Purple RDP

Red and Blue Tradecraft around the Remote Desktop Protocol

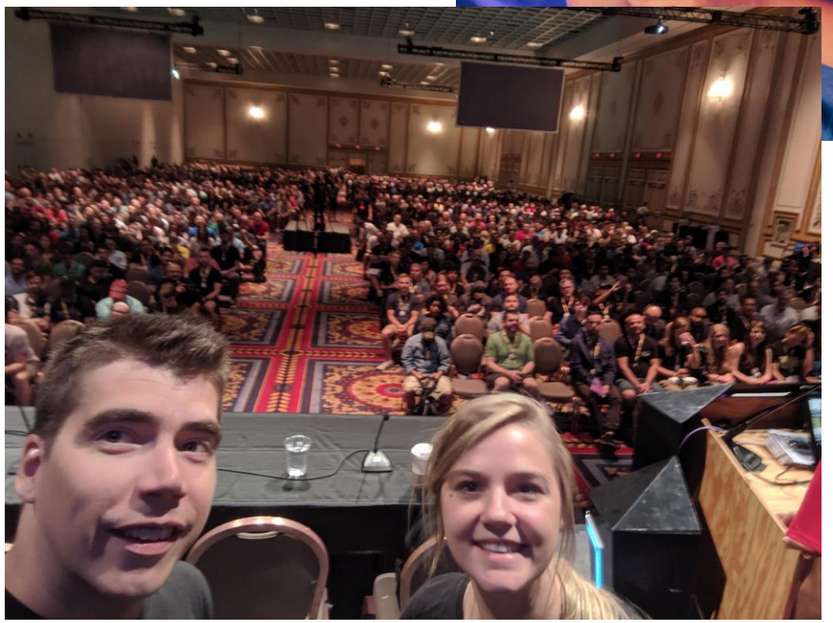
Olivier Bilodeau (@obilodeau), GoSecure

GoSecure

Are You Qualified?

Olivier Bilodeau

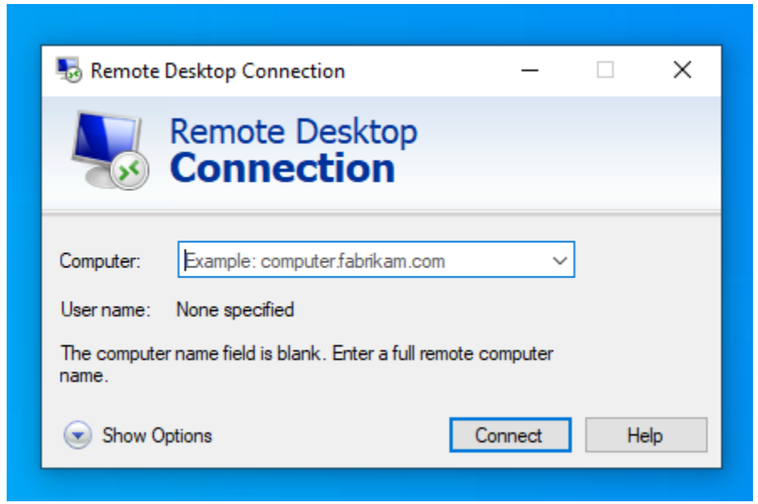
- Cybersecurity Research Director at **GoSecure** Inc.
- Acting President and Hacker Jeopardy host for the **NorthSec** Conference and CTF
- Co-found **MontréHack** (hands-on security workshops)
- International public speaker at events like RSAC, **BlackHat USA**, SecTor, HackFest, etc.

