Distance over Velocity:

Practical tips from the field for Red and Blue teams

Yossi Sassi

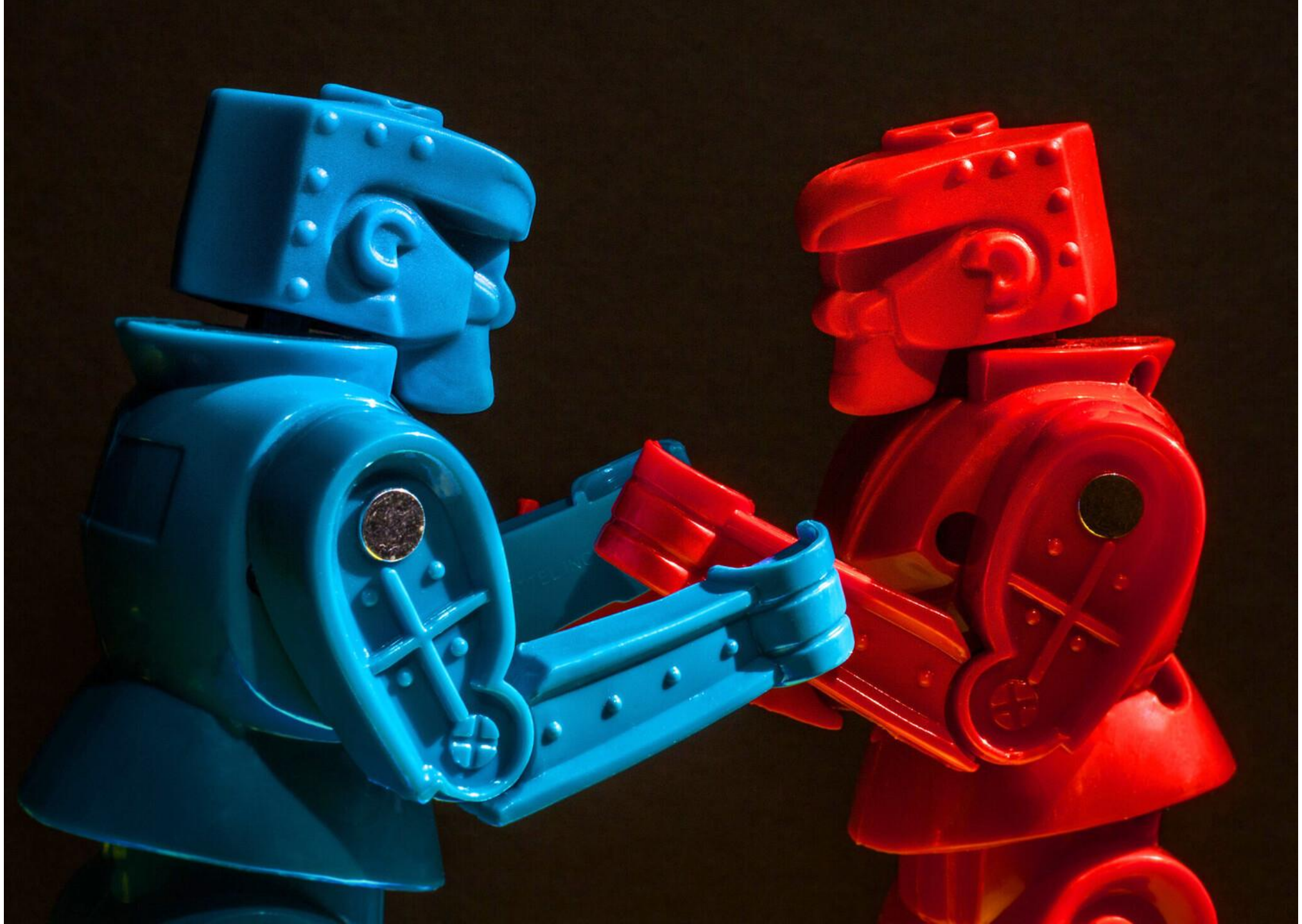
10 ROOT CYBER SECURITY

t2.FI INFOSEC

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

WhoAmI

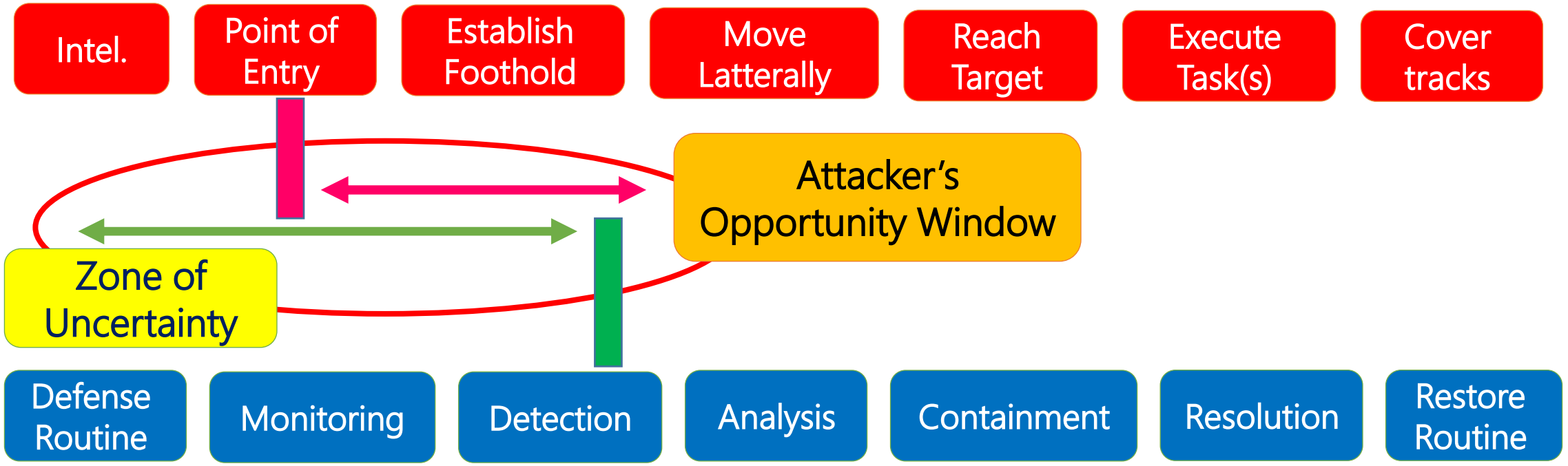
- InfoSec Researcher; friendly H@ɔk3r
- Red mind, Blue heart
- Co-Founder @ 10 ROOT CYBER SECURITY
- Consulting in 4 continents (Banks/gov/F100)
- 35 years of keyboard access – Code, IT Security, Network communications
- 'The HAcktive Directory guy'; Ex-Javelin (Acquired by Symantec)
- Ex-Technology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



What Makes or Breaks a Successful Cyber Attack?

a Mindset
focused on time.

Anatomy of an Attack Vs. Defense Controls



‘Living off the land’ mindset

Remote Connection or Lateral Movement?

