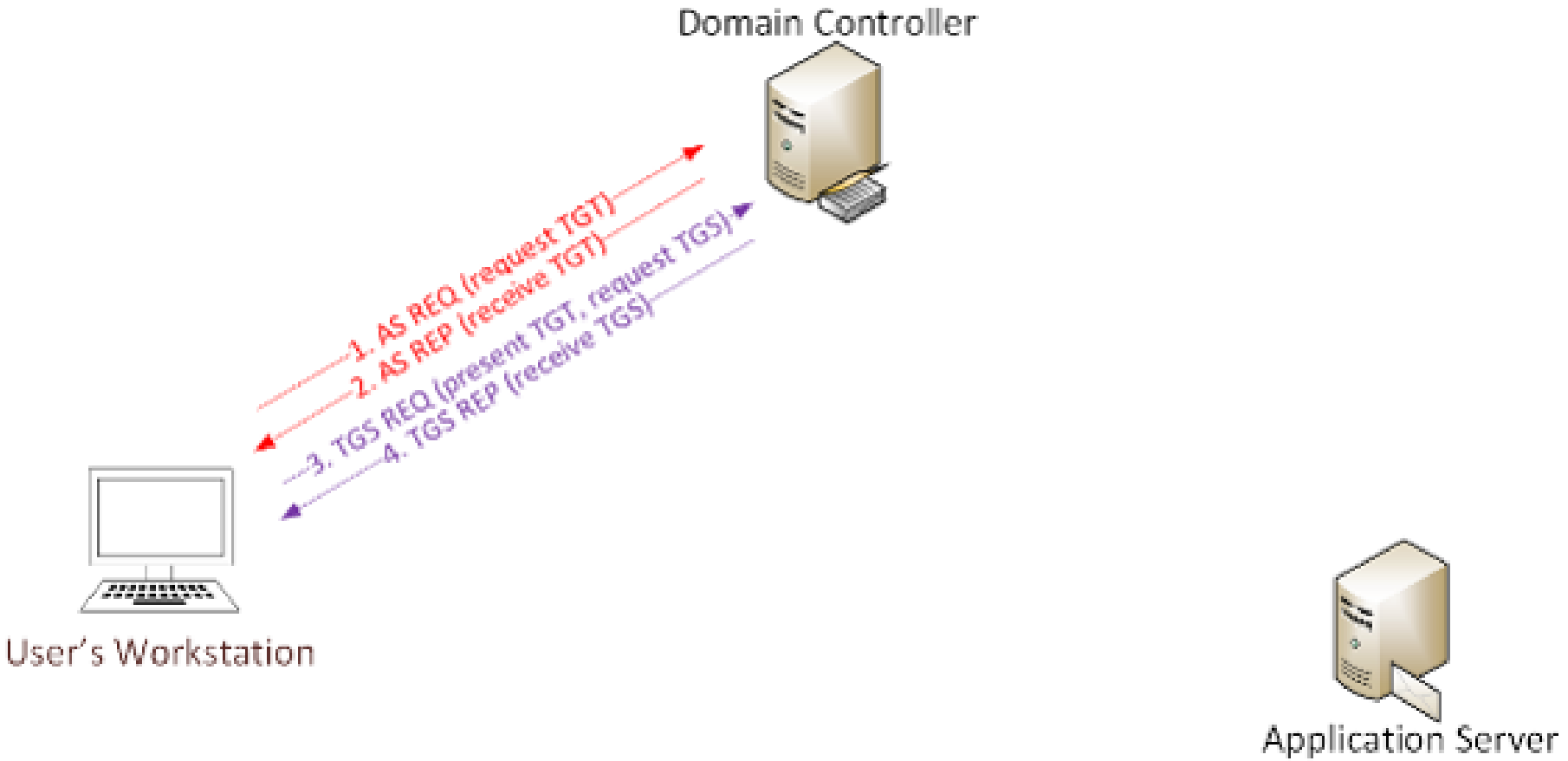
- Data Access
- Exfiltration
- Persistence

* Privilege Escalation if Required

Defender Goals (Blue Team)

