Active Directory Attacks and Detection Part -II

#Whoami

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

Key Takeaways

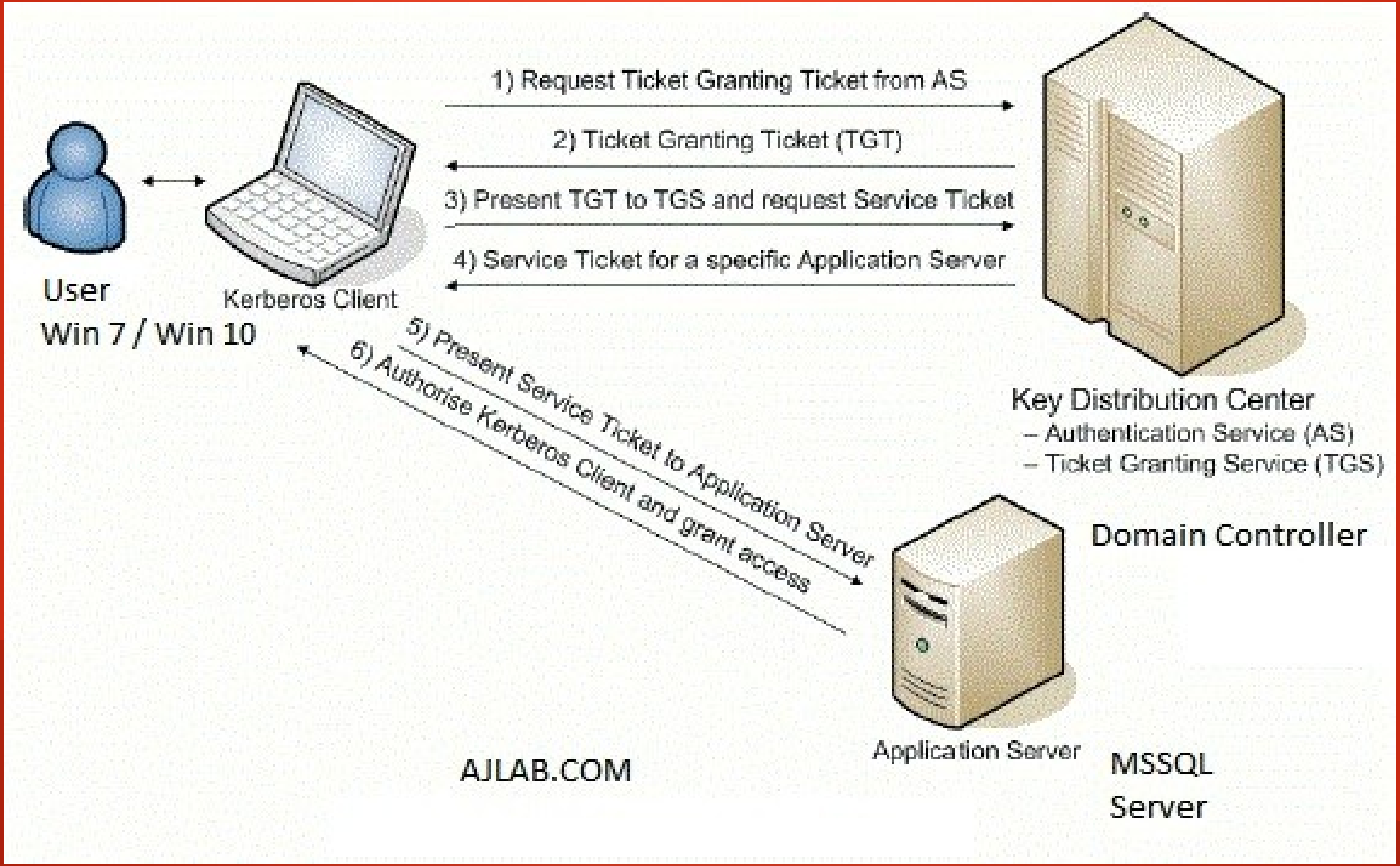
- How to abuse Three headed dog (Kerberos)
- Pass the Ticket and over Pass the Hash
- How to impersonate as a Domain Controller
- Zero to Hero(Domain Admin user) in 5 Minutes
- How to add Memes strategically in the Deck