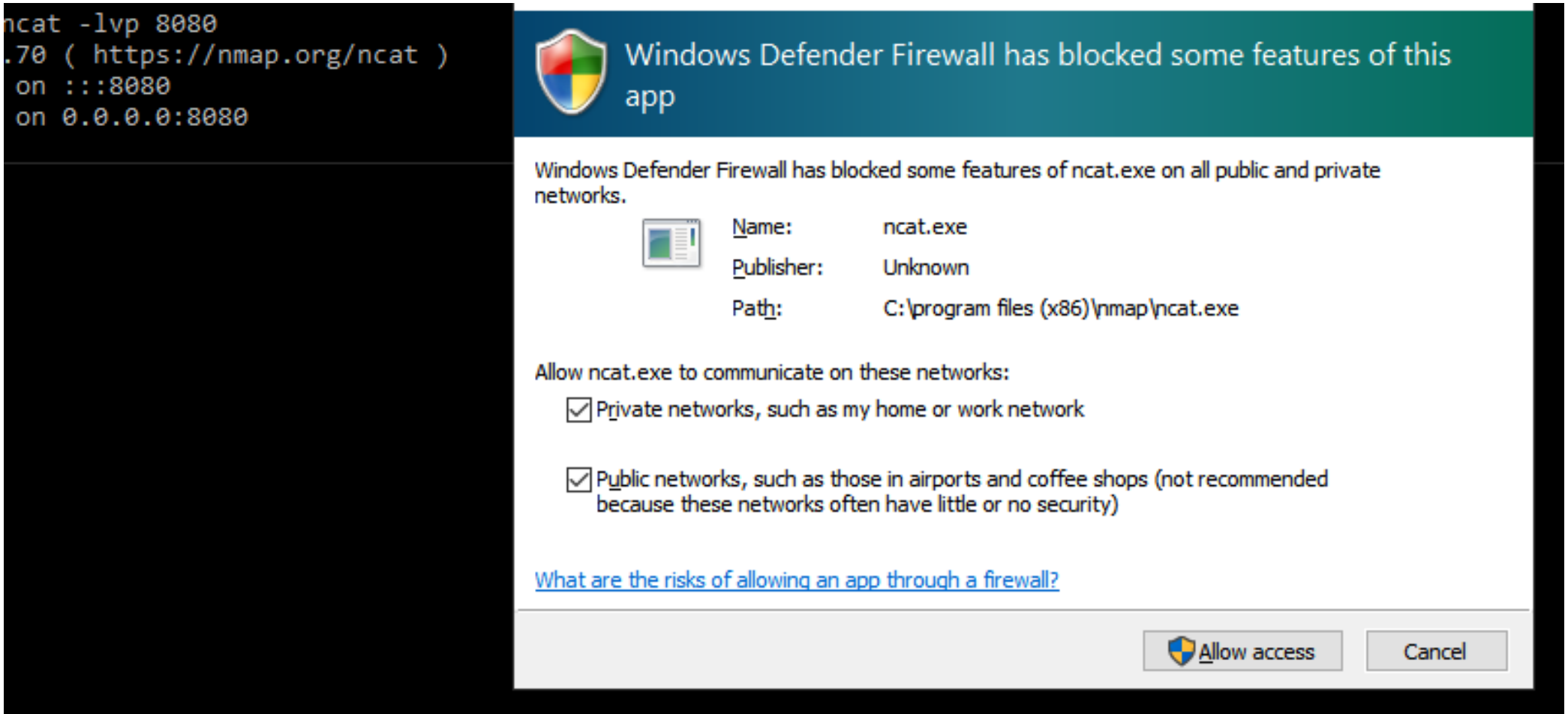
Inter-Process Communications (IPC)

- 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 ☺



Why use **PsExec***, when you can run a

Named-Pipe/SMB One-liner?

(Exfiltrate data/C2 with No socket bind)

*** Time**


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

- ETW provider for creation of/connection to named pipes out-of-the-box (a **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**

Windows admins favorite feature

‘Living off the land’ time-focused defense example - RDP

- Windows Server online (RDP open, 17 chars password):

*** 39,484** Failed RDP logon events in less than 4 hours(!)

* 15,458 events - user name does not exist (most tried ADMINISTRATOR, then Admin, then TEMP, etc.)

*** 24,026** events - user name is correct (administrator) but the password is wrong

- *After* renaming the administrator account:

40,156 Failed logon events in less than ~4 hours

ALL events: **user name does not exist.**

- **Not even 1 *real* attempt of password guessing …**
- **Can also change Port number ☺**

If it’s a little harder for you,
It is more hard for the attacker.*

If it is very convenient/easy for you,
It is VERY easy for the attacker.

* Time

How would you detect all RDP hosts, quickly & stealthy?


SRV2 on ACPC
Windows PowerShell
PS C:\>
6:32 AM
Saturday
4/6/2024

Defense tip ‘Living off the land’ style - Customize it

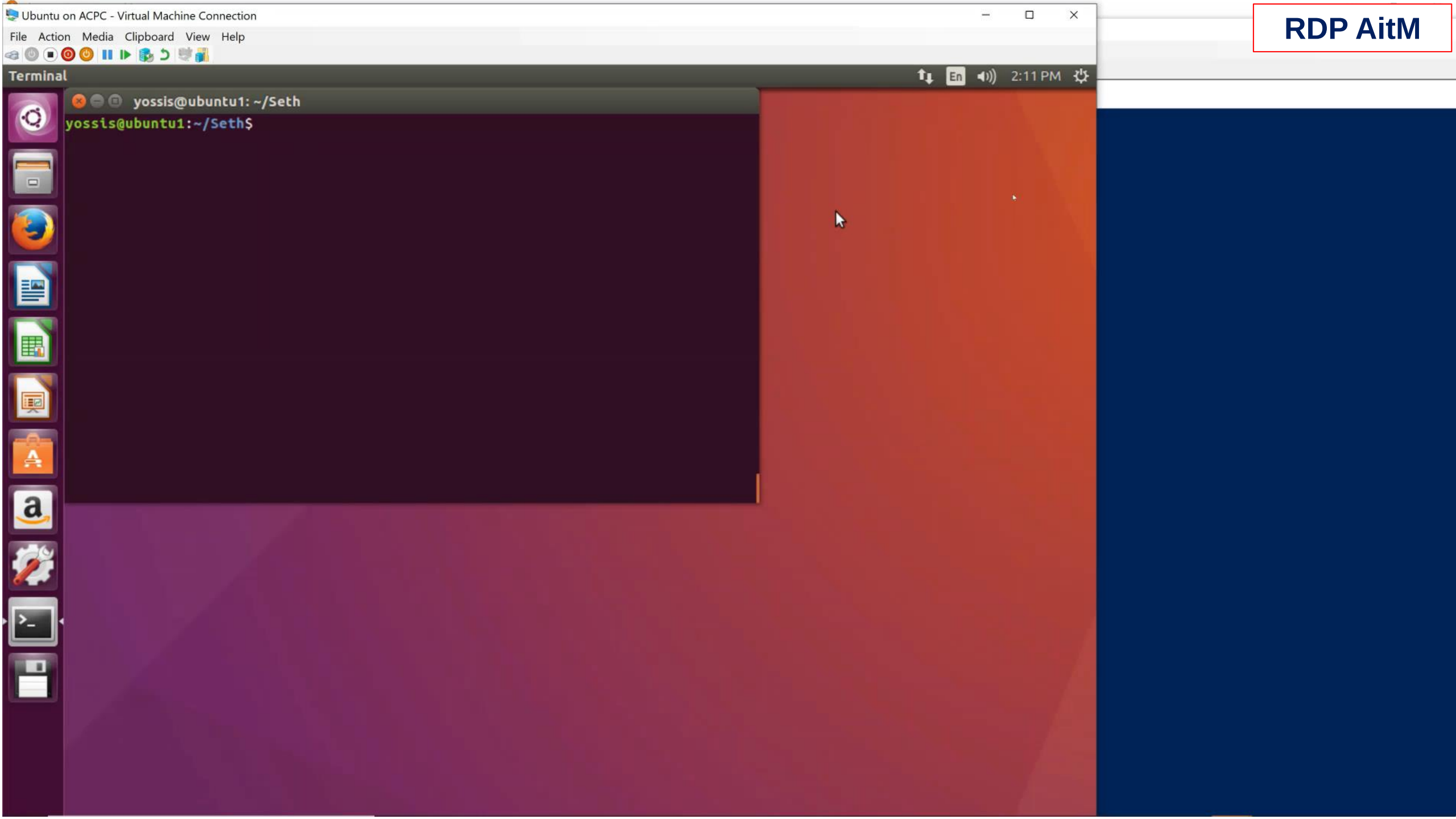
- Extending the ‘RDP port change’ tactic to other protocols and services
- Evaluate customization of APIs/ports/Services, and *Monitor* the ‘normaly expected’ values

- .. Or, in other words, defenders:

  *buy yourself **time**!*

RDP AitM

- 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 AitM

Detecting targets ‘Living off the land’ style (RDP w/o NLA enforced)

- ([adsisearcher]'(&(serviceprincipalname=*TERMSRV*)(operatingsystem=*windows*server*200*))').FindAll()

