Microsoft

Lateral movement

Threats targeting the hybrid & cloud identity platforms

External resources disclaimer

This material includes links to external publicly available articles, projects, and research papers which are provided to you as a convenience and for informational purposes only.

Microsoft bears no responsibility for the accuracy, legality, content or any other aspect of the external site. Use of external hyperlinks does not constitute an endorsement by Microsoft of the linked content.

The external content referenced in this document belongs exclusively to their respective author(s). Inclusion in this presentation does not grant you with any right on the external content. You must comply with the original source’s applicable policies.

How to use this document

Why this document?

This document is provided as a companion of the video lessons. Additional information is included here which would not fit the video format or would exaggeratedly lengthen the videos. As you are watching the videos, the instructor will point you to additional content in this document.

Structure

The structure of this slide deck follows the structure of the lessons. One slide deck is provided for each module. The slide deck has the same structure (naming of chapters and sections) as the associated video so that you can quickly jump to the slides of the lesson you are currently watching.

Foreword

This deck contains some design artefacts which all have their importance…

This sticky note icon is used to introduce the **abbreviation** of a concept or a technical word. Once the abbreviation has been introduced, the full version is no longer mentioned.

You will also find a list of all abbreviations at the end of the deck.

We were all young once. A section with this icon will tell you the **history** you might have missed by not working with the technology for the last 20 years.

Just because you are new does not mean you do not have to know how we got here!

Professor Useful will introduce some **tricky technical details** which might not seem relevant at first but could end up being really useful if you want to dig deeper in the technology.

This frame contains…

- Takeaways so important that we framed them

How to know the slide level

This deck contains 3 different content levels:

1. Regular level, the common slide
2. Advanced level, a slide with this indicator at the top left 

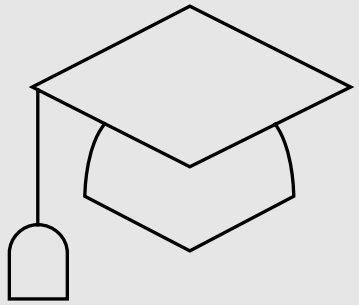
3. Additional content, all hidden slides

Sequence

4

Lateral movement

Learning Objectives



Describe the main components of an Azure AD environment integrated with AD

Agenda

1. Introduction to the lateral movement
2. Misusing the WDigest protocol to steal plaintext credentials
3. Pass-the-Hash Attacks (PtH)
4. Abusing the NTLM protocol
5. Pass-The-Ticket attacks
6. RDP session theft
7. Azure AD token attacks
8. Pivot from virtualization administrator to AD administrator
9. Abuse of Kerberos Delegation

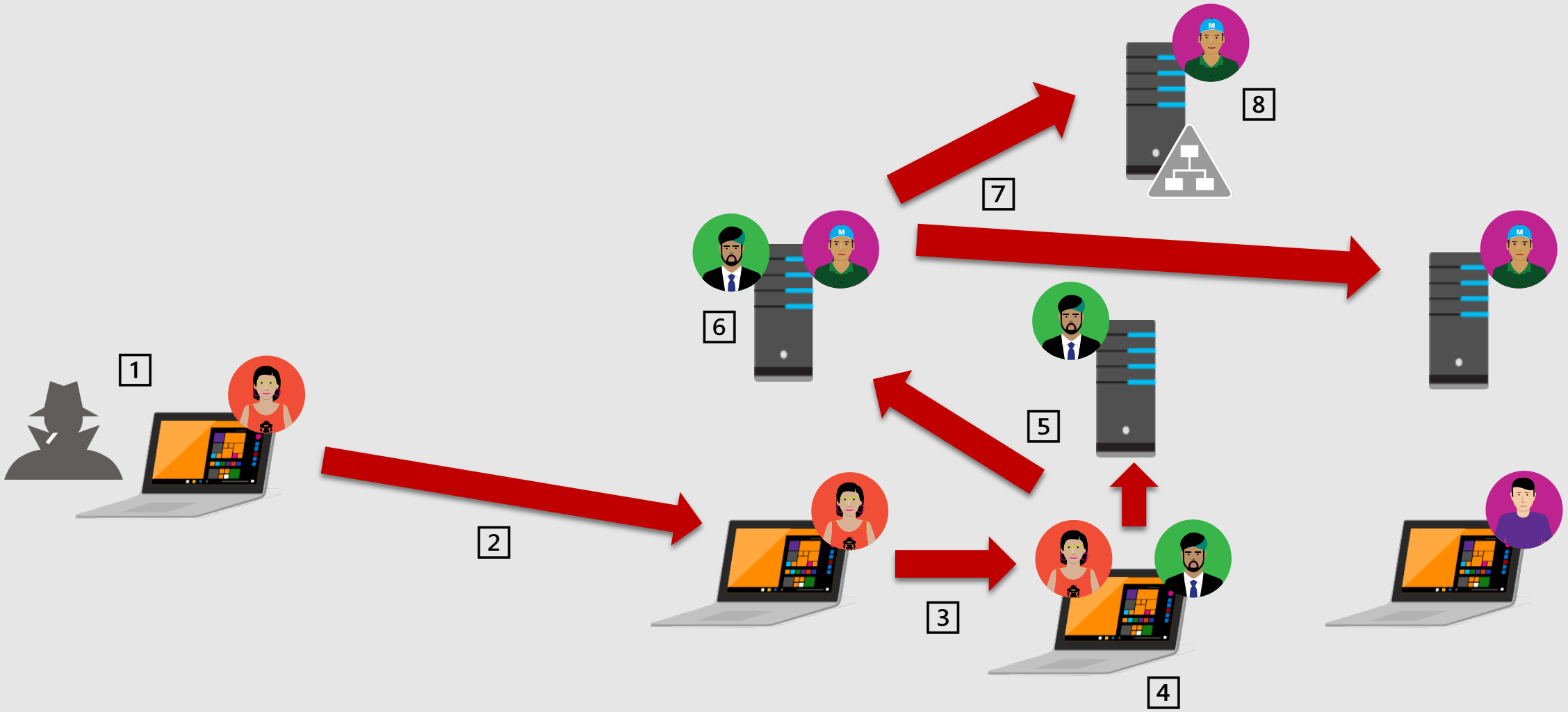
Chapter

2.4.1

Introduction to lateral movement

🎯 Explain the principles of lateral movement

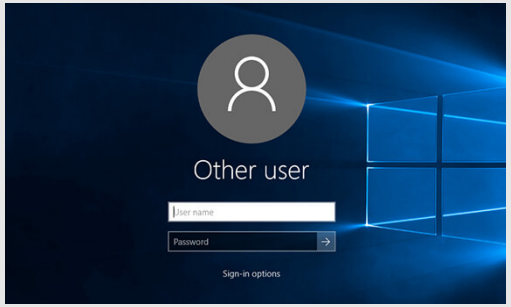
What is lateral movement?



Credential stealing

winlogon.exe

1



2

LSASS

3

Kerberos

NTLM

WDigest

...

SeDebugPrivilege

4

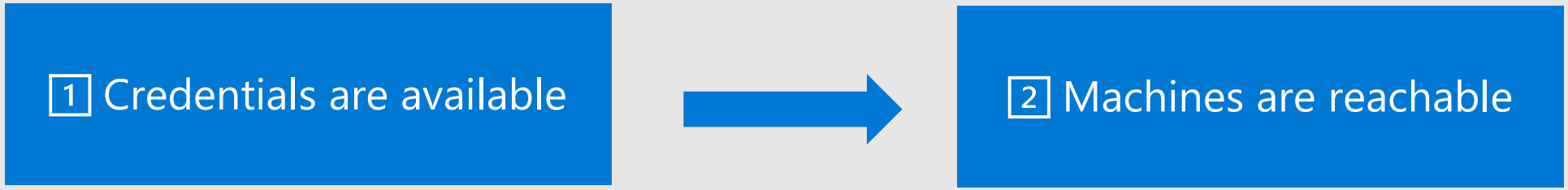
Credential stealing

- **SeDebugPrivilege** is required to steal credentials live from the memory

BUT If the attacker can perform a memory dump of LSASS using Windows built-in features, credential stealing tool can be used on the attackers' machine against the dump.

Monitor and/or block LSASS memory dumps

Reduce lateral movement

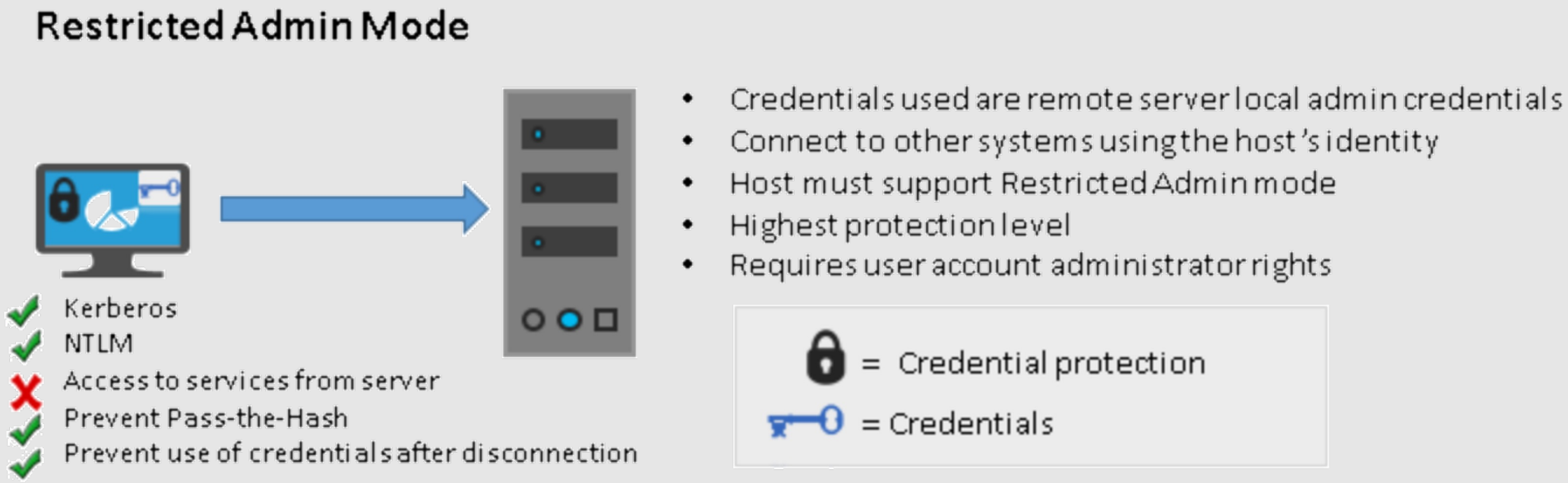


- Do not sign into systems where you shouldn't
- If you need to, do it in a way that doesn't cache credentials
- Make credentials harder to extract

- Different local accounts for administration
- Prevent users from accessing by policy
- Block peer to peer

A safer way to RDP

- mstsc.exe /restrictedadmin
- Needs to be enabled on the target
  - `HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin = 0x0`