Lab Setup

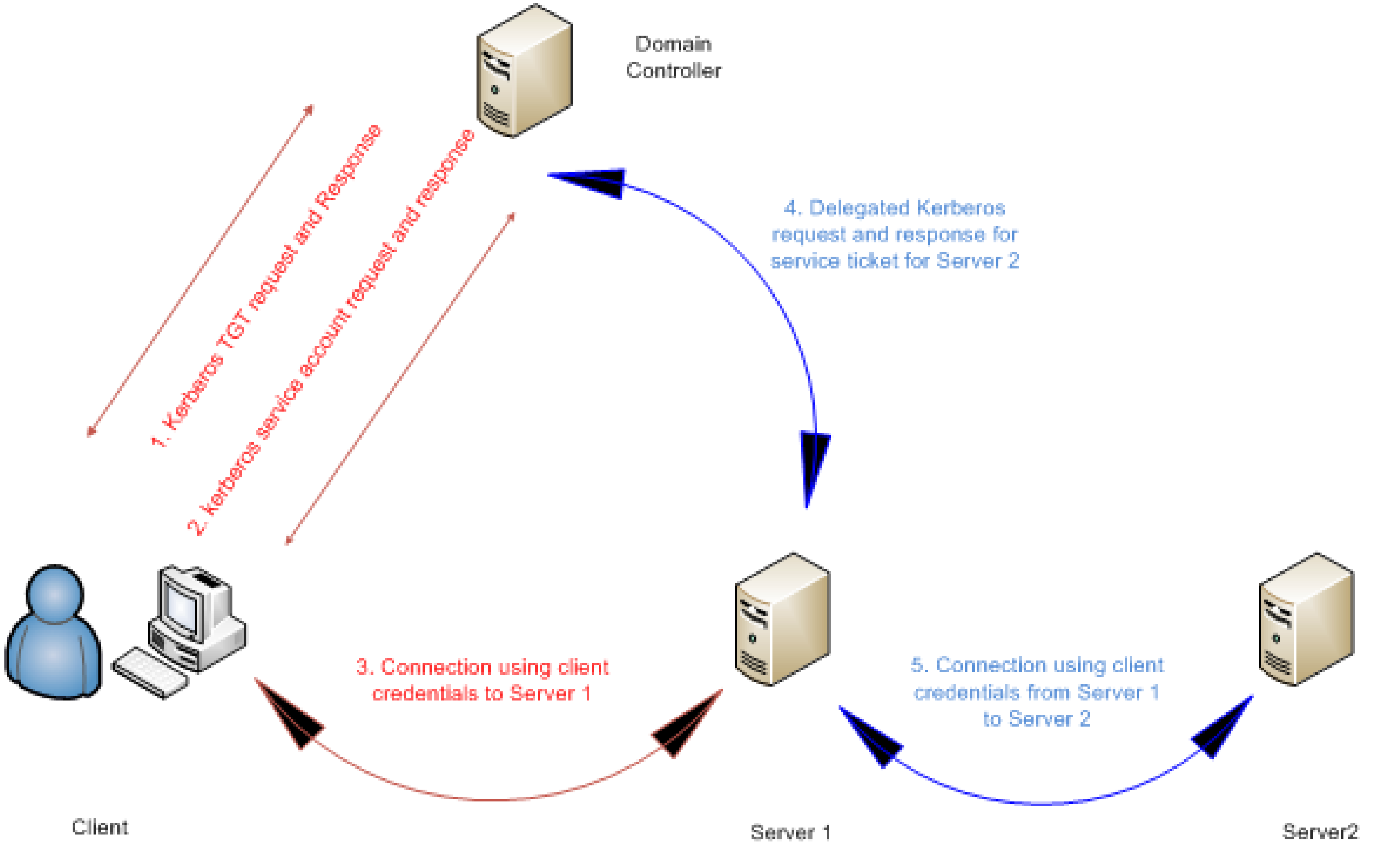
- AJLAB.COM:
- 2 Domain Controller – Win 2008 & Win 2012 r2
- 1 MSSQL Server – Running on Win2012 r2
- Win7,Win10 – Workstation Machines
- PFSense used as gateway(Just in Case Internet is required)

  * The lab setup remains the same.

