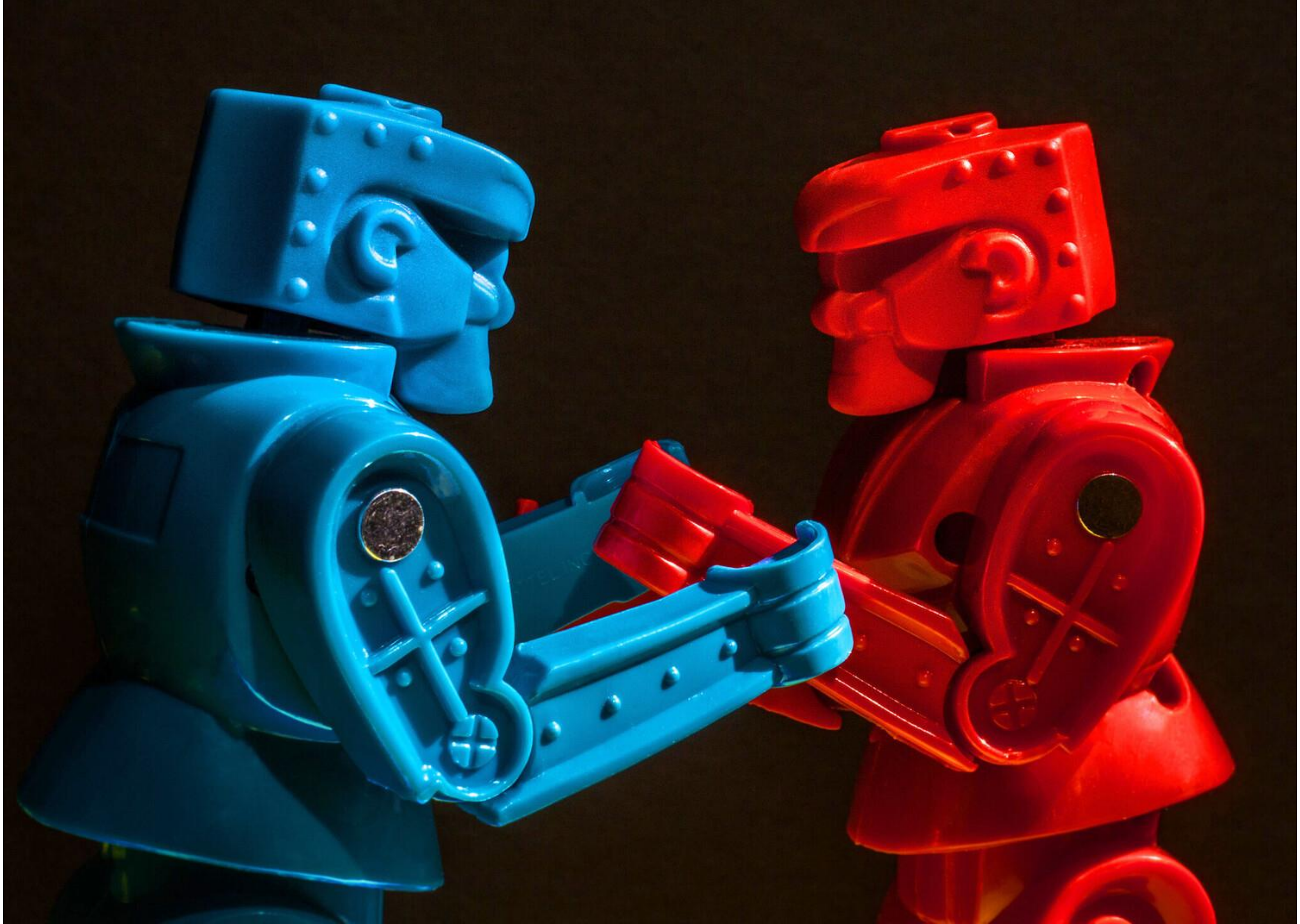
The Att@כk3r Mindset:
Practical Lessons from the Field