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)
```

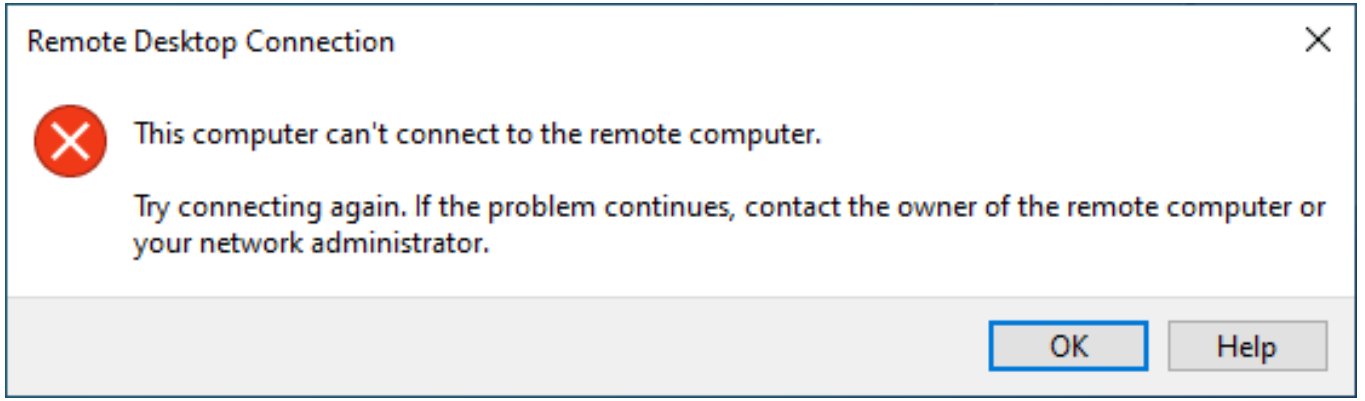
- **Can use inveigh/responder to relay the Registry command, and/or 'net localgroup administrators /add user'**
- More silent, efficient & quicker than mimikatz etc. ;-)

Mitigations / Detections – RDP AitM

- 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-Authenticted hosts

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



Mitigations / Detections – RDP AitM (Cont.)

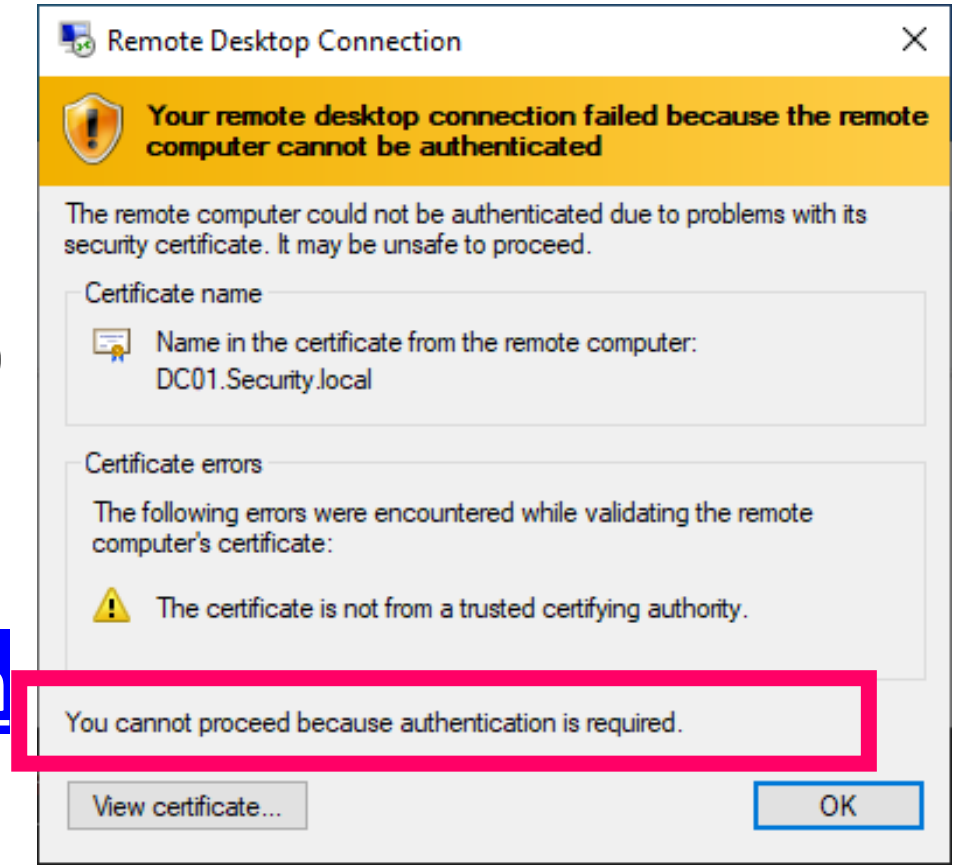
- Enroll Certificates + GPO: Computer configuration > Policies > Administrative Templates > Windows Components >Remote Desktop Services > Remote Desktop Connection Client > **Configure server authentication for client**

Disallow the connection,

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

Will *Not* prevent NetNTLM,

but will prevent clear text + Block connection



Understanding Changes, Fast:
“Hacktive Directory” forensics

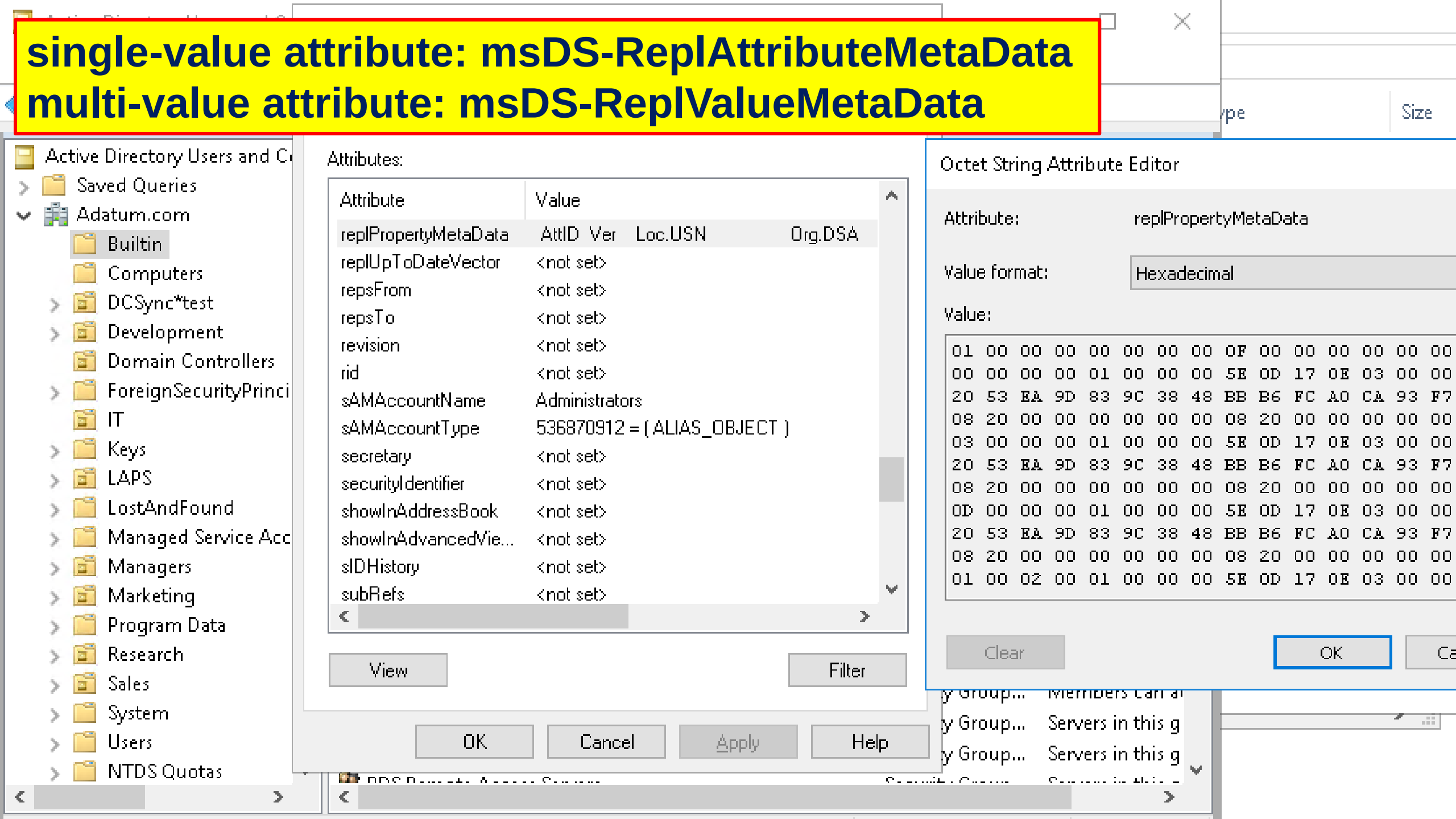
שע' 6 · @fouroctets **fouroctets**

A short story in event IDs

4625
4625
4625
4625
4625
4625
4625
4625
4625
4625
4624
4732
4688
4688
1102

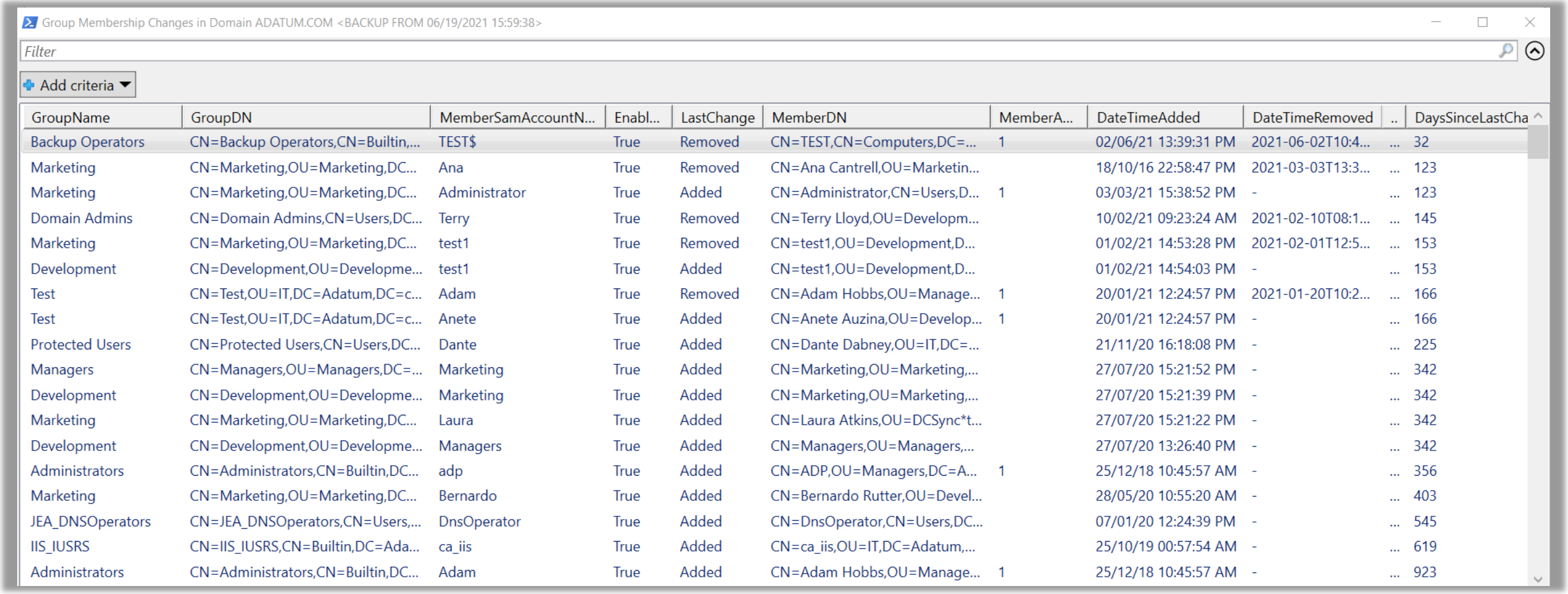
?

single-value attribute: msDS-ReplAttributeMetaData
multi-value attribute: msDS-ReplValueMetaData

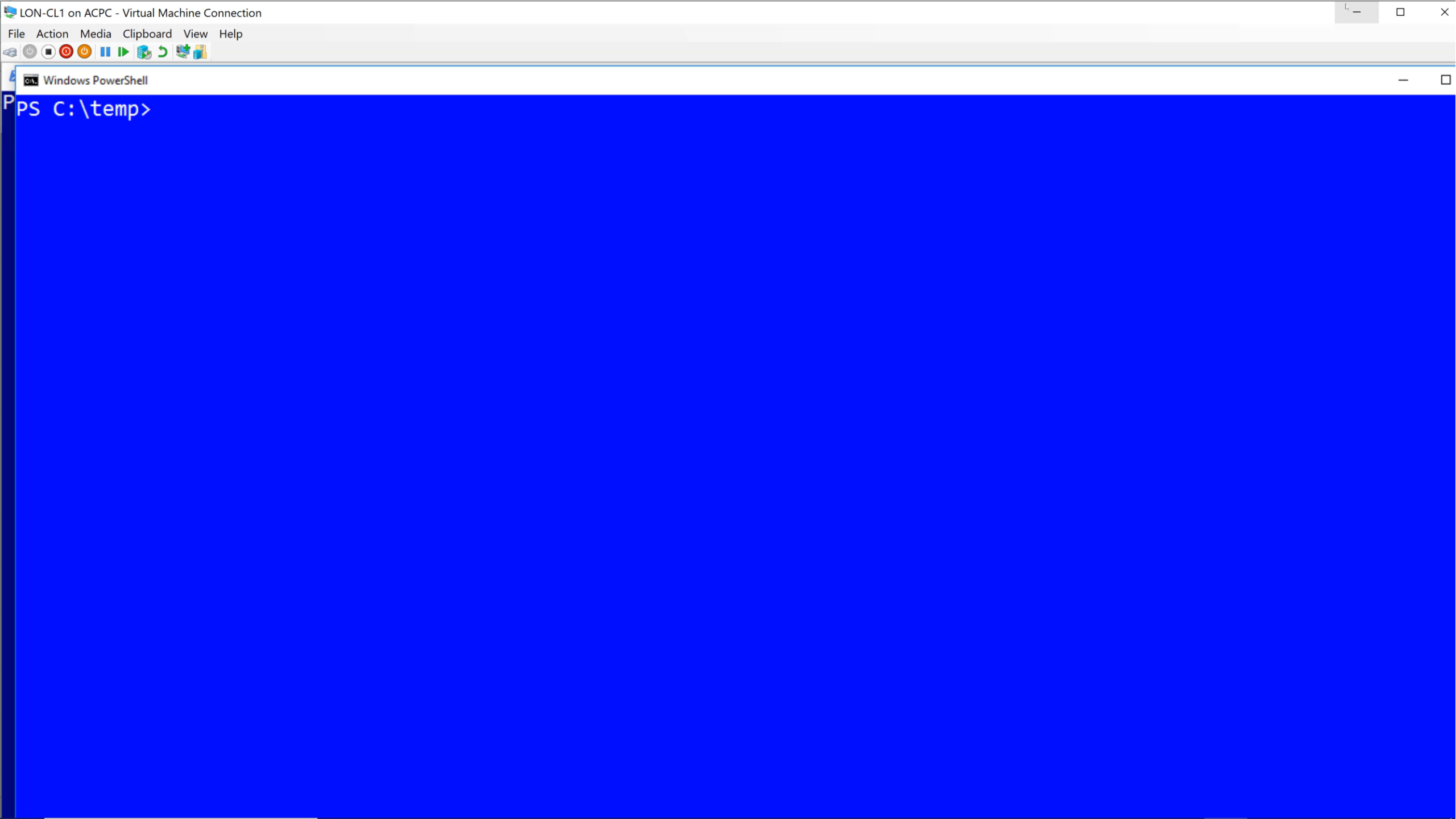


Where is this msds-Repl* ??!

Wouldn’t it be nice…



GroupName	GroupDN	MemberSamAccountN...	Enabl...	LastChange	MemberDN	MemberA...	DateTimeAdded	DateTimeRemoved	..	DaysSinceLastCha