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
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

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

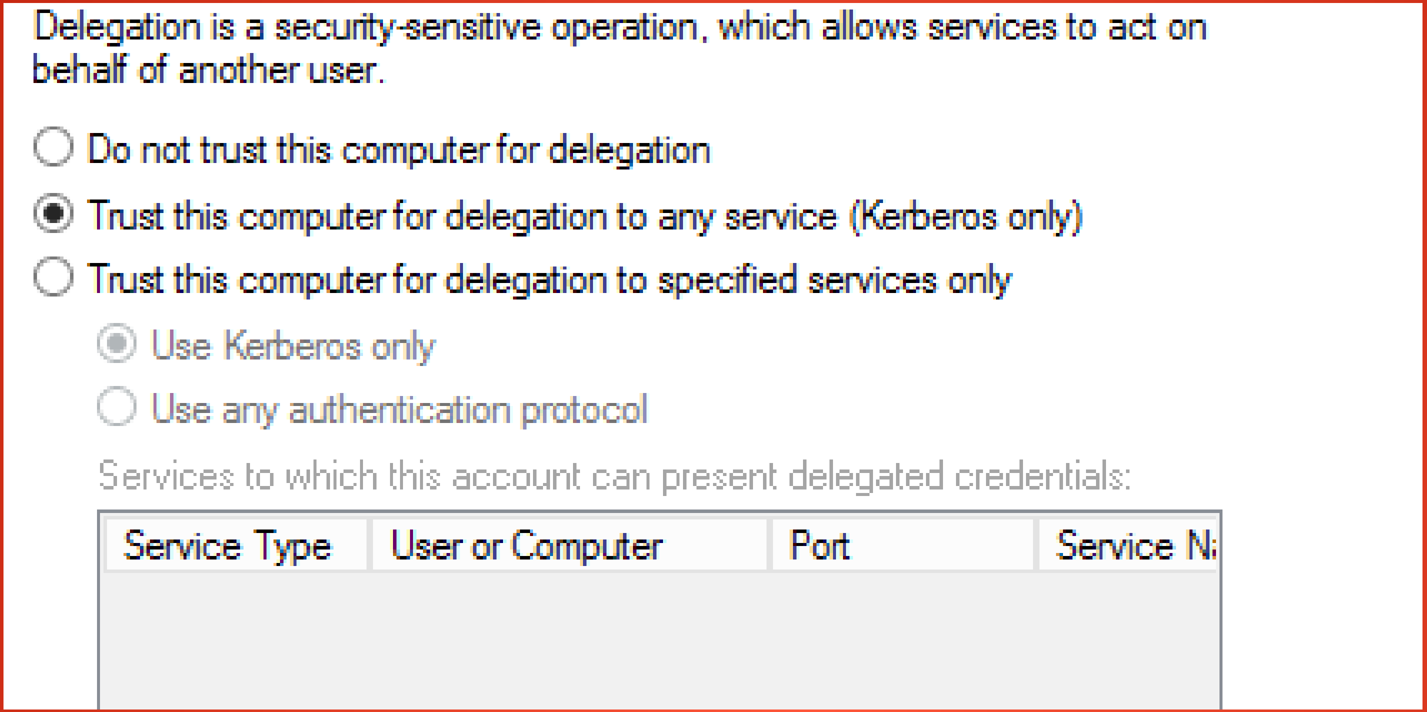
Client

Server 1

Server2

Kerberos Double Hop

- 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

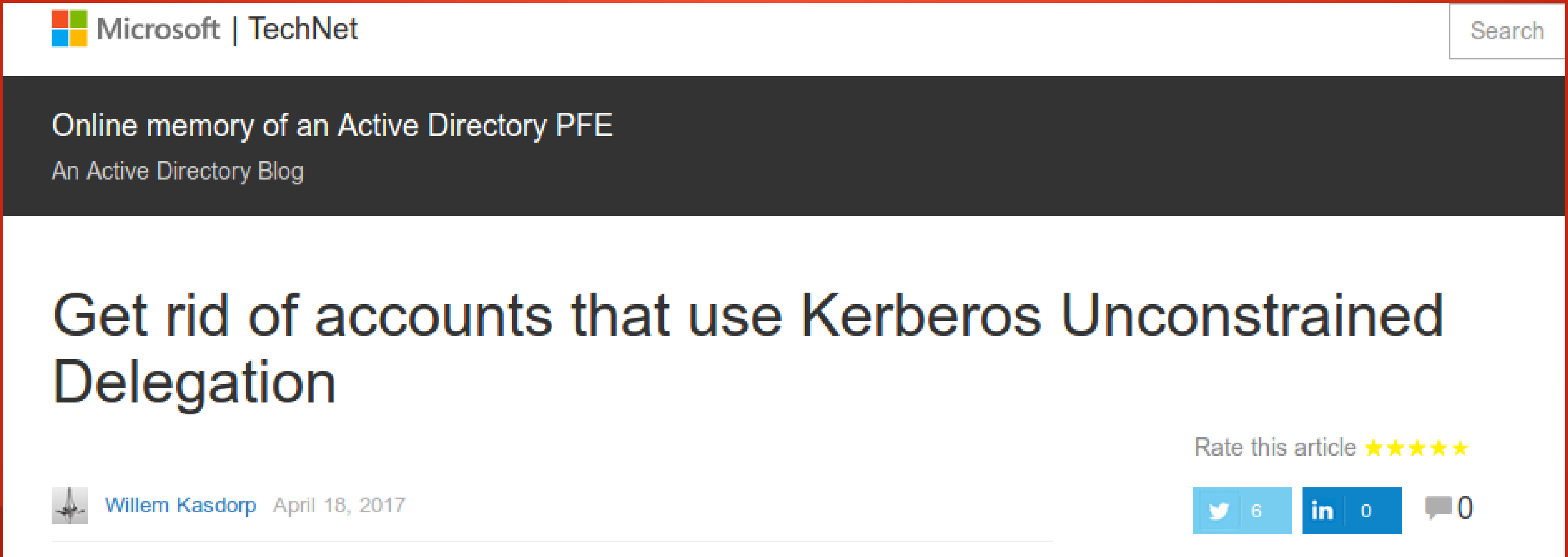
Services to which this account can present delegated credentials:

