Is This My Domain Controller

A New Class of Active Directory Protocol Injection Attacks

About Us

Sagi Sheinfeld (@sagish1233)

- Senior Engineer @CrowdStrike (Former @Preempt)
- Previously Presented At DEFCON

Eyal Karni (@eyal_karni)

- Senior Engineer @CrowdStrike (Former @Preempt)
- Previously presented on Black Hat, DEFCON

Yaron Zinar (@YaronZi)

- Sr. Manager, Engineering @CrowdStrike (Former @Preempt)
- 2xDEFCON, 3xBlack Hat (completing the series…)

Today's Talk

A Technique called ***DC injection*** (Kerberos And NTLM)

The Plan

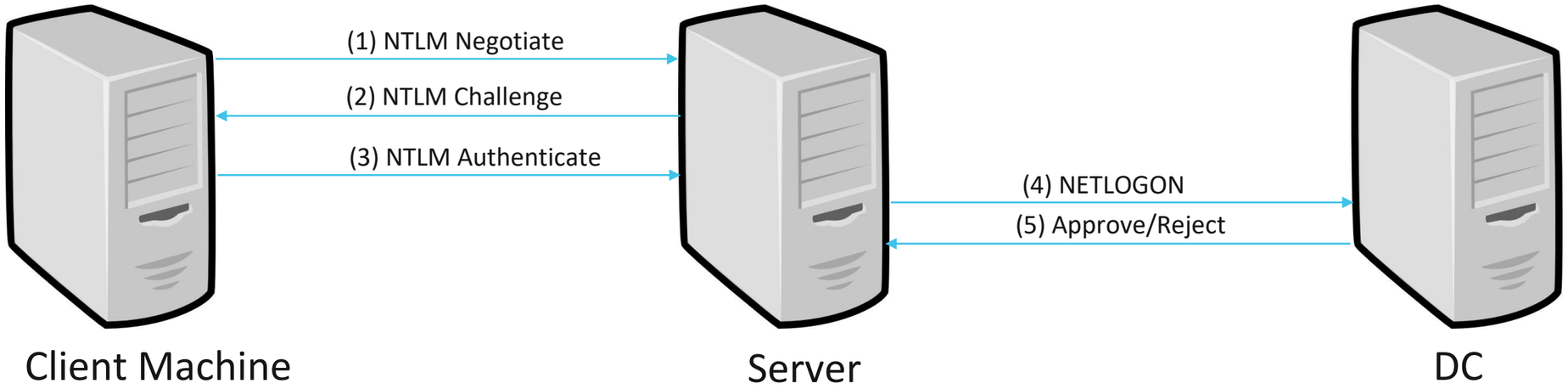
NTLM Part

- Intro
- Vulnerabilities and Mitigations
- Demonstration of DC injection (1 case)

Kerberos Part

- Intro
- Vulnerabilities and Mitigations
- Demonstration of DC injection (3 cases)

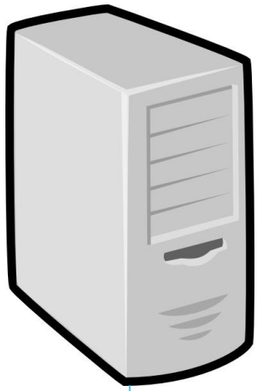
NTLM Basics



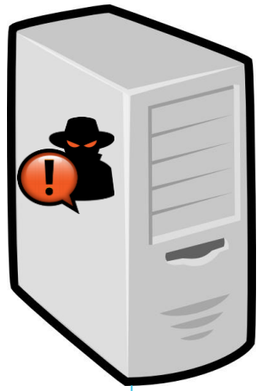
NTLM Injection

The client has some difficulty to match the identity of the excepted server with the identity of the server

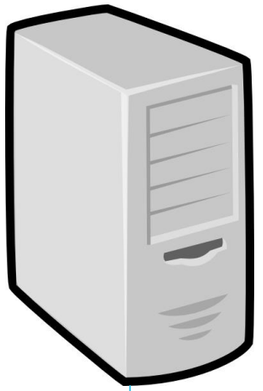
A MITM server can answer the NTLM request directly as if it were the original server