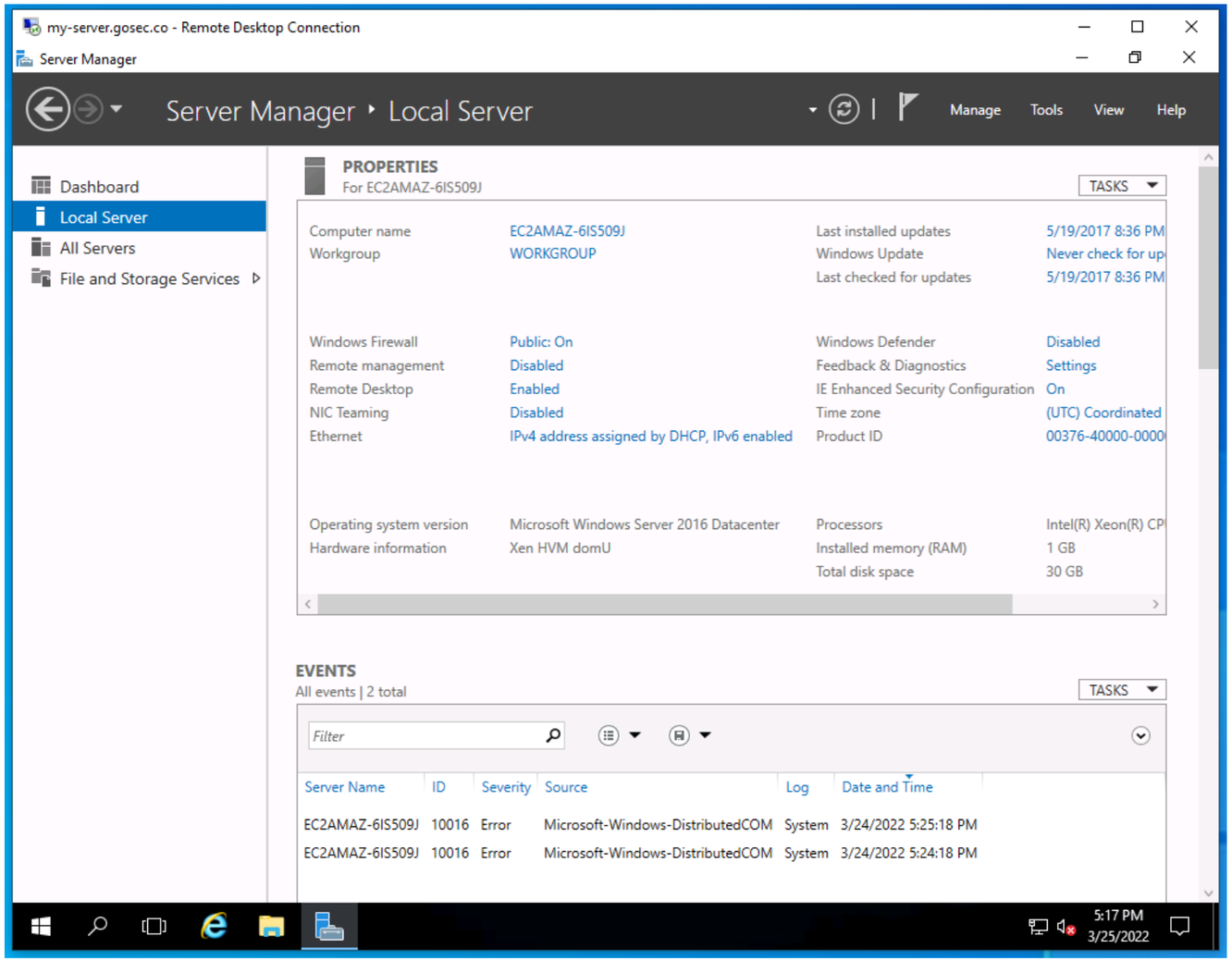


Introduction to RDP

GoSecure

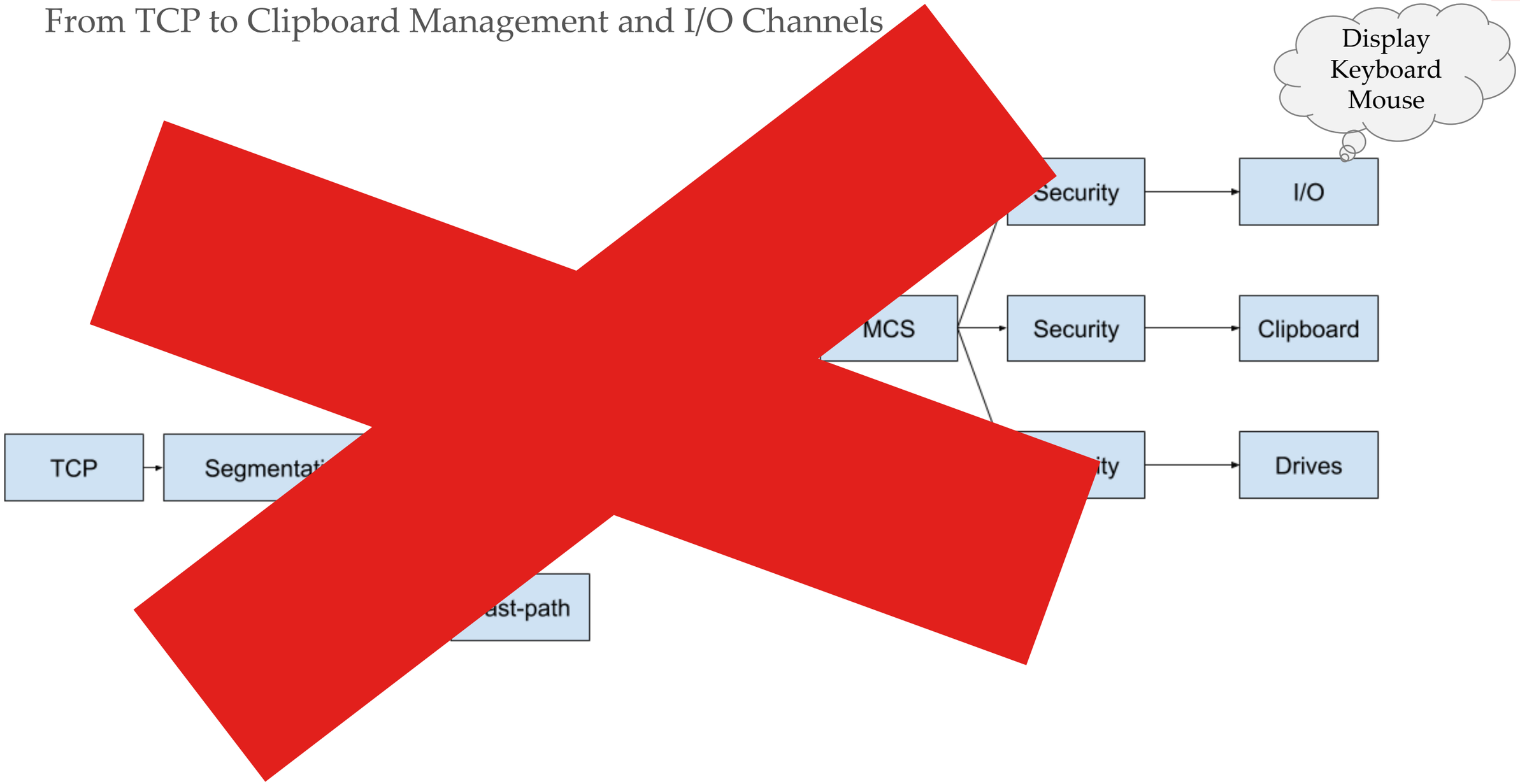
Remote Desktop Protocol





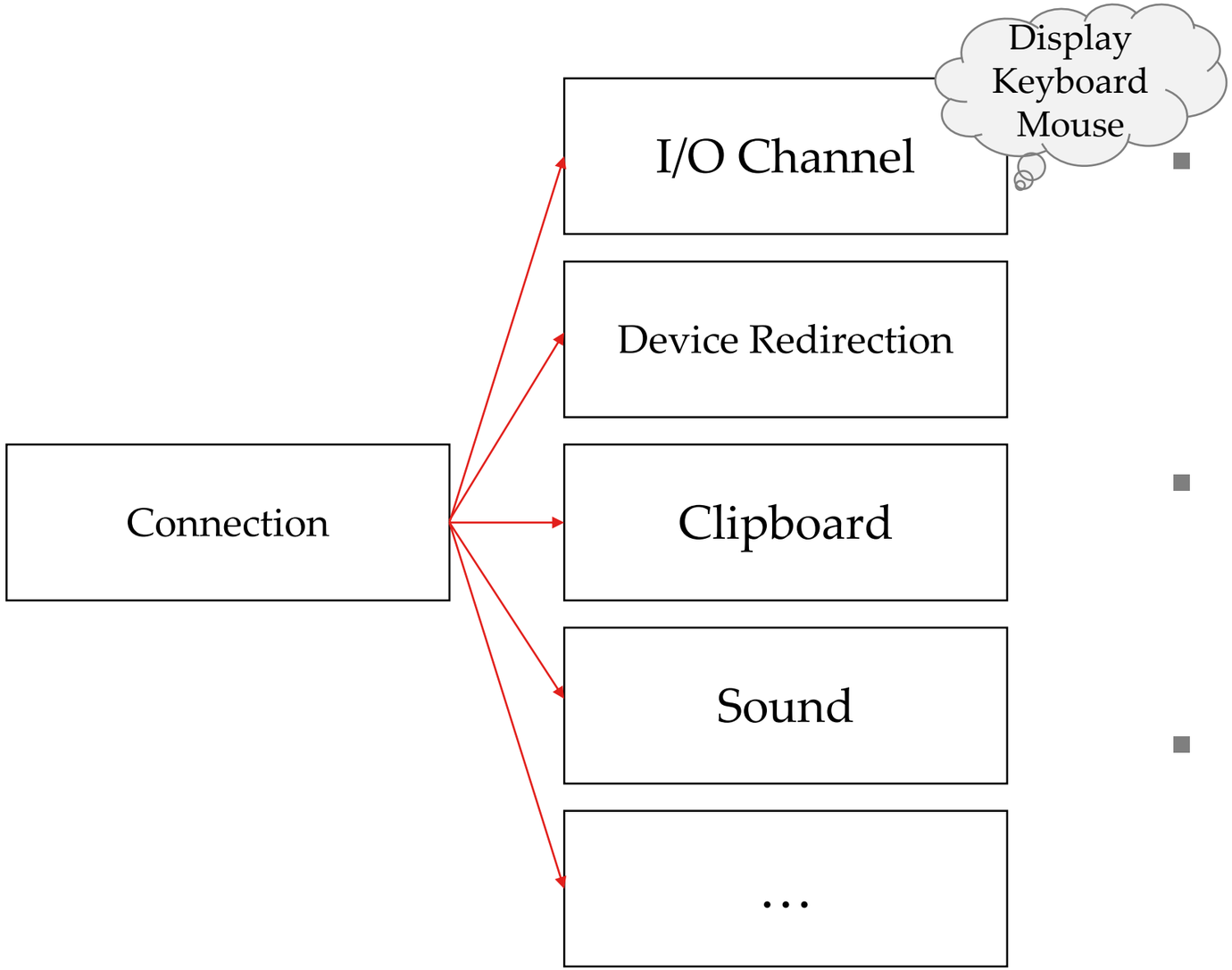
RDP Layers

From TCP to Clipboard Management and I/O Channels

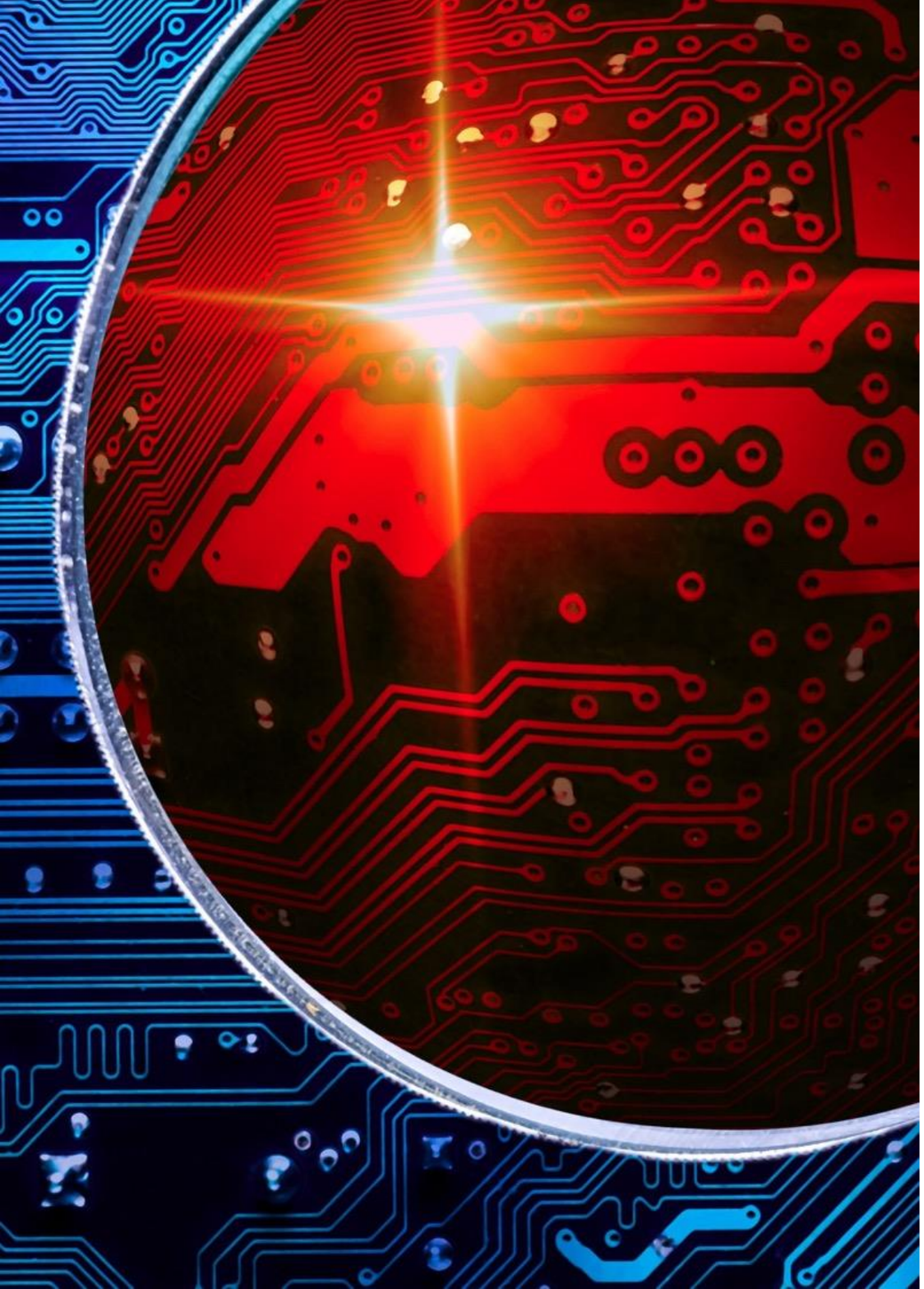


RDP Virtual Channels

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

Wire protocol

- RC4 + Graphical login (dead)
- TLS + Graphical login (legacy)
- TLS + Network Level Authentication (NLA) which relies on CredSSP

Credential Protection

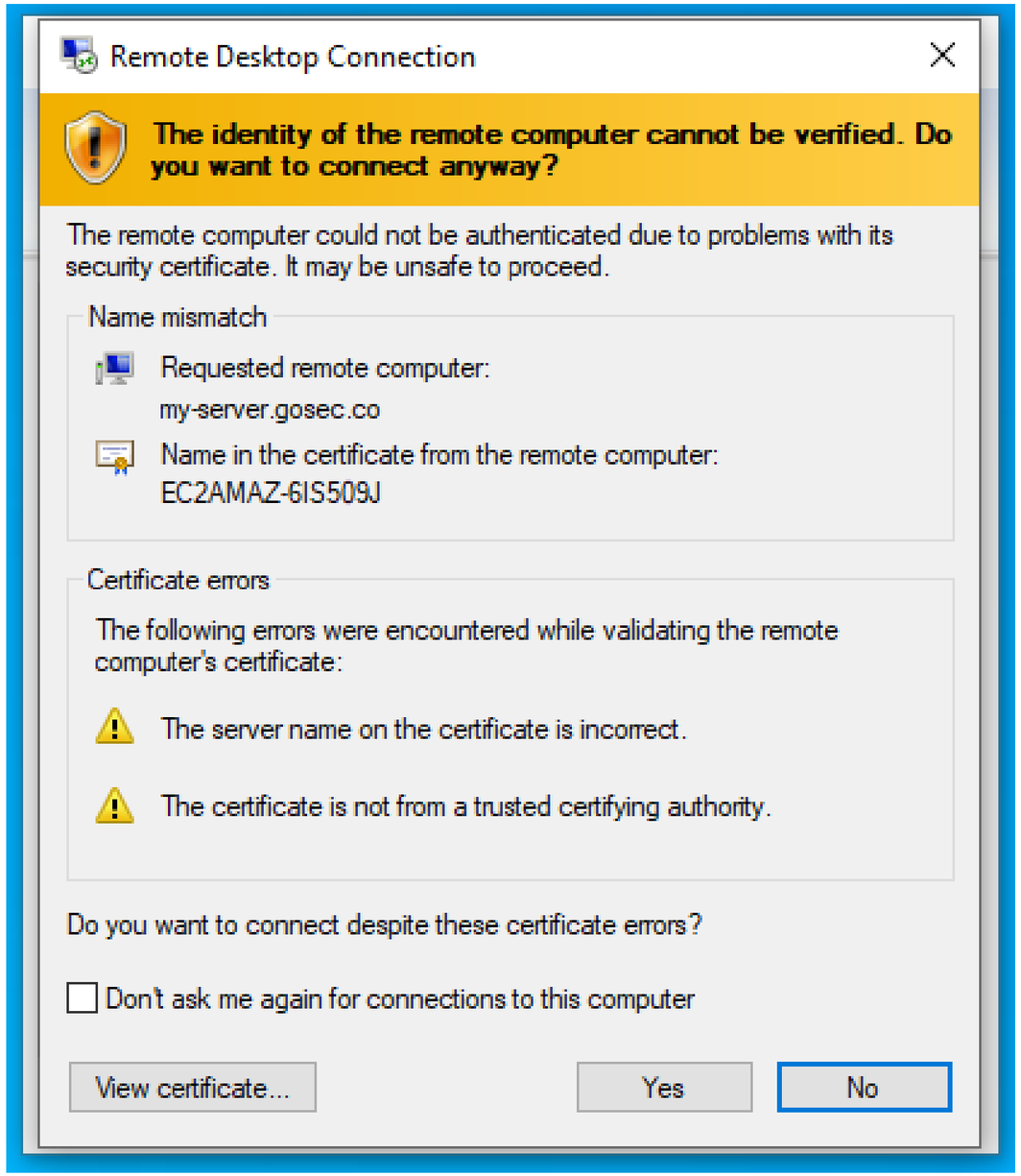
- Remote Credential Guard
- Restricted Admin

Attack: MITM Legacy RDP

GoSecure

MITM Risks

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



*: implementation pending

Demo: NLA Downgrade + MITM

Noticeable Certificate Error

(link to video)

GoSecure

How? By Our Open Source Attack Tool: PyRDP

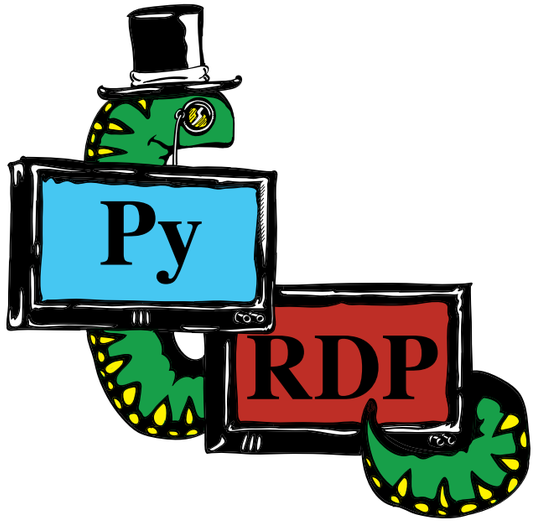
Learn More About It!

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

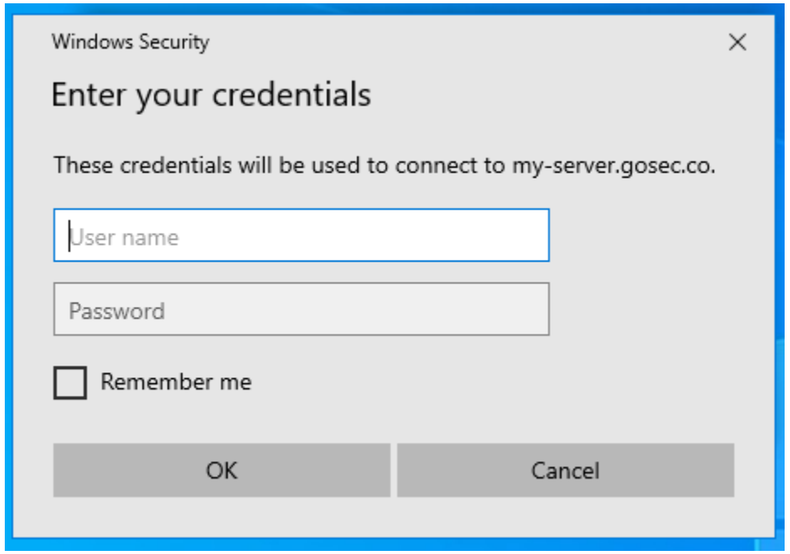
- Introduction Blog Post
- NorthSec 2019 Talk
- BlackHat Arsenal 2019
- Blog: PyRDP on Autopilot
- DerbyCon 2019 (Video)
- DEFCON 28 Demo Labs
- Blog: Announcing PyRDP 1.0
- 1.0 released at SecTor 2020
- BlackHat Arsenal 2021

