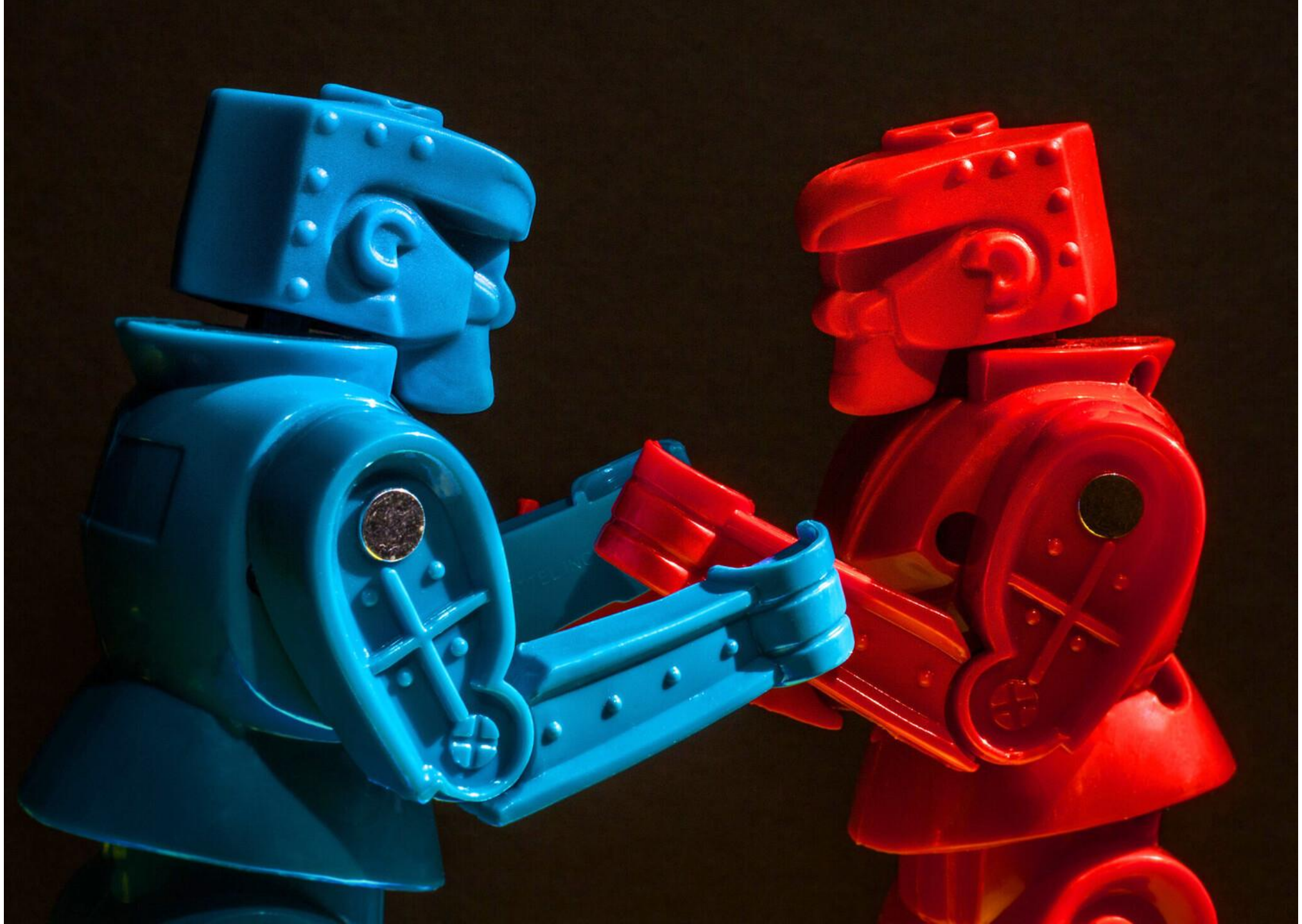
That’s Just a Tool – Not Good Nor Bad. That’s up to YOU.

Yossi Sassi

HackCon

The Norwegian cyber security convention



```
[>] Duplicating CreateProcessWithLogonW handles..
[!] No valid thread handles were captured, exiting!
PS ► while ($Bouzoukitara.Plugged -eq $true) {Enjoy-Moment -Recurse}
..hack
```

WhoAmI

- InfoSec Researcher; friendly H@ɔk3r
- Red mind, Blue heart
- Co-Founder @ 10 ROOT CYBER SECURITY
- Consulting in 4 continents (Banks/gov/F100)
- 35 years of keyboard access – Code, IT Security, Network communications
- 'The HAcktive Directory guy' ☺ (25 years of AD); Ex-Javelin (Acquired by Symantec)
- Ex-Technology Group Manager @ Microsoft (Coded Windows Server Tools)
- Volunteer (Youth at risk); Pilot; Oriental Rock Bouzoukitarist

What we'll talk about

- Mindset: "Living off the Land" examples
- RPC, IPC, RDP, WinRM / PSRemoting
- Credentials exposure during Remote Operations
- Do you need a TCP connection for a C2?
- Tips & open-source toolZ

Tools in a ‘Living off the land’ mindset

- Leveraging functionality that is already available
- Built-in tools/APIs abuse (e.g. powershell)
- “Blend in” as a legitimate process

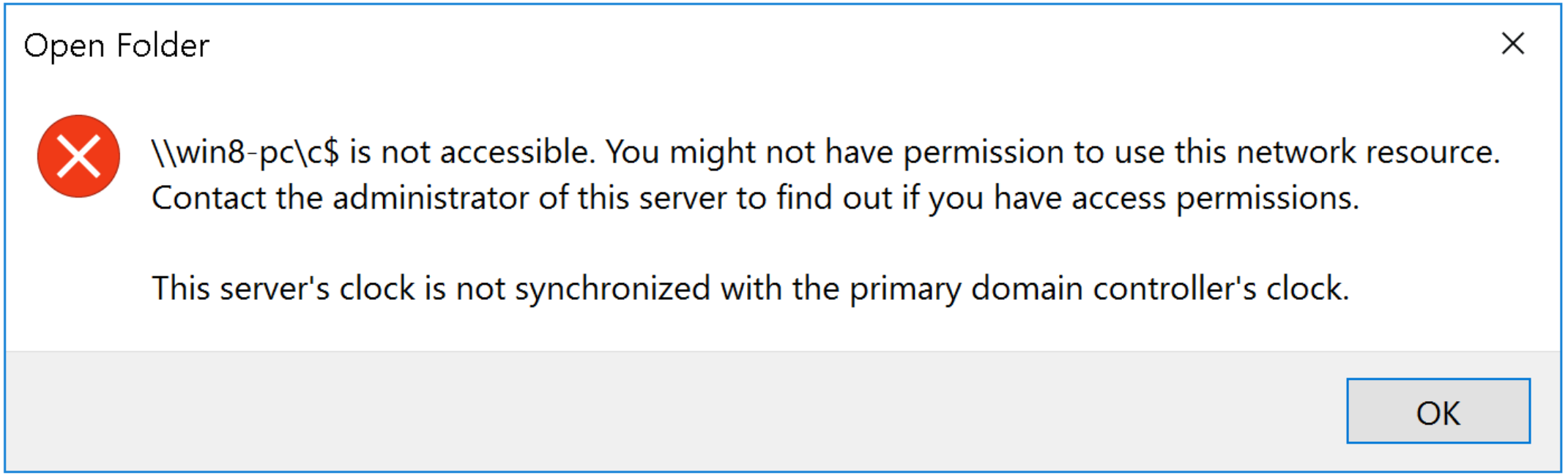
Remote Management or Lateral Movement?