Client Machine



Rogue Server



Server

(1) NTLM Negotiate

(2) NTLM Challenge

Target name: Rogue Server

No Verification

(3) NTLM Authenticate

(4) NetLogonSamLogon Request

DC accepts request since Target is **Rogue Server**

(5) NetLogonSamLogon Response

Contains: session key

(6) accept-complete

(7) Some request (LDAP, DCERPC,…)

(8) Rouge Response

NTLM Injection Vs NTLM Relay

NTLM Injection

- Attacking the client
- Need an AD account

NTLM Relay

- Attacking the server
- Only MITM is required (not controlling anything)

NTLM Injection Example – GPO Update

- MS15-011 targets GPO update using LDAP or SMB
  - discovered by Luke Jennings (@jukelennings)

- Leads to remote code execution

MS Fixes for MS15-011

- GPO retreival can no longer operate with NTLM
  - Control by specific registry key

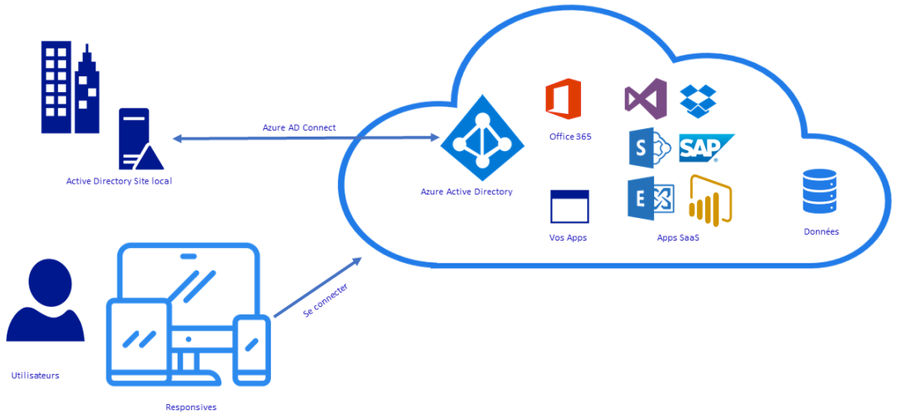
- Hardened UNC Paths
  - Configuration to block NTLM usage in SMB
  - Default registry values (regular expressions):