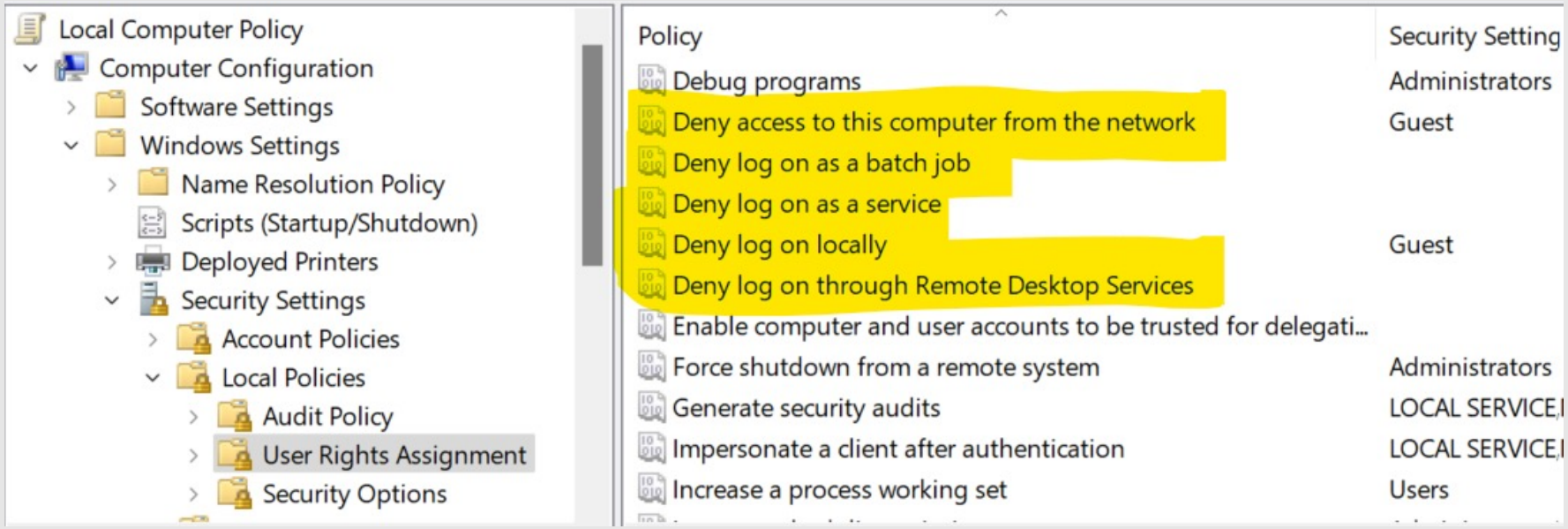


Restricted Admin Mode

- What does this security enhancement provide?
  - Once connected to a target in RestrictedAdmin mode
  - Power user will not be able to seamlessly access other network resources from that host
  - Re-provide of credential is required to access other network resources
  - Target and client must be Windows 8.1 and Windows Server 2012 R2 (Host and Client)
  - Supported Windows 7 and 2008 R2 can have this feature if they install update 2984972
- Users can use remote desktop without having to worry about exposing their credentials to a weaker/less secure system

User Right Assignments

- You can use group policies and the User Right Assignment section to restrict who can access a computer and how
- If sensitive accounts cannot log in on a machine, they cannot expose their credentials in memory



Adv.

Local account restrictions

You know the local admin's password? Well too bad you can't use it on the network

You can restrict how local accounts can be used

By limiting what privilege those principal have on a system

- User Right Assignment with the following two well-known SIDs:
  - S-1-5-113 – Local account
  - S-1-5-114 – Local account and member of Administrators group
- Can be deployed via GPOs

Local Administrator Password Solution

LAPS

- Deploy LAPS to have unique password for local Administrator (or similar solution)
- LAPS changes the local administrator password automatically

By default, every 30 days

Complex and random

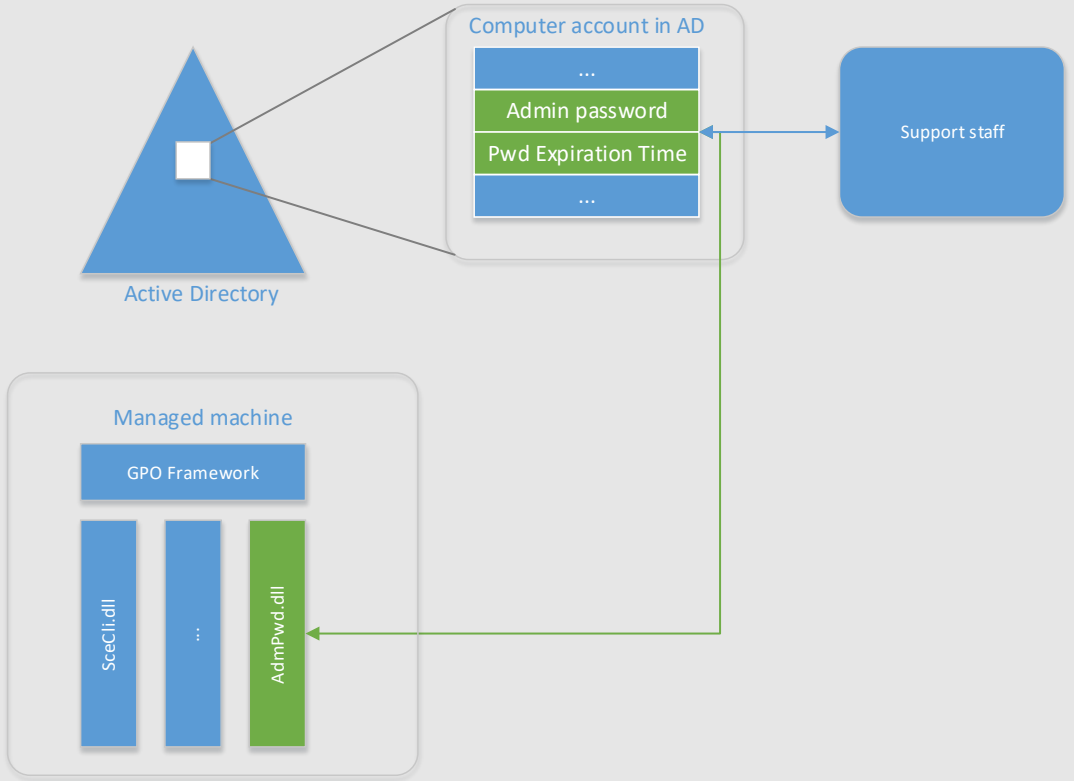
Store the new value in AD in a confidential attribute

Deploy a solution like LAPS on all member servers and workstations

- When all local passwords are different, the compromise of one system **does not lead** to the compromise of other systems

LAPS legacy architecture

- The ms-Mcs-AdmPwd attribute is confidential
  - It is not encrypted, it is protected by a DACL
  - By default, only the domain admins can read it
  - You need to create delegations for other teams
- LAPS also comes with a light GUI tool
  - But you can use any method you want to query the value of the password in AD



The Windows Firewall

P2P

- You can prevent lateral movement by blocking **p**eer-**to**-**p**eer traffic
  - Preventing RPC and SMB between workstations is a good start as it is often used by attackers to move laterally
  - Some client applications might require P2P (such as instant communication apps)

WDFAS

- You can use the built-in firewall
  - **W**indows **D**efender **F**irewall with **A**dvanced **S**ecurity
  - Configurable through GPO
  - Can create exceptions based on AD groups
  - Natively speaks IPSec

Restricting logon locations

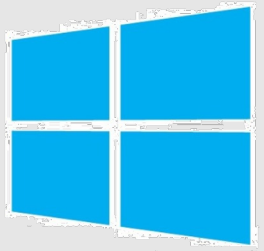
userWorkstations

▼

Group policy user right assignments

▼

Authentication policies



Restricting logon locations

- Authentication Policies can be used to limit where an account can be used
  - Domain admin accounts can be limited to login only on tier-0 assets
  - It requires Kerberos Armoring
  - It requires Windows Server 2012 R2 DFL
- Policies enable the following
  - Restrict user accounts to specific devices and hosts
  - Provide custom TGT lifetimes
  - Restrict service ticket issuance that is based on user account and security groups
  - Restrict service ticket issuance based on user claims or device account, security groups, or claims

Authentication Policies and Silos

- Authentication Policies can be used along with Authentication Policy Silos
  - Containers in which we group computers and users to facilitate Authentication Policies' deployment
- A user applying a policy cannot use NTLM
  - Unless you re-enable NTLM on the policy (Windows Server 2016)

Chapter

2.4.2

Misusing the WDigest protocol to steal plaintext credentials

🎯Disable the WDigest protocol from Windows machines

Once upon a time… WDigest

- Security Support Provider
- It’s old…
- No longer used
- And… Needs to store the secret in memory
- Disabled by default but…

  Can be re-enabled… And attackers do.

No more clear-text passwords

- Let's face it. Nobody uses it… Disable it!
  - For Windows Server 2012 R2/2016 Windows 8.1/10 it is already disabled
  - For the Windows 2008 R2/2012 Windows 7/8 it requires KB2871997 AND a registry modification
- Else… Attackers can use simple tools to retrieve the password

```
HKLM\System\CurrentControlSet\Control\SecurityProviders\Wdigest
 UseLogonCredential = dword:00000000
```

Enforce UseLogonCredential to 0 using Group Policies

Extract WDigest plain text password

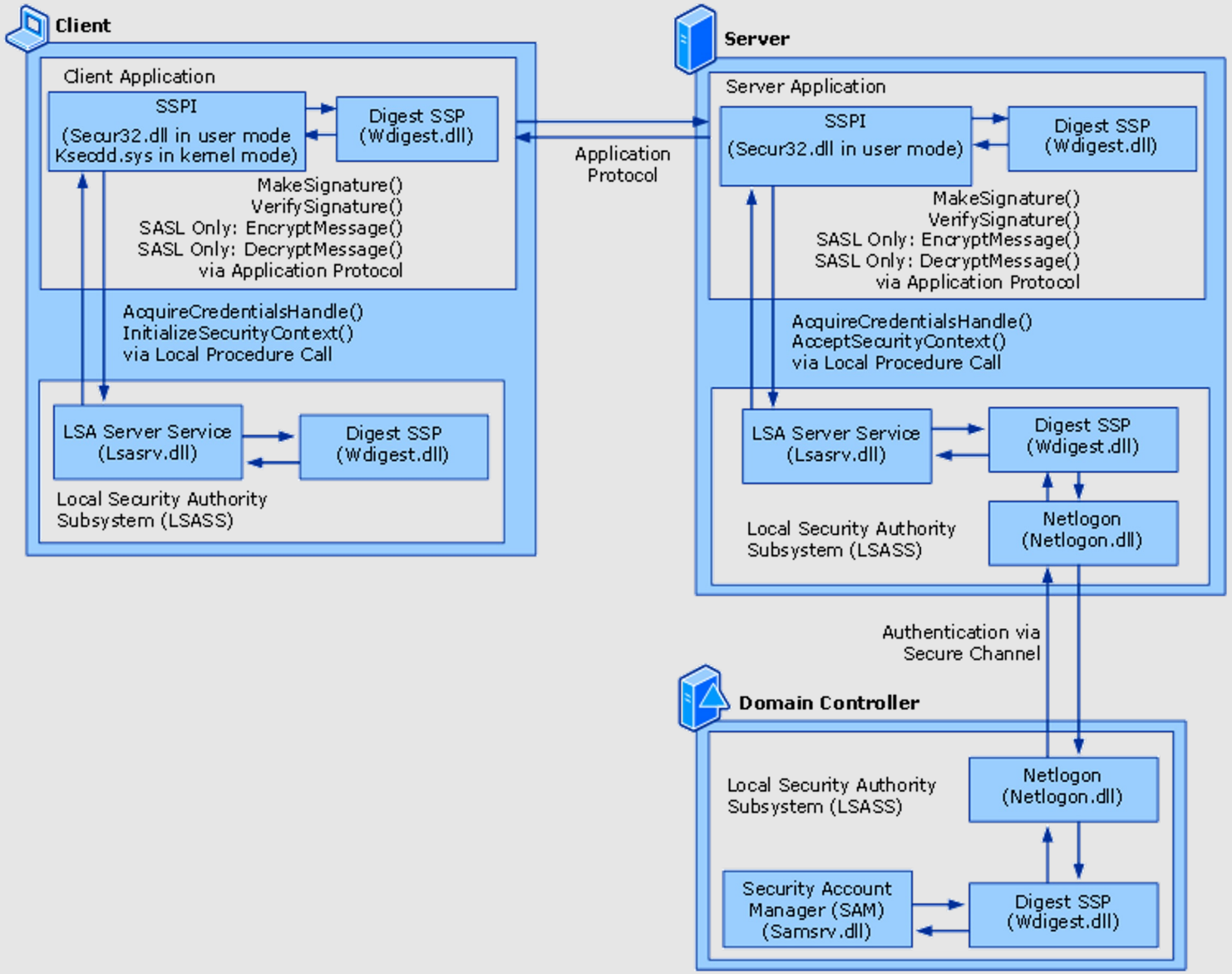
mimikatz

```
mimikatz
privilege::debug
sekurlsa::wdigest
```