Yossi Sassi

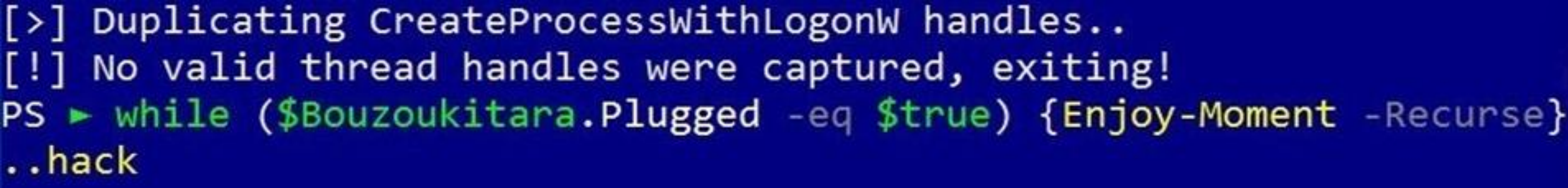
10 ROOT CYBER SECURITY

DEEPSEC



What we’ll talk about

- Why should we care about it?
- Understanding the Attacker Mindset
  - Concepts
  - Examples
- Practical tips for defense & offense



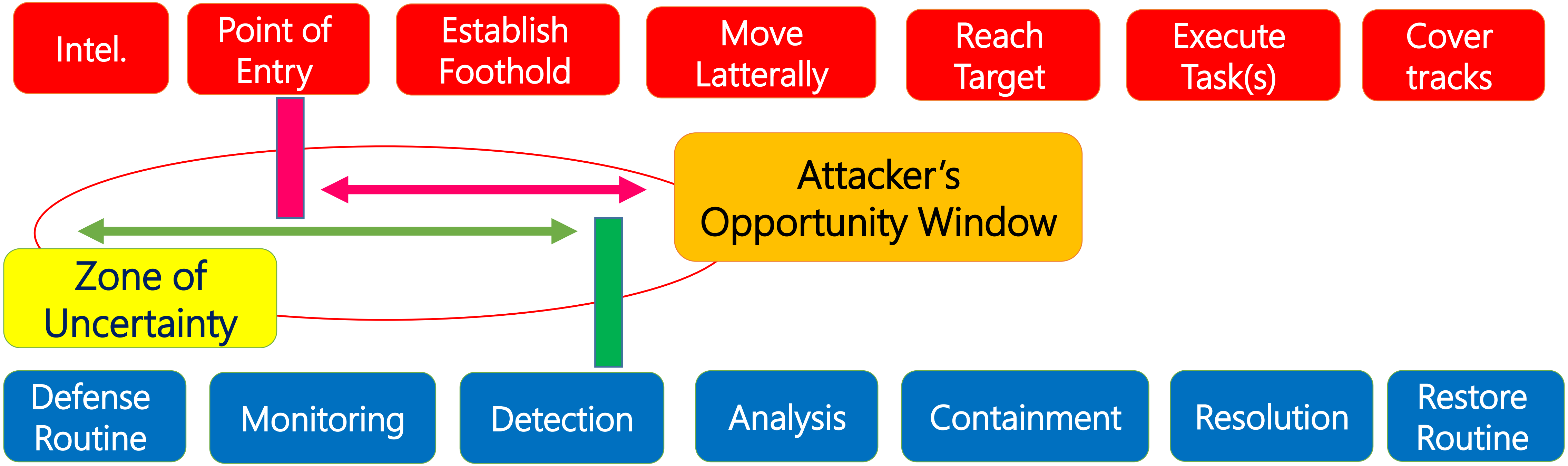
```
[>] Duplicating CreateProcessWithLogonW handles..
[!] No valid thread handles were captured, exiting!
PS ► while ($Bouzoukitara.Plugged -eq $true) {Enjoy-Moment -Recurse}
..hack
```

WhoAmI

- InfoSec Researcher; H@ɔk3r (1nTh35h311)
- Red mind, Blue heart
- Co-Founder @ 10ROOT CYBER SECURITY
- Consulting in 4 continents (Banks/gov/F100)
- 35 years of keyboard access – Code, IT Sec, Net Comms.
- The HActive Directory guy; Ex-Javelin Networks (Acquired by Symantec)
- Ex-Technology Group Manager @ Microsoft (Coded Windows Server Tools)
- Volunteer (Youth at risk); Aviator; Oriental Rock Bouzoukitarist