Remote Procedure Call (RPC)

- System service that is an inter-process communication (**IPC**) mechanism, enabling data exchange and invocation of functionality that is located in a *different* process.
- The different process can be on the same computer, on the LAN, or in a remote location
- The RPC service serves as the RPC Endpoint Mapper and Component Object Model (COM) Service Control Manager (Remotely – DCOM)
- *Many* services depend on the RPC service to start successfully

https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/service-overview-and-network-port-requirements

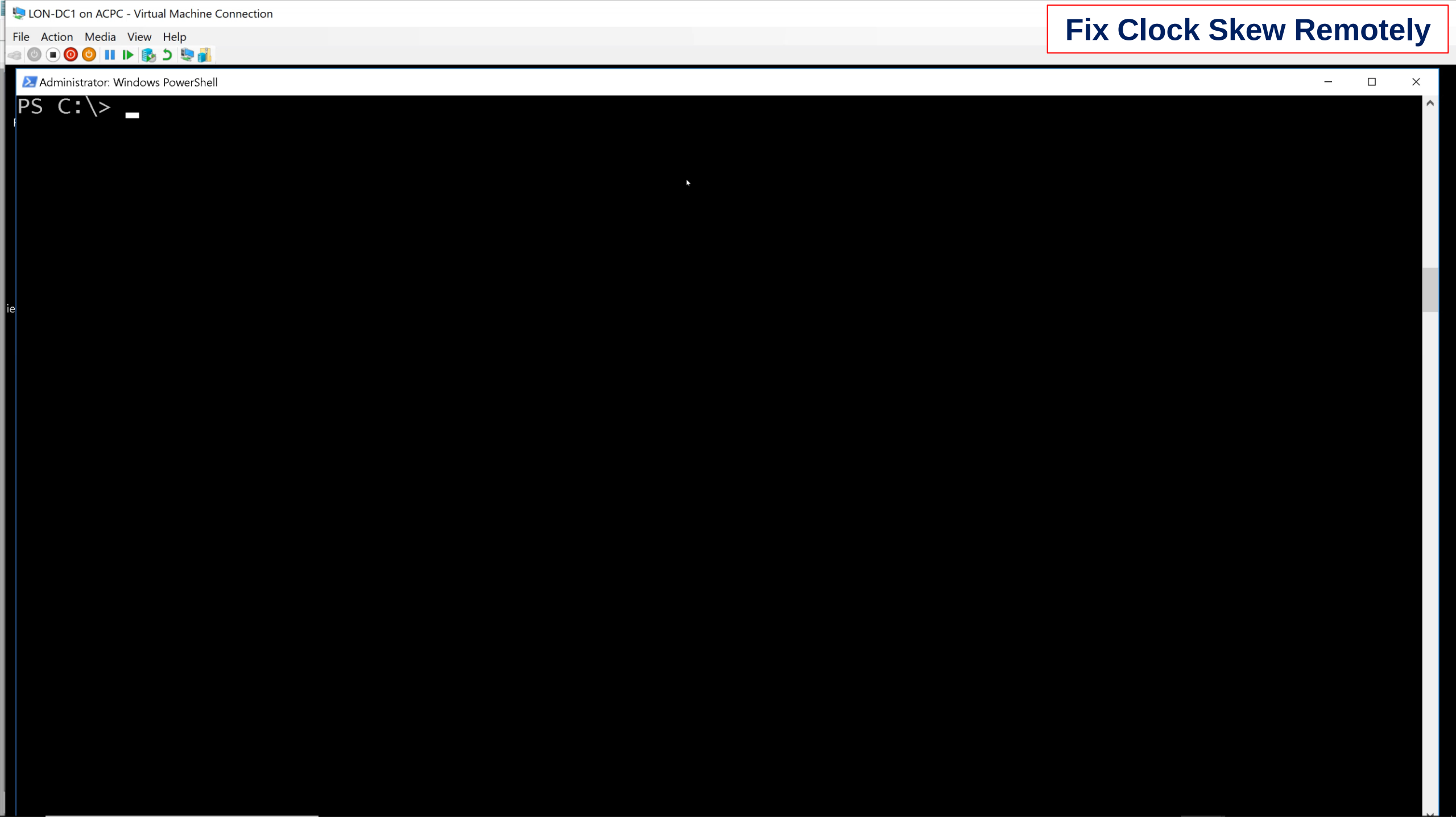
‘RPC Not Available’ / Kerberos Clock Skew



TIP: Fixing Clock Skew Issues Remotely

- e.g. ‘RPC not available’ errors (host is online, yet no Kerberos)
- Determine if clock skew exists
  - Net time \\computer (*does Not* require special permissions)
- $varDate = Get-Date; Invoke-Command -ComputerName **<IP>** -ScriptBlock {set-date **$using:**varDate} -Authentication **Negotiate**
- Cannot run winrm, or even ping(!) the host, because clock Diff, and no KRB? **try WMI process create w/IP (NTLM)**

Invoke-WmiMethod -ComputerName **<IP>** -Class win32_process -Name Create -ArgumentList "w32tm /resync"


LON-DC1 on ACPC - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell
PS C:\>
Fix Clock Skew Remotely

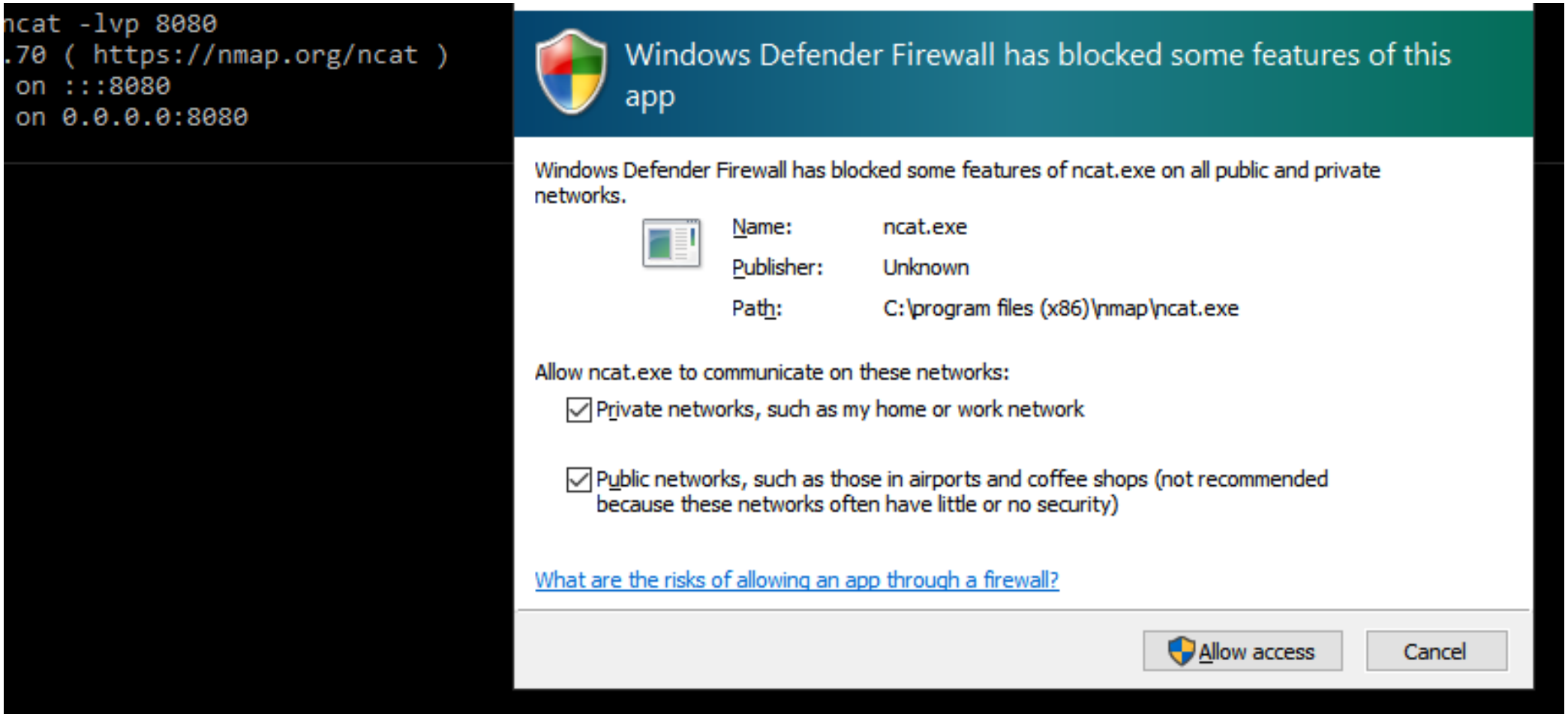
Inter-Process Communications (IPC)