Windows Credential Editor tool [1]

```
wce.exe -w
```

How Digest Authentication Works



WDigest abuse summary

Attack's pre-requisites

- WDigest is enabled
- A victim is connected to the system, or a service is running under a user account
- seDebugPrivilege, or LSASS memory dump

Protection

- Disable WDigest
- Enforce it through group policies

Chapter

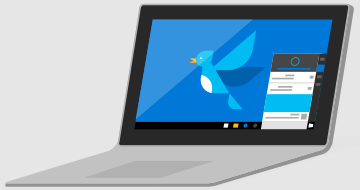
2.4.3

Pass-the-Hash Attacks (PtH)

🎯Describe Pass-the-Hash Attacks

New Technology Lan Manager

1 User
Alice



2 Server
File1

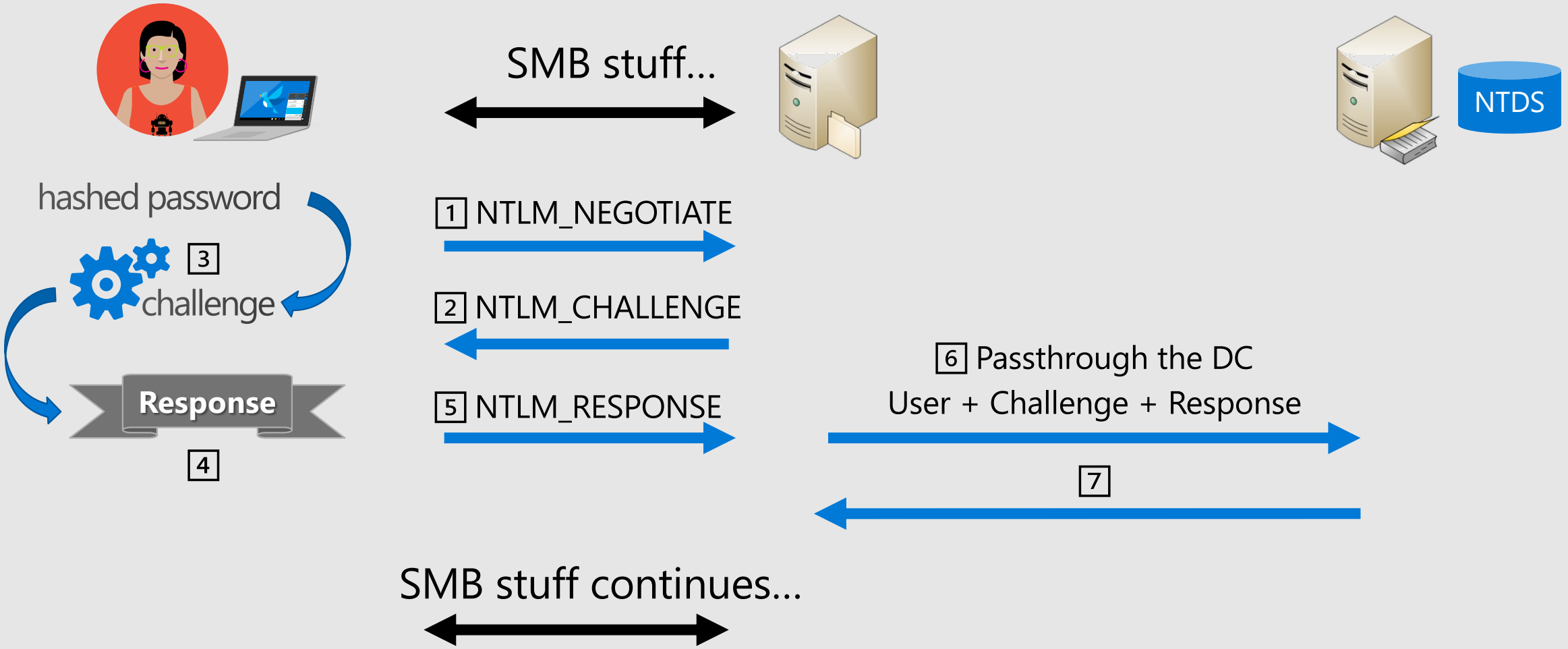
3 Domain Controller
DC1

Knows Alice

Stores Alice password's hash

NTDS

NTLM basic flow

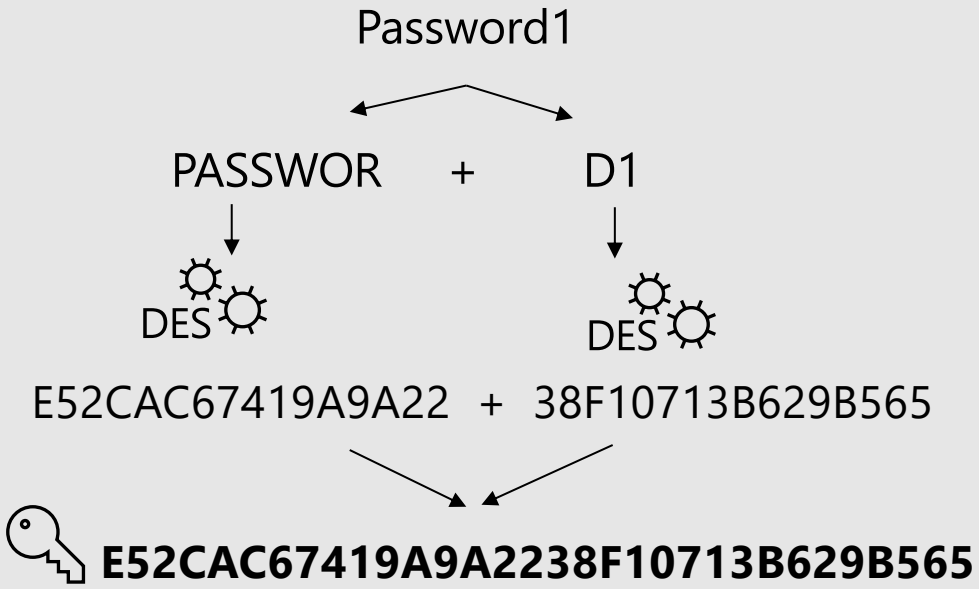


Hash generation

User's password: Password1

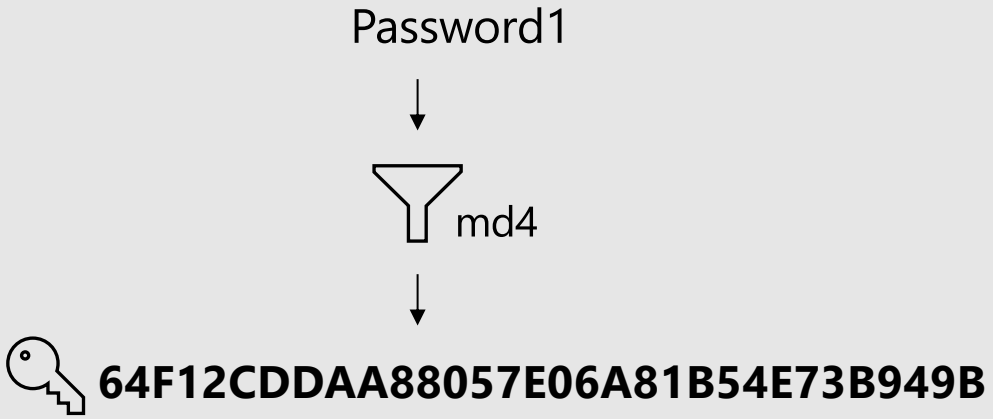
LMHash

LMHash (LM OWF)



NTHash

NTHash (NT OWF)



Note: One Way! You cannot find Password from Hash. True but if I use Rainbow Table?

Pass the NThash

- Extract the hash from the LSASS memory
  - This requires the seDebugPrivilege
  - Requires that the targeted identity has cached its credentials
- Inject the hash into your current session
  - Either locally, or later on other systems
  - The “new” hash is used to calculate NTLM responses
- Does not trigger any failed authentication attempts