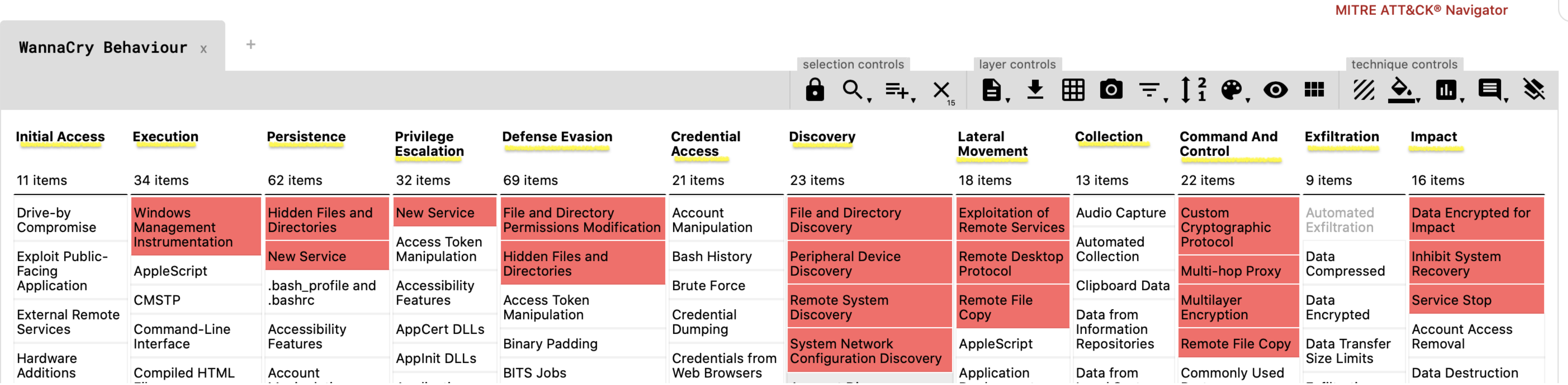
Why should we care about the Attacker Mindset?