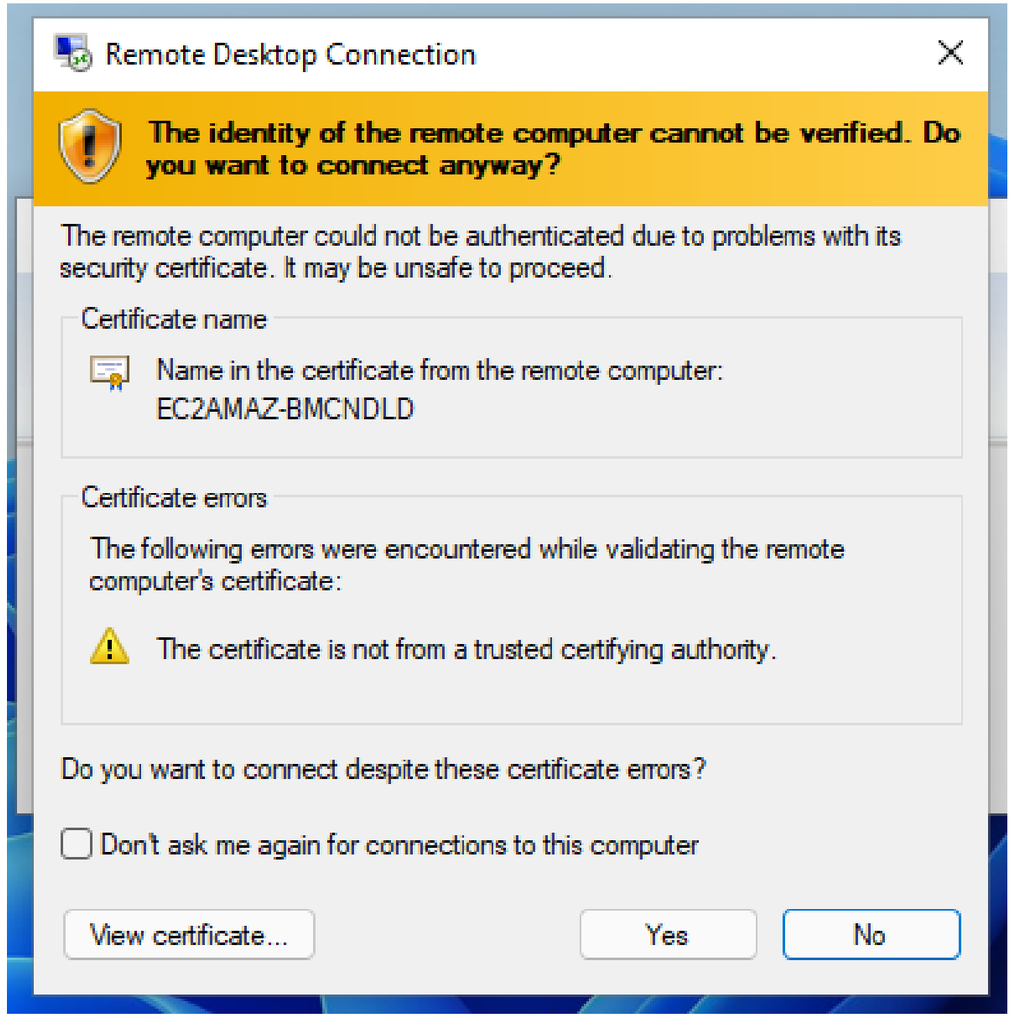


Defense: Detect Security Downgrade

Detect Security Protocol Downgrade

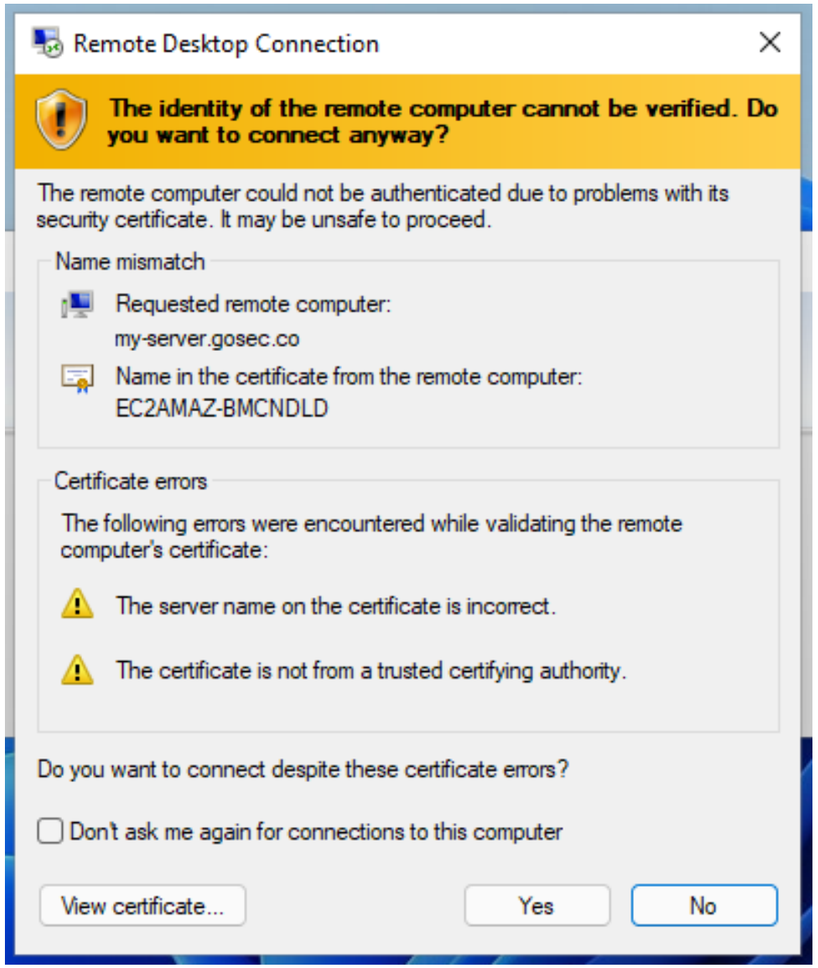
Normal Flow

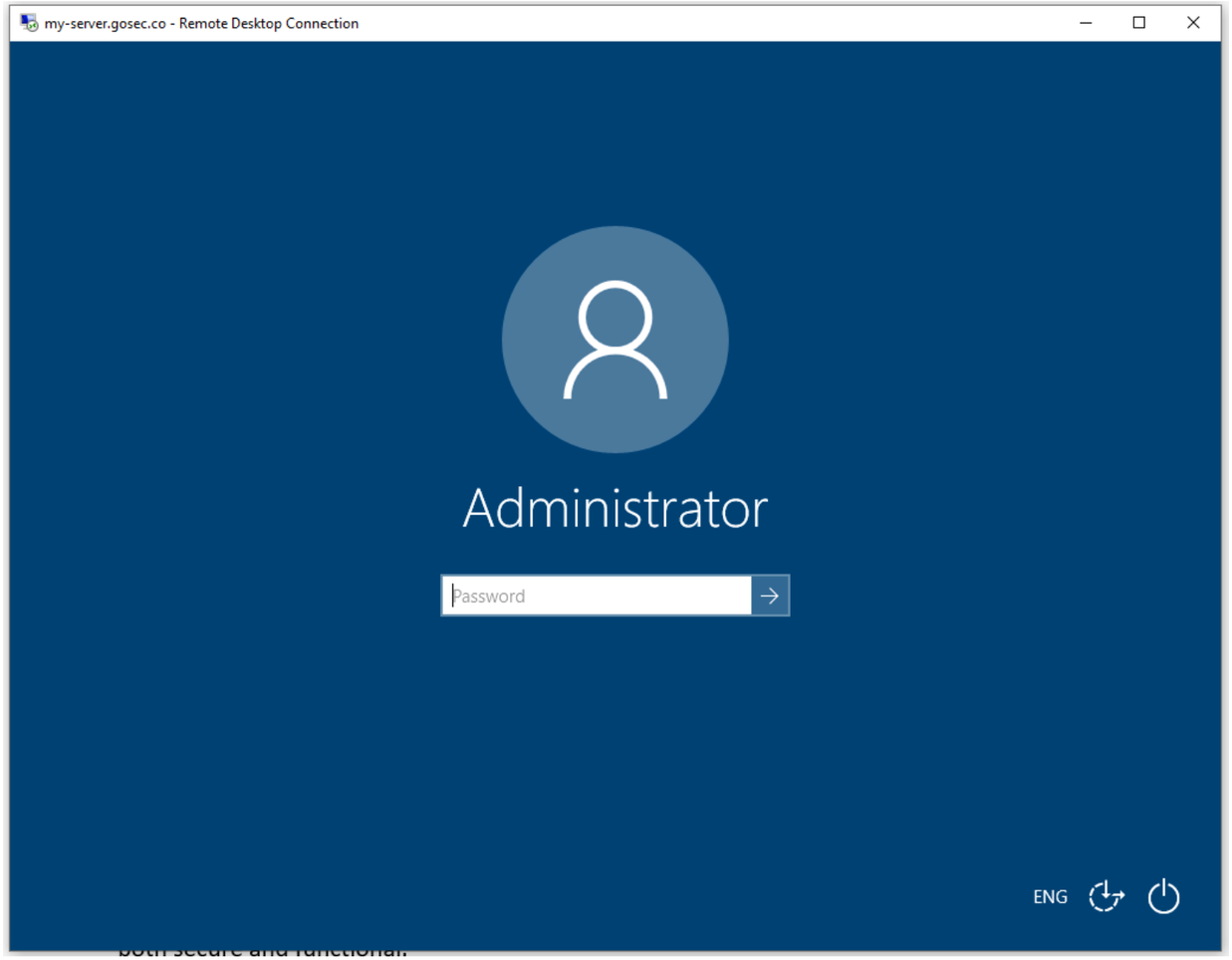




Detect Security Protocol Downgrade

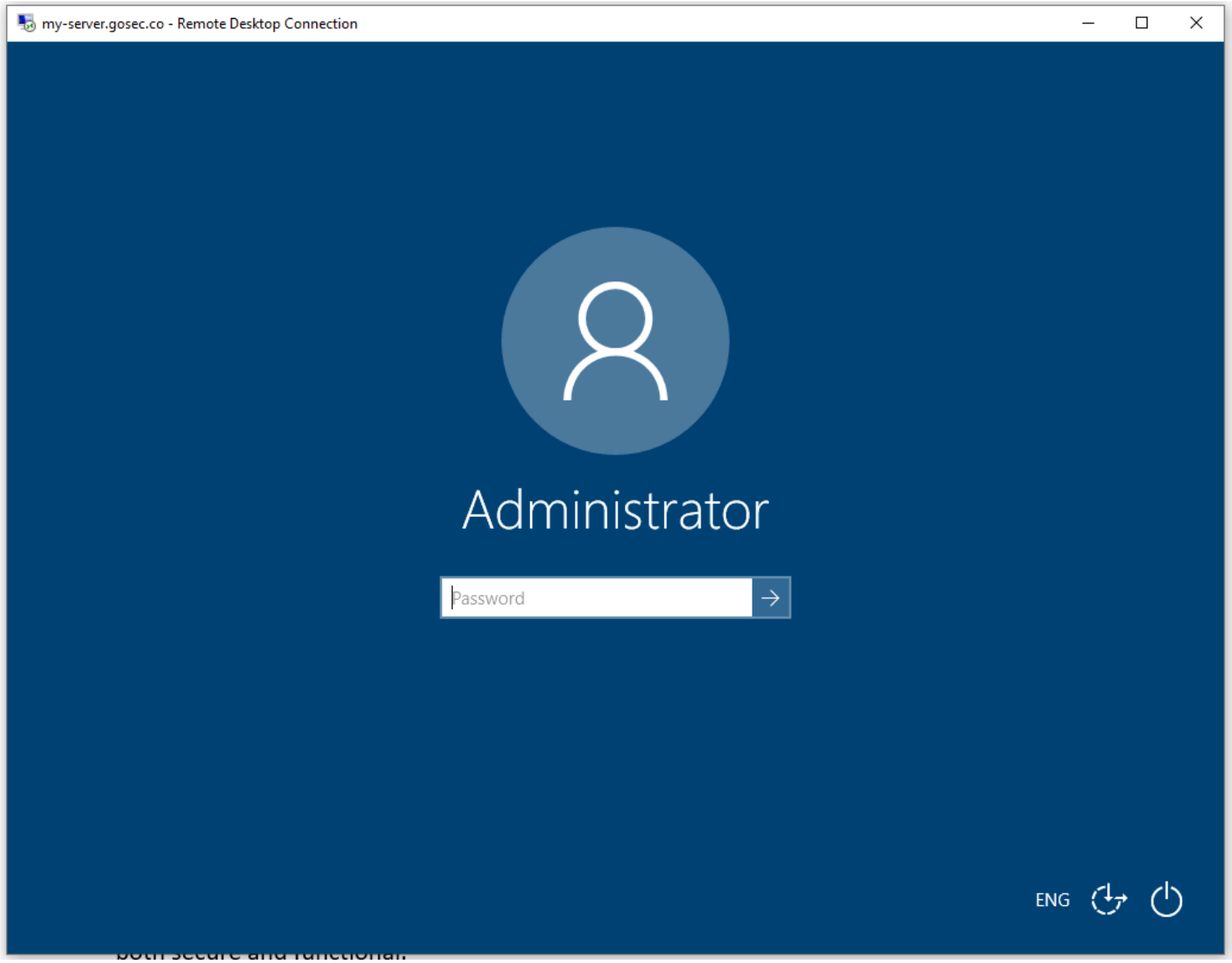
Degraded Flow

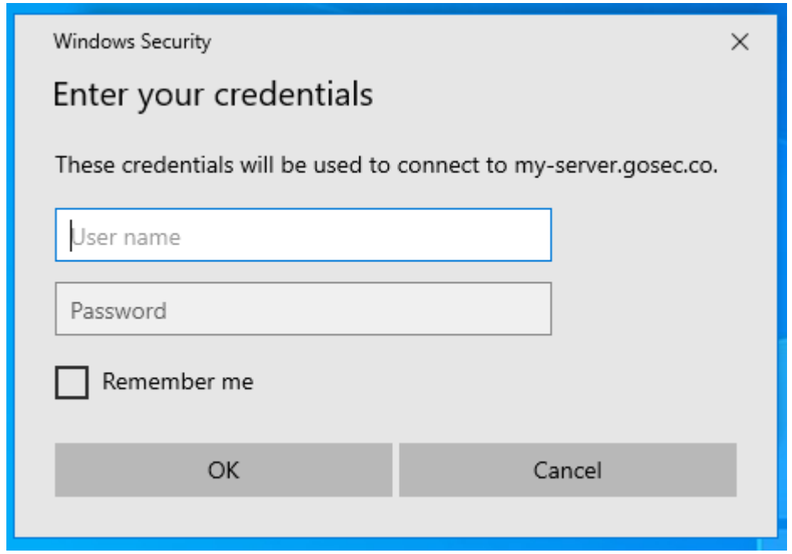




Detect Security Protocol Downgrade

Graphical Login => instead of => NLA Prompt



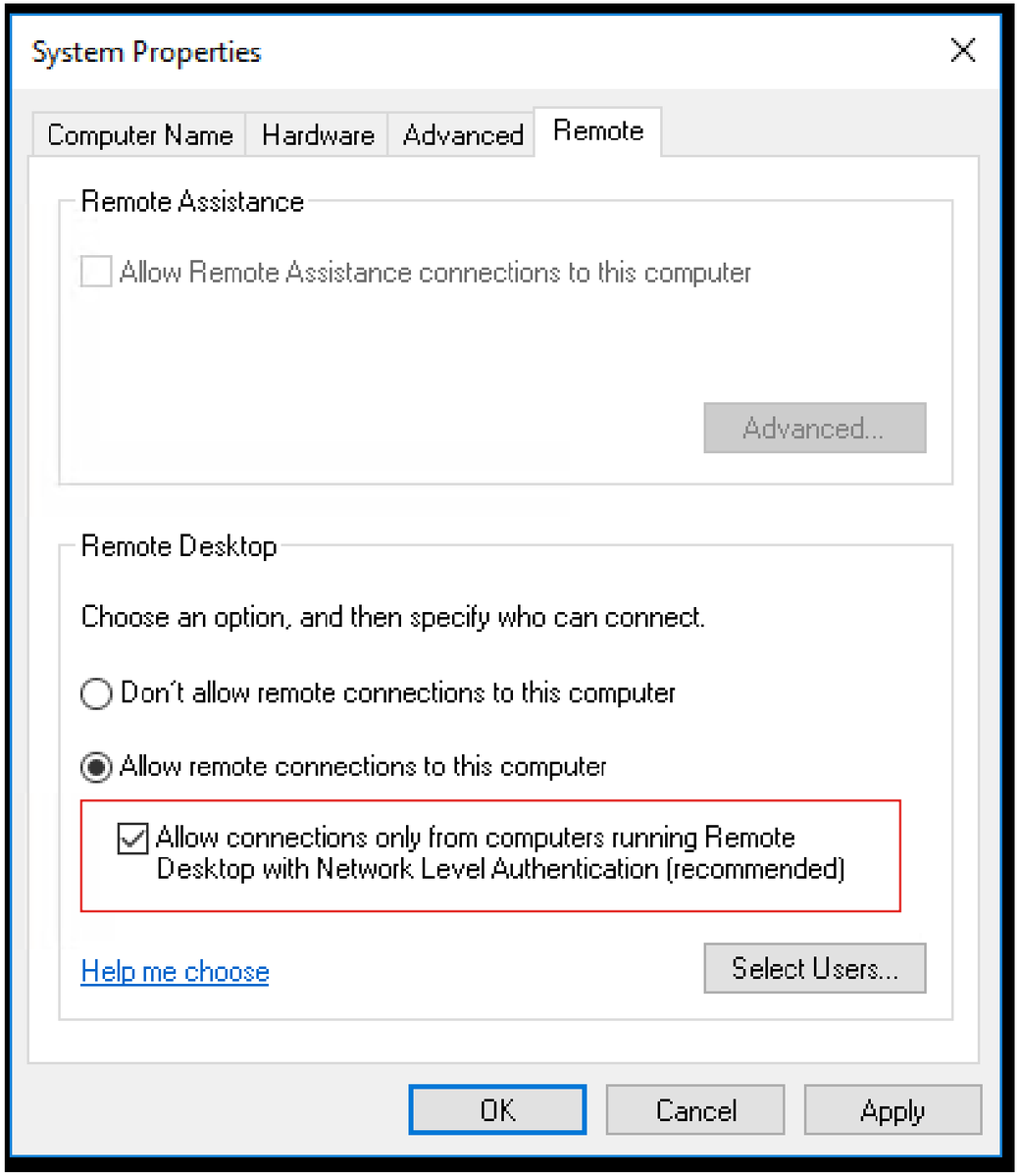


What is Network-Level Authentication (NLA)?