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

Blue Team Response



Microsoft | TechNet

Search

Online memory of an Active Directory PFE

An Active Directory Blog

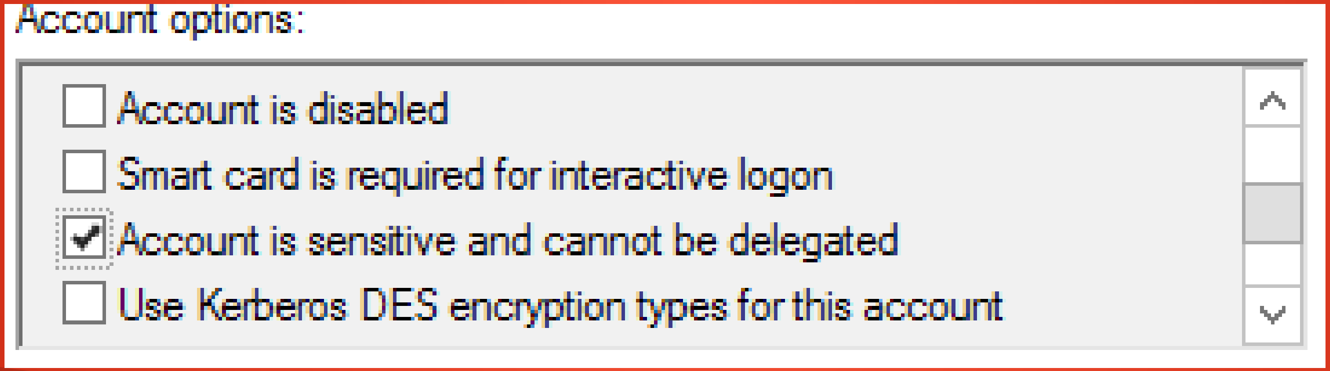
Get rid of accounts that use Kerberos Unconstrained Delegation

Rate this article ★★★★★

Willem Kasdorp April 18, 2017

Blue Team Response

- Don’t use Kerberos with Unconstrained Delegation, Instead 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.