- Pass strings/objects/execute code between processes, ***local*** or ***remote*** – using Named Pipes

- Pass info between processes on same machine easily through IPC$

- Communicate between local or remote powershell runspaces over one/two-way, encrypted pipe

- Can also use it for **C2**, ***without*** opening FW port, ***without*** local admin privileges.
  - No need to Bind() server local port, just “rides” 445 ☺



Named-Pipe/SMB One-liner

(Exfiltrate data/C2 with No socket bind)


LON-CL1 on ACPC - Virtual Machine Connection
File Action Media Clipboard View Help
PowerShell
PS C:\>
IPC C2

NamedPipes – Detection Gaps

- *No ETW provider* for creation of/connection to named pipes out-of-the-box (need **file system minifilter driver**)

NamedPipes – Detection Gaps (Cont.)

kobykahane / NpEtw Public

Notifications | Fork 14

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master | 1 branch | 0 tags | Go to file | Code

kobykahane Build with Visual Studio 2019. ad1bfbb on Jul 24, 2020 44 commits

NpEtw	Build with Visual Studio 2019.	3 years ago
NpEtwSetup	Build with Visual Studio 2019.	3 years ago
.gitattributes	Initial commit to add default .gitIgnore and .gitAttribute files.	8 years ago
.gitignore	Build with Visual Studio 2019.	3 years ago
NpEtw.sln	Build with Visual Studio 2019.	3 years ago
README.md	Add AppVeyor build status.	7 years ago

README.md

#NpEtw

build passing

NpEtw is a sniffer for named pipe I/O operations on Windows. It can be used to monitor create, read, write and other operations on named pipes in the system.

About

Named pipe I/O ETW provider for Windows

Readme

56 stars

11 watching

14 forks

Releases

No releases published

Packages

No packages published

Languages

C++ 63.0% Roff 25.5% C 11.5%

NamedPipes – Detection Gaps

- *No ETW provider* for creation of/connection to named pipes out-of-the-box (need **file system minifilter driver**)
- Can observe named pipe events by monitoring **Kernel Object Handle provider** (info on *all* handles that are opened and closed, very "noisy“, ID 4656)

```
auditpol /set /subcategory:"Handle Manipulation" /success:enable /failure:enable
```

- Can use **Sysmon -** <PipeEvent onmatch="include">
  - …still “noisy” (filter duration -gt 10 seconds)
- Can monitor **SMB open files with “\” prefix**

RDP – Windows admins' favorite feature

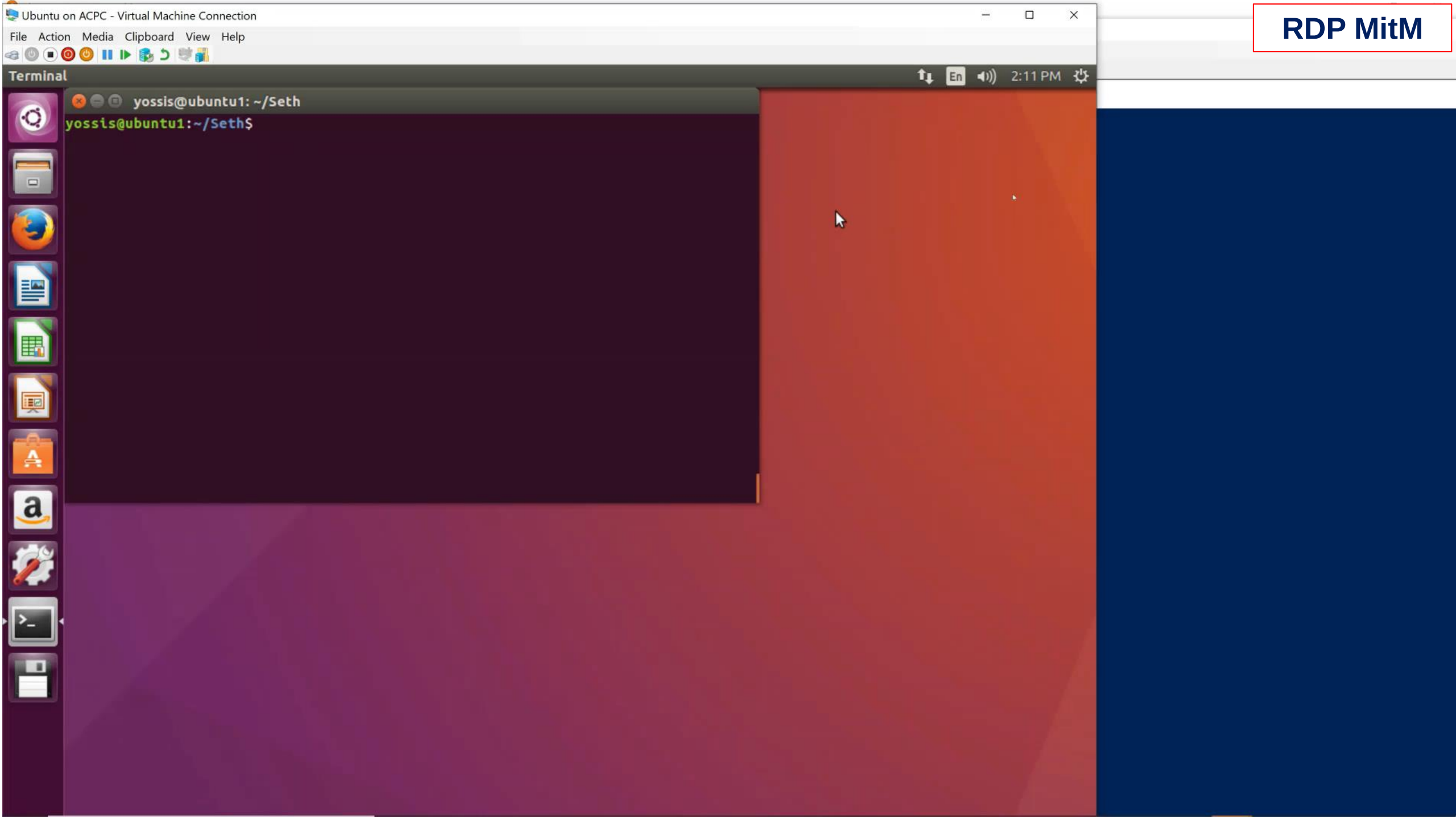
RDP Attacks & adversary tools

- Brute force
- MitM
  - Seth.sh
  - pyRdp
- “TS Shadowing”
  - Taking over disconnected RDP sessions

.. and more

RDP MitM

- Get netNTLM, at minimum.
- Can also get **clear text password**.
- Downgrades session, fakes certificate, attempts CredSSP.
- Can also get clipboard/typed text directly to attacker.
- Victim is totally unaware (RDP session functions normal, just a bit slower initial connection time)


Ubuntu on ACPC - Virtual Machine Connection
File Action Media Clipboard View Help
Terminal
En
2:11 PM
yossis@ubuntu1: ~/Seth
yossis@ubuntu1:~/Seth$
RDP MitM

Getting Clear-Text password from any RDP Server

- With proper permissions – can disable NLA remotely – either by modifying the Regkey directly, or via Powershell:

```
(Get-WmiObject -class Win32_TSGeneralSetting
-Namespace root\cimv2\terminalservices
-ComputerName SRV1 -Filter "TerminalName='RDP-tcp'").SetUserAuthenticationRequired(0)
```