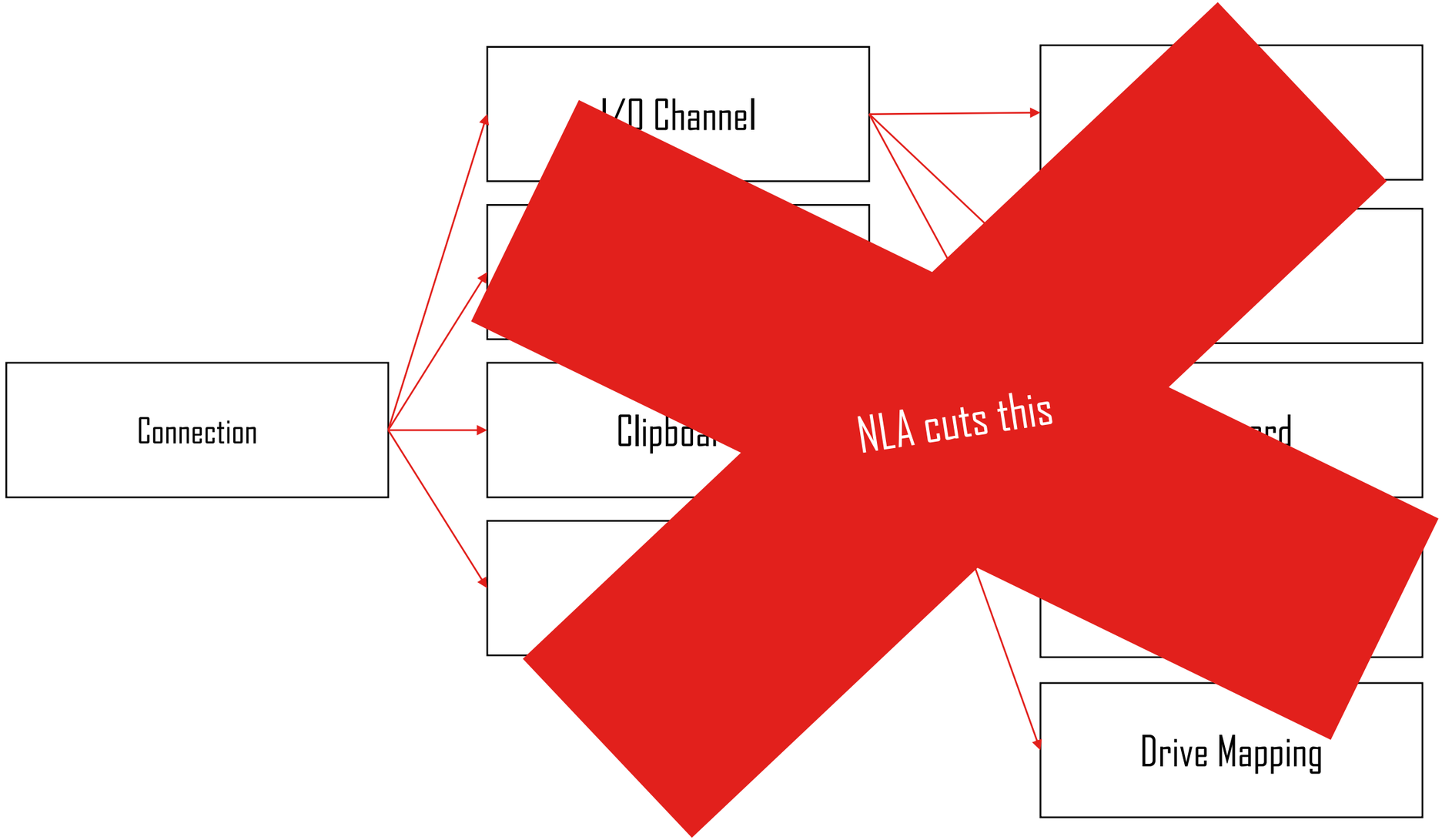
GoSecure

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
  - Windows Server 2012
  - Windows 8