This is possible because the hash is in the memory

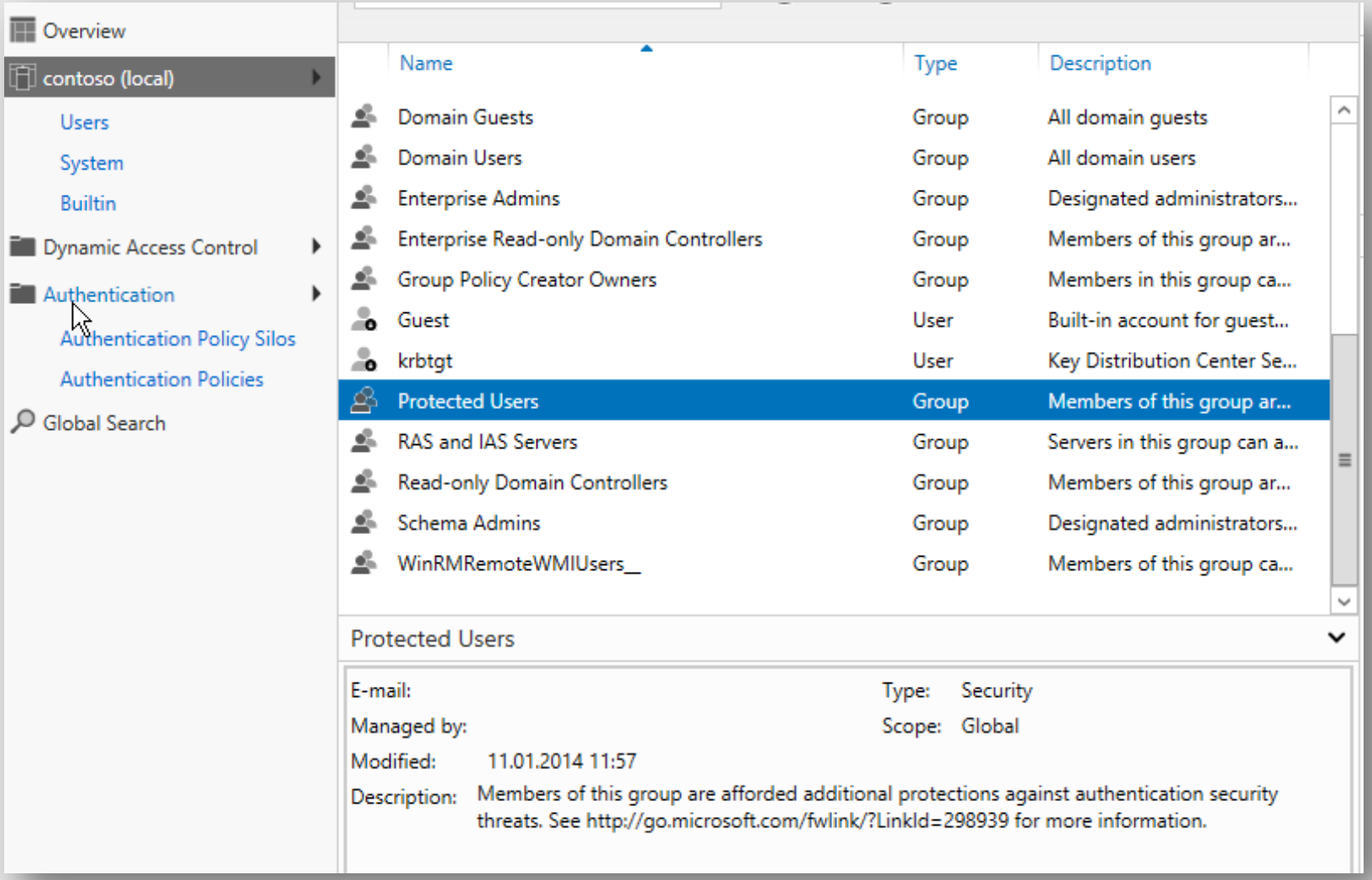
Needed for Single Sign-On

Protected Users Group

- New group arrived with Windows Server 2012 R2
  - Members of this group do not cache certain keys in LSASS memory
  - Additional protections with 2012 R2 DFL
  - Special event logs on the DCs to facilitate troubleshooting while implementing

Device Protections	Domain Protection (when DFL 2012R2)
Does not cache credentials when using CredSSP No wdigest cache No NT OWF cache No DES or RC4 for requests	Requires AES keys No NTLM No DES or RC4 No Kerberos delegation No TGT renewal

Protected Users Group



Pass-the-hash summary

Attack's pre-requisites

- A victim is connected to the system, or a service is running under a user account
- seDebugPrivilege, or LSASS memory dump

Protection

- Healthy administration practices (do not connect to untrusted systems with privileged accounts, use RDP restricted mode)
- Use the Protected Users group (for privileged accounts)
- Block NTLM on systems where it is not used (very difficult in large environments)

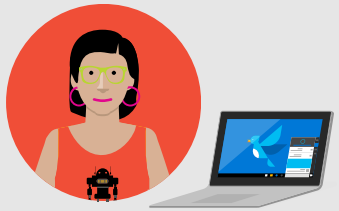
Chapter

2.4.4

Abusing the NTLM protocol

🎯Describe the NTLM relay attack

NTLM Relay Attack



I want in...

Challenge = 123

I want in...

Challenge = 123

Response = 456

Response = 456

SMB as 

NTLM Passthrough

✅ Alice

Mitigating

- Security settings to restrict MTLM usage


Network security: LAN Manager authentication level


Network security: Restrict NTLM: NTLM authentication in this domain


Network security: Restrict NTLM: Incoming NTLM traffic


Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers

Mitigating

- Enforce signing on the underlying protocols
  - Creates a dependency between the transport protocol and the authentication material
  - On all servers:
    - Microsoft network server: Digitally sign communications (always)
  - On domain controllers:
    - Domain controller: LDAP server signing requirements
    - Domain controller: LDAP server channel binding token requirements
  - On web services, enable HTTPS and Extended Protection

Adv.

LmCompatibilityLevel

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LmCompatibilityLevel

Client

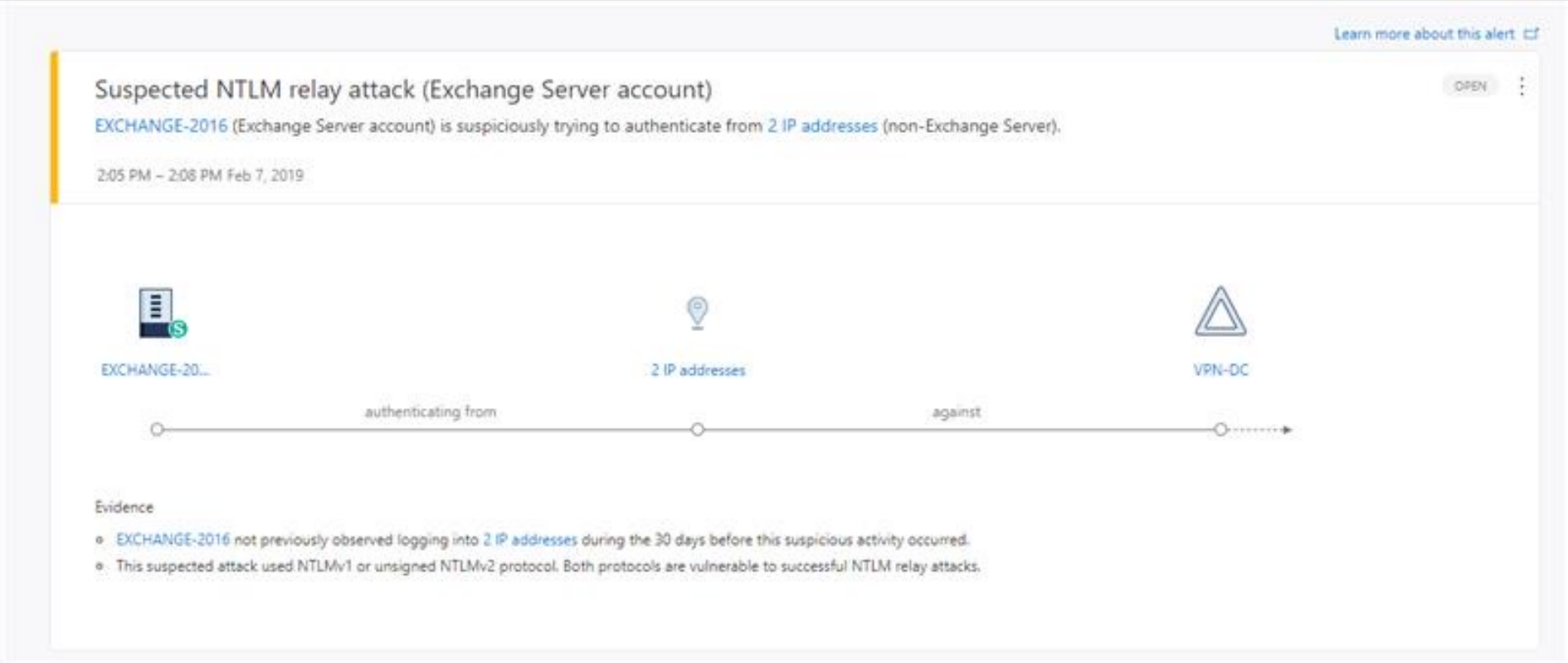
Level	Sends	Accepts	Prohibits Sending
0	LM, NTLM	LM, NTLM, NTLMv2	NTLMv2, Session security
1	LM, NTLM, Session security	LM, NTLM, NTLMv2	NTLMv2
2	NTLM, Session security	LM, NTLM, NTLMv2	LM and NTLMv2
3	NTLMv2, Session security	LM, NTLM, NTLMv2	LM and NTLM

Server

Level	Sends	Accepts	Prohibits Accepting
4	NTLMv2, Session security	NTLM, NTLMv2	LM
5	NTLMv2, Session security	NTLMv2	LM and NTLM

Detection

- Example of alerts from Microsoft Defender for Identity



NTLM relay attack summary

Attack's pre-requisites

- Coerce the victim to connect to a controlled server (could be done with name resolution spoofing, ARP spoofing, phishing, PetitPotam PoC…)
- Network connectivity to both the victim and the target

Protection

- Enforce LDAP signing
- Enforce LDAPs channel binding
- Enforce SMB signing
- Enforce HTTPs with Extended Protection
- Disable NTLM on web services
- Use the Protected Users group (for privileged account)
- Block NTLM on system where it is not required (hard to achieve)
- Disable NTLM v1

Chapter

2.4.5

Pass-The-Ticket attacks

🎯Describe Pass-The-Ticket attacks

Pass the Ticket

- Extract the TGT from the LSASS memory
  - This requires the seDebugPrivilege
  - Requires that the targeted identity has cached its credentials
- Inject the TGT into your current session
  - Either locally, or later on other systems by exporting it to a file
  - The “new” ticket is used to request new service tickets
- Does not trigger any failed authentication attempts

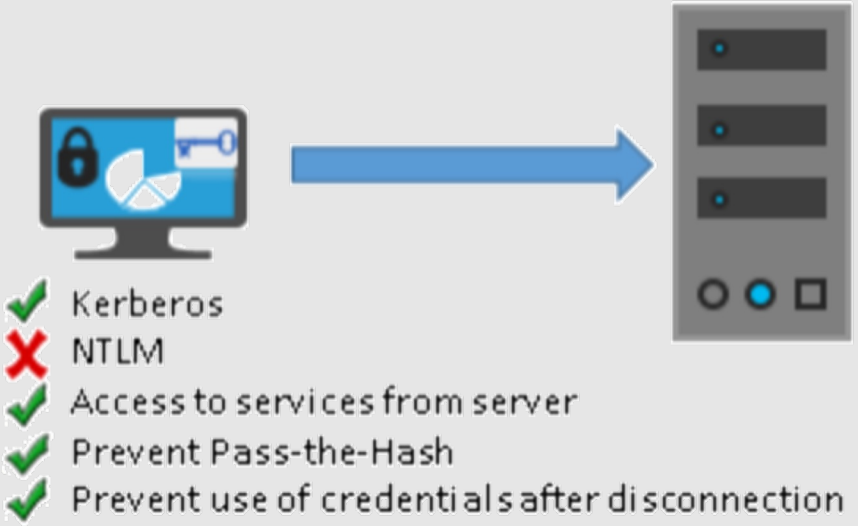
This is possible because the hash is in the memory

Needed for Single Sign-On

A better way to RDP: Remote Credential Guard

- mstsc.exe /remoteguard
  - Ticket are not on the target machine, nothing to steal
- Needs to be enabled on the target
  - (same as for the restrictedadmin mode)