Backup Operators	CN=Backup Operators,CN=Builtin,...	TEST$	True	Removed	CN=TEST,CN=Computers,DC=...	1	02/06/21 13:39:31 PM	2021-06-02T10:4...	...	32
Marketing	CN=Marketing,OU=Marketing,DC...	Ana	True	Removed	CN=Ana Cantrell,OU=Marketin...		18/10/16 22:58:47 PM	2021-03-03T13:3...	...	123
Marketing	CN=Marketing,OU=Marketing,DC...	Administrator	True	Added	CN=Administrator,CN=Users,D...	1	03/03/21 15:38:52 PM	-	...	123
Domain Admins	CN=Domain Admins,CN=Users,DC...	Terry	True	Removed	CN=Terry Lloyd,OU=Developm...		10/02/21 09:23:24 AM	2021-02-10T08:1...	...	145
Marketing	CN=Marketing,OU=Marketing,DC...	test1	True	Removed	CN=test1,OU=Development,D...		01/02/21 14:53:28 PM	2021-02-01T12:5...	...	153
Development	CN=Development,OU=Developme...	test1	True	Added	CN=test1,OU=Development,D...		01/02/21 14:54:03 PM	-	...	153
Test	CN=Test,OU=IT,DC=Adatum,DC=c...	Adam	True	Removed	CN=Adam Hobbs,OU=Manage...	1	20/01/21 12:24:57 PM	2021-01-20T10:2...	...	166
Test	CN=Test,OU=IT,DC=Adatum,DC=c...	Anete	True	Added	CN=Anete Auzina,OU=Develop...	1	20/01/21 12:24:57 PM	-	...	166
Protected Users	CN=Protected Users,CN=Users,DC...	Dante	True	Added	CN=Dante Dabney,OU=IT,DC=...		21/11/20 16:18:08 PM	-	...	225
Managers	CN=Managers,OU=Managers,DC=...	Marketing	True	Added	CN=Marketing,OU=Marketing,...		27/07/20 15:21:52 PM	-	...	342
Development	CN=Development,OU=Developme...	Marketing	True	Added	CN=Marketing,OU=Marketing,...		27/07/20 15:21:39 PM	-	...	342
Marketing	CN=Marketing,OU=Marketing,DC...	Laura	True	Added	CN=Laura Atkins,OU=DCSync*t...		27/07/20 15:21:22 PM	-	...	342