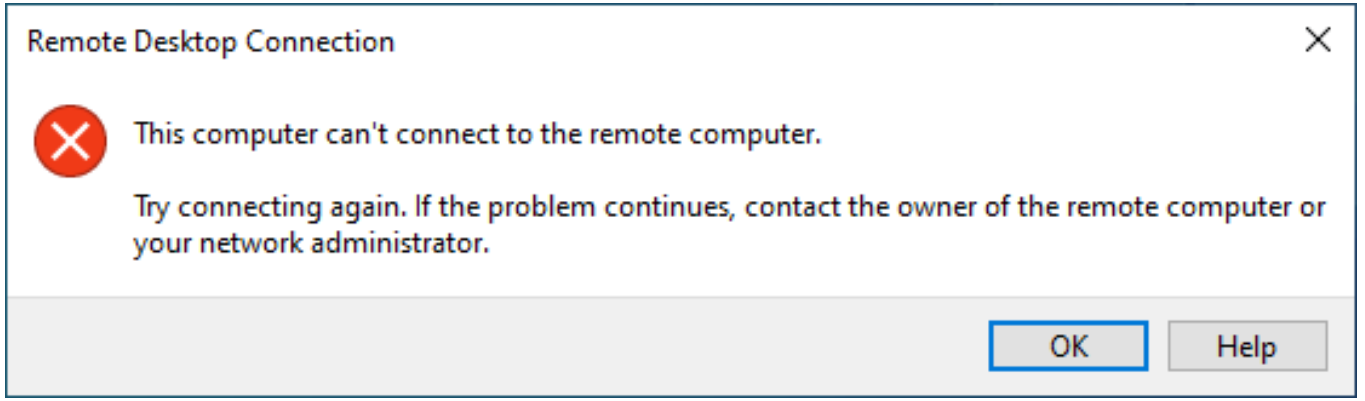
- **Can use inveigh/responder to relay the Registry command, and/or 'net localgroup administrators /add user'**
- More silent, efficient & quicker than mimikatz etc. ;-)

Mitigations / Detections – RDP MitM

- GPO: Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security > **Require user authentication for remote connections by using Network Level Authentication** > Enabled

  Will block the rdp connection from non-AuthN hosts

  Will *NOT* prevent NetNTLM+Clear text, yet block RDP & Alert



Mitigations / Detections – RDP MitM (Cont.)

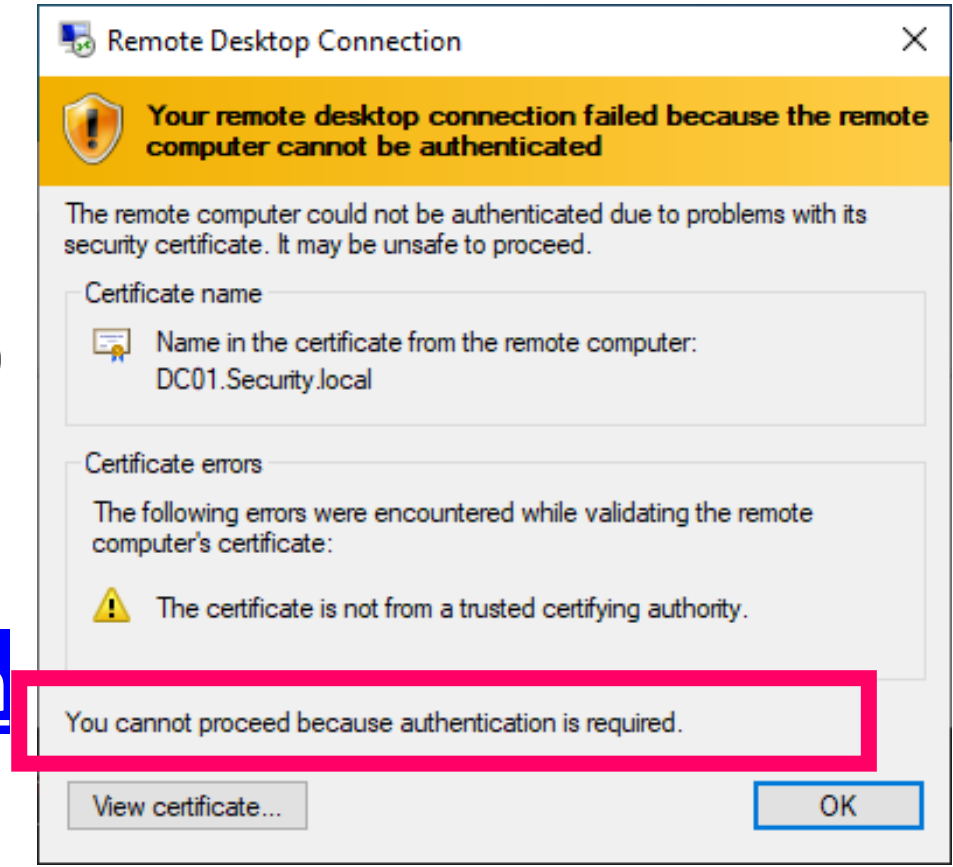
- Configure Certificates + GPO: Computer configuration > Policies > Administrative Templates > Windows Components >Remote Desktop Services > Remote Desktop Connection Client > **Configure server authentication for client**

Disallow the connection,

IF certificate cannot be validated **(Req. PKI/Certs)**

Will *Not* prevent NetNTLM,

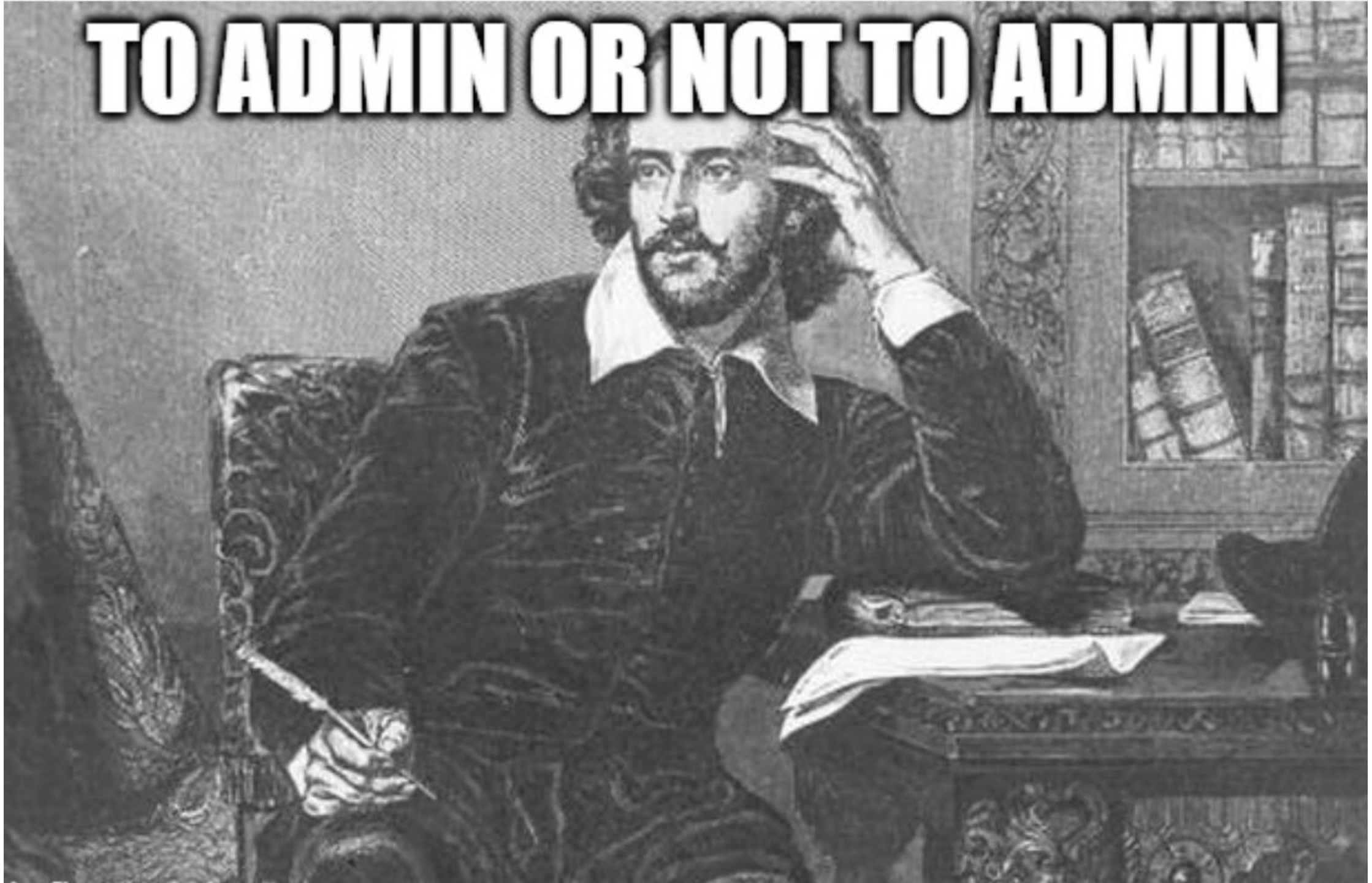
but will prevent clear text + Block connection