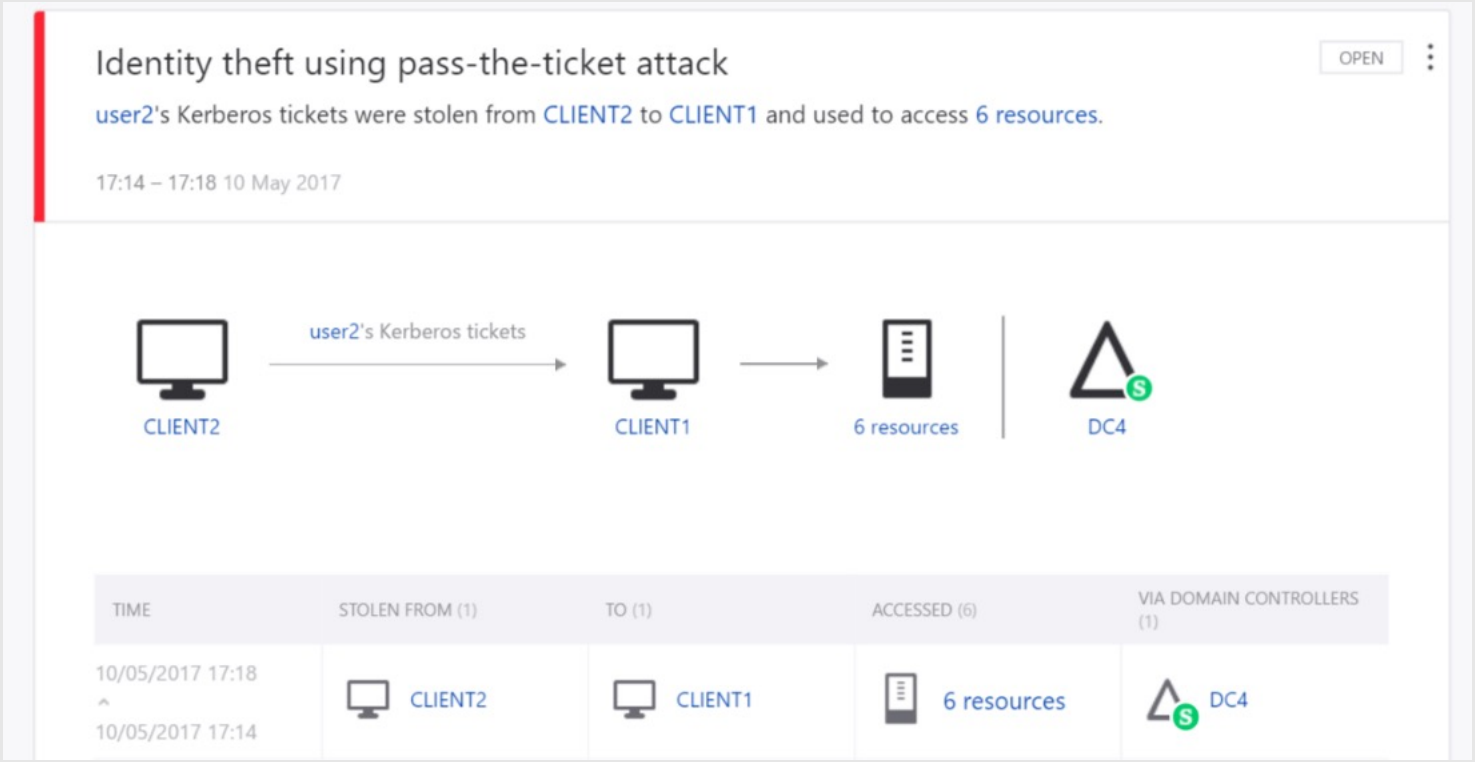
  `HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin = 0x0`



- Credentials protected by Windows Defender Remote Credential Guard
- Connect to other systems using SSO
- Host must support Windows Defender Remote Credential Guard

Detection

- Example of alerts from Microsoft Defender for Identity



Pass-the-Ticket attack summary

Attack's pre-requisites

- A victim is connected to the system, or a service is running under a user account
- seDebugPrivilege, or LSASS memory dump

Protection

- Healthy administration practices (do not connect to untrusted systems with privileged accounts, use RDP restricted mode or remote credential guard)

Chapter

2.4.6

RDP session theft

🎯Explain the techniques of RDP session theft

Living off the land

- Attackers are targeting open RDP server (server exposed on the internet with the RDP service)
  - One they compromise a local account, they can move on and try to steal sessions
- To steal an RDP session, you need:
  - A local administrator (can be a local user)
  - No outside tools, you can use tools available by default on the OS
  - Another user connected to the system (either through RDP or the console)
- The objective: redirect the user's session into your session
  - The attacker is now in the user's session and can access things on the network

Detection and prevention

- The attack leaves quite a lot of artefacts behind
  - Process creation for tscon.exe running as SYSTEM
  - Creation of a new service
- Most EDRs will detect it
- To prevent it… It's all about good administrative practices
  - Users should not leave RDP session signed-in while inactive
  - Admins should not connects using RDP to servers where the local administrators have less privileges than them on the network then no privilege escalation are possible
  - Use /retrictedadmin mode, you can still have your session taken over, but no privilege escalation are possible

RDP session take over

List current sessions

```
query user
query session
```

Create a service to run tscon as SYSTEM

```
sc create FakeService binpath= "cmd.exe /k tscon 2 /dest:console“
net start FakeService
```

RDP session takeover attack summary

Attack's pre-requisites

- Local administrator on the target
- The victim connected to the console or through an RDP session

Protection

- Healthy administration practices (do not connect to untrusted system with privilege accounts, use RDP restricted mode)

Chapter

2.4.7

Azure AD token attacks

🎯Describe Azure AD token attacks

Abusing Azure AD PRT

PRT

- Primary Refresh Token is the SSO artifact of Azure AD
- The machine needs a corresponding device object in AAD
- Protected by the TPM
- PRT can be used to request tokens (Refresh Token & Access Token)