Development	CN=Development,OU=Developme...	Managers	True	Added	CN=Managers,OU=Managers,...		27/07/20 13:26:40 PM	-	...	342
Administrators	CN=Administrators,CN=Builtin,DC...	adp	True	Added	CN=ADP,OU=Managers,DC=A...	1	25/12/18 10:45:57 AM	-	...	356
Marketing	CN=Marketing,OU=Marketing,DC...	Bernardo	True	Added	CN=Bernardo Rutter,OU=Devel...		28/05/20 10:55:20 AM	-	...	403
JEA_DNSOperators	CN=JEA_DNSOperators,CN=Users,...	DnsOperator	True	Added	CN=DnsOperator,CN=Users,DC...		07/01/20 12:24:39 PM	-	...	545
IIS_IUSRS	CN=IIS_IUSRS,CN=Builtin,DC=Ada...	ca_iis	True	Added	CN=ca_iis,OU=IT,DC=Adatum,...		25/10/19 00:57:54 AM	-	...	619
Administrators	CN=Administrators,CN=Builtin,DC...	Adam	True	Added	CN=Adam Hobbs,OU=Manage...	1	25/12/18 10:45:57 AM	-	...	923


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

Forensic Scripts for AD

Get-ADGroupChanges, Replication Attribute Metadata history, etc.

- No special permissions ☺
- No agent – works with LDAP/ADWS, or an ntds.dit file
- No dependencies or external files (just .ps1)

1nTh35h3ll

YossiSassi

Follow

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

212 followers · 2 following

Overview | Repositories 36 | Projects | Packages | Stars 6

Pinned

HackCon2024 Public

Presentation from HackCon talk - 'It's just a tool. Not bad nor good. That part is up to YOU.'

1

hAcKtive-Directory-Forensics Public

42 6

PowerShell 88 8

nCheck Public

npares with a previous run, to nt permission(s)

PowerShell 14 2

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 17 3