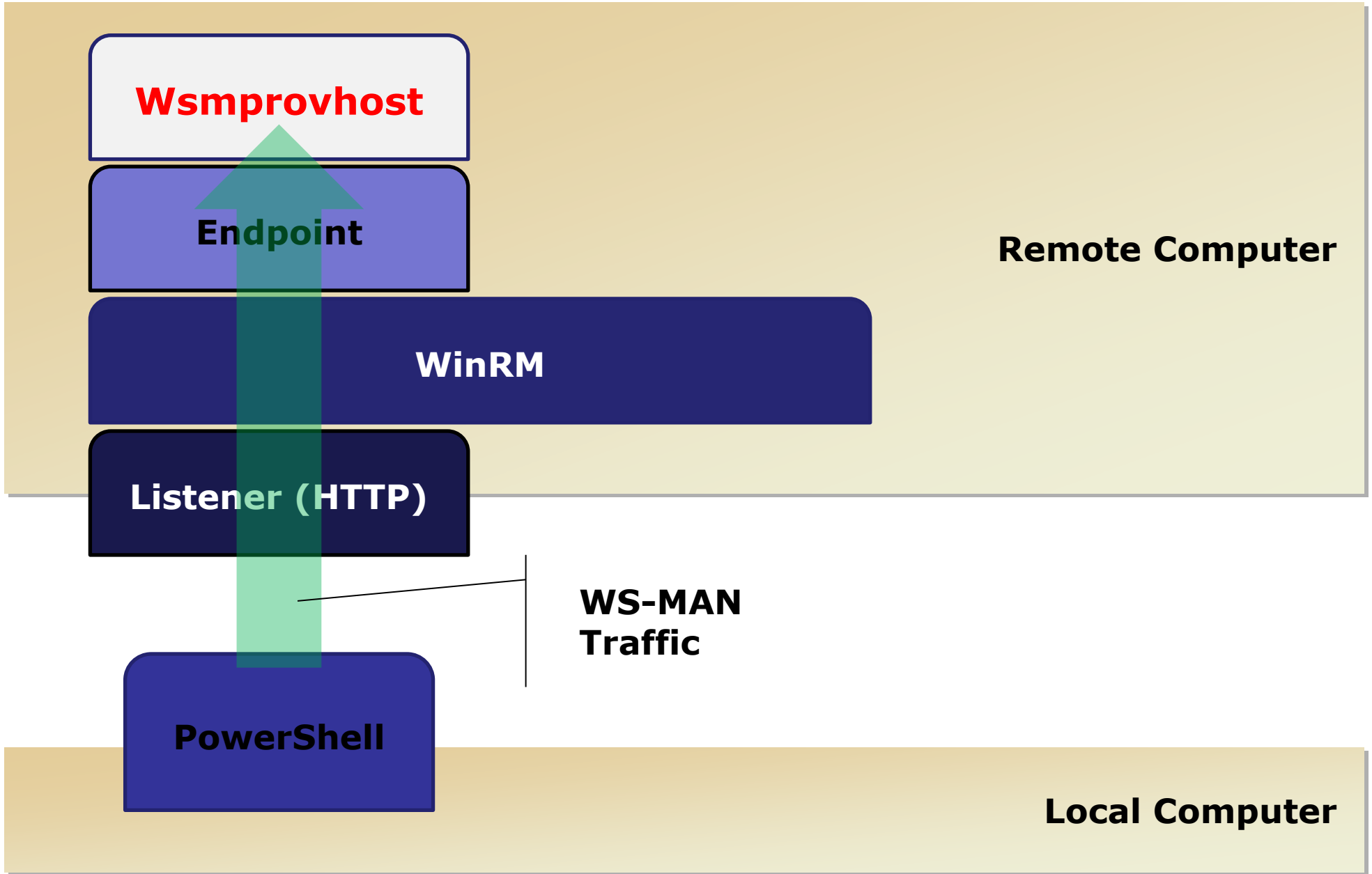
RDP Session Hijacking w/USB

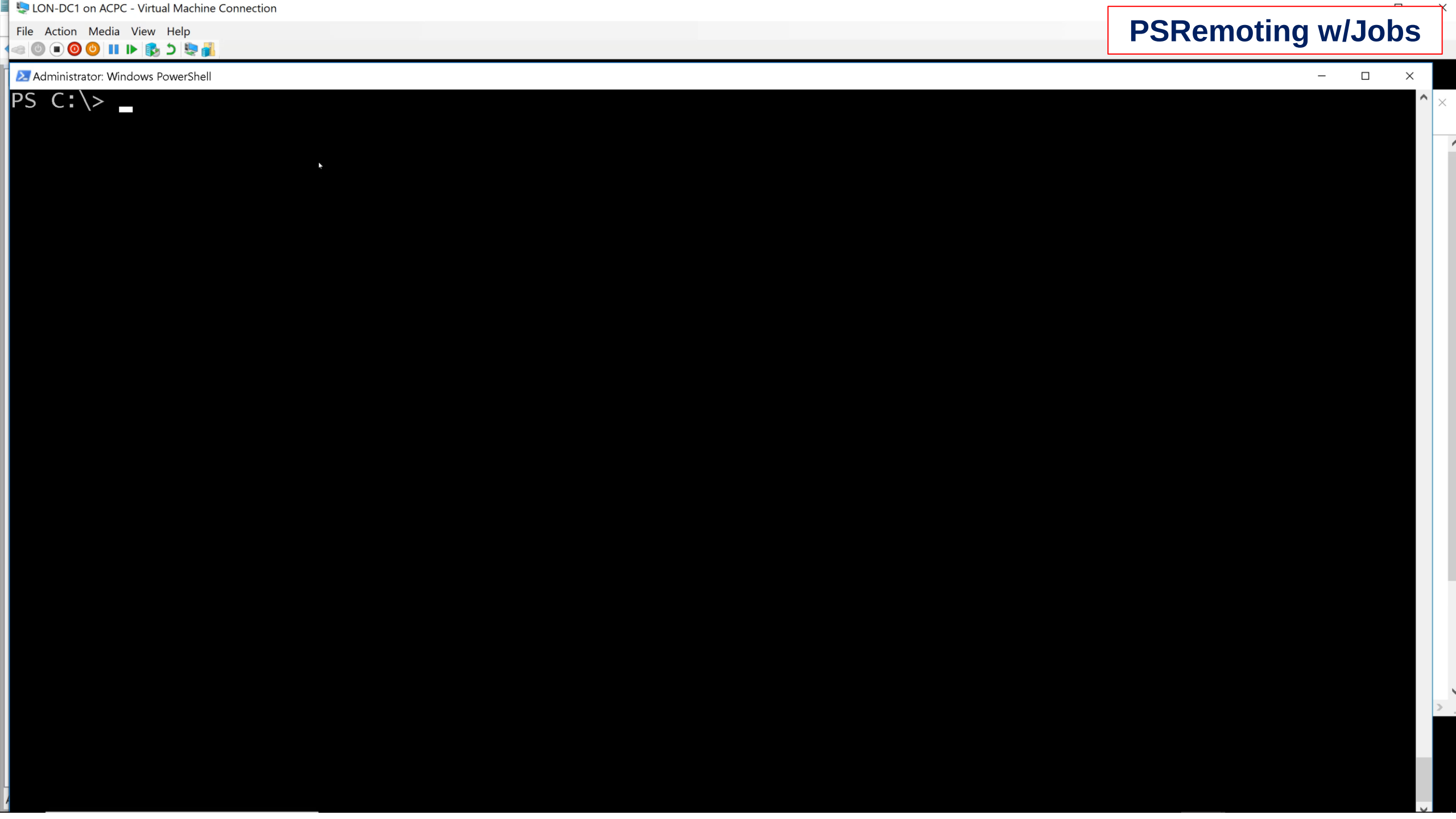
Mitigations – RDP Risks (Cont.)