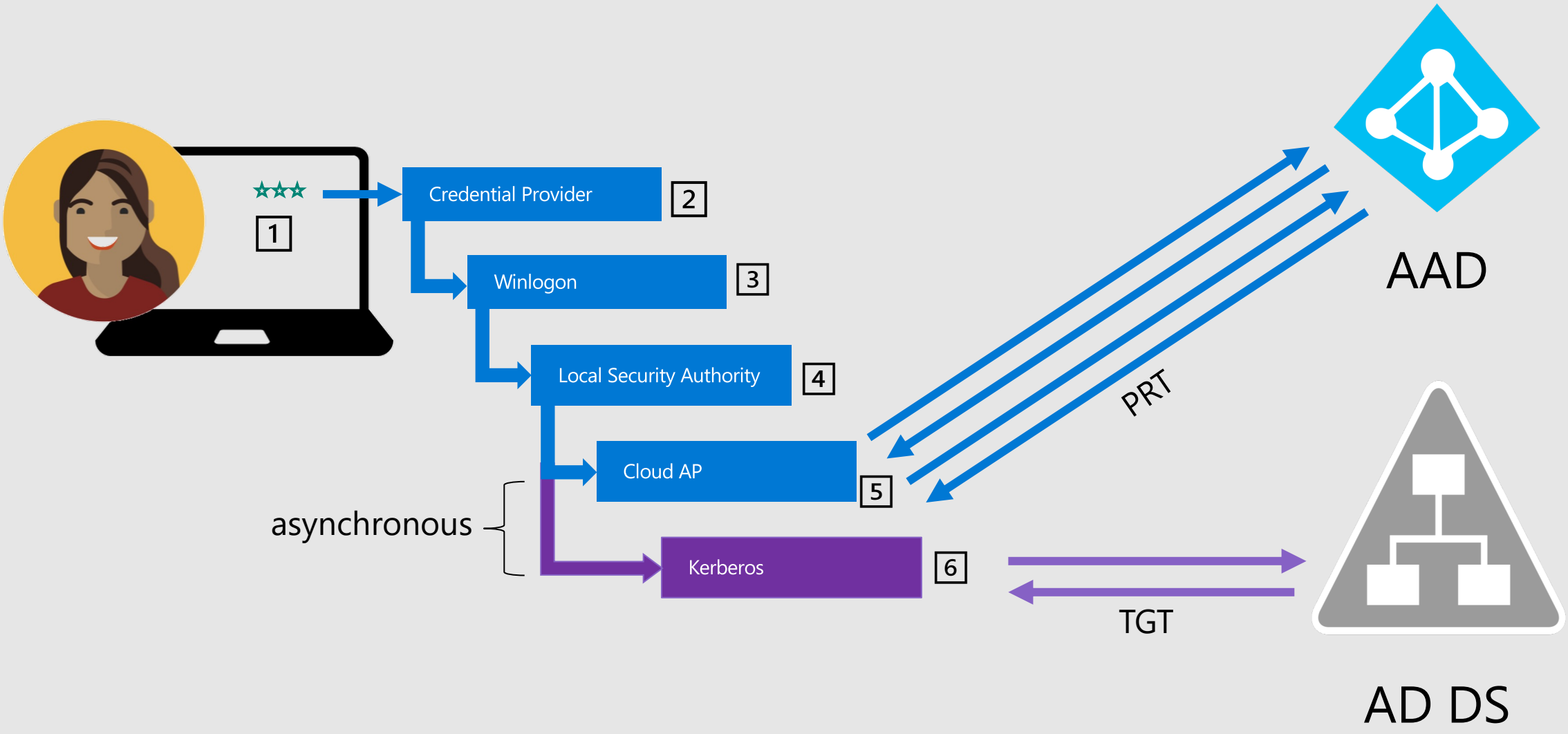
RT

AT

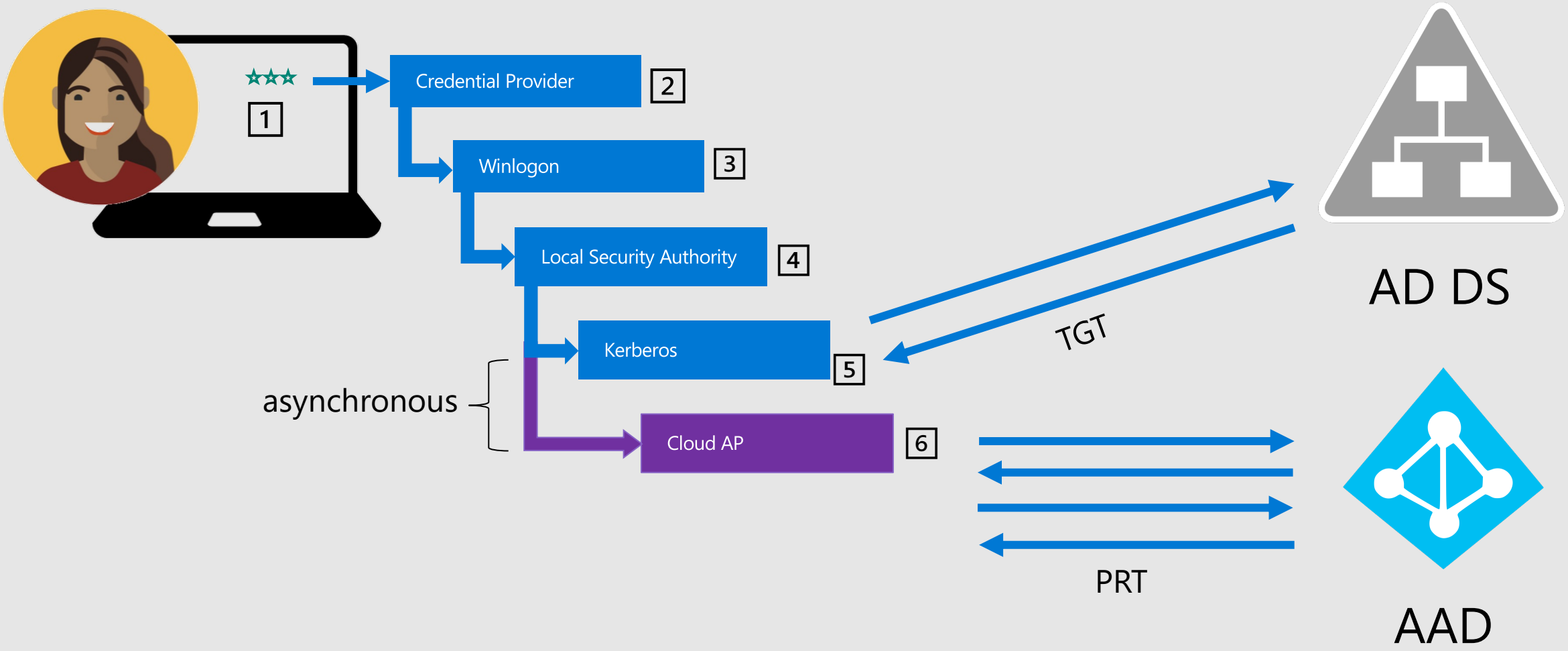
- Browser access is using cookies to handle sessions

1. Use the PRT to derive keys
2. Generate your own cookies
3. Inject your cookies in your browser
4. Access the application

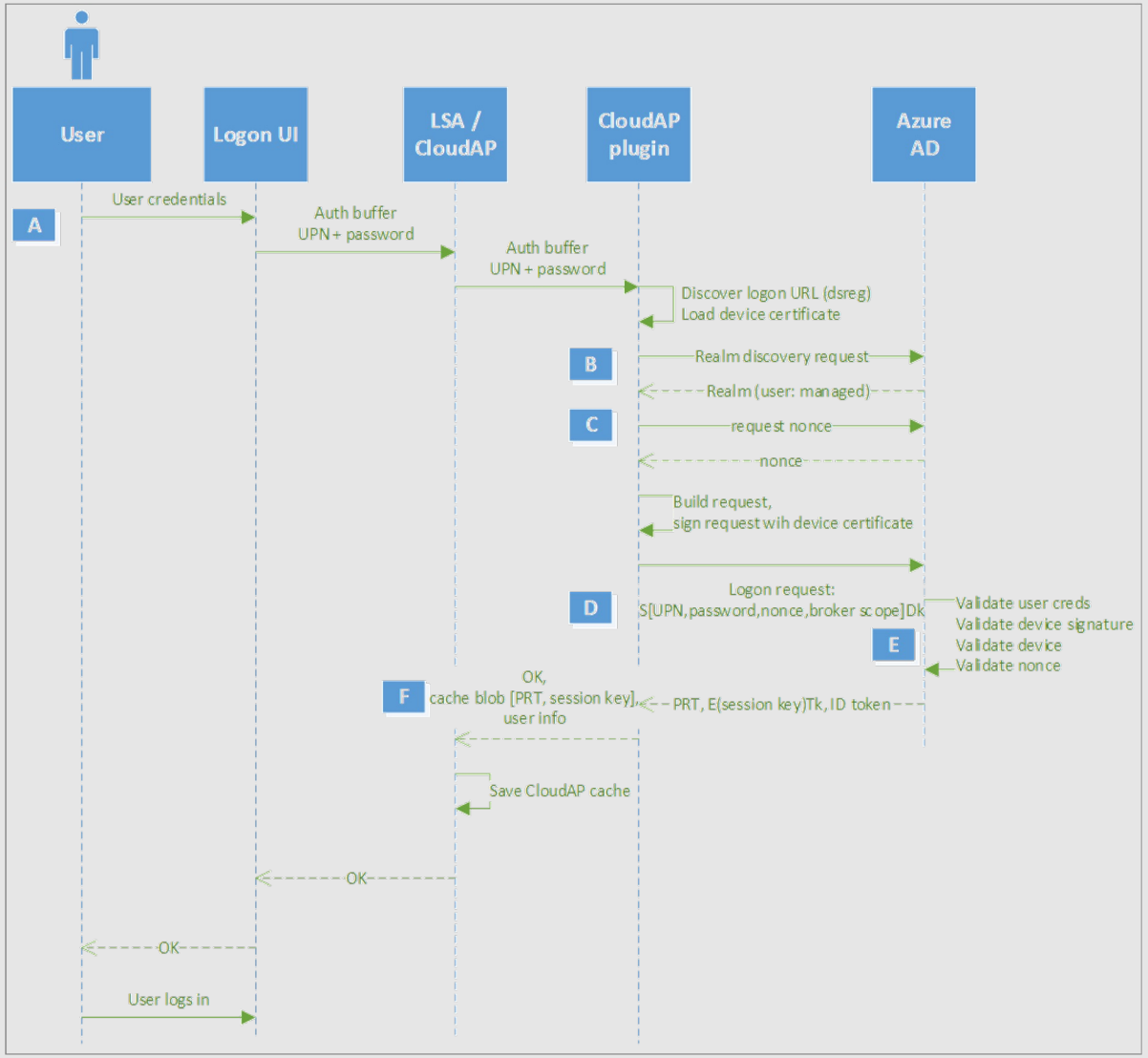
PRT issuance on Azure AD Joined machine



PRT issuance on Hybrid Azure AD Joined machine



PRT issuance during first sign in



Abusing Azure AD PRT to access APIs

- The same technique can also be used to request AC and access backend APIs
- Tools such as `mimikatz` and the PowerShell module `AADInternals` have made the attack quite straight forward

PRT and cookie manipulation

Using mimikatz

```
privilege::debug
sukurlsa::cloudap
token::elevate
dpapi::cloudapkd /keyvalue:<key> /unprotect
dpapi::cloudapkd /prt:<prt> /derivedkey:<key>
```

RDP session takeover attack summary

Attack's pre-requisites

- Local administrator on the target
- The target is Azure AD Joined or Hybrid Azure AD Joined
- The victim connected to target (interactive session)

Protection

- Enable TPM (doesn't prevent the attack but is coercing the attacker to derive keys locally)
- Detect suspicious behavior with Identity Protection
- Conditional Access Policy and Continuous Evaluation (to limit time and scope of the attack)

Chapter

2.4.8

Pivot from virtualization administrator to AD administrator

🎯List and limit control paths to AD

Move from physical access to domain admins

- Ensure domain controllers' physical security

➡️If you cannot trust the physical security, consider RODC
➡️Secure the backups!

- What if the DCs are virtual?

➡️ The admins of the host control the guests

Read-only Domain Controllers

- Reduces the attack surface on unsecure physical locations
  - It's like a DC but it does not have the secrets
  - It does not have confidential attributes
  - If it gets stolen, the thief doesn't have the hashes
- Password Replication Policies
  - You pick what are the secrets which can be cached on an RODC
- You can have a local admin!
  - You can delegate the local admin permissions to users without giving them permissions on AD
- It's not designed for disconnected scenarios
  - If an account's secret isn't cached, we need to forward authentication requests to a Read-Write Domain Controller (or if there is a write operation to be performed)

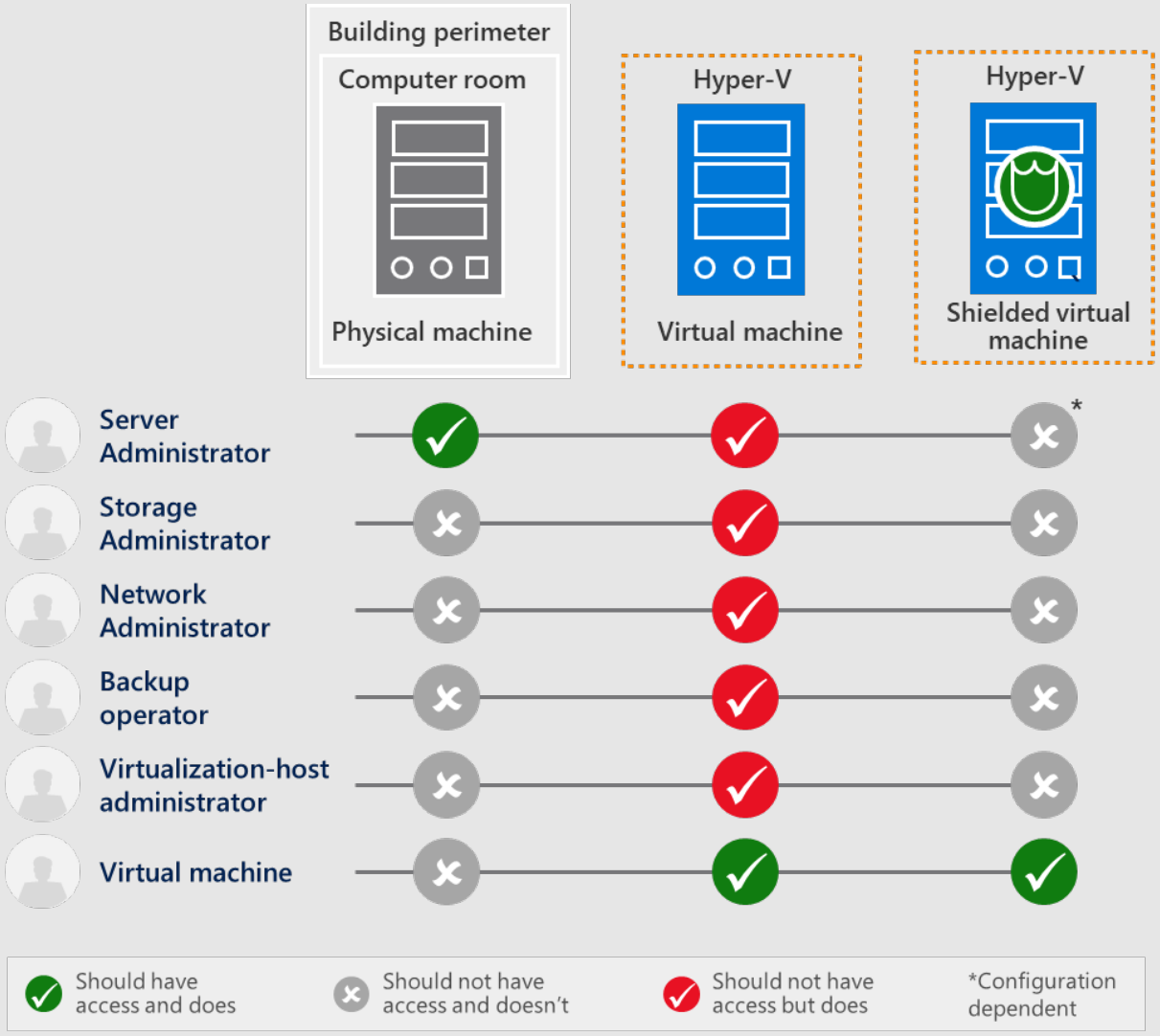
RODC isolation

- Cryptographic isolation: each RODC has its own krbtgt account!
  - Krbtgt_XXXX
  - Which makes it easy to invalidate all TGTs it has issued
- If it's stolen, you can reset only the secrets of the accounts cached on it
  - All cached accounts are stored in an attribute on the RODC computer accounts