Anatomy of an Attack Vs. Defense Controls



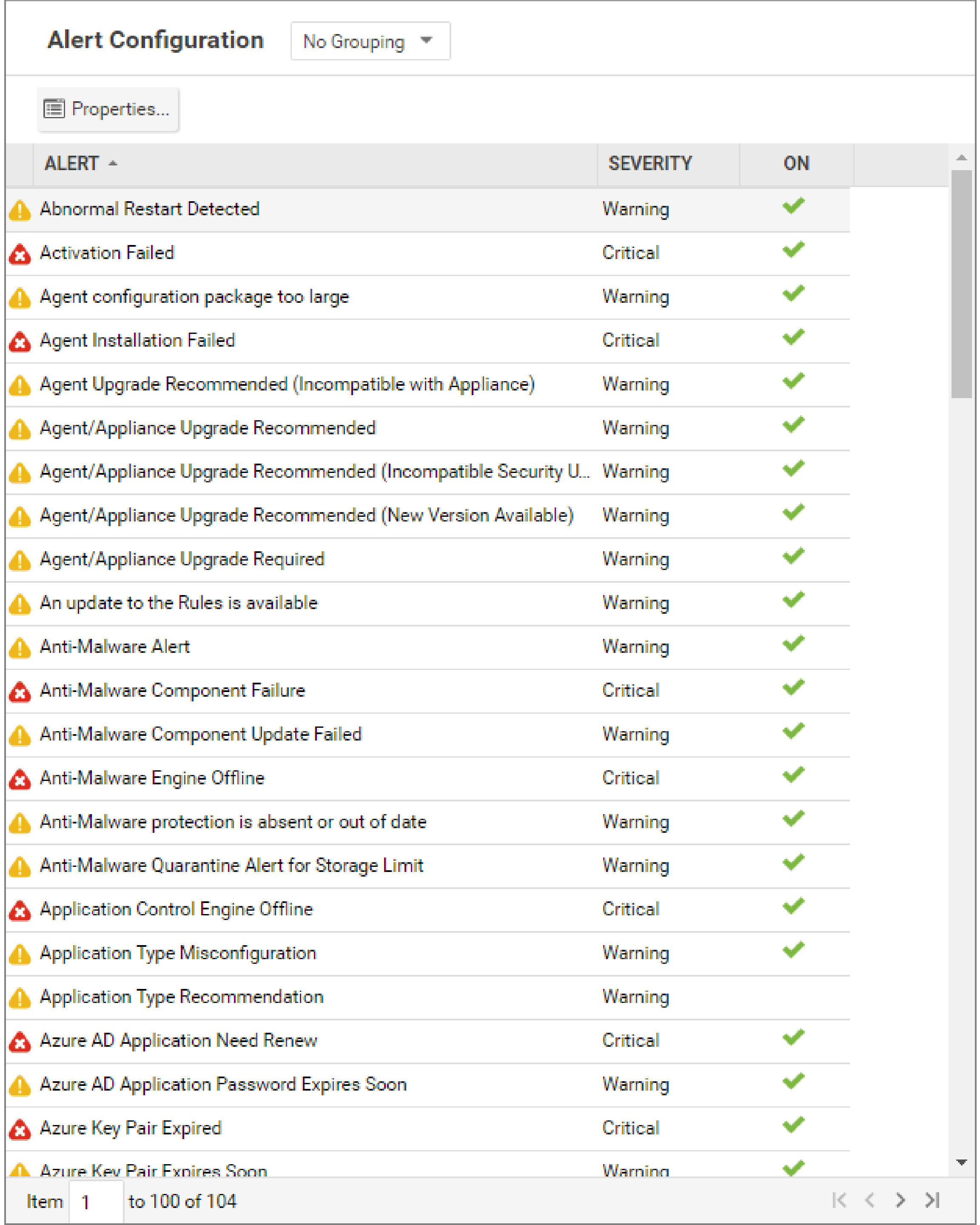
Understanding the Attacker Mindset

MITRE & TTPs



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	Windows Management Instrumentation	Hidden Files and Directories	New Service	File and Directory Permissions Modification	Account Manipulation	File and Directory Discovery	Exploitation of Remote Services	Audio Capture	Custom Cryptographic Protocol	Automated Exfiltration	Data Encrypted for Impact
Exploit Public-Facing Application	AppleScript	New Service	Access Token Manipulation	Hidden Files and Directories	Bash History	Peripheral Device Discovery	Remote Desktop Protocol	Automated Collection	Multi-hop Proxy	Data Compressed	Inhibit System Recovery
External Remote Services	CMSTP	.bash_profile and .bashrc	Accessibility Features	Access Token Manipulation	Brute Force	Remote System Discovery	Remote File Copy	Clipboard Data	Multilayer Encryption	Data Encrypted	Service Stop
Hardware Additions	Command-Line Interface	Accessibility Features	AppCert DLLs	Binary Padding	Credential Dumping	System Network Configuration Discovery	AppleScript	Data from Information Repositories	Remote File Copy	Data Transfer Size Limits	Account Access Removal
	Compiled HTML	Account	AppInit DLLs	BITS Jobs	Credentials from Web Browsers		Application	Data from	Commonly Used		Data Destruction