- Detect
- Mitigate
- Prevent

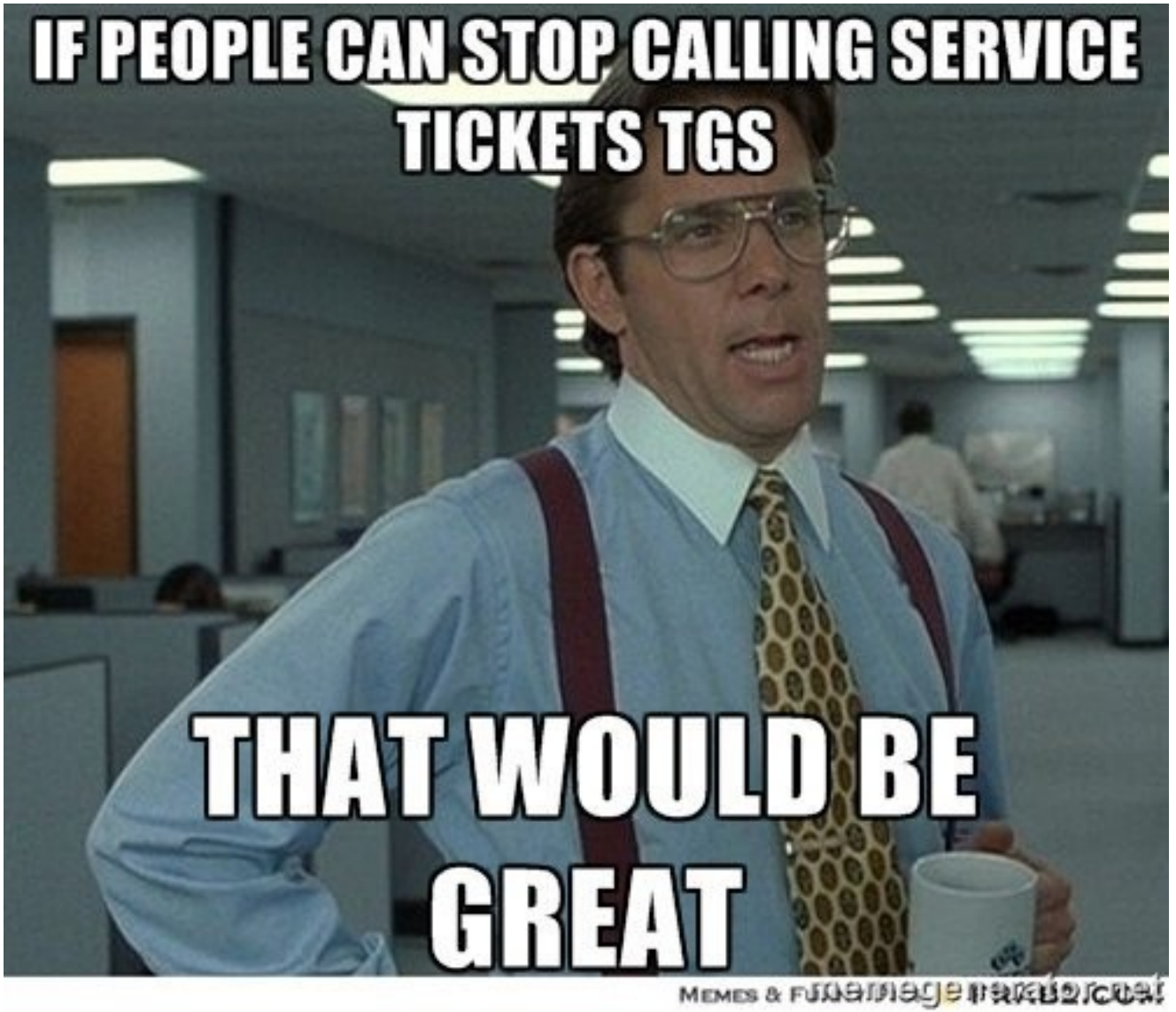
Cracking Service accounts with Kerberoasting



“SPN Scanning” Service Discovery

- SQL servers, instances, ports, etc.
  - MSSQLSvc/adsmsSQLAP01.ajlab.com
- Exchange Client Access Servers
  - exchangeMDB/adsmsEXCAS01.ajlab.com
- RDP
  - TERMSERV/adsmsEXCAS01.ajlab.com
- WSMan/WinRM/PS Remoting
  - WSMAN/adsmsEXCAS01.ajlab.com
- Hyper-V Host
  - Microsoft Virtual Console Service/adsmsHV01.ajlab.com
- VMWare VCenter
  - STS/adsmsVC01.ajlab.com

- SPN scan for SQL servers with service accounts:
  - cmd : setspn -T <<domain>> -Q */*
- After identifying the target, we 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>>'
    - Make sure the Ticket requested has the RC4 encryption type
- Once the ticket is is received by the client, we can use Mimikatz (or other) to export all Kerberos tickets in the user's memory space without elevated rights.
- After exporting the service ticket to a file, that file can be sent to our attacker machine running Kali Linux with Kerberoast. Depending on our wordlist file, we may be able to crack the service account's password associated with the ticket (file).
- We will crack the TGS offline, No Traffic is sent to the Target and no Elevated rights required.