    ***\SYSVOL**

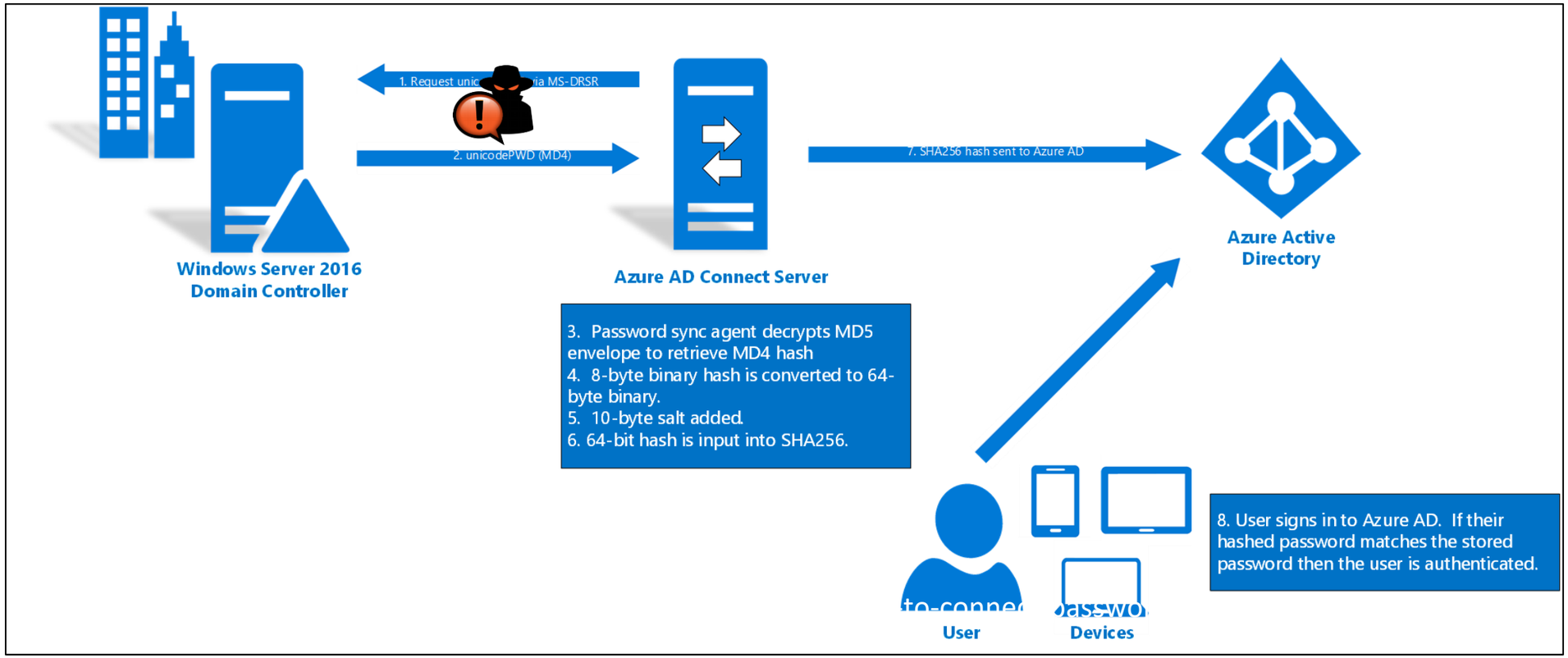
    ***\NETLOGON**

New Attack Case - Azure AD Connect

- Seamless sign-on
- Use AD Identity on Cloud
- Vulnerable to DC Injection (NTLM & Kerberos)



Azure AD Connect



NTLM Injection Against AD Connect

Attack Steps:

- Establish a full MITM between Azure AD Connect Server and the DC
- Make Kerberos fail while allowing LDAP to pass to the original DC
- Wait for domain replication (MS-RPC) and intervene:

  Inject a fake password change for an account of our choice

- Wait for Uploading to AAD
- Log in to Azure AD with the injected password ☺

Demo

Microsoft Response

Recommend blocking NTLM.

Status: Won’t fix.