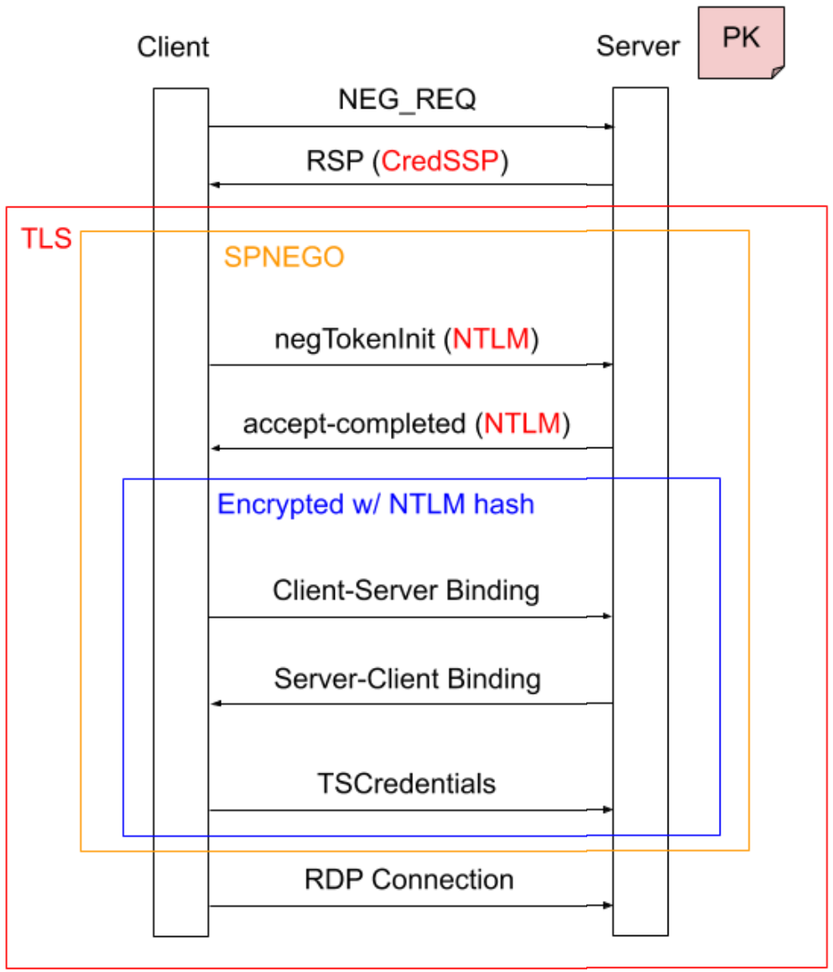
Attack Surface Reduction



Authentication: CredSSP

NLA's Authentication Mechanism

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

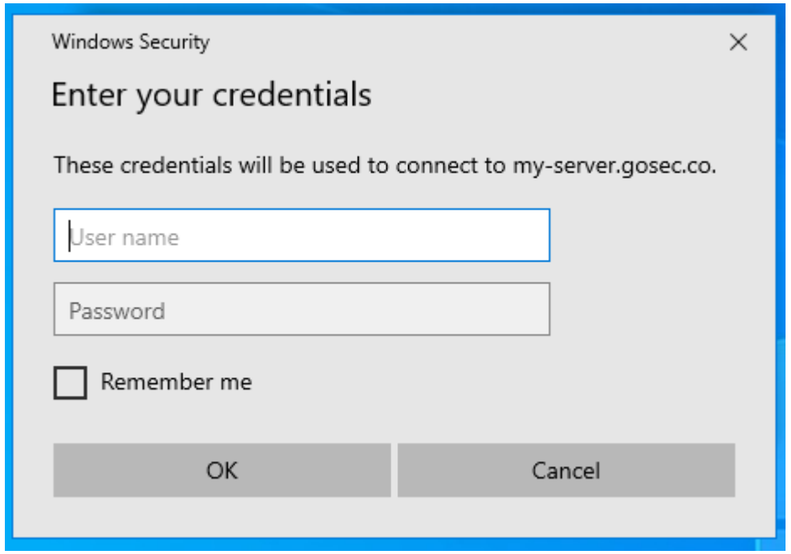


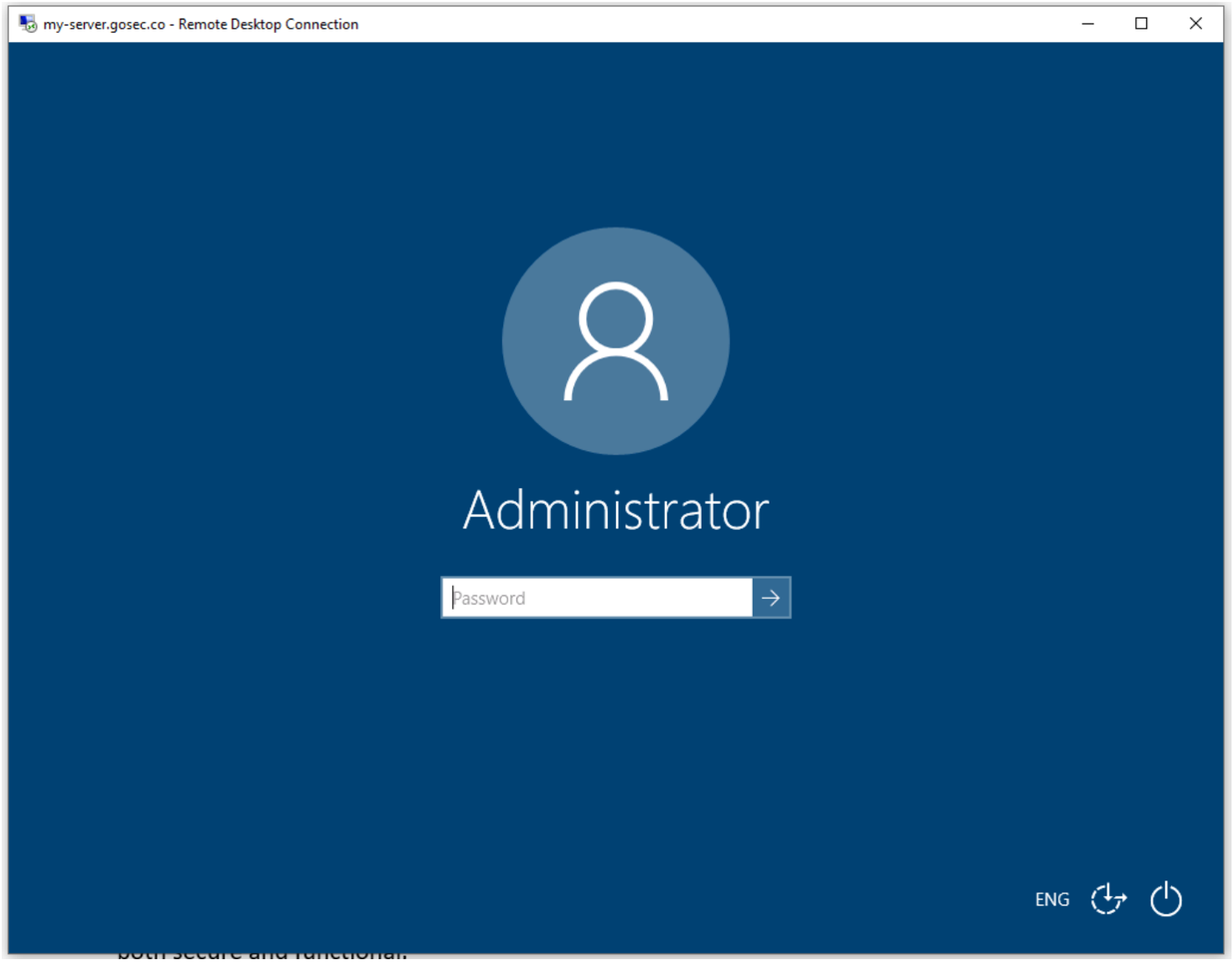
Attack: NLA Downgrade

GoSecure

NLA Attack #1: Downgrade Attack

Downgrade the NEG_REQ to remove CredSSP from supported protocols

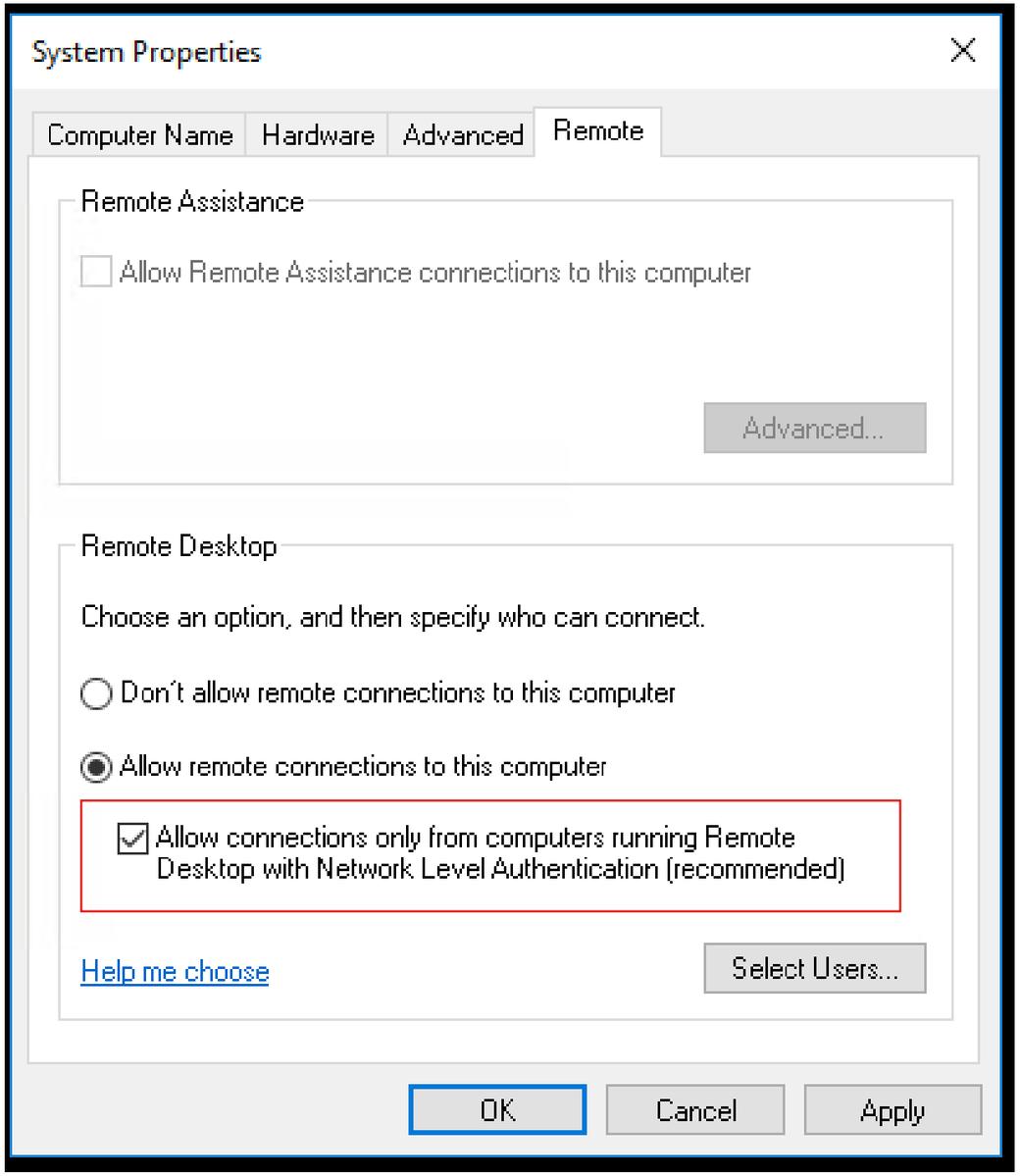




Defense: Network-Level Authentication (NLA) Enforcement

Prevent NLA Downgrade Attacks

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



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**

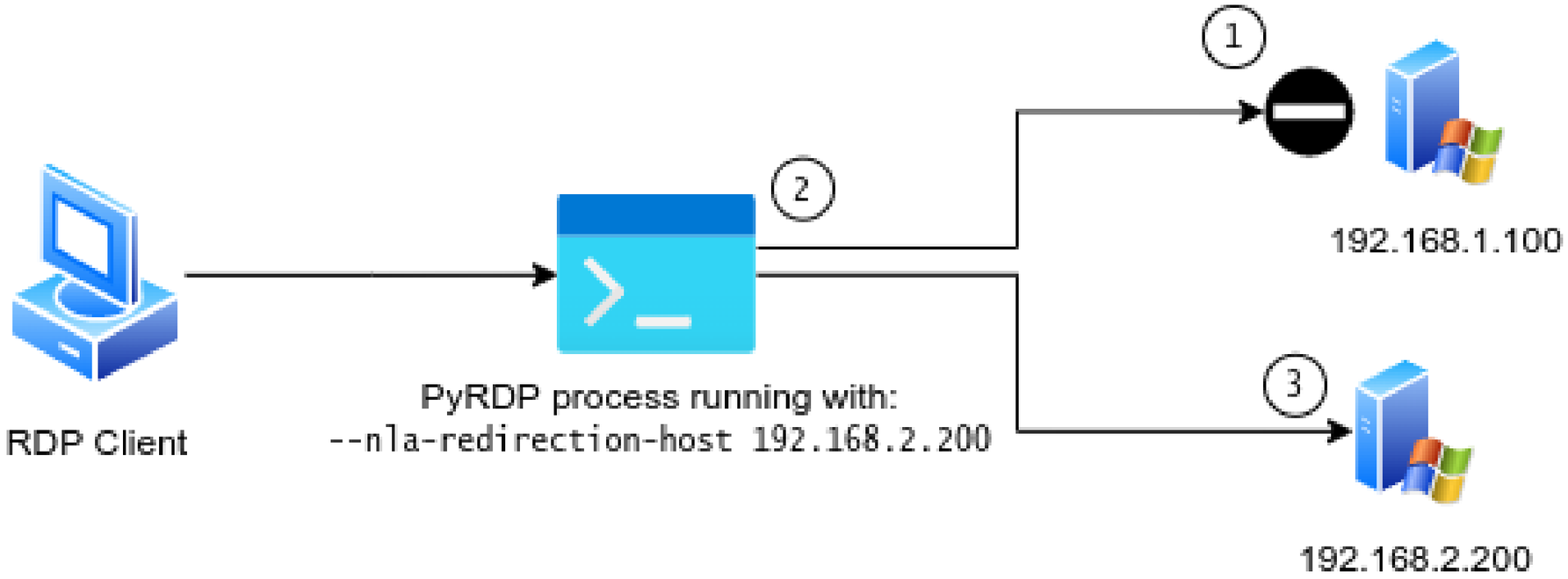
Can't be disabled by users afterwards 👍

Attack: NLA Redirection

GoSecure

NLA Attack #2: Redirection to Non-NLA

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

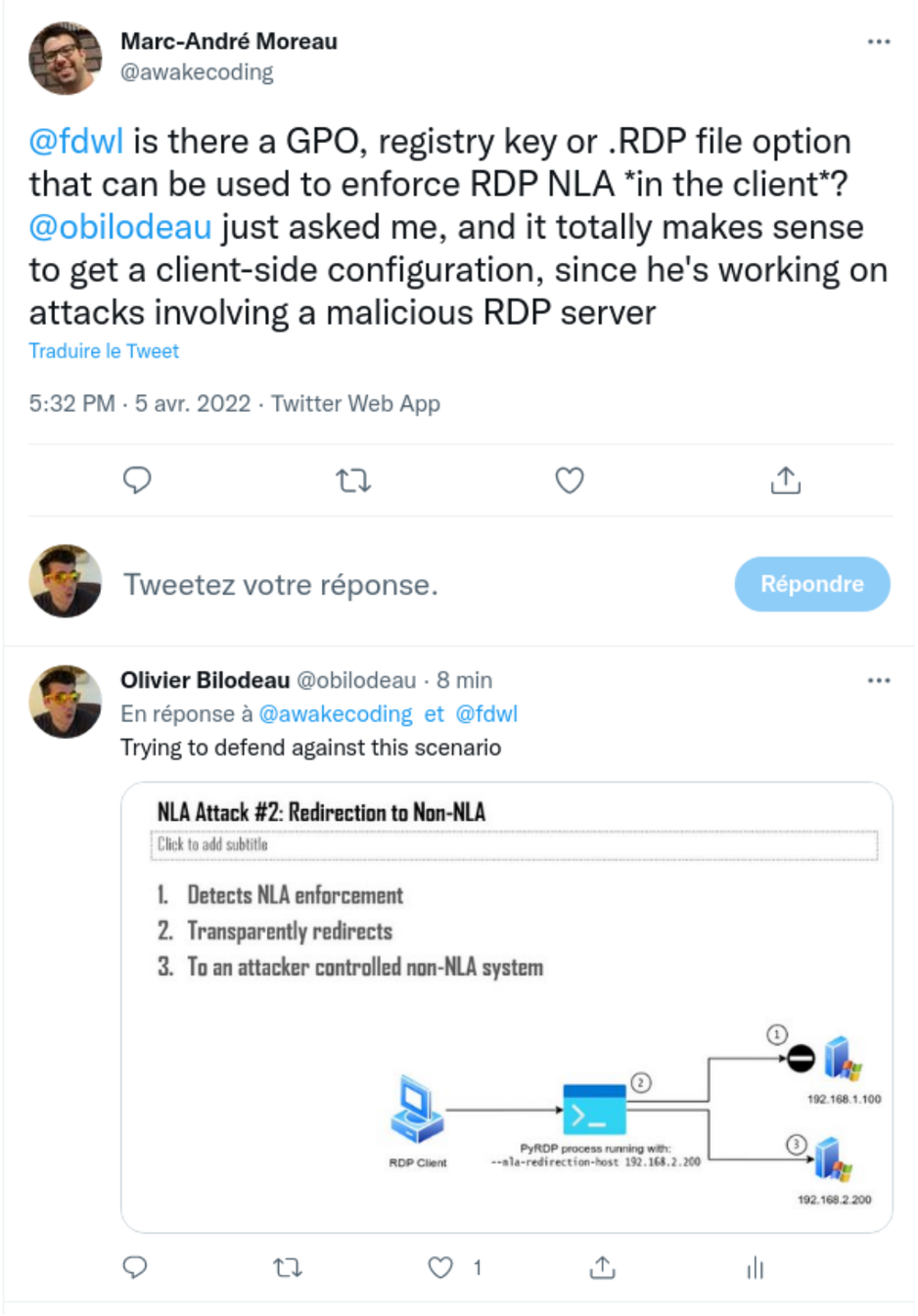


Prevent Redirection to Non-NLA

Bad News

No specific way to enforce NLA on the client side

sad trombone

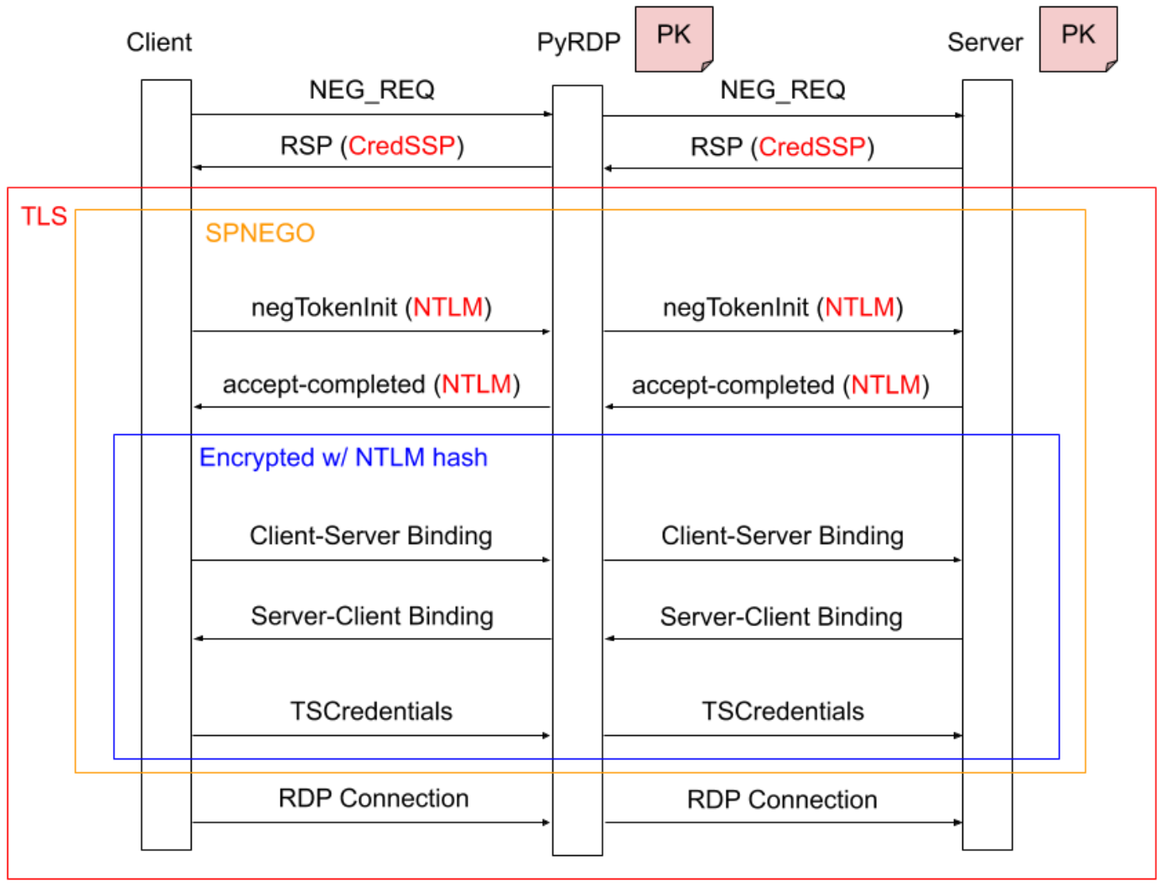


Attack: NLA Bypass

GoSecure

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

Demo: NLA Bypass

Noticeable Certificate Error

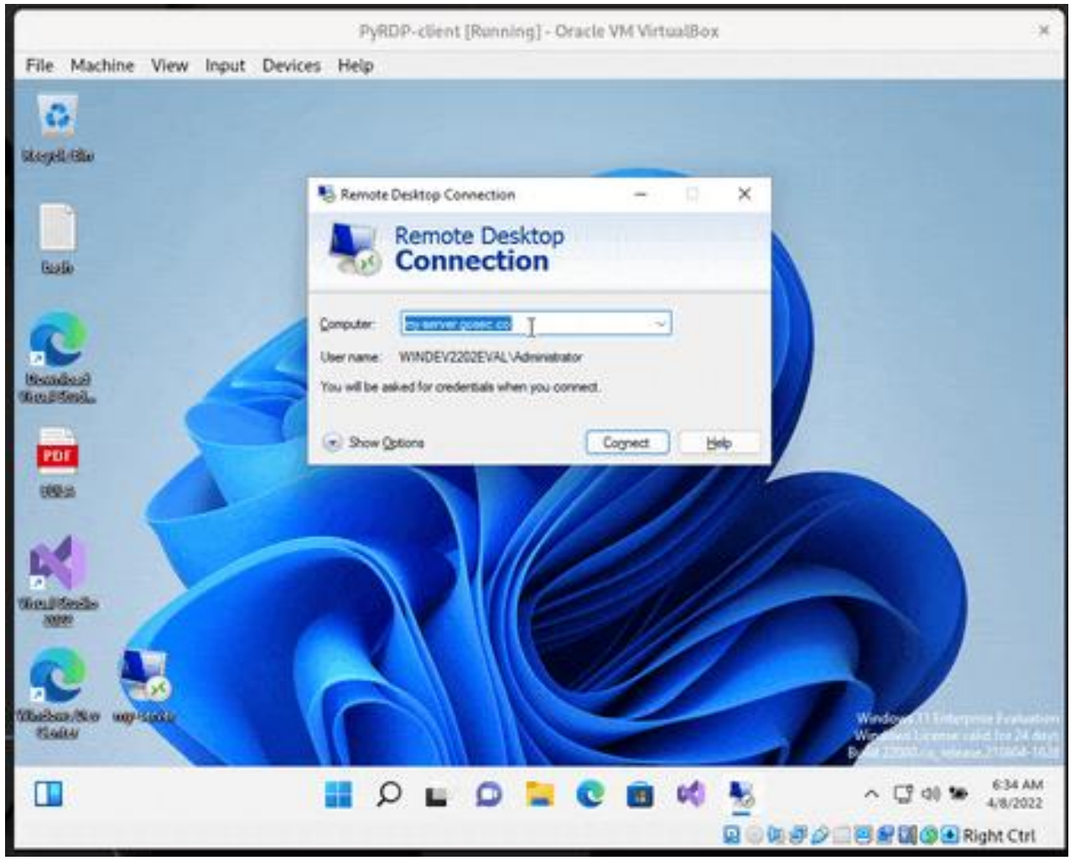
(link to video)

GoSecure

Defense: 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
- Solution!
  - [Let's Encrypt for Internal Hostnames](#) by Julien Savoie



Attack: Supply Trusted Certificates

GoSecure

Attacker Controlled Let's Encrypt Signed Certificate

Easy way to increase trust in a server

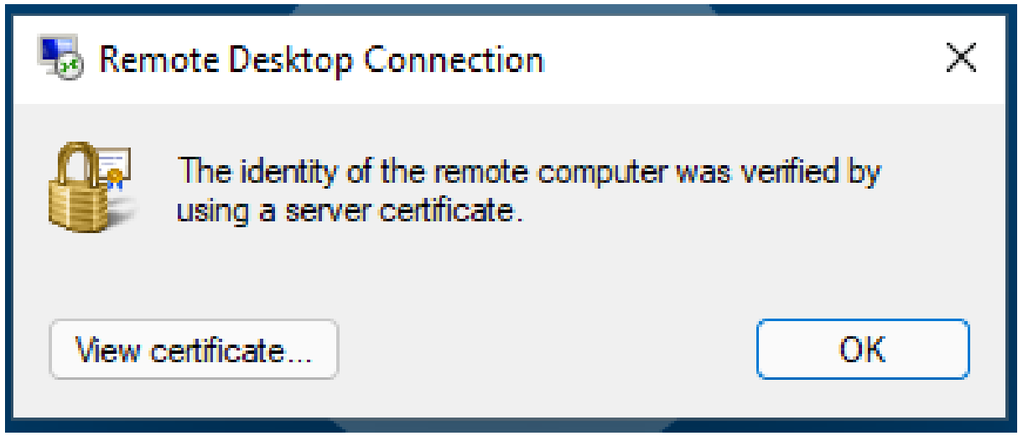
In Non-NLA only PyRDP requires the certificate

```
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.
```

Step by step:

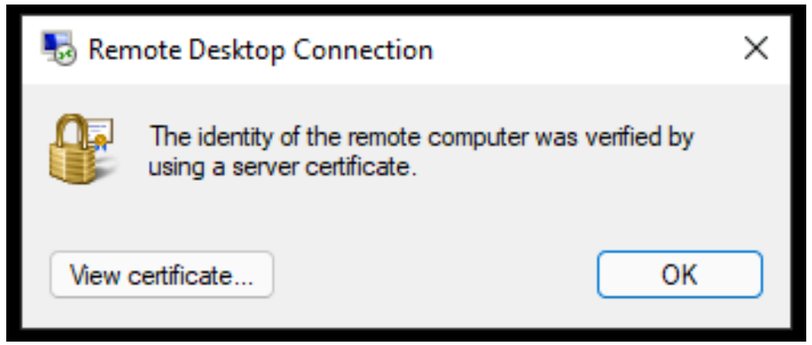
```
# with DNS already pointing to the PyRDP server
snap install core; snap refresh core
snap install --classic certbot
certbot certonly –standalone
```




```
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



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";
```