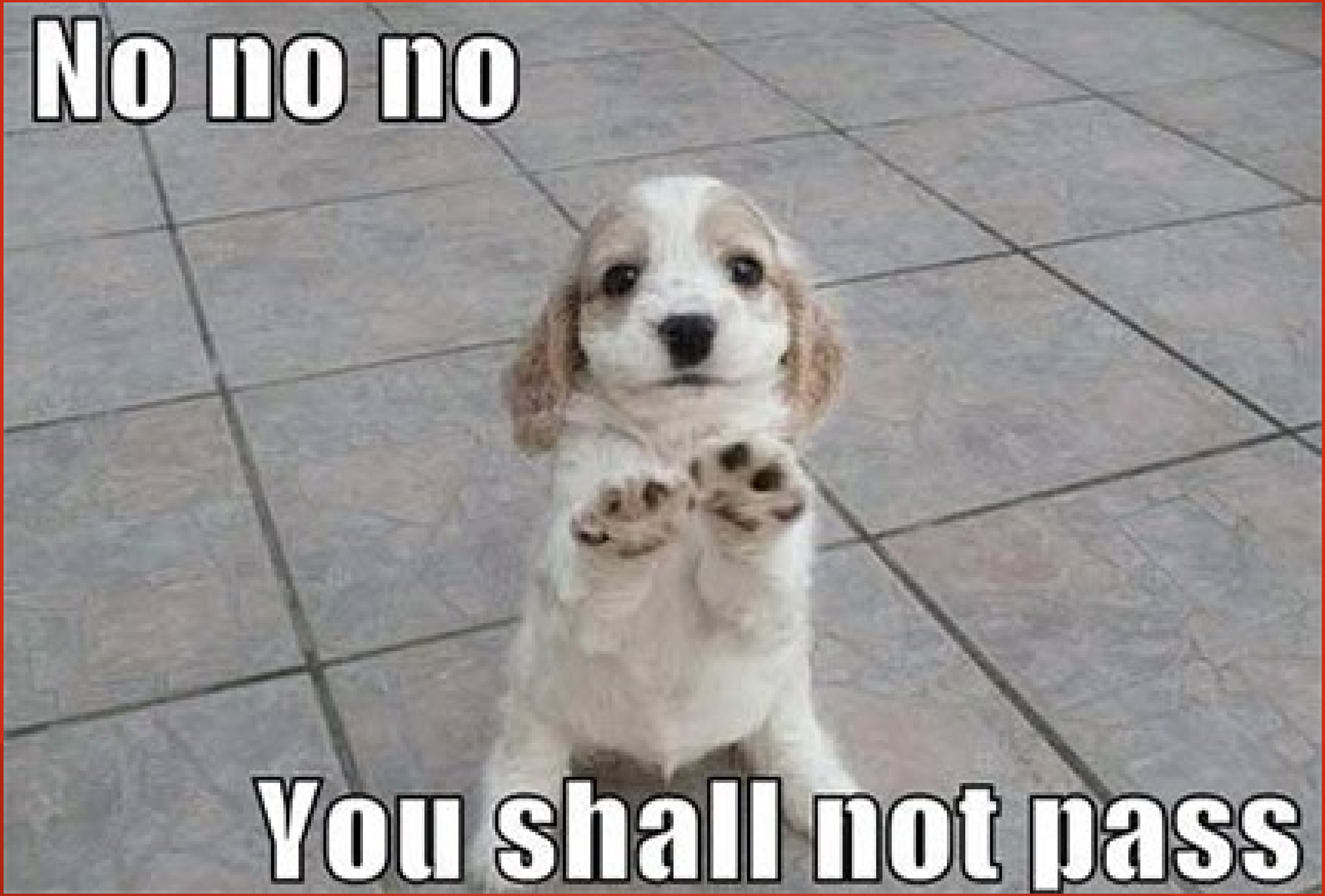
- What is Pass the Ticket (PtT) ?