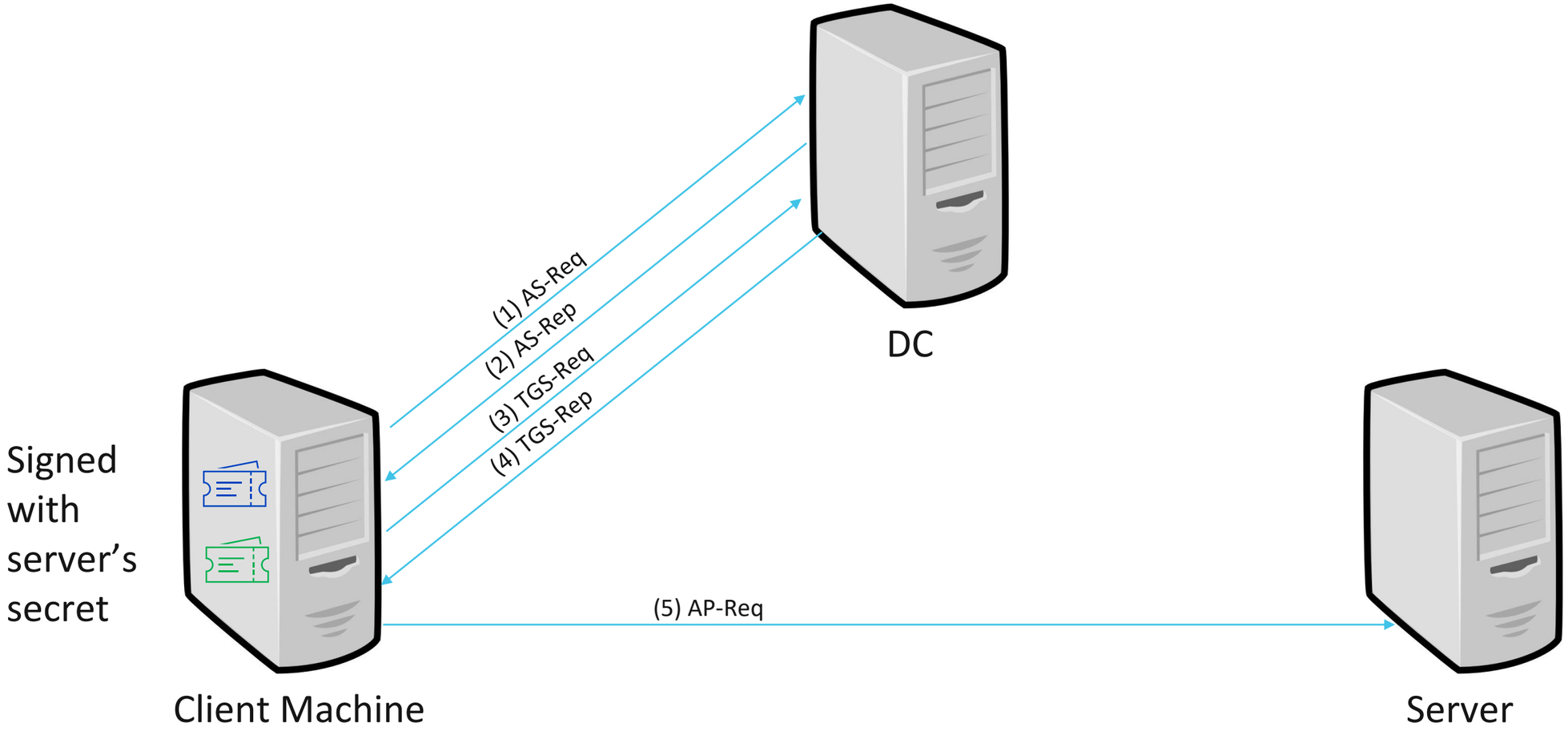
Harden your Azure AD Connect server

We recommend that you harden your Azure AD Connect server to decrease the security attack surface for this critical component of your IT environment. Following these recommendations will help to mitigate some security risks to your organization.

- Treat Azure AD Connect the same as a domain controller and other Tier 0 resources. For more information, see Active Directory administrative tier model.
- Restrict administrative access to the Azure AD Connect server to only domain administrators or other tightly controlled security groups.
- Create a dedicated account for all personnel with privileged access. Administrators shouldn't be browsing the web, checking their email, and doing day-to-day productivity tasks with highly privileged accounts.
- Follow the guidance provided in Securing privileged access.
- Deny use of NTLM authentication with the AADConnect server. Here are some ways to do this: Restricting NTLM on the AADConnect Server and Restricting NTLM on a domain

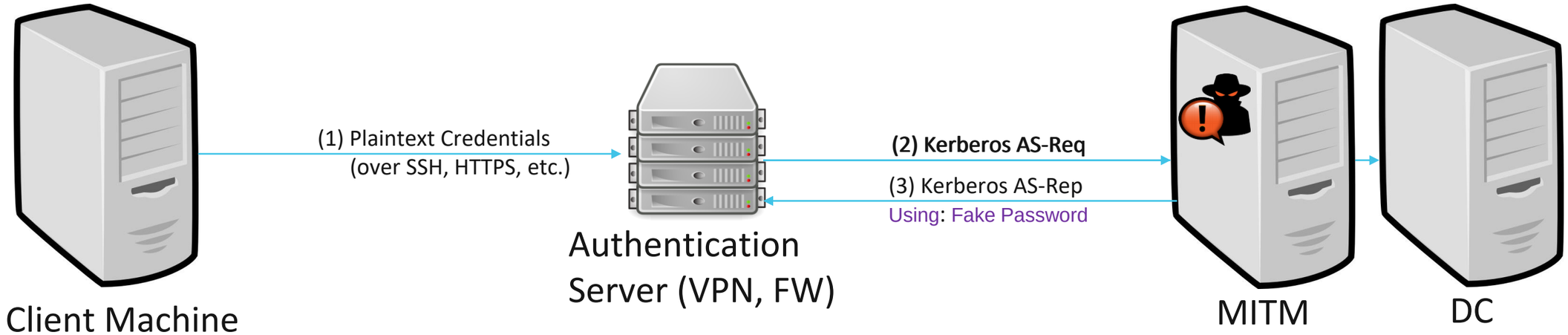
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites