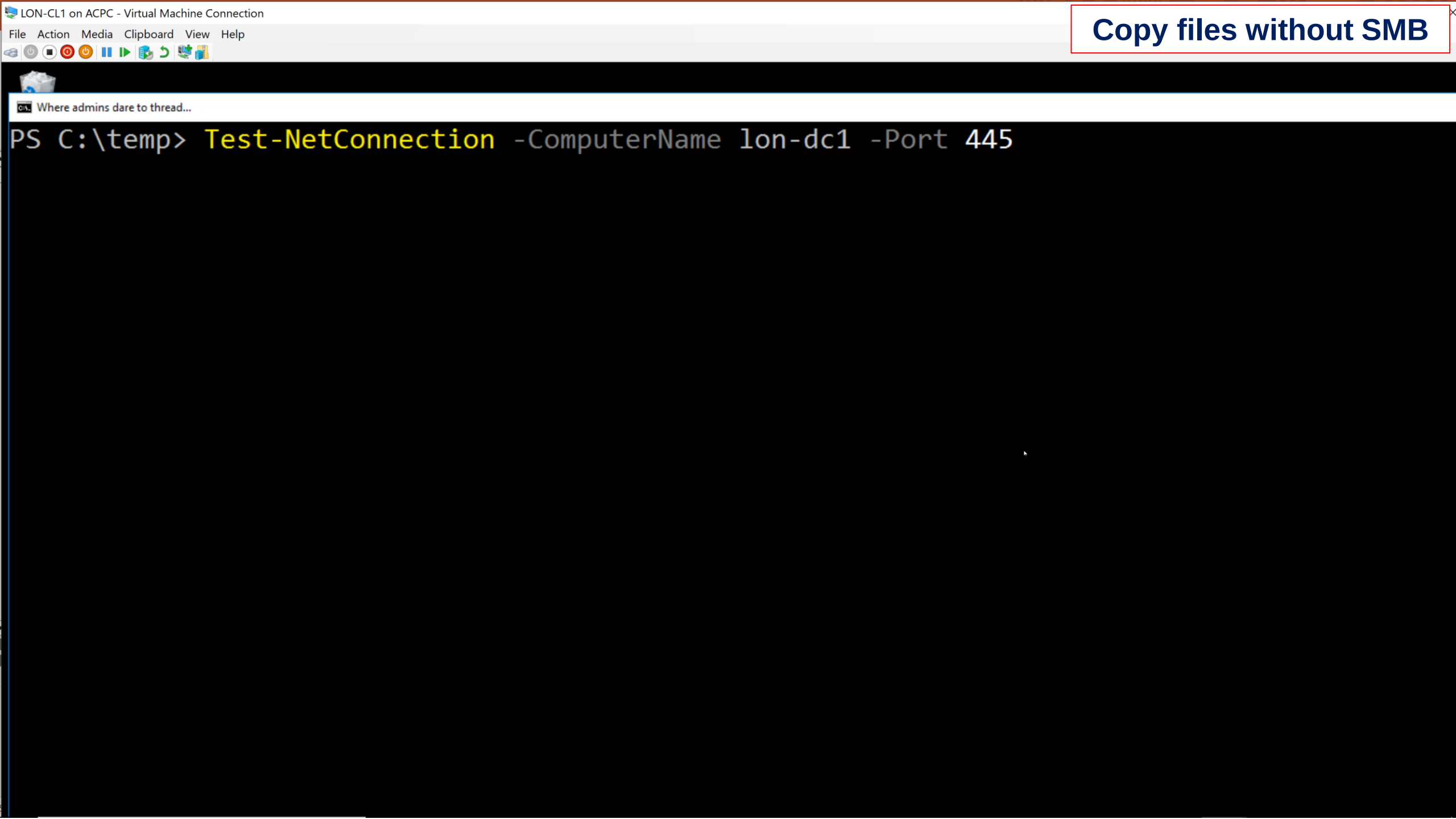
- The “Classics” –
  - Enforce MFA
  - Rename local sid 500 account
- Change RDP listening Port
- Do not leave RDP sessions disconnected(!)
  - Enforce logoff (GPO not suitable/not enough!)
  - Identify disconnected sessions with Get-UserSession.ps1


TO ADMIN OR NOT TO ADMIN

PSRemoting Architecture



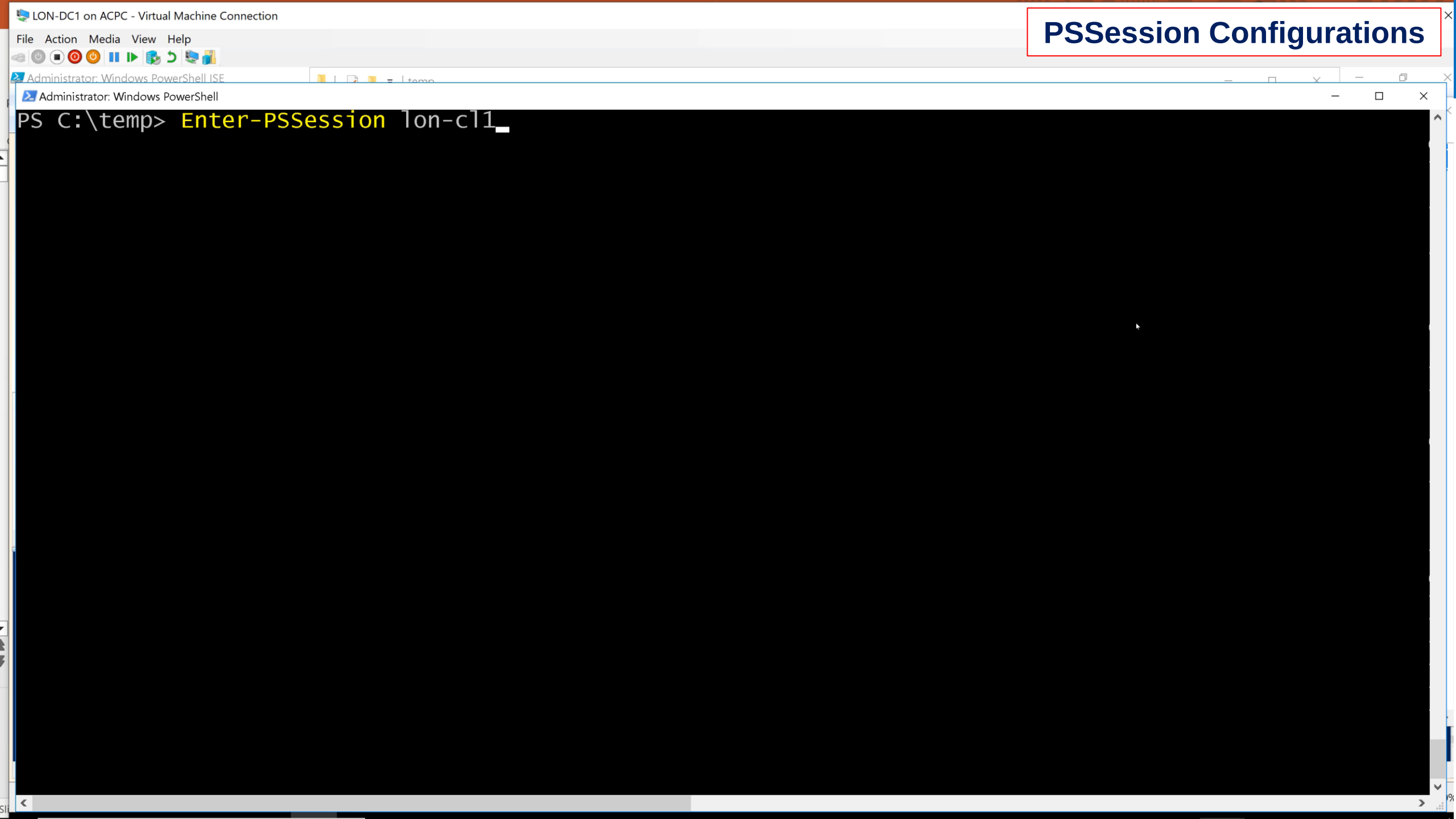

LON-DC1 on ACPC - Virtual Machine Connection
File Action Media View Help
PSRemoting w/Jobs
Administrator: Windows PowerShell
PS C:\>