AD-Replication-Metadata Public

Track past changes in your AD accounts (users & computers), even if no event logs exist - e.g. not collected, no retention/overwritten, wiped (e.g. during an Incident Response) etc. Uses Replicatio...

PowerShell 11 1

115 contributions in the last year

Myth:

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


A
U
T
P

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

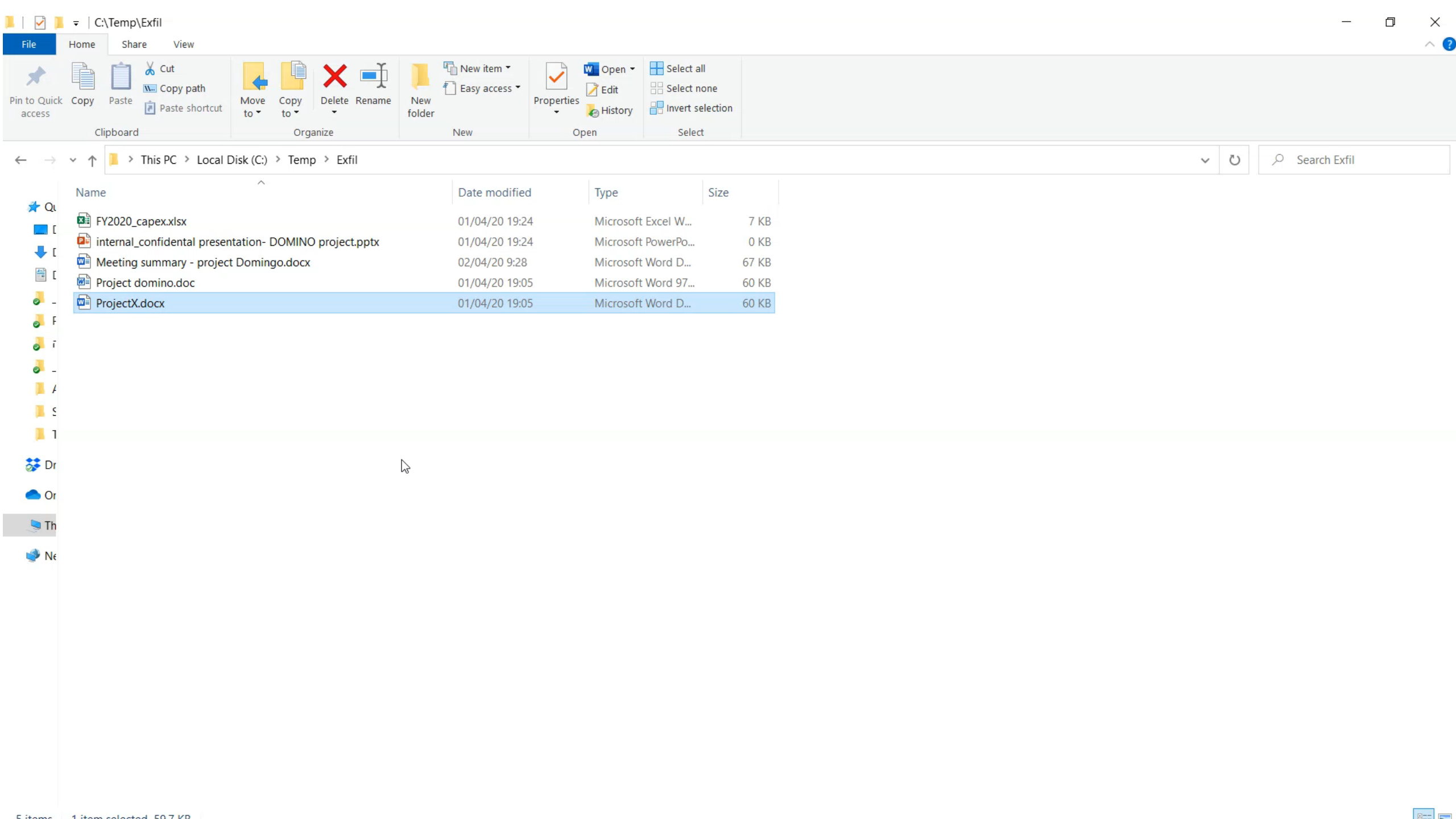
C2 is not about an established connection.

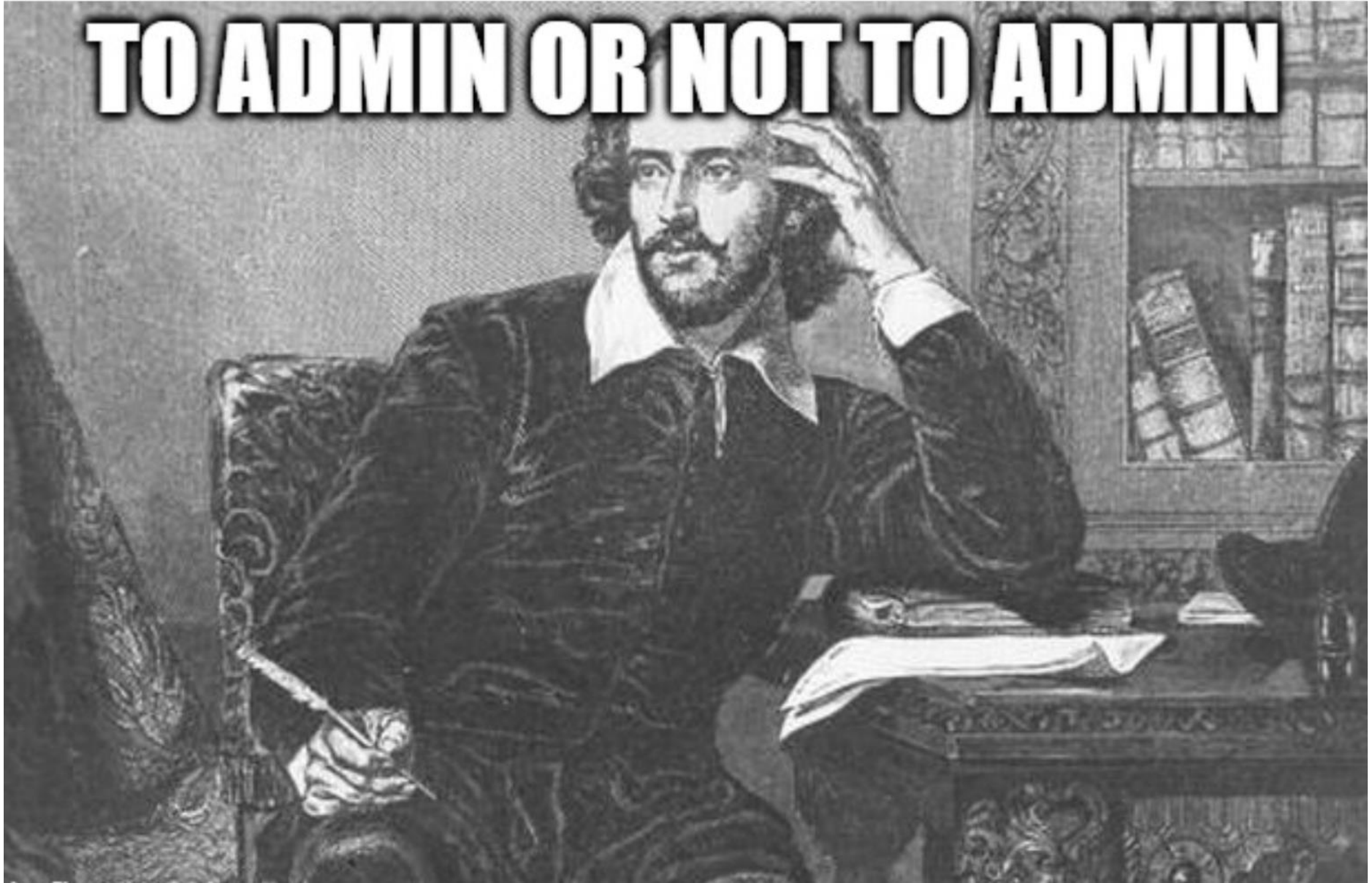
Not TCP, nor UDP.

It’s a MINDSET.

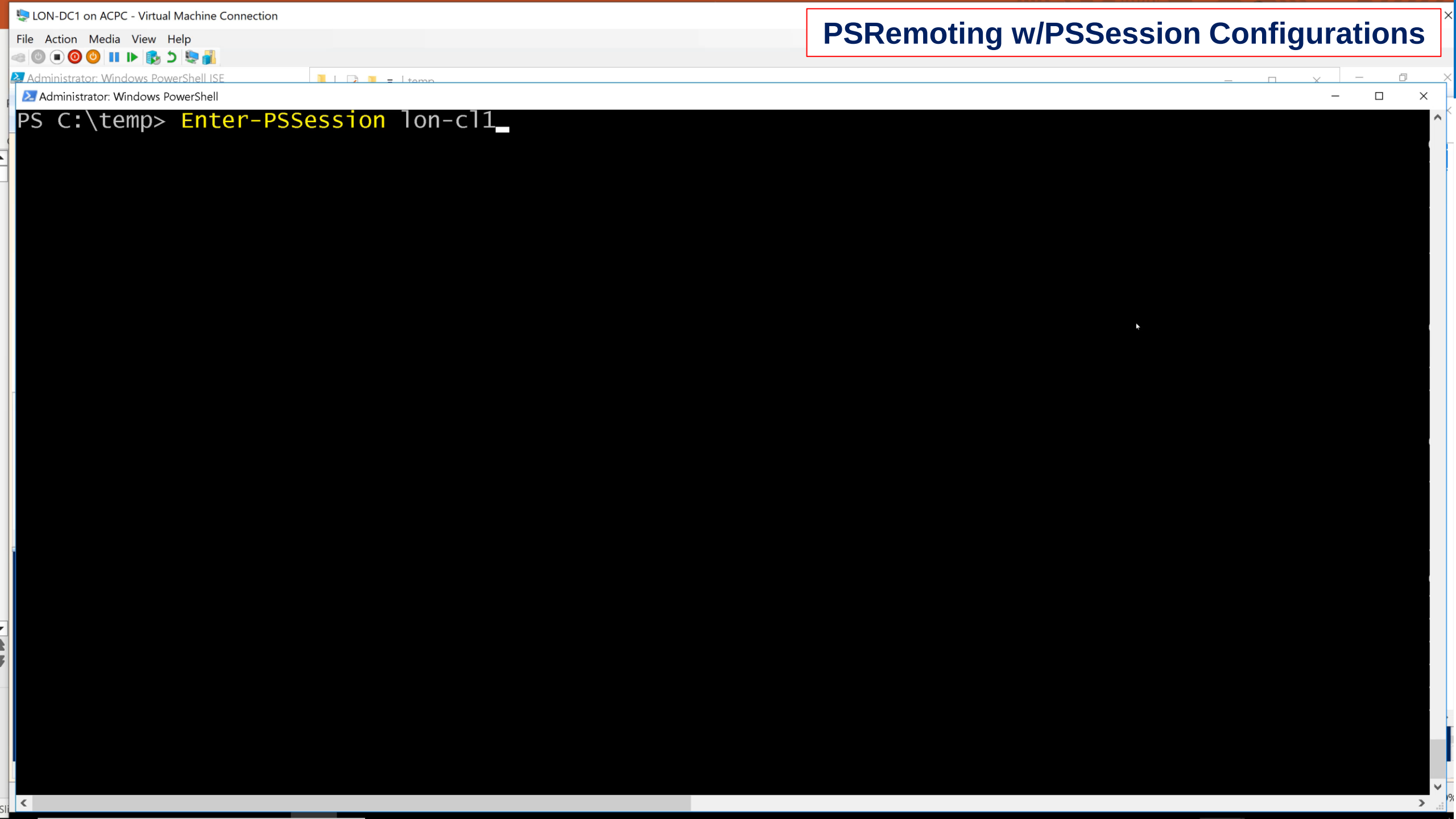
How about your **email client**?

When Outlook goes Rouge


C:\Temp\Exfil
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Local Disk (C:)
Temp
Exfil
Search Exfil
Name
Date modified
Type
Size
FY2020_capex.xlsx 01/04/20 19:24 Microsoft Excel W... 7 KB
internal_confidental presentation- DOMINO project.pptx 01/04/20 19:24 Microsoft PowerPo... 0 KB
Meeting summary - project Domingo.docx 02/04/20 9:28 Microsoft Word D... 67 KB
Project domino.doc 01/04/20 19:05 Microsoft Word 97... 60 KB
ProjectX.docx 01/04/20 19:05 Microsoft Word D... 60 KB


TO ADMIN OR NOT TO ADMIN

PSRemoting w/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 LogonType=3 without 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

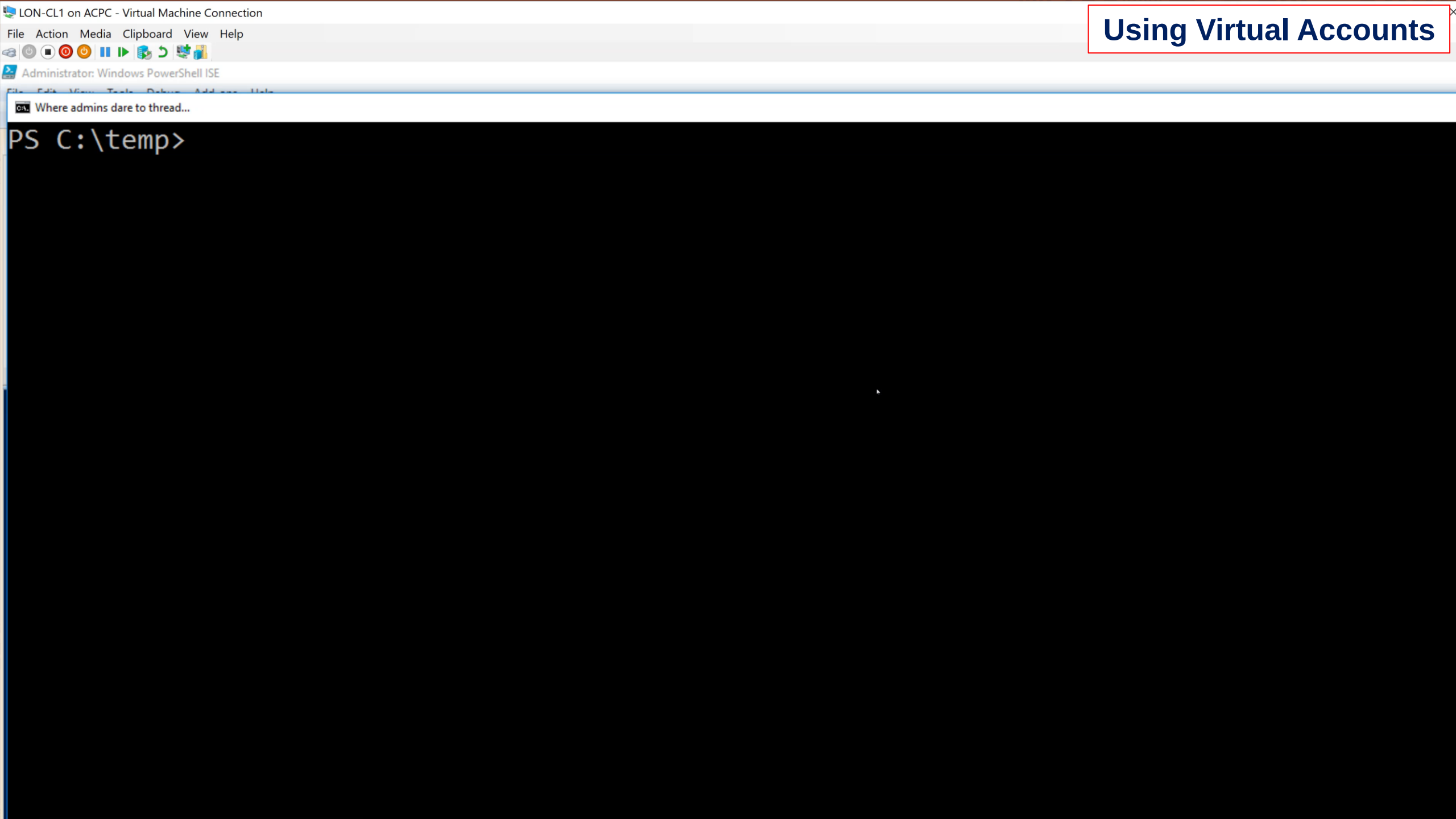
Actions

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

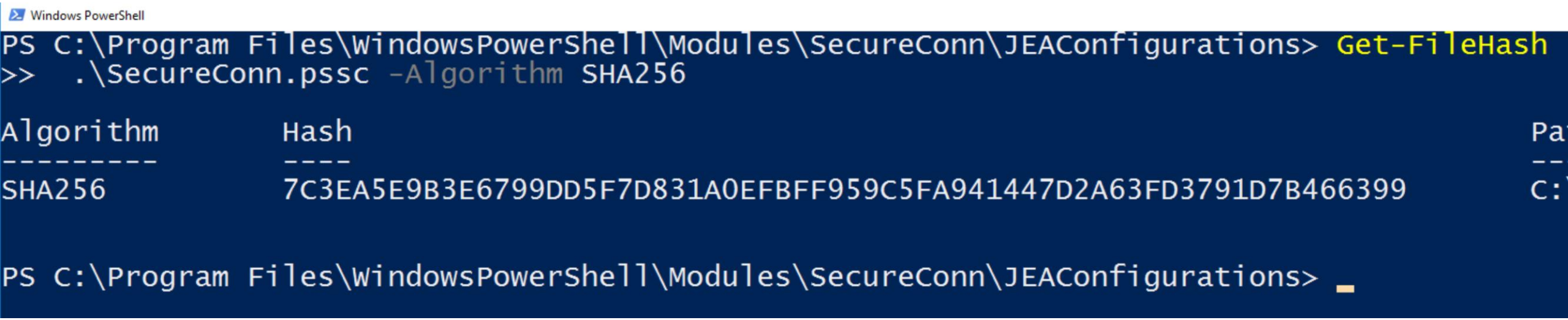
But... the adversary can edit the Role Capabilities file ☺