Kerberos Basics



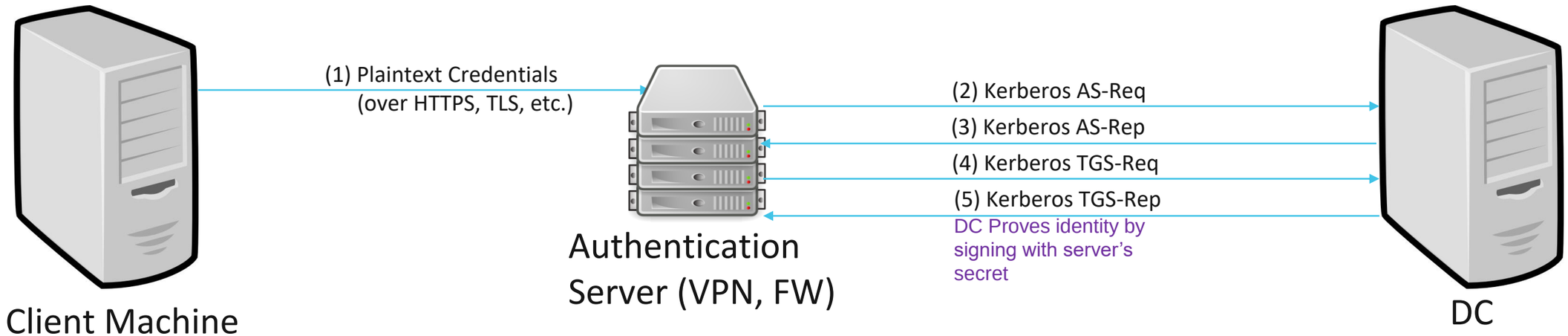
KDC Spoofing

- KDC Spoofing
  - Old Technique
  - Using MITM for authentication bypass
  - Typically exists in VPNs, FWs