LON-CL1 on ACPC - Virtual Machine Connection
File Action Media Clipboard View Help
Copy files without SMB
Where admins dare to thread...
PS C:\temp> Test-NetConnection -ComputerName lon-dc1 -Port 445

For the Blue Team -
Just Enough Access –
Secure constrained remote access

- Utilizes *PS Session Configurations*
  - –WSMan config (per nic/IP, http/s, limit bandwidth and more)
  - –All the Logging you can ask for
  - –Transcriptions
  - –ConstrainedLanguage
  - –Virtual Account (virtual SID)
  - –Whitelist scripts, apps, commands, parameters – *anything!*

PSSession Configurations



Remote Operations: Credentials Exposure

Action/Tool	Logon Type	Creds on Target	Notes
Console login	**2**	Yes*	* Except when Credential Guard is enabled
RunAs	**2**	Yes*	* Except when Credential Guard is enabled
RDP	**10**	Yes*	* Except when Remote Credential Guard enabled
Net Use	**3**	**No**	Inc. /u: parameter
PS Remoting	**3**	**No**	-u <username> -p <pass>
PsExec w/Creds	**3+2**	**Yes**	
PsExec no Creds	**3**	**No**	
Remote SchedTask	**4**	**Yes**	Password saved in LSA (on disk)
Run as a Service	**5**	**Yes**	Password saved in LSA (w/account)
Remote Registry	**3**	**No**	

Let's get advice from Microsoft... ☺

learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Shows Events

Filter by title

- Identity and Access
- Solutions and Scenario Guides
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Rights Management Service
- Active Directory Certificate Services
- **Administrative tools and logon types reference**
- Software Restriction Policies
- Windows Local Administrator Password Solution

Learn / Windows Server / Identity and Access /

Administrative tools and logon types

Article • 08/15/2022 • 3 minutes to read • 2 contributors

Feedback

This reference information is provided to help identify the risk of credential exposure associated with different administrative tools for remote administration.

In a remote administration scenario, credentials are always exposed on the source computer so a trustworthy privileged access workstation (PAW) is always recommended for sensitive or high impact accounts. Whether credentials are exposed to potential theft on the target (remote) computer depends primarily on the windows logon type used by the connection method.

This table includes guidance for the most common administrative tools and connection methods:

Connection method	Logon type	Reusable credentials on destination	Comments
Log on at console	Interactive	v	Includes hardware remote access / lights-out cards and network KVMs.
RUNAS	Interactive	v	
RUNAS /NETWORK	NewCredentials	v	Clones current LSA session for local access, but uses new credentials when connecting to network resources.

Administrative tools and logon types

11/22/2022 • 3 minutes to read

This reference information is provided to help identify the risk of credential exposure associated with different administrative tools for remote administration.

In a remote administration scenario, credentials are always exposed on the source computer so a trustworthy privileged access workstation (PAW) is always recommended for sensitive or high impact accounts. Whether credentials are exposed to potential theft on the target (remote) computer depends primarily on the windows logon type used by the connection method.

This table includes guidance for the most common administrative tools and connection methods:

CONNECTION METHOD	LOGON TYPE	REUSABLE CREDENTIALS ON DESTINATION	COMMENTS
PowerShell WinRM	Network	-	Example: Enter-PSSession server

Get TGT from network connection + no NTLM hash

Process token -> TGT

Hyper-V Manager

File Action View Help

Hyper-V Manager
ACPC

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuration Version
LON-CL1	Running	0%	1430 MB	00:05:00		9.0
LON-DC1	Running	0%	4754 MB	00:38:07		8.3
SRV2	Off					9.0
Ubuntu	Saved					9.0
WIN8-PC	Saved					9.0
Win 1.0	Off					9.0

Checkpoints

- Automatic Checkpoint - LON-CL1 - (08/06/19 - 00:28:13 AM)
  - Before_NamedPipe_Malware_AFTER_easyhook32_inst
    - Before PSREMOTING - (22/06/19 - 20:33:19 PM)
      - LON-CL1 - (28/03/21 - 19:09:51 PM)-accidental
        - Now

LON-CL1

Created: 12/24/2018 20:54:45
Configuration Version: 9.0
Generation: 1
Notes: None

Clustered: No
Heartbeat: OK (Applications Healthy)