Virtual Domain Controllers

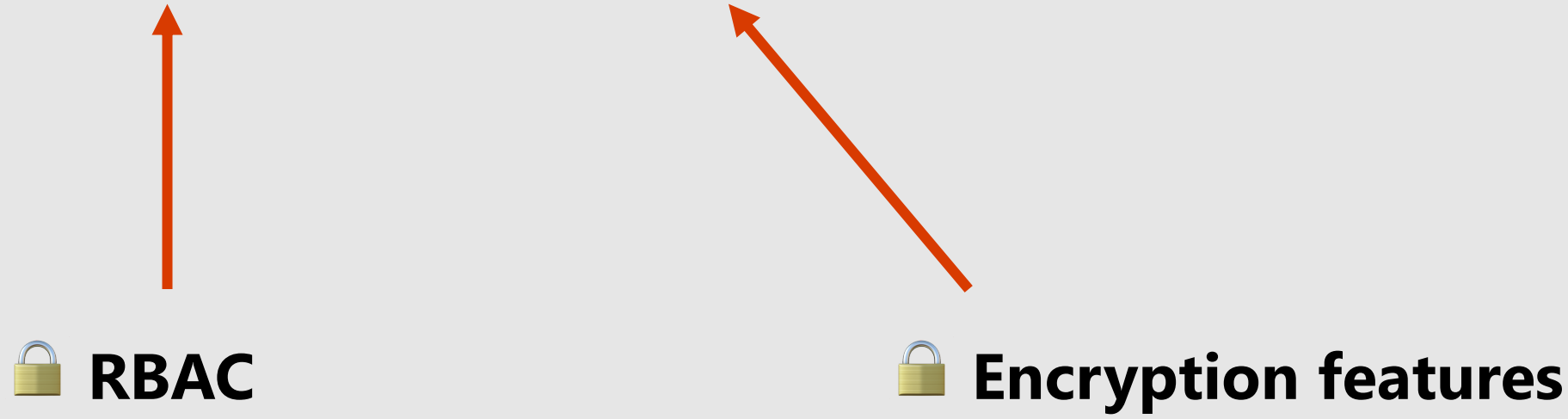
- What can virtual admins do on virtual domain controllers?
  - Do you trust them?
  - Do they comply with the same security policies than AD admins?
- What about the storage admins?
- The virtual platform admins are your hidden domain admins, they can:
  - Read the DC memory
  - Copy the VM
  - Copy the virtual hard drive (hence the DB and its encryption keys)

Virtual machines, real risks



Infrastructure as a Service

- A cloud admin could pivot to a VM in the cloud
- Execute code, access virtual hard drive



Active Directory Backup

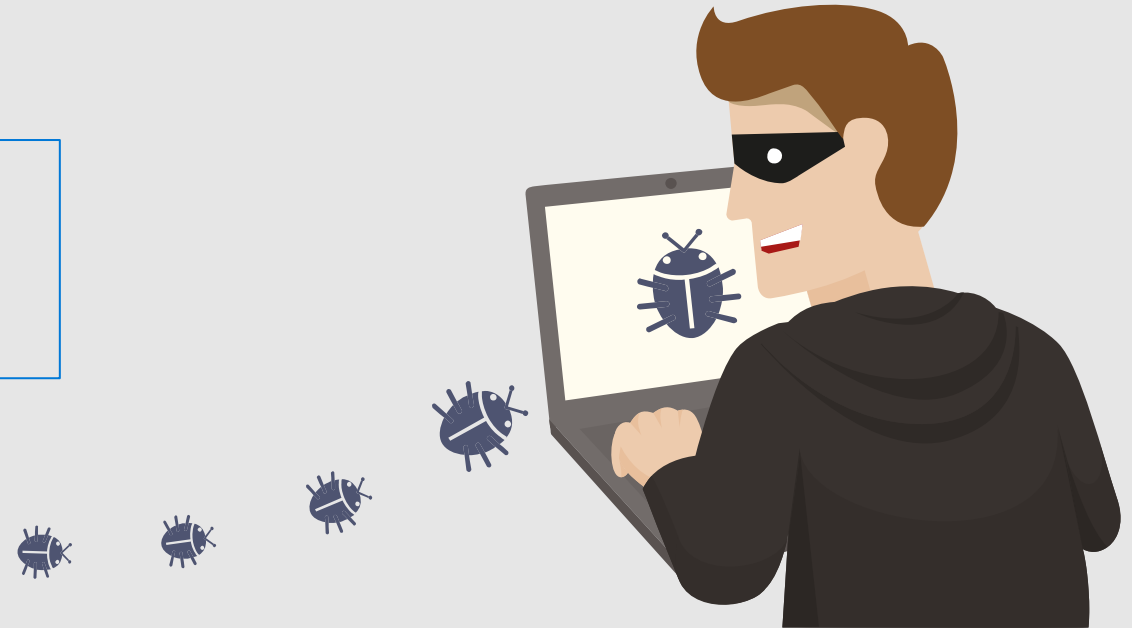
- Whether there are…
  - Bare metal backups of the OS
  - System states of the DC
  - Full backups of the VM
- It needs to be secured
  - Storage
  - Encryption
  - Access control
  - Cloud-based backups

The print spooler

- Enabled by default
  - It is to prune print queues published in AD

Can be exploited by an attacker… Check out Print Nightmare vulnerability

Disable the Print Spooler service on domain controllers



Pivot from an application

- If you have an agent installed on a domain controller
- Or a machine used by privileged accounts

⚠️ The agent’s platform is in control

RDP session takeover attack summary

Attack's pre-requisites

- Local administrator on the virtualization platform or permission to execute code on the IaaS platform or accessto a