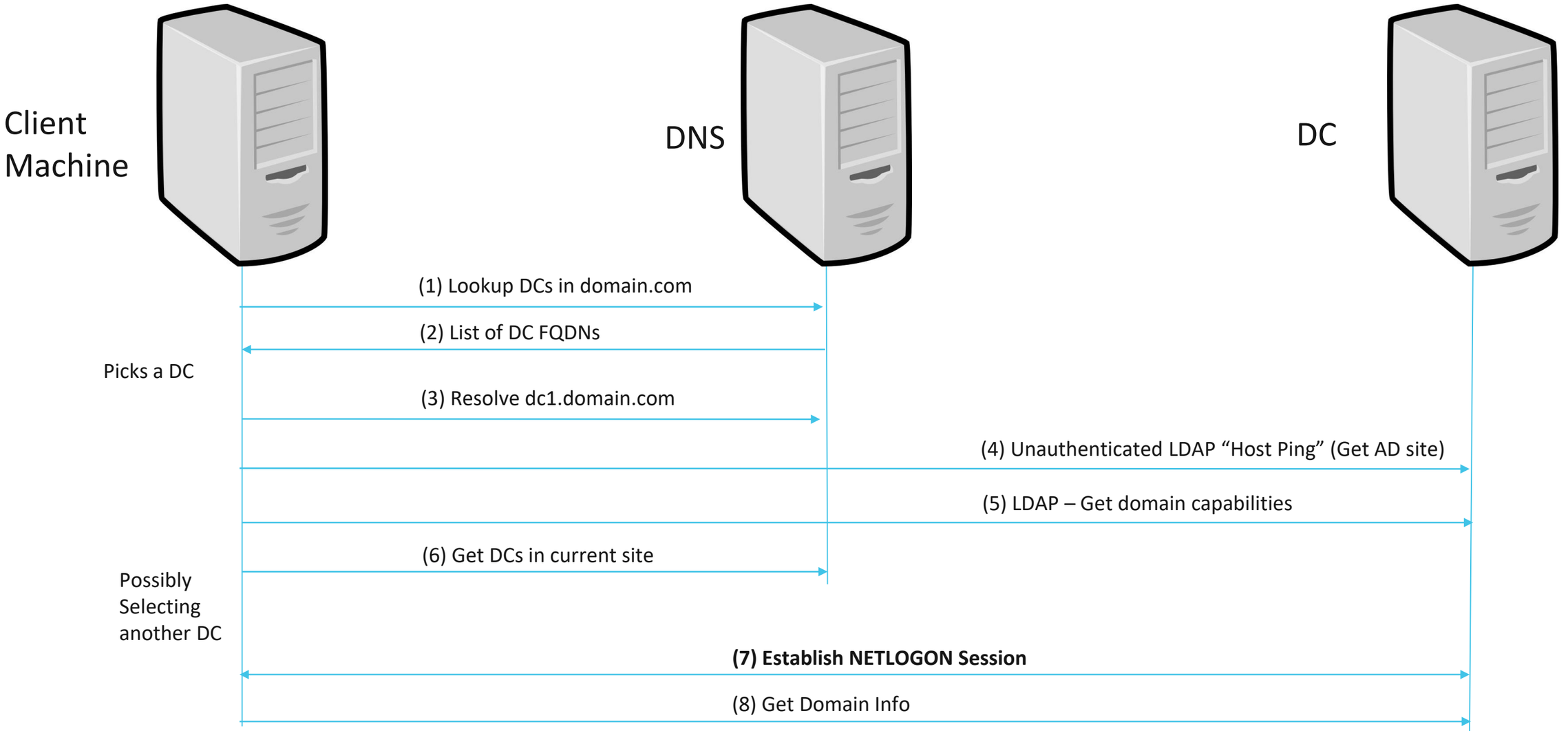
KDC Spoofing Protection

- **Very old technique**
- Protection
  - Create a computer account for authentication server
  - Create a TGS ticket to self using TGT



Kerberos Injection

So, we cannot manipulate TGT and TGS, what now?



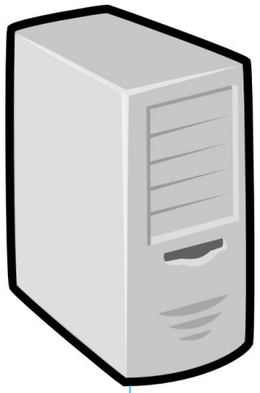
Kerberos Injection

The DC Selection process is not protected by default!

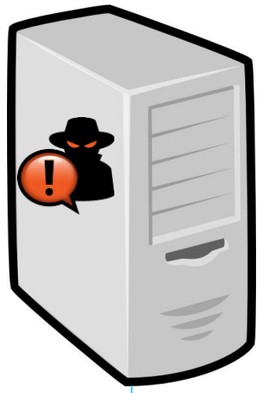
(As long as NETLOGON secure channel is not required)

So….

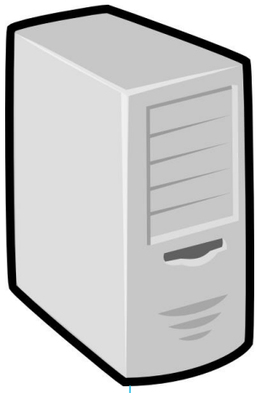
1. We convince the client to talk to a different machine that we own
2. We relay Kerberos to the real DC
3. The client asks to talk to the DC (Fake DC)
4. We are able to serve subsequent requests



Client Machine



Rogue Server



DC

(1) DC Selection Process

(2) Injected DC

Using: Rogue Server

(3) Kerberos AS-Req

(4) Kerberos AS-Req

(6) Kerberos AS-Rep

(5) Kerberos AS-Rep

(7) Kerberos TGS-Req

(8) Kerberos TGS-Req

(10) Kerberos TGS-Rep

Signing with client secret

(9) Kerberos TGS-Rep

Signing with client secret

(11) Kerberos TGS-Req (LDAP)

(12) Kerberos TGS-Req

(14) Kerberos TGS-Rep

Signing with Rogue server's secret

(13) Kerberos TGS-Rep

Signing with Rogue server's secret

(15) LDAP Search

(16) LDAP Search Response

Malicious injected data

What we need for the attack

- An application that:
  - Uses Kerberos (the usual case…)
  - Ingests data from DC without certificate/netlogon validation (the usual case…)
  - Does not have a fixed DC configured (the usual case…)
  - MITM between the server/endpoint and the DC

- Ability to register the needed SPNs on a machine (ms-DSMachineAccountQuota)