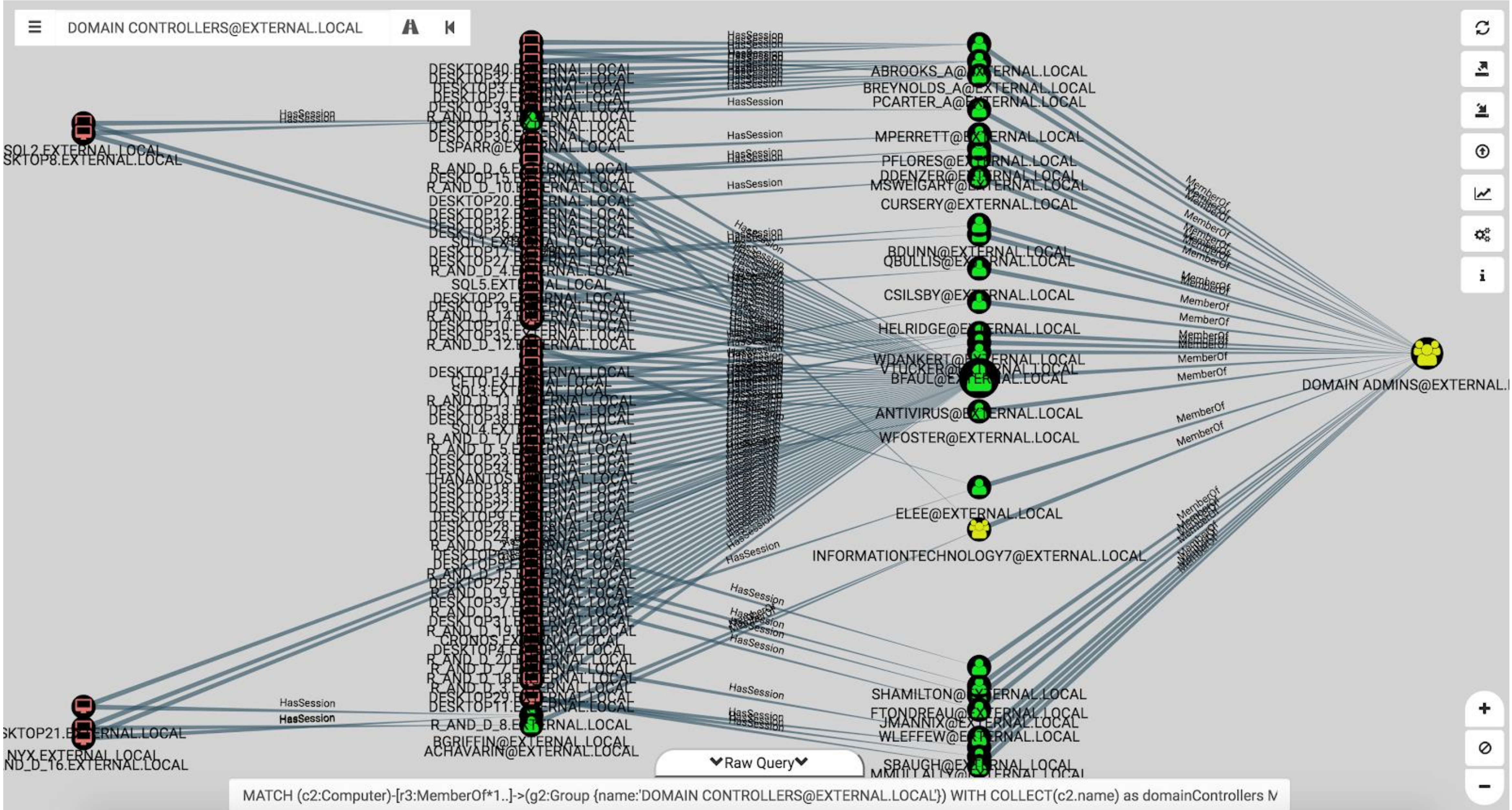
Defenders ‘think’ with Lists



ALERT	SEVERITY	ON
Abnormal Restart Detected	Warning	✓
Activation Failed	Critical	✓
Agent configuration package too large	Warning	✓
Agent Installation Failed	Critical	✓
Agent Upgrade Recommended (Incompatible with Appliance)	Warning	✓
Agent/Appliance Upgrade Recommended	Warning	✓
Agent/Appliance Upgrade Recommended (Incompatible Security U...	Warning	✓
Agent/Appliance Upgrade Recommended (New Version Available)	Warning	✓
Agent/Appliance Upgrade Required	Warning	✓
An update to the Rules is available	Warning	✓
Anti-Malware Alert	Warning	✓
Anti-Malware Component Failure	Critical	✓
Anti-Malware Component Update Failed	Warning	✓
Anti-Malware Engine Offline	Critical	✓
Anti-Malware protection is absent or out of date	Warning	✓
Anti-Malware Quarantine Alert for Storage Limit	Warning	✓
Application Control Engine Offline	Critical	✓
Application Type Misconfiguration	Warning	✓
Application Type Recommendation	Warning	
Azure AD Application Need Renew	Critical	✓
Azure AD Application Password Expires Soon	Warning	✓
Azure Key Pair Expired	Critical	✓
Azure Key Pair Expires Soon	Warning	✓

Item 1 to 100 of 104

Attackers ‘think’ laterally



```
MATCH (c2:Computer)-[r3:MemberOf*1..]->(g2:Group {name:'DOMAIN CONTROLLERS@EXTERNAL.LOCAL'}) WITH COLLECT(c2.name) as domainControllers M
```