Protection

- Hyper-V
- Proper RBAC model

Chapter

2.4.9

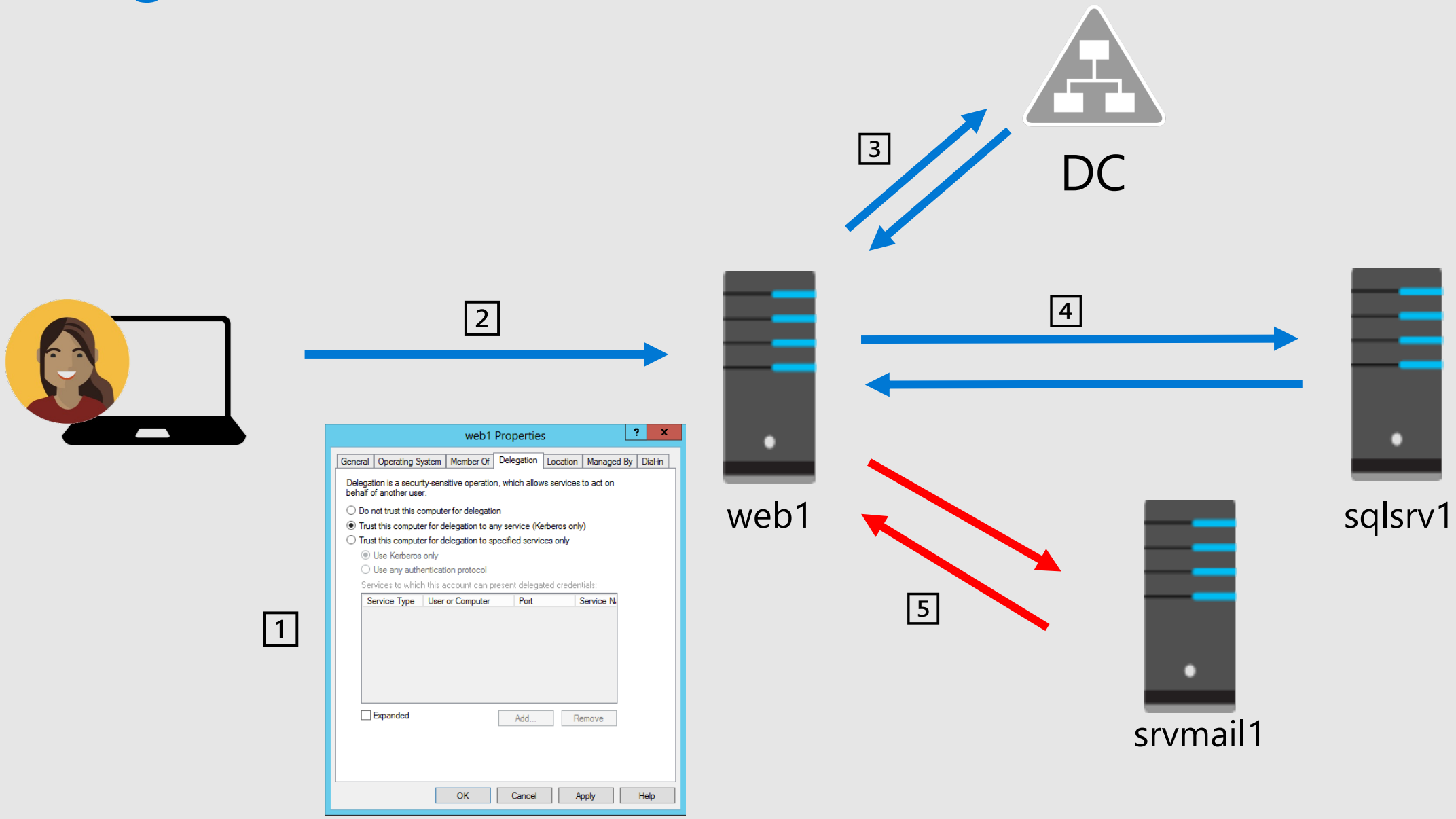
Abuse the Kerberos Delegation

🎯Describe and control Kerberos delegation

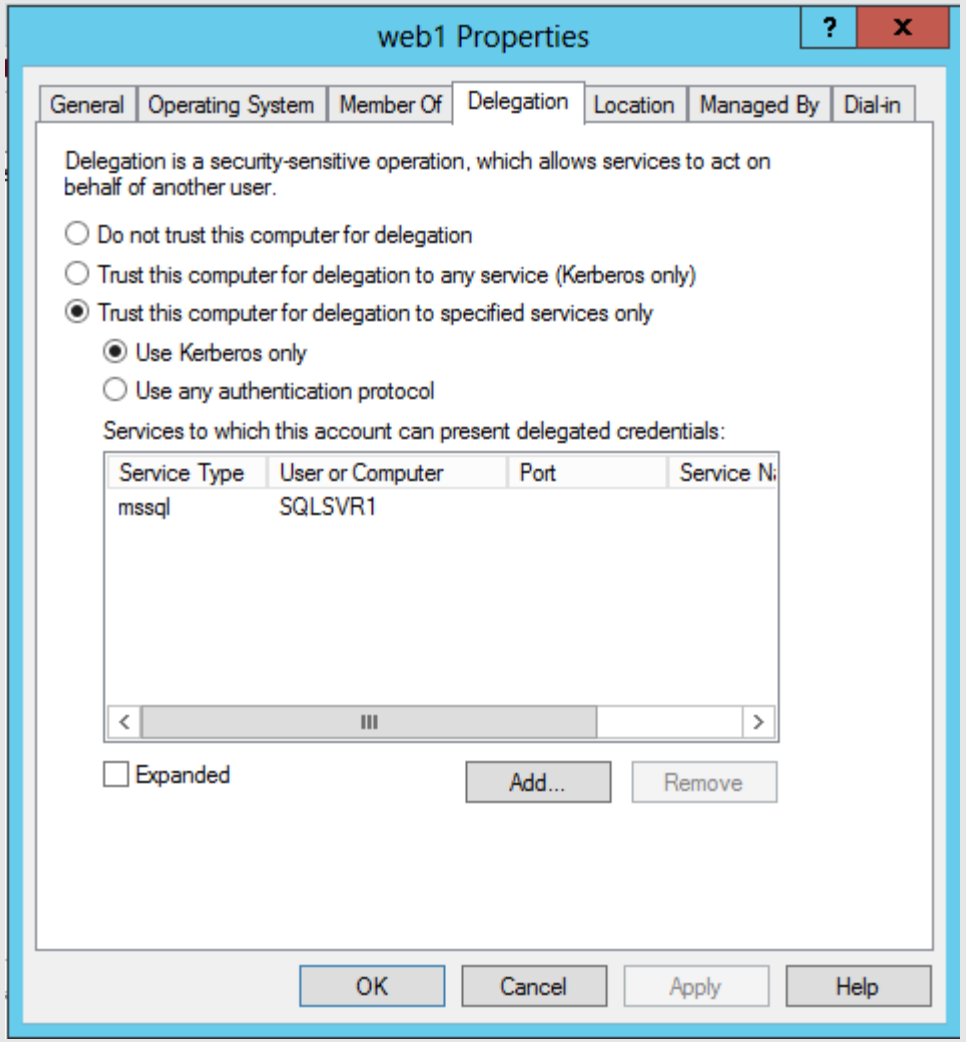
What is Kerberos delegation

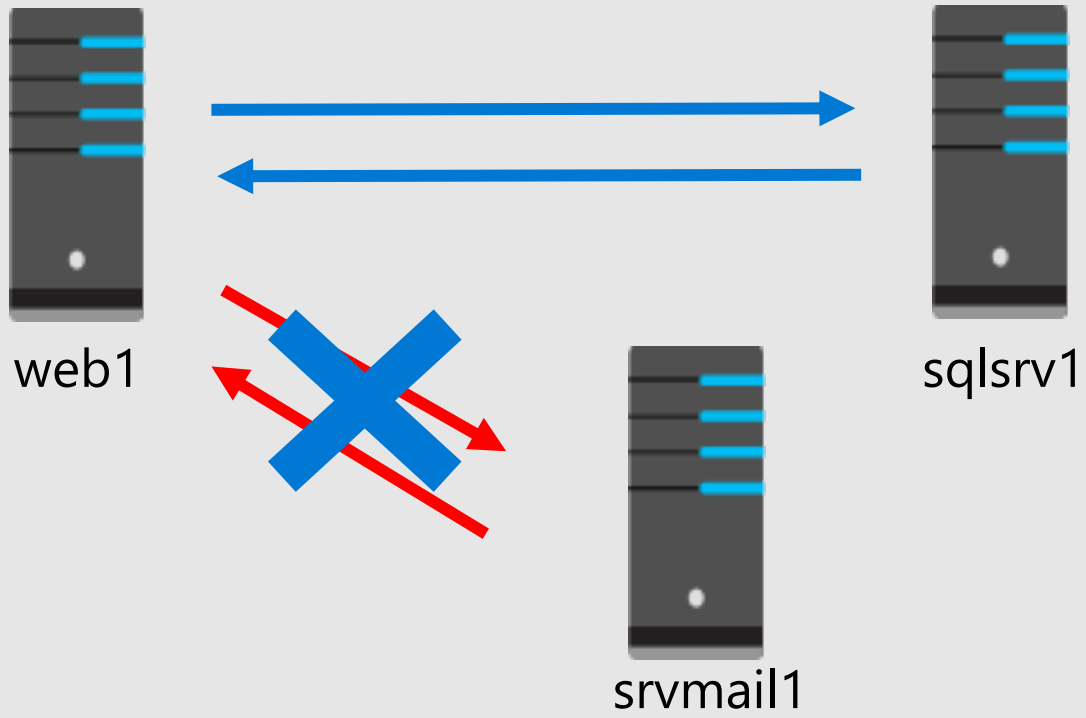
- It allows an application to impersonate a user to access other services on its behalf
  - SSO experience for the user
  - End-to-end security and auditing for the user
- Unconstraint delegation
  - It allows the service to access everything on behalf the user
- Constraint delegation
  - It allows the service to access only the configured backend services
- Any application and system with the privilege to do Kerberos delegation are ideal targets for attackers
  - Attacker will try to steal the credentials of these accounts to impersonate other accounts
  - Attackers might leverage Kerberos delegation vulnerabilities against unpatched domain controllers

Delegation in action

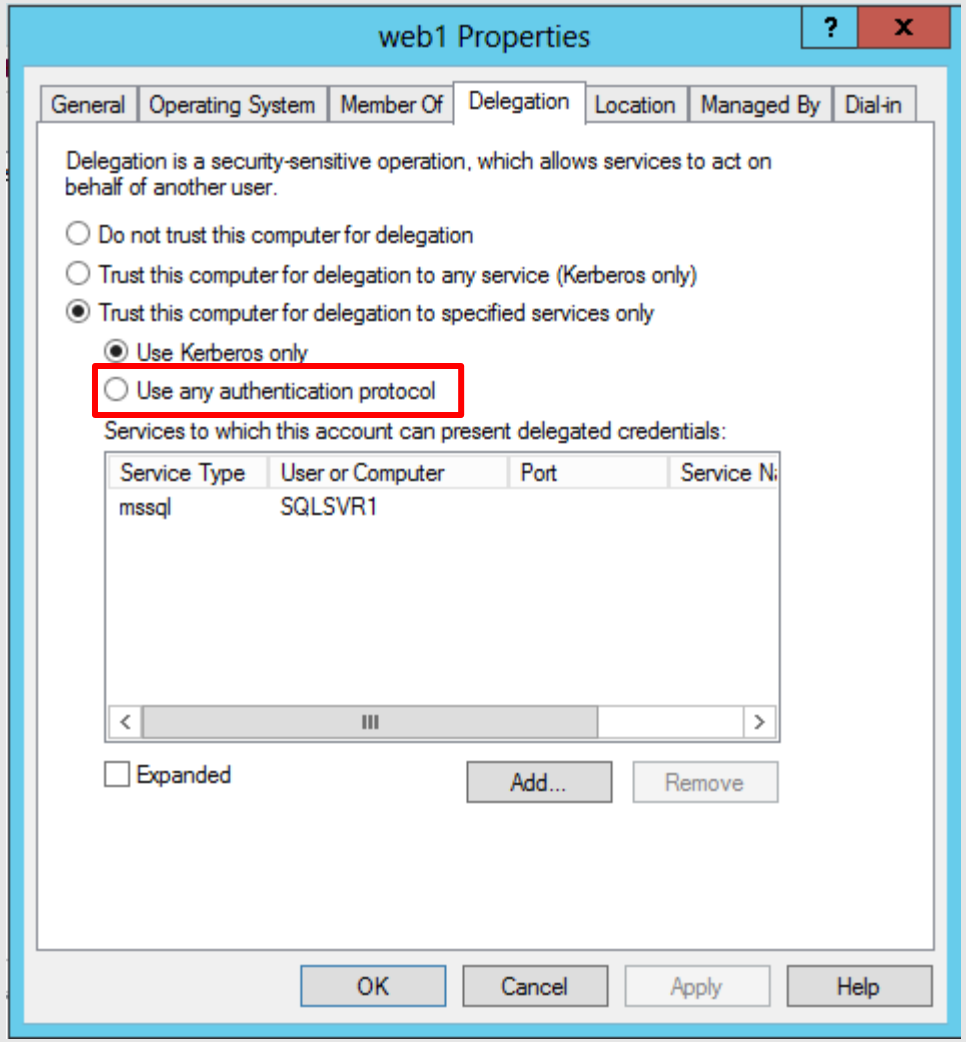


Unconstraint delegation





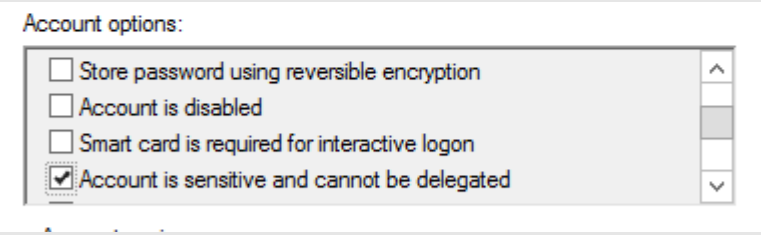
What is Kerberos delegation



- Constraint delegation with protocol transition allows the service to access only the configured backend services but for any users
  - Normally to exploit delegation, the attacker needs to coerce the user to connect to the controlled service. With protocol transition, the attacker can impersonate the user at anytime but only against the pre-configured backend services

Tighten delegation

- Remove delegation on computer and service accounts where it is not needed
- Avoid unconstraint delegation
  - Disable unconstraint delegation over trusts
- If delegation really must be used, use constraint delegation
  - And closely monitor the system where it is used as they are prime targets
- Disable delegation on sensitive accounts
  - Consider using the Protected Users group for privileged accounts
  - Mark the account as sensitive



LDAP filters to identify account with delegation

Machines with unconstrainted delegation

```
(&(objectCategory=computer)(objectClass=computer)(userAccountControl:1.2.840.11
3556.1.4.803:=524288))
```

Users with unconstrainted delegation

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1
.4.803:=524288))
```

Computer with constrained delegation and protocol transition enabled

```
(&(objectCategory=computer)(objectClass=computer)(userAccountControl:1.2.840.11
3556.1.4.803:=16777216))
```

Users with constrained delegation and protocol transition enabled

```
(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1
.4.803:=16777216))
```

RDP session takeover attack summary

Attack's pre-requisites

- Control an account with Kerberos delegation permissions
- Abuse of an unpatched domain controller

Protection

- Remove delegation permissions when not needed
- Disable delegation on sensitive users
- Use constraint delegation when delegation is required
- Disable unconstraint delegation on users, computer and trust
- Use Protected Users group (for privileged accounts)
- Update all domain controllers

Microsoft

List of abbreviations

LAPS – Local Administrator Password Solution
LMHash – Lan Manager Hash
NTHash – New Technology Lan Manager Hash
PRT – Primary Refresh Token
RT – Refresh Token
AT – Access Token
VM – Virtual Machine
TPM – Trusted Platform Module