#1 – Azure AD Connect

- AAD Connect is exploitable to our Kerberos injection attack
- Same attack scenario – injecting a known password
- AAD Connect uses the following SPNs:
  - ldap/DC/Domain (e.g., ldap/dc01.contoso.com/contoso.com)
  - E3514235-4B06-11D1-AB04-00C04FC2DCD2/GUID/Domain

#1 – Azure AD Connect

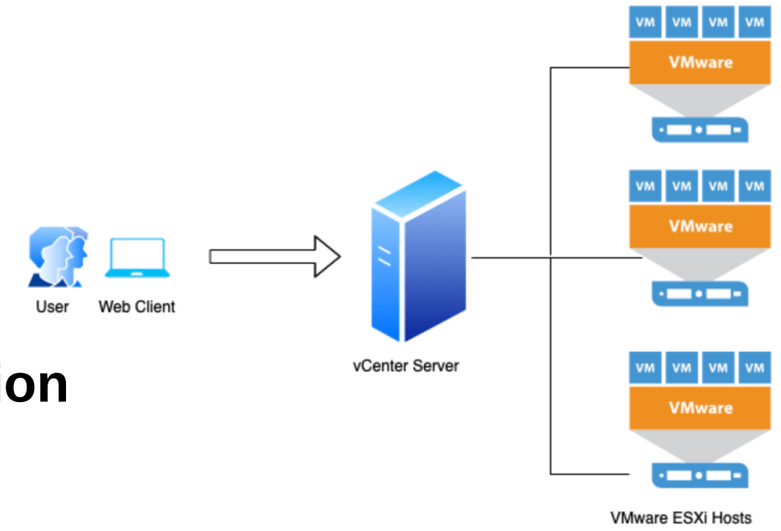
- Can we write these SPNs?
  - Not with ms-DS-MachineAccountQuota created machines
  - Attacker needs a **full control ACL** over at least one AD account

- This makes attack scenario more difficult…

#2 – VMWare vCenter

vCenter

- Centralize configuration of ESX servers and the virtual machines
- Supports windows authentication
- Allows configuring privileges via AD security groups
- **Vulnerable to DC injection resulting in privilege escalation**



Attack Scenario

1. Register the SPN (LDAP) and establish MITM
2. Login with an unprivileged account
3. vCenter will authenticate the user with the standard Kerberos flow
4. When assessing privileges vCenter will use LDAP to translate group names to RIDs, which we manipulate
5. Gain admin privileges

Demo

#3 – BeyondTrust ADBridge

ADBridge

- Enables domain-join of Mac/Linux machines
- Allows configuring privileges (e.g, SUDOers) via AD security groups
- **Vulnerable to DC injection resulting in privilege escalation**

Attack Scenario

1. Register the SPN (LDAP) and establish MITM
2. SSH with an unprivileged account
3. ADBridge will authenticate the user with the standard Kerberos flow
4. When assessing privileges ADBridge will use LDAP to translate group names to RIDs, which we manipulate
5. Gain sudo privileges

Demo

Kerberos Injection – How to Mitigate?

- Authenticate DC
  - Establish a NETLOGON channel and sending at least one message over it
  - Use LDAPS with certificate validation
  - Use Kerberos Armoring (we have not tested this…)
- Windows GPO is still safe…

Responsible Disclosure

Azure AD

NTLM Injection - Microsoft have issued a guidance on how to disabled NTLM for AADConnect service account

Kerberos Injection(CVE-2021-36949) - Microsoft has issued CVE-2021-36949 which fixed the issue

BeyondTrust ADBridge (CVE-2021-36757)

BeyondTrust has acknowledged the issue and are working on a fix

VMWare vCenter

VMWare has acknowledged the issue, and are releasing a security advisory with recommended actions

Closing Remarks

- Securing Protocols from MITM is hard
- Kerberos is not validating DC identity properly
- GSS-API does not guarentee protection from MITM

Tips for Defenders

- Network Hardening
  - Enable server/client signing
  - Monitor and reduce NTLM traffic
  - Regularly patch software
  - Treat critical servers (e.g., AAD Connect) the same as DC
- Kerberos Injection
  - Monitor suspiciously registered SPNs
- Avoid being MITM'd… :P