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

What's your secret sauce?


you can kill
the man
but you can never kill
the idea
Catmin

Creating a decoy admin

- Privileged account (DA?)
- Enabled, with:
  - logonHours set to none?
  - logonWorkstations - Same dilemma
- SPN (kerberoasting) - with a Longgggg password
- Pre-AuthN not required – with a Longgggg password
- **Reputation matters!**
  - Handle LogonCount etc.
  - “Convert” accounts from users who left the organization

... many more tips

The Challenge: Reducing FPs and FNs

True Positive (TP):

- Reality: A wolf threatened.
- Shepherd said: "Wolf."
- Outcome: Shepherd is a hero.

False Positive (FP):

- Reality: No wolf threatened.
- Shepherd said: "Wolf."
- Outcome: Villagers are angry at shepherd for waking them up.

e.g. mgmt. tools, non-efficient honeypots/tokens

False Negative (FN):

- Reality: A wolf threatened.
- Shepherd said: "No wolf."
- Outcome: The wolf ate all the sheep.

e.g. no sensor, no detection at defense control (e.g. EDR), no alert at SOC

True Negative (TN):

- Reality: No wolf threatened.
- Shepherd said: "No wolf."
- Outcome: Everyone is fine.

Quick re-cap: DS Replication Attacks

- DCSync
  - Derives from permission(s) for replicating changes
  - Ability to get replication change notifications

- DC Shadow
  - PC act as DC -> Push Changes to other DCs directly
  - **Change system-controlled attributes**
  - Difficult to detect -> bypass Auditing
  - Difficult to prevent -> Not a vulnerability; no ‘patch’