  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>>
```


No no no
You shall not pass

Demo Time

Blue Team Response

- Detection: Difficult
- 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.
  - Set all admin accounts to “sensitive & cannot be delegated” .

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

Demo Time

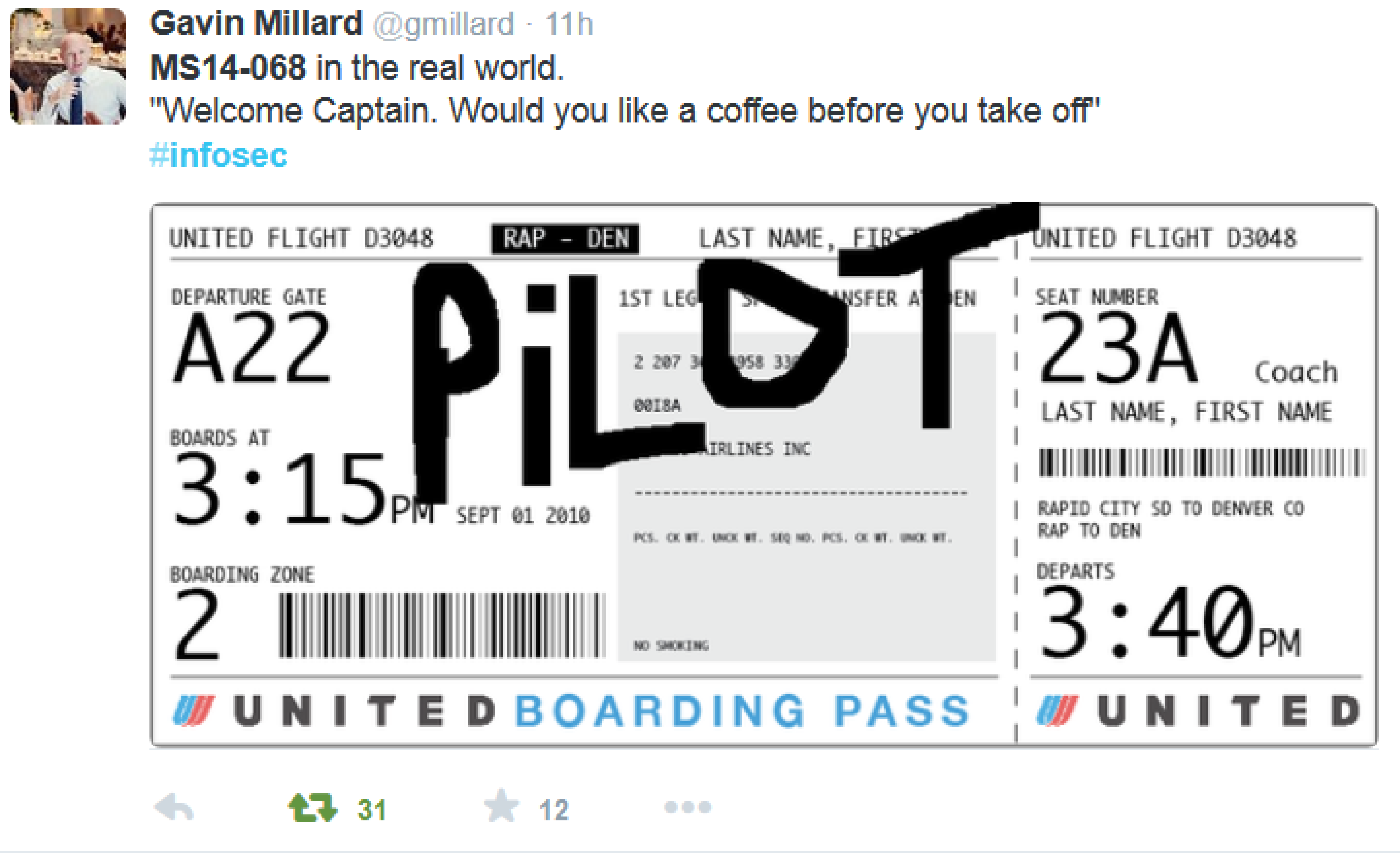
Blue Team Response

- Identify all Domain Controller IP addresses and add to “Replication Allow List”.
- 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

UNITED FLIGHT D3048 RAP - DEN LAST NAME, FIRS

PILOT

DEPARTURE GATE
A22

BOARDS AT
3:15PM SEPT 01 2010

BOARDING ZONE
2

1ST LEG NSFER A EN

2 207 3 958 33

00I8A

AIRLINES INC

PCS. CK WT. UNCK WT. SEQ NO. PCS. CK WT. UNCK WT.

NO SMOKING

UNITED BOARDING PASS

UNITED FLIGHT D3048

SEAT NUMBER
23A Coach

LAST NAME, FIRST NAME

RAPID CITY SD TO DENVER CO
RAP TO DEN

DEPARTS
3:40PM

UNITED

Demo Time

Blue Team Response

- Detection:
  - IDS Signature for Kerberos AS-REQ and TGS-REQ both containing “include PAC: False”
- Mitigation:
  - Patch all the Domain controllers with KB3011780

References

- adsecurity.org
- blog.gentilkiwi.com/mimikatz
- msdn.microsoft.com/en-us/library/cc228532.aspx
- Google.com (everything else)

Thank You