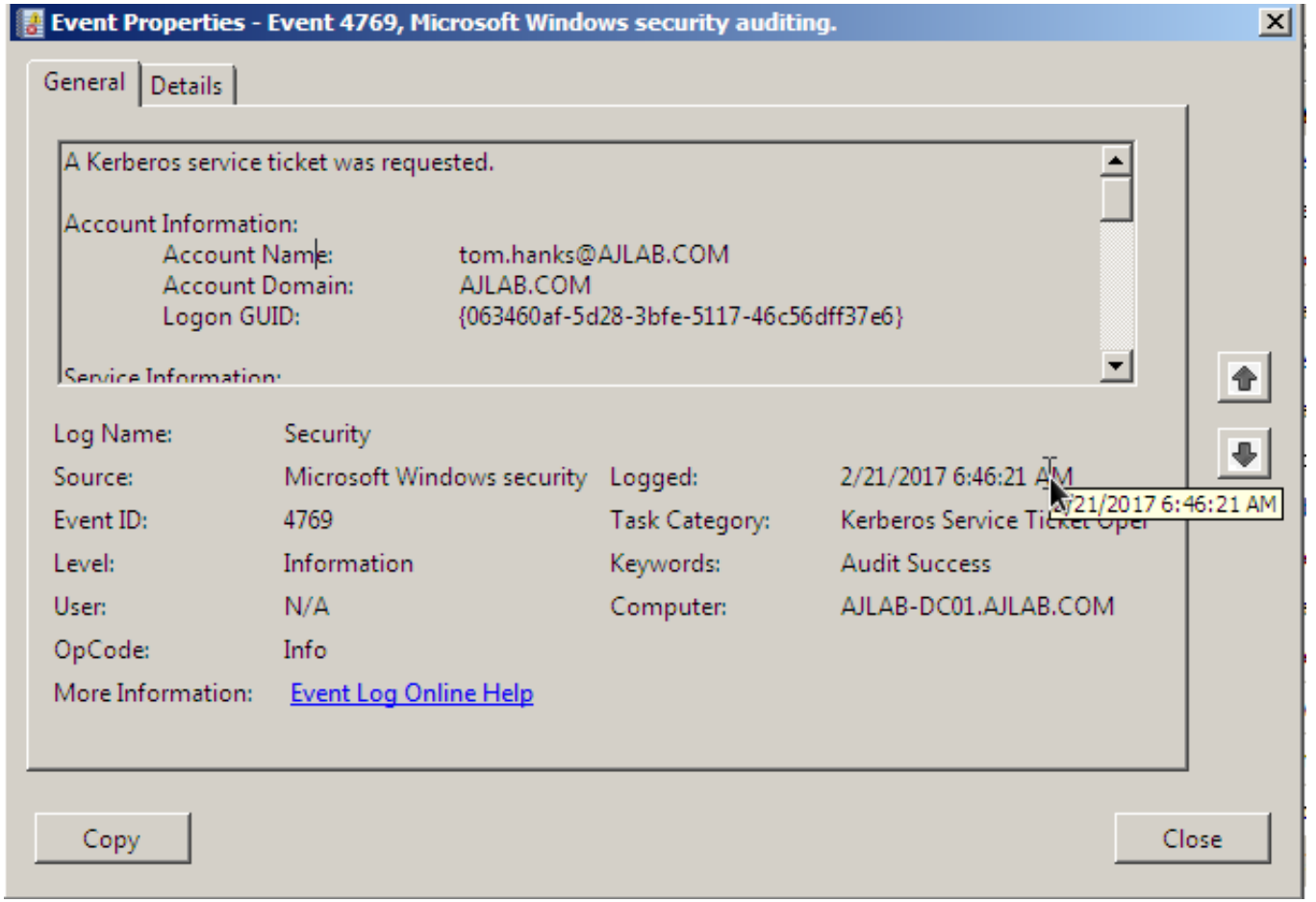

IF PEOPLE CAN STOP CALLING SERVICE TICKETS TGS
THAT WOULD BE GREAT
MEMES & FUNNY

Demo Time

Kerberoasting

Blue Team Response

- It is very difficult to detect, Event ID which would interest us is 4769: A kerberos Service Ticket was requested.
- We can monitor users requesting large number of TGS request and can be flagged.



Mitigation:

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

Group Policy Preferences Credential Storage

- 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\
- 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.