Summary Memory Networking

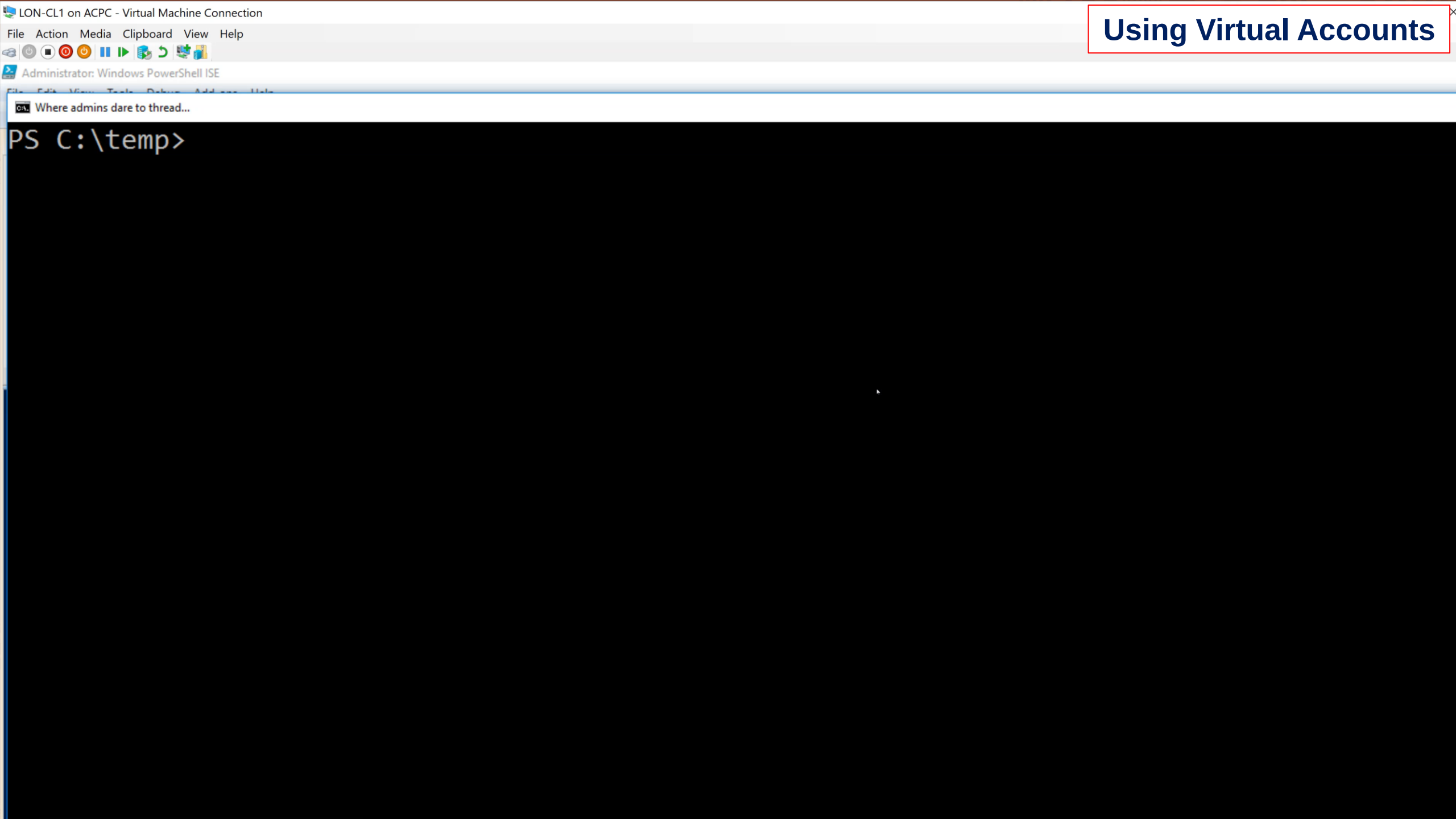
Actions

ACPC
- Quick Create...
- New
- Import Virtual Machine...
- Hyper-V Settings...
- Virtual Switch Manager...
- Virtual SAN Manager...
- Edit Disk...
- Inspect Disk...
- Stop Service
- Remove Server
- Refresh
- View
- Help

LON-CL1
- Connect...
- Settings...
- Turn Off...
- Shut Down...
- Save
- Pause
- Reset
- Checkpoint
- Revert...
- Move...
- Export...
- Rename...
- Help

ACPC: 1 virtual machine selected.

Potential Mitigation – Use Virtual accounts



Using Virtual Accounts

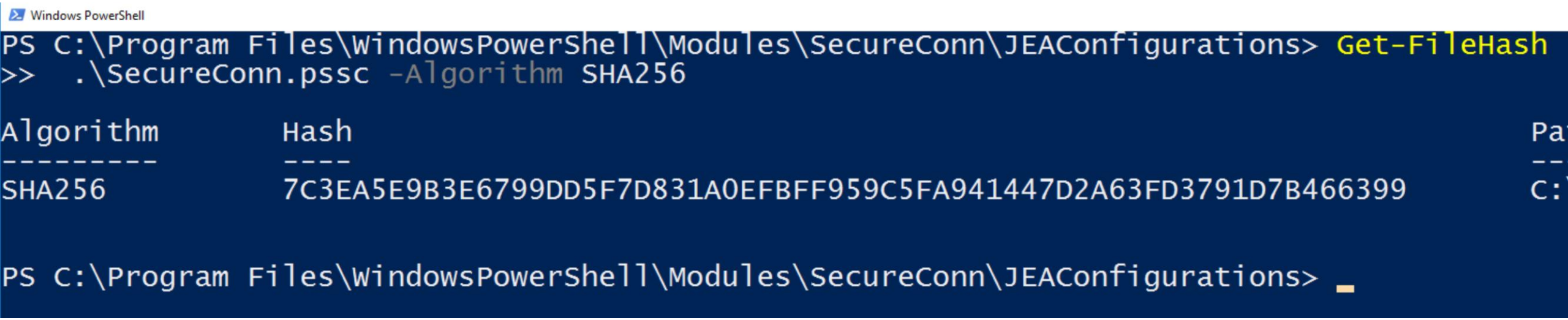
But... the adversary can edit the Role Capabilities file ☺

SecureConn.pssc - Notepad

File Edit Format View Help

```
@{

# Version number of the schema used for this document
SchemaVersion = '2.0.0.0'

# ID used to uniquely identify this document
GUID = '6a24463f-3949-4a94-b0db-dbc556bc6c42'

# Author of this document
Author = 'Adam'

# Description of the functionality provided by these settings
# Description = ''

# Session type defaults to apply for this session configuration. Can be 'RestrictedRemoteServer' (recommended),
SessionType = 'RestrictedRemoteServer'

# Directory to place session transcripts for this session configuration
TranscriptDirectory = 'C:\ProgramData\JEA\Transcripts'

# Whether to run this session configuration as the machine's (virtual) administrator account
RunAsVirtualAccount = $false

# Scripts to run when applied to a session
# ScriptsToProcess = 'C:\ConfigData\InitScript1.ps1', 'C:\ConfigData\InitScript2.ps1'

# User roles (security groups), and the role capabilities that should be applied to them when applied to a sess
RoleDefinitions = @{
```

But… Defenders can monitor for file/config changes, hash change etc' (e.g. sign config file)




ADVERSARIES RESPONSE ...
WHEN HEARING YOU SIGN ALL CONFIG FILES, MONITOR FOR CHANGES AND RESPOND TO IT
imgflip.com

Myth:

“You need a TCP/IP connection for a C2 Server”

“*Do we* need a TCP/IP connection for a C2 Server?”

C2 is not about an established connection.

Nor TCP, or UDP.

It’s a MINDSET

How about your **email client**?

When Outlook goes Rouge

Key Takeaways

- Embrace ‘Living off the land’ tools mindset (Red & Blue)
- Note Credentials exposure during Remote Operations.
- Any tool can be part of a C2 channel.
- PSRemoting Rocks! And JEA is effective. *But ….*
  - Almost *No Security features are enabled by default*. proper configuration is needed.
- Check out **github.com/YossiSassi** for tools & scripts 

1nTh35h3ll

YossiSassi

github.com/YossiSassi

Red Team // The HAcktive Directory guy @ 10Root // People.Music.Code // Aviate.Navigate.Communicate // Knowledge is Power(shell)

Edit profile

200 followers · 2 following

10Root
wherever I lay my IP
yossis@protonmail.com
@yossi_sassi

Pinned

Customize your pins

SEC-T_21-One-Liners-Powershell Public

Code & other materials from SEC-T 2022 talk "When SysAdmin & Hacker Unite: 21 One-Liners to make you convert from bash to Powershell"

PowerShell 12 4

hAcKtive-Directory-Forensics Public

28 6

Get-ChangesInADUser Public

Get-LDAPperformance Public

...alyzes them to CSV & Grid.
...ies, either for Threat Hunting

AD-Replication-Metadata Public

This simple script allows you to track past changes on your AD objects, even if event logs were wiped (e.g. during an IR), using Replication metadata history

PowerShell 7 1

Get-ADGroupChanges Public

"Pure" powershell command (no dependencies, no special permissions etc') to retrieve change history in an AD group membership. relies on object metadata rather than event logs. useful for DF/IR, tr...

PowerShell 5 3

192 contributions in the last year

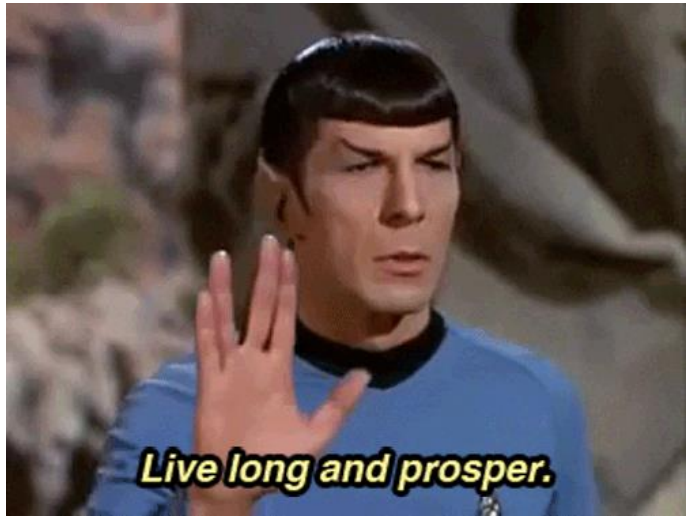
Contribution settings

Remember –
It’s just a tool.

It’s neither bad nor good.

That part is up to you ☺

Takk!



Yossi_Sassi

yossis@protonmail.com

Enjoy Lunsj HackCon!

The Norwegian cyber security convention