Demo: NLA Bypass with Certificates

This is as bad as it can get…

(link to video)

GoSecure

Attack:
NetNTLMv2 Hash Capture

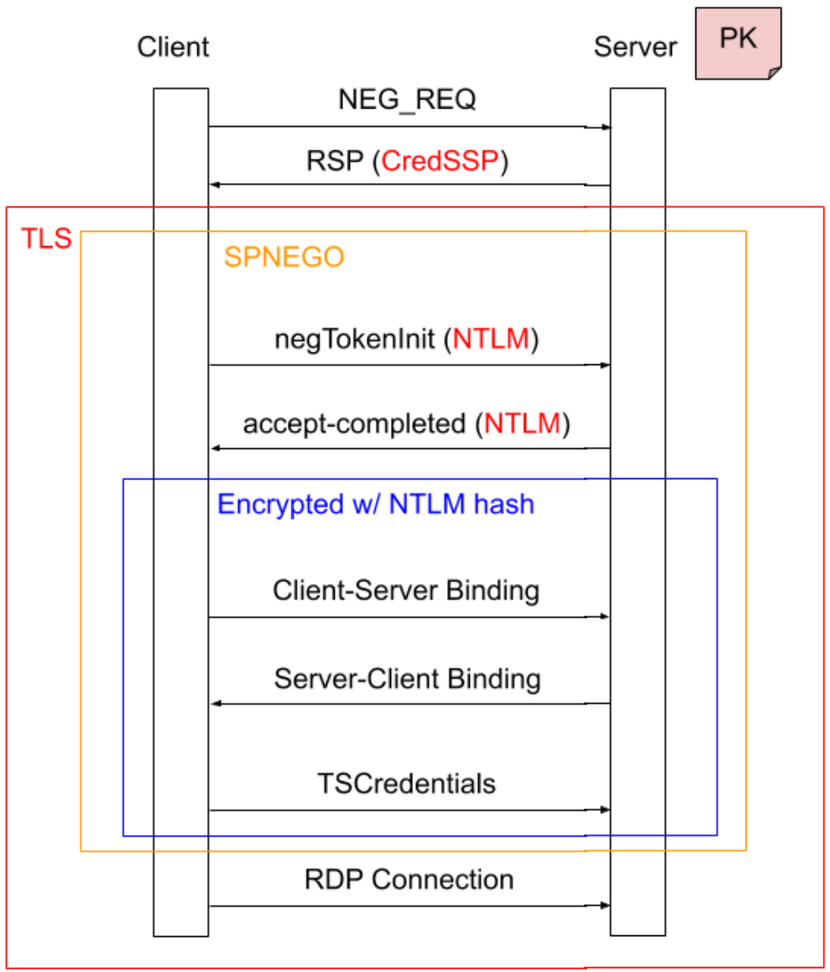
GoSecure

NetNTLMv2 Hash Capture

Inspired by Responder

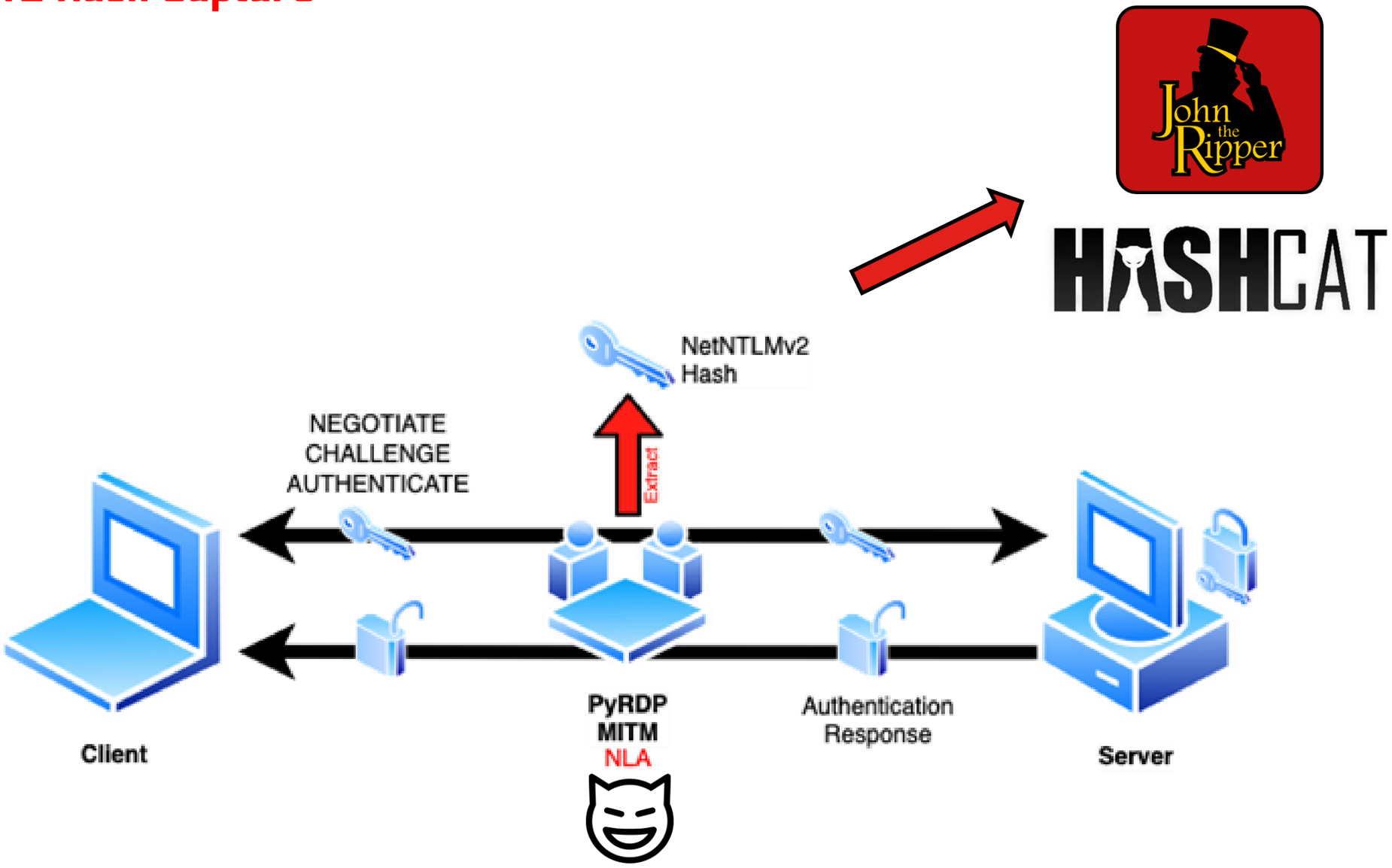
On an NLA authentication if we are in a MITM position we can collect NetNTLM hashes

- 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

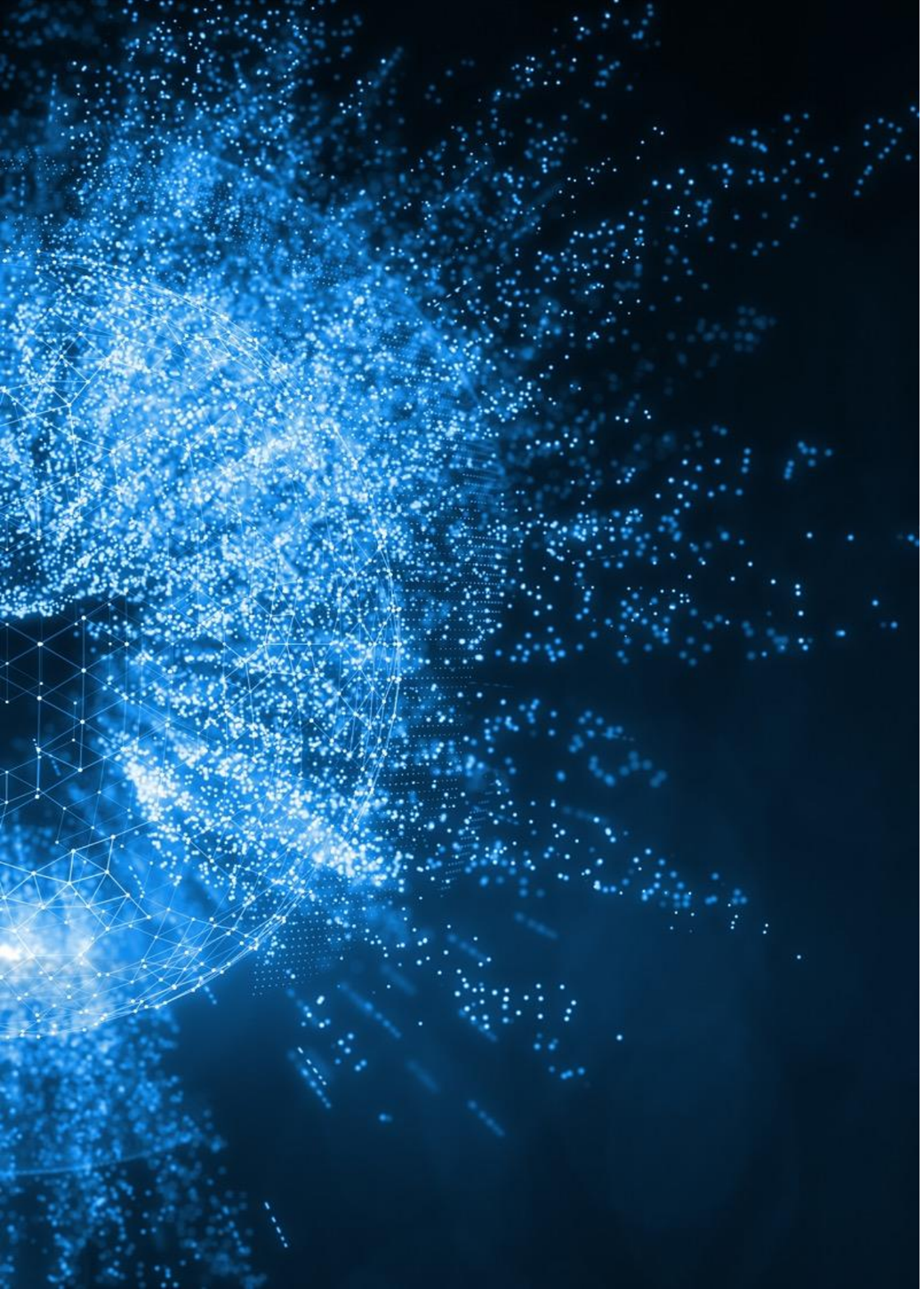
```
[2021-11-10 22:52:28,343] - INFO - Karen105427 - pyrdp.mitm.connections.ntlmssp - [!] NTLMSSP Hash:
admin:::937f60a48cea8943:f298d601927699c77aab319e7de5b9ac:0101000000000000000debca285d6d7015f3d313dc29e3
80c0000000002000a00570049004e004e00540001000a00570049004e004e00540004000a00570049004e004e00540003000a00
570049004e004e00540005000a00570049004e004e0054000600040002000000a0010000000000000000000000000000000000
0090022005400450052004d005300520056002f006c006f00630061006c0068006f00730074000000000000000000000000000000
000000000000000000000000000000000
```

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

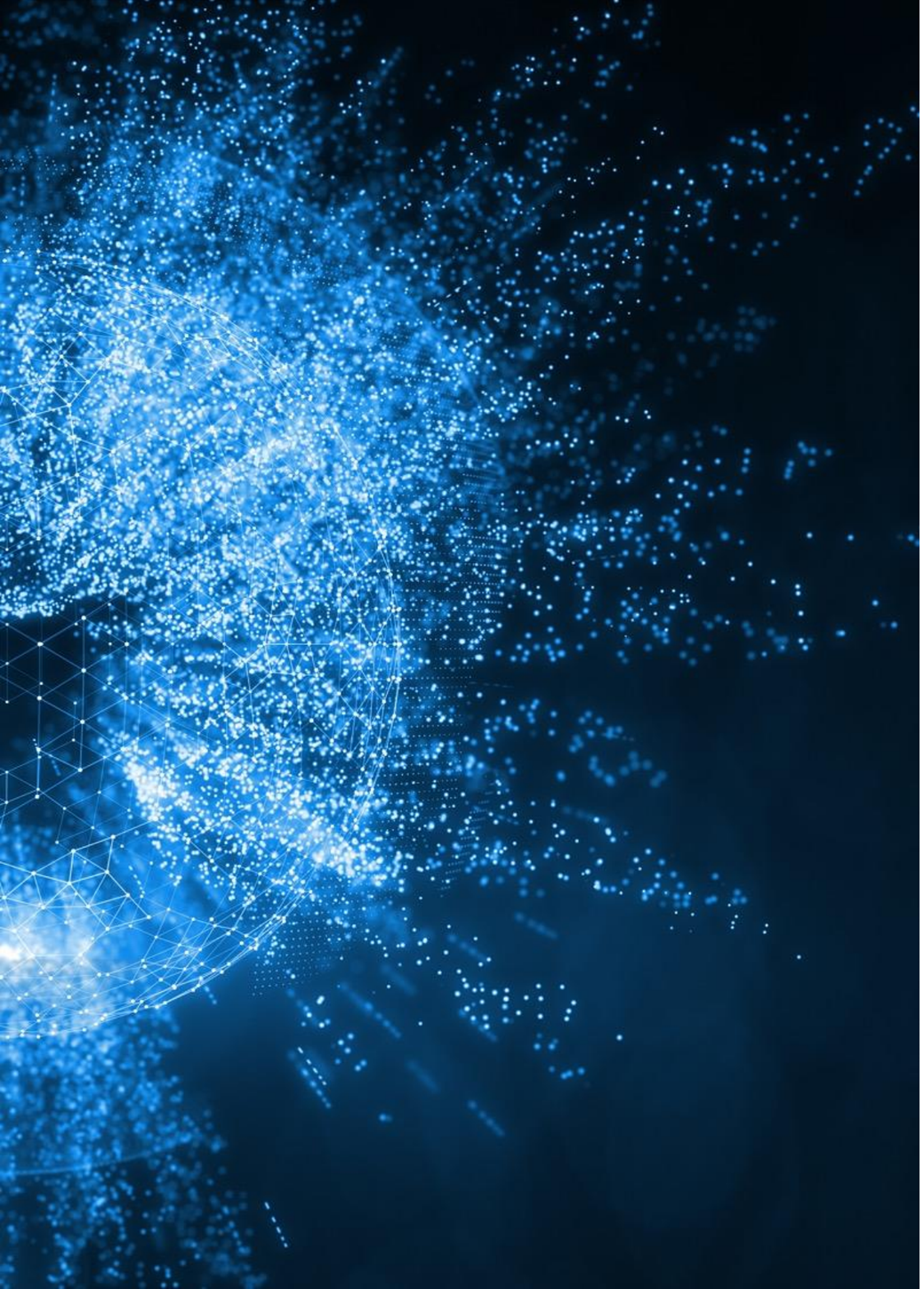
- Verify connection to RDP server
  - Server address
  - Domain name
- Always look for valid certificates
  - Attack tools will often use hardcoded certificate values
- But…

Demo: How Bad is it Really?

(link to video)

GoSecure

Defense: Preventing Hash Capture



Preventing Hash Capture

After what we found…

- Never use RDP on untrusted networks!
- Avoid NTLM => Use Kerberos
- Audit NTLM usage*

Attack: Rogue RDP

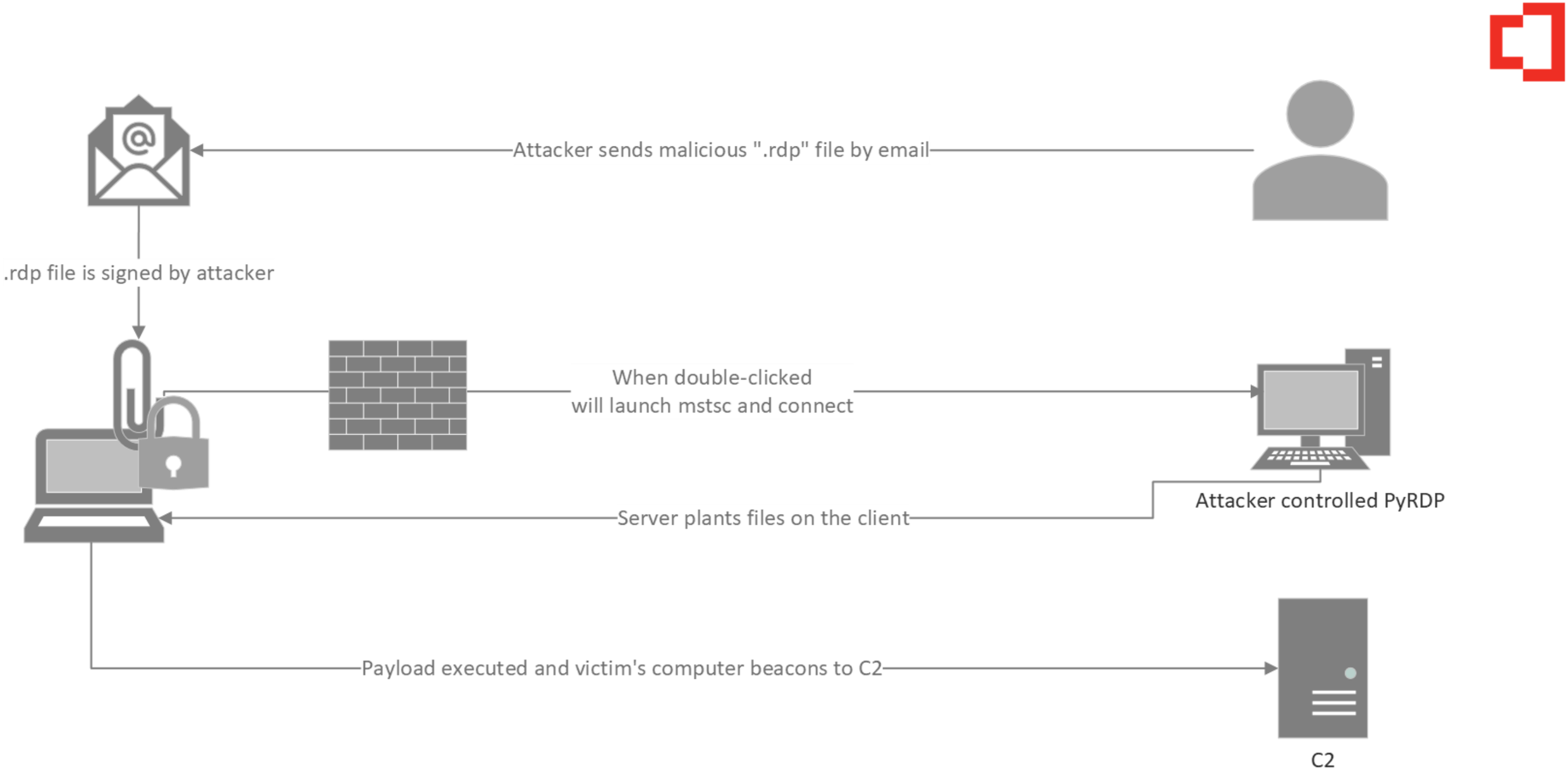
By Mike Felch (@ustayready)

GoSecure

Rogue RDP

Red Team tradecraft luring a victim to be an RDP **client** where the goal is to **avoid detection** at the cost of efficiency

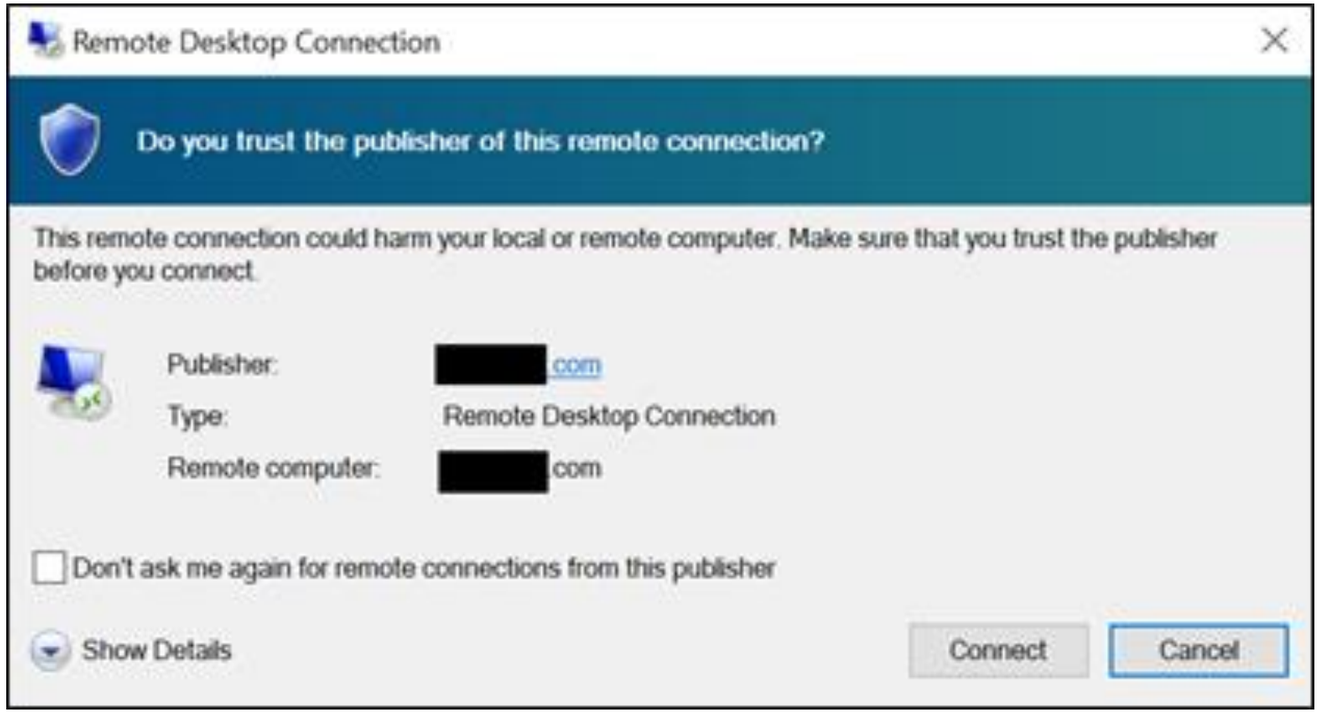
- RDP Phishing
- Victim connects to a weaponized RDP Server
- Server implants files on the client side



Full Attack Description: https://www.blackhillsinfosec.com/rogue-rdp-revisiting-initial-access-methods/

Attack Prerequisites

- Can receive ".rdp" attachments (default)
- Outbound access to 3389 or 443 (default)
- User convinced to click on "Connect"
  - Let's Encrypt works!
- Can map a drive via RDP (default)



Payloads

- DLL Sideloading
- LNK file on desktop
- Drop an executable in Startup Items
- Exfiltrate sensitive files
- Clipboard stealing

Why?

- EDRs don’t monitor Remote Desktop Services
- “.rdp” files can dictate RDP client features
- Rogue server is trusted

Defense: Preventing Rogue RDP

Preventing Rogue RDP Attacks

- Block ".rdp" files in email
- Prevent drive redirection via GPO

```
Group Policy Settings
Computer Configuration\
    Administrative Templates\
        Windows Components\
            Remote Desktop Services\
                Remote Desktop Session Host
```

More advanced detection tradecraft: https://blog.thickmints.dev/mintsights/detecting-rogue-rdp/

Defense: Avoid Bad Clients

Bad RDP Clients

Most clients that saved the certificate and credentials can be **downgraded** from NLA to non-NLA

Windows Credentials Store does save the server's security setting

mstsc.exe uses the Windows Credentials Store

Don't use most other clients

MobaXterm

mRemoteNG

Multi-Remote Next Generation

Remote Desktop Plus

Attack: Stealing Client Credentials from the Server

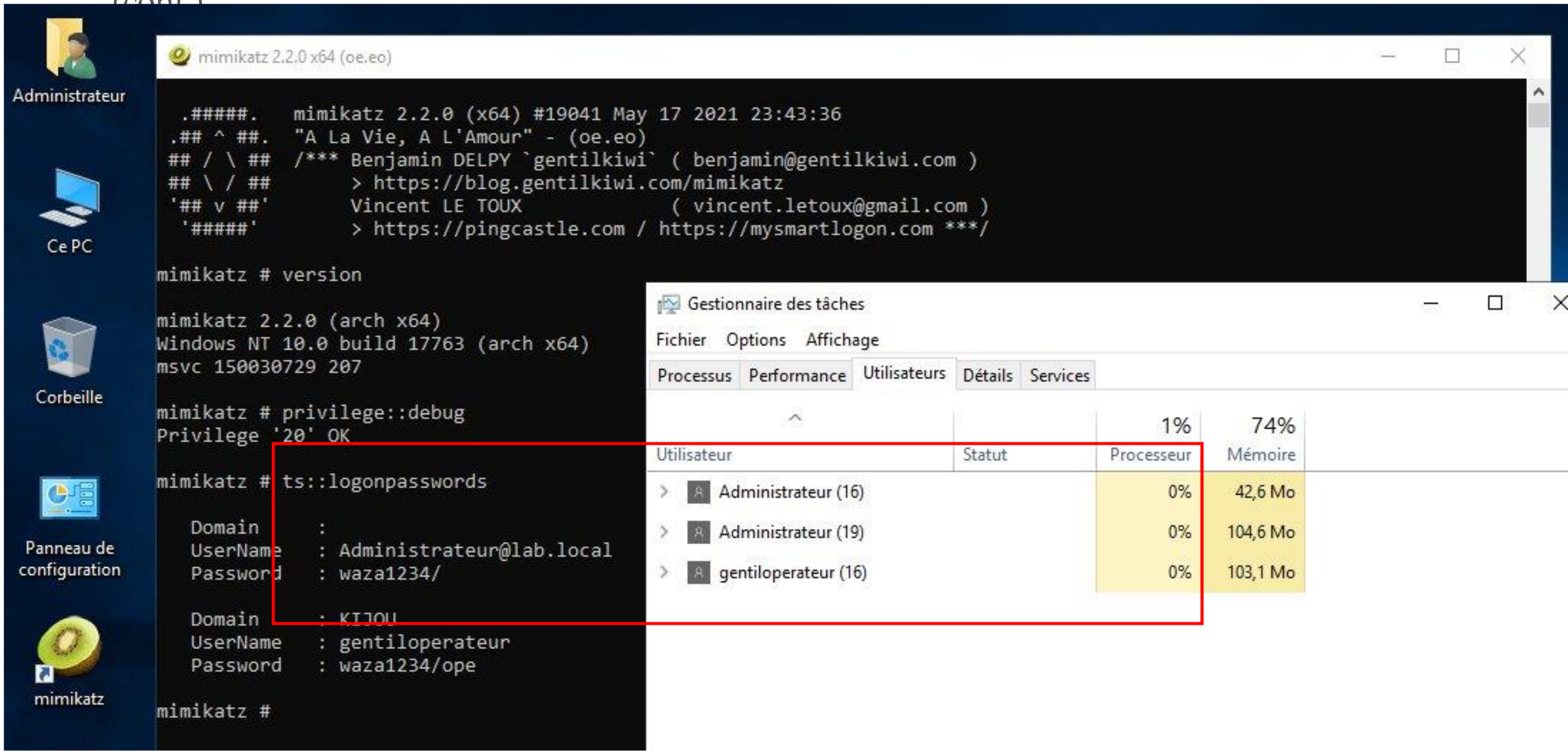
GoSecure

Stealing Client Credentials from the Server

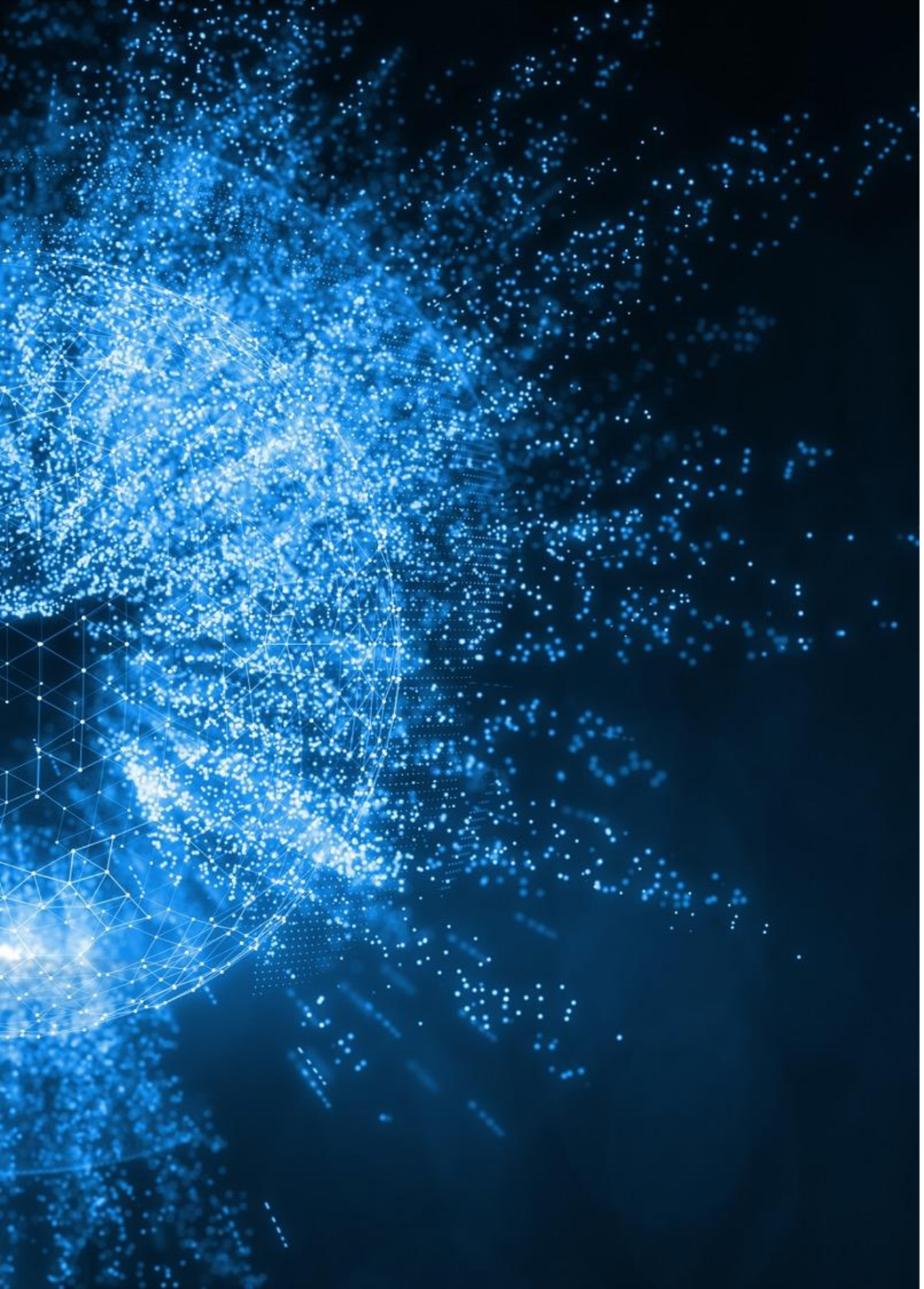
- Credentials are sent as part of NLA connection
- Terminal Service saves passwords in memory
- Passwords are in cleartext
- Mimikatz to the rescue :)

Stealing Credentials with mimikatz

(cont.)



Defense: Preventing Credential Theft



Preventing Credentials Theft

Three ways of protecting from this attack:

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

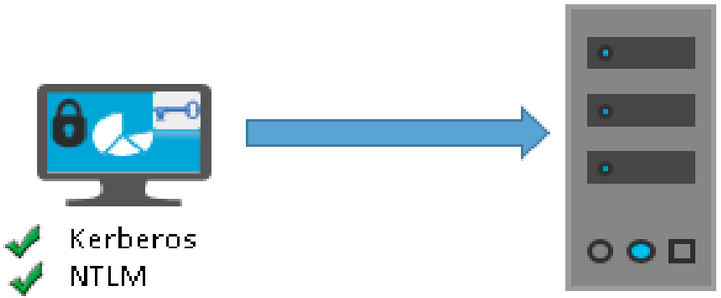
Preventing Credentials Theft

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

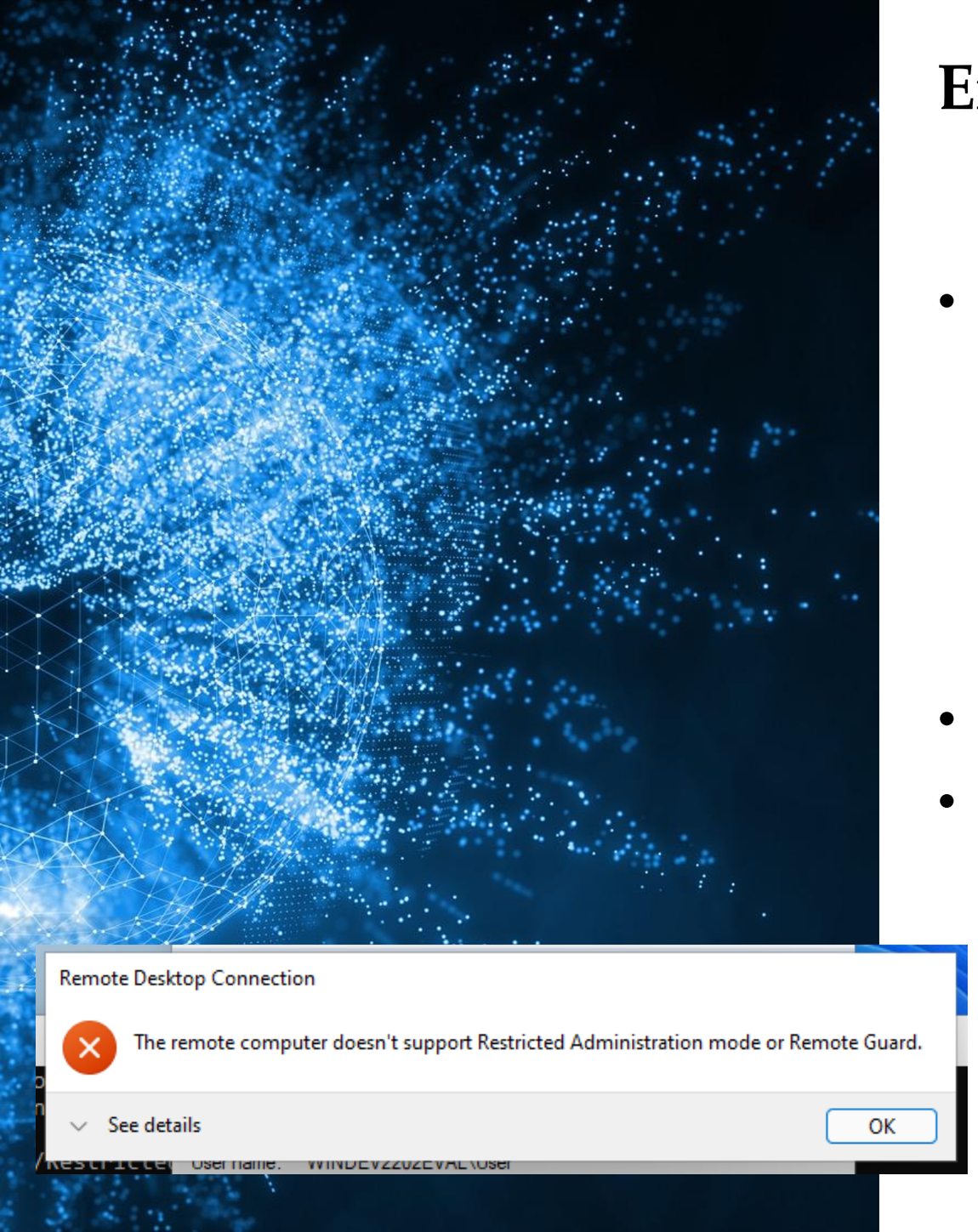
- Credentials used are remote server local admin credentials
- Connect to other systems using the host's identity
- Host must support Restricted Admin mode
- Highest protection level
- Requires user account administrator rights

= 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**. For more information about patches (software updates) related to Restricted Admin mode, see Microsoft Security Advisory 2871997.
Helps prevent	N/A	• Pass-the-Hash • Use of a credential after disconnection	• Pass-the-Hash • Use of domain identity during connection
Credentials supported from the remote desktop client device	• **Signed on** credentials • **Supplied** credentials • **Saved** credentials	• **Signed on** credentials only	• **Signed on** credentials • **Supplied** credentials • **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



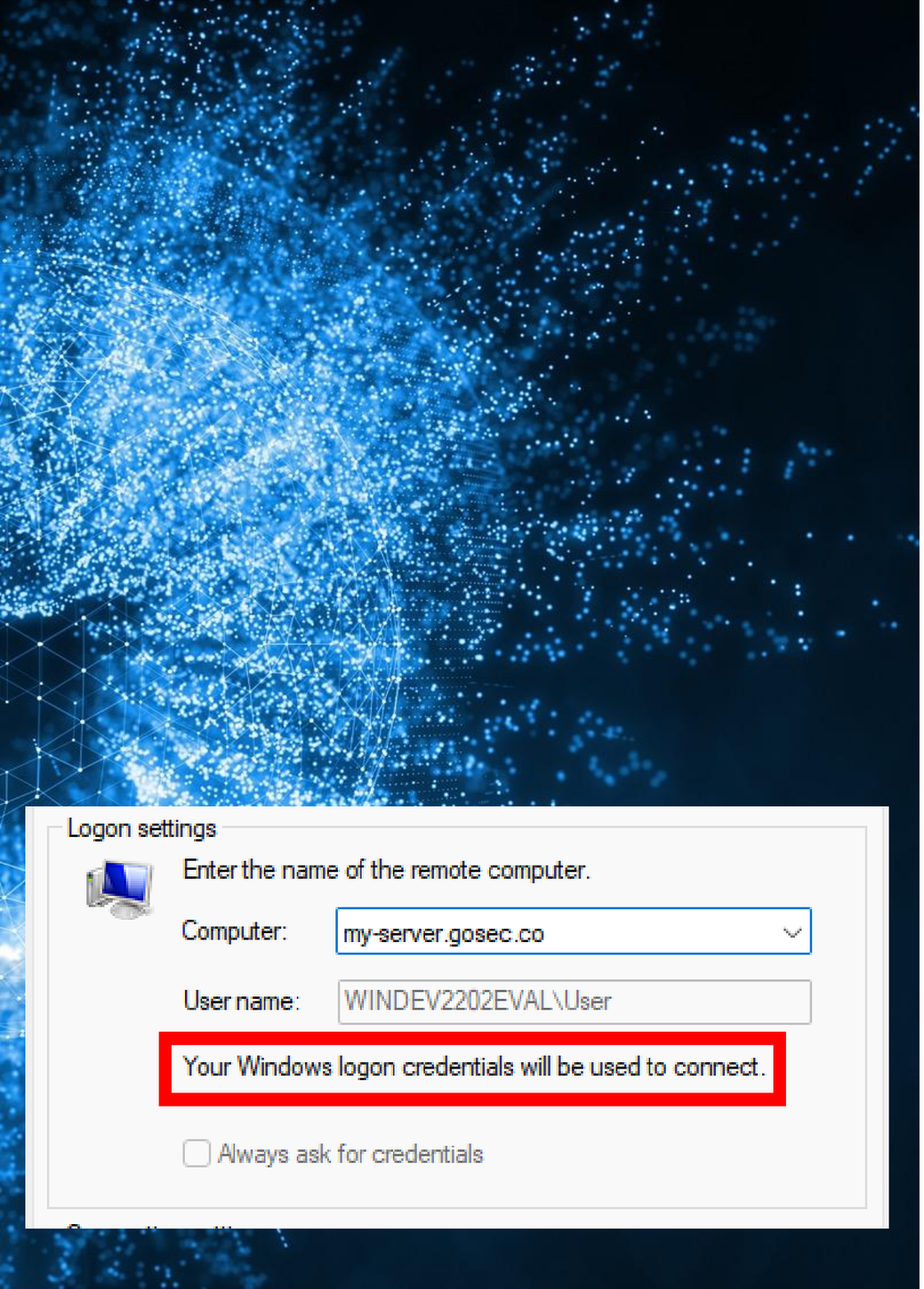
- Edit the RDP server's registry and enable this mode:

```
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
```

Enabling Remote Credential Guard



- 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

Wrapping Up

GoSecure

Recap of the Risks

Attacks on the Client

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

Attacks on the Server

- Credential Bruteforcing
- Session takeover
- Command injection
- Client Credential Stealing

Future Work

Blue Side

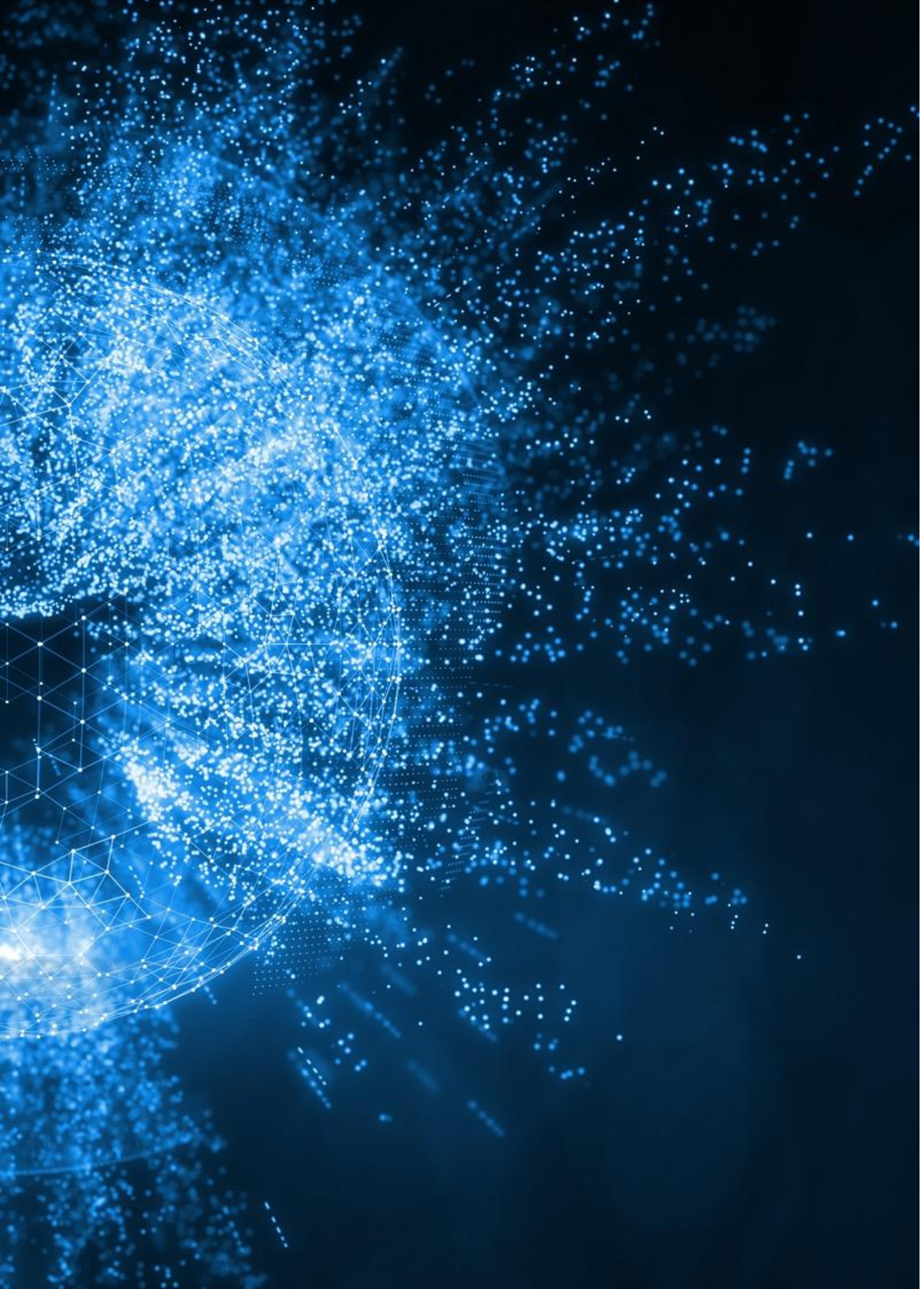
- RD Gateway / AVD
- Require valid TLS with specific CA
- NTLM Restrictions
- Shadow Attack Framework (AutoRDPwn)
- Enterprise-scale mitigation
- Blog, blog, blog!

Offensive Side

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

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!
  - No EDR/XDR coverage (that I'm aware of)



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

Special Shoutout!

Big shout out to Marc-André Moreau (@awakecoding)!

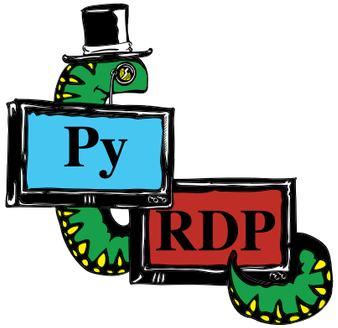
Thank You!

And Resources

Special Thanks to those that made PyRDP possible!

- Citronneur, Emilio Gonzalez, Francis Labelle, Maxime Carbonneau, Alexandre Beaulieu, Lisandro Ubiedo and coolacid

Questions?



References

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