```
PS C:\temp> Get-ADObject "dc=adatum,dc=com" -Properties whencreated


DistinguishedName : dc=adatum,dc=com
Name              : Adatum
ObjectClass       : domainDNS
ObjectGUID        : 4d7ee4df-119d-4e70-9ed7-4e0343b84198
whencreated       : 10/18/2016 12:47:30 PM



PS C:\temp> get-aduser adp -Properties passwordlastset


DistinguishedName : CN=ADP,OU=Managers,DC=Adatum,DC=com
Enabled           : True
GivenName         : ADP
Name              : ADP
ObjectClass       : user
ObjectGUID        : 8bef5856-0a83-478d-9893-e3d43bfe2d8e
PasswordLastSet   : 1/19/1992 5:47:09 AM
SamAccountName    : adp
SID               : S-1-5-21-4534338-1127018997-2609994386-5601
Surname           :
UserPrincipalName : adp@Adatum.com
```

Red Team Tip:

Find if SecOps are messing with you

- Mmm.. Maybe, check replication metadata LastOriginatingChangeTime? ☺

LON-CL1 on ACPC - Virtual Machine Connection

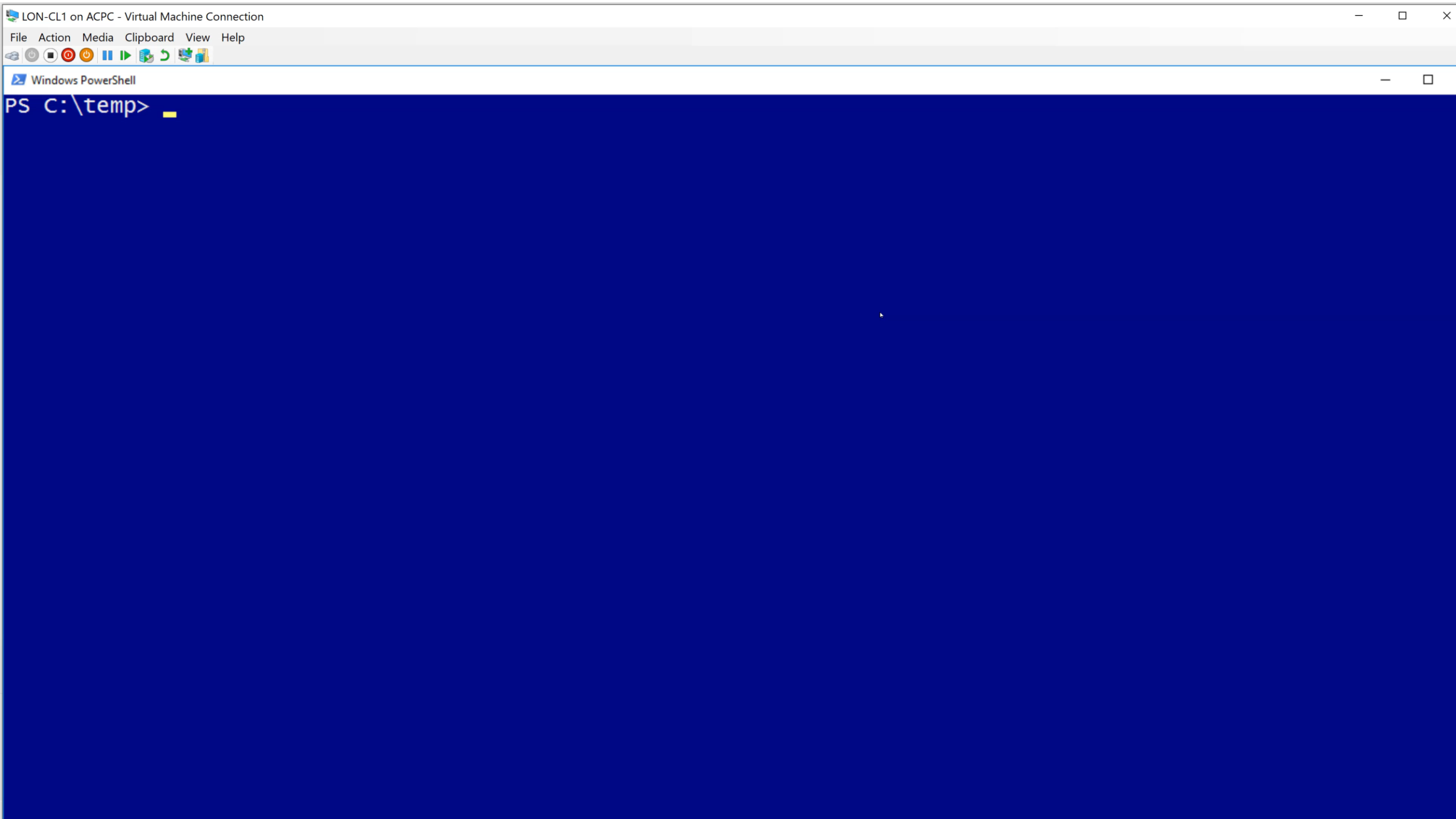
File Action Media Clipboard View Help

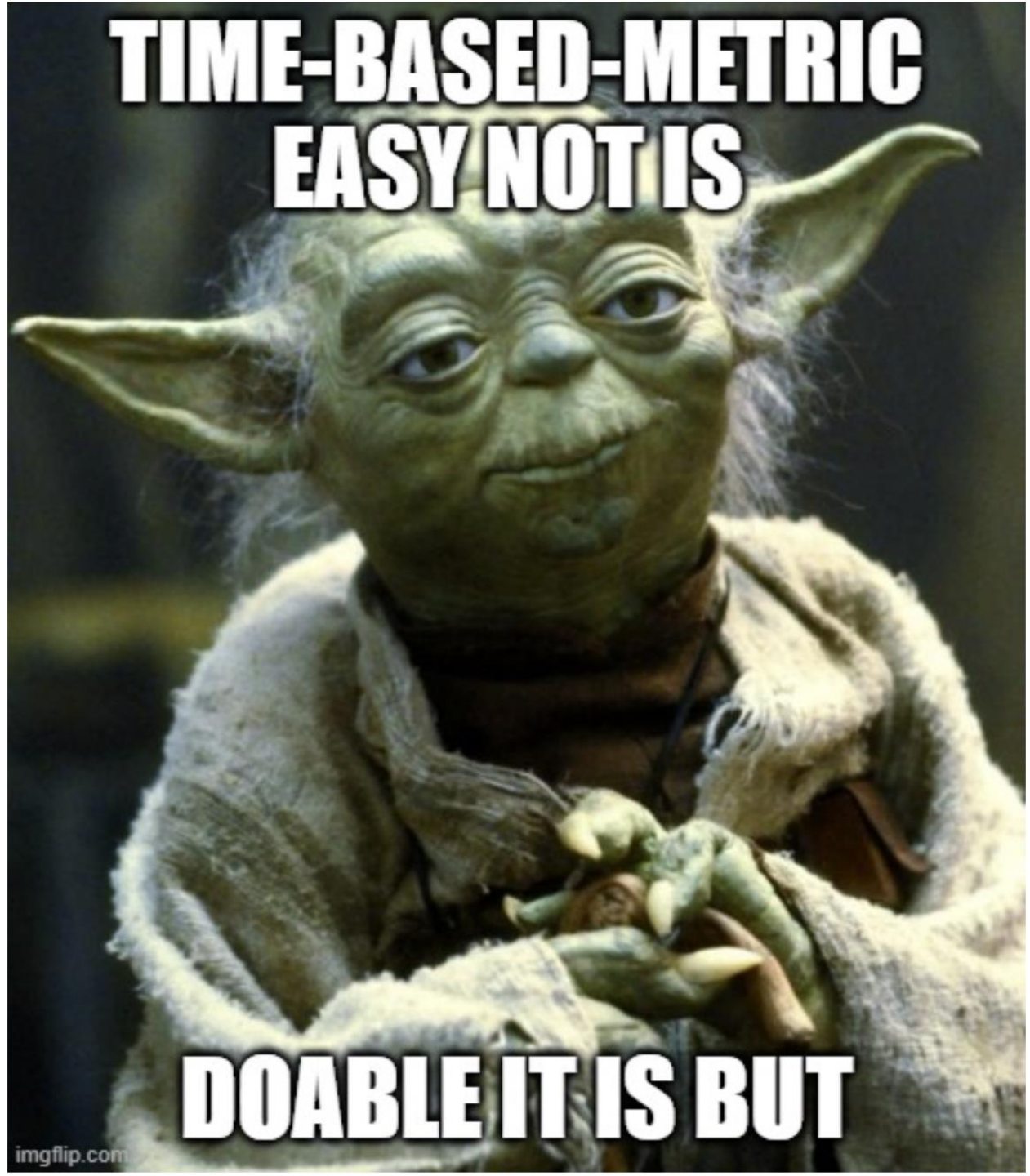
Windows PowerShell

```
PS C:\temp>
```

Blue Team Tip:

Handle the replication metadata as well ☺


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


TIME-BASED-METRIC
EASY NOT IS
DOABLE IT IS BUT
imgflip.com

Key Takeaways

- The right `Mindset` can “make or break” a cyber attack
  - Whether “Living off the land”, a C2 channel or forensic tool
- `Time` is the most important measurement in Cyber Security
- Be aware of Credentials Exposure at Remote Operations
- Find your `secret sauce`!
- Check out github.com/**YossiSassi** for tools & scripts

Everything is a set of nested ‘if’ statements

```
if () {}
    if () {}
        if () {}
            if () {}
                if () {}
                    if () {}
                        if () {}
                            if () {}
                                if () {}
                                    if () {}
                                        if () {}
                                            if () {}
                                                if () {}
                                                    if () {}
                                                        if () {}
                                                            if () {}
                                                                if () {}
                                                                    if () {}
                                                                        if () {}
                                                                            if () {}
                                                                                if () {}
                                                                                    if () {}
                                                                                        if () {}
                                                                                            if () {}
                                                                                                if () {}
                                                                                                    if () {}
                                                                                                        if () {}
                                                                                                            if () {}
                                                                                                                if () {}
                                                                                                                    if () {}
                                                                                                                        if () {}
                                                                                                                            if () {}
                                                                                                                                if () {}
                                                                                                                                    if () {}
                                                                                                                                        if () {}
                                                                                                                                            if () {}
                                                                                                                                                if () {}
                                                                                                                                                    if () {}
```

K11to5

Yossi_Sassi

yossis@protonmail.com

Enjoy !

t2.fi INFOSEC