–

-

```
<?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>
```

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

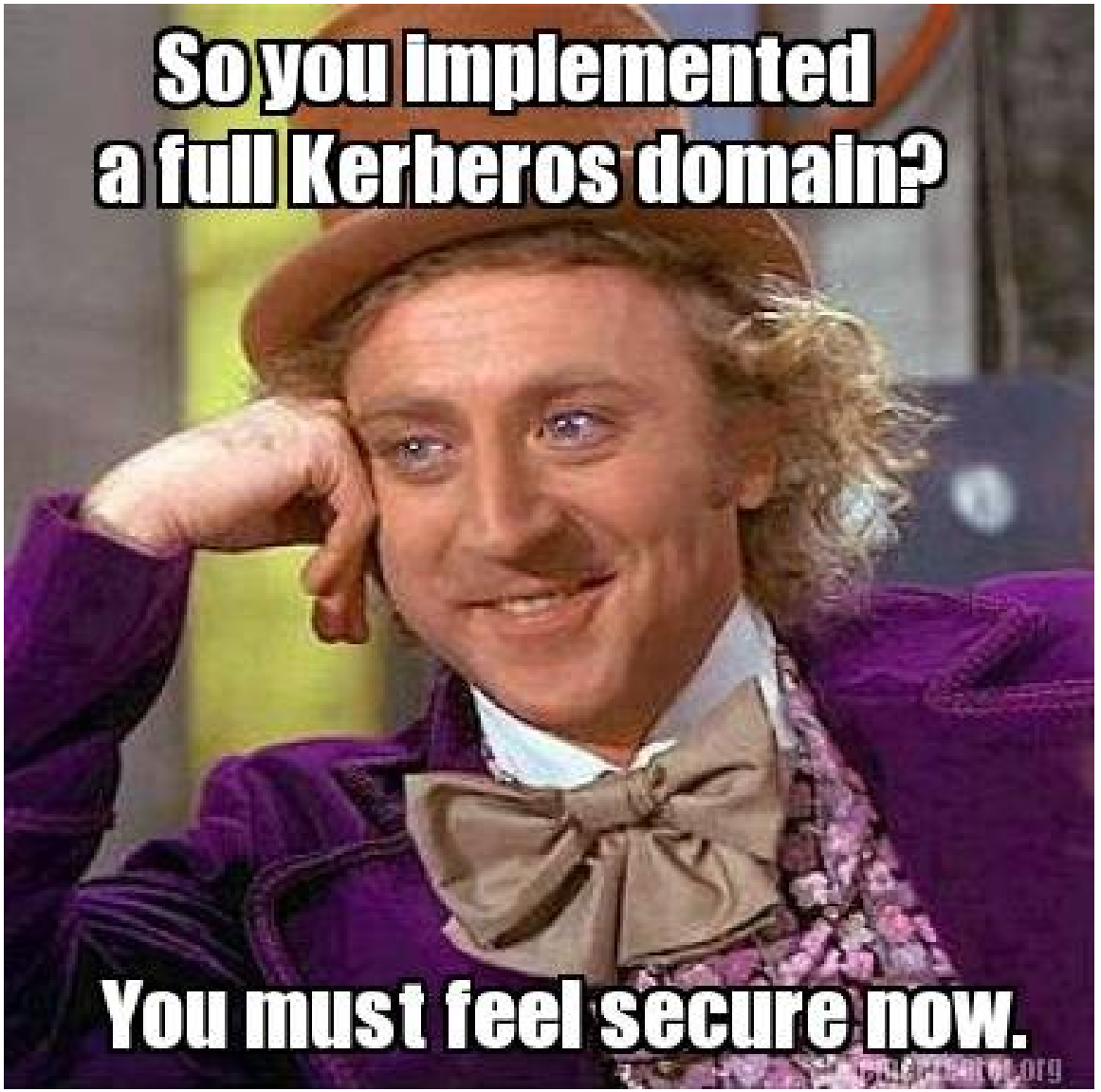
2.2.1.1.4 Password Encryption

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


So you implemented
a full Kerberos domain?
You must feel secure now.

Demo Time

Credential Storage in Groups.xml

Blue Team Response

- Detection:
  - 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)
- Then extract the Hashes from NTDS file and Start cracking the hashes....

Demo Time

Extracting NTDS.dit and Cracking Hashes

Blue Team Response

- Detection: Difficult
- Mitigation:
  - Protect DC backups & storage
  - Protect admin credentials
  - Admins only logon to specific systems
  - Limit Service Account rights/permissions
  - Set all admin accounts to “sensitive & cannot be delegated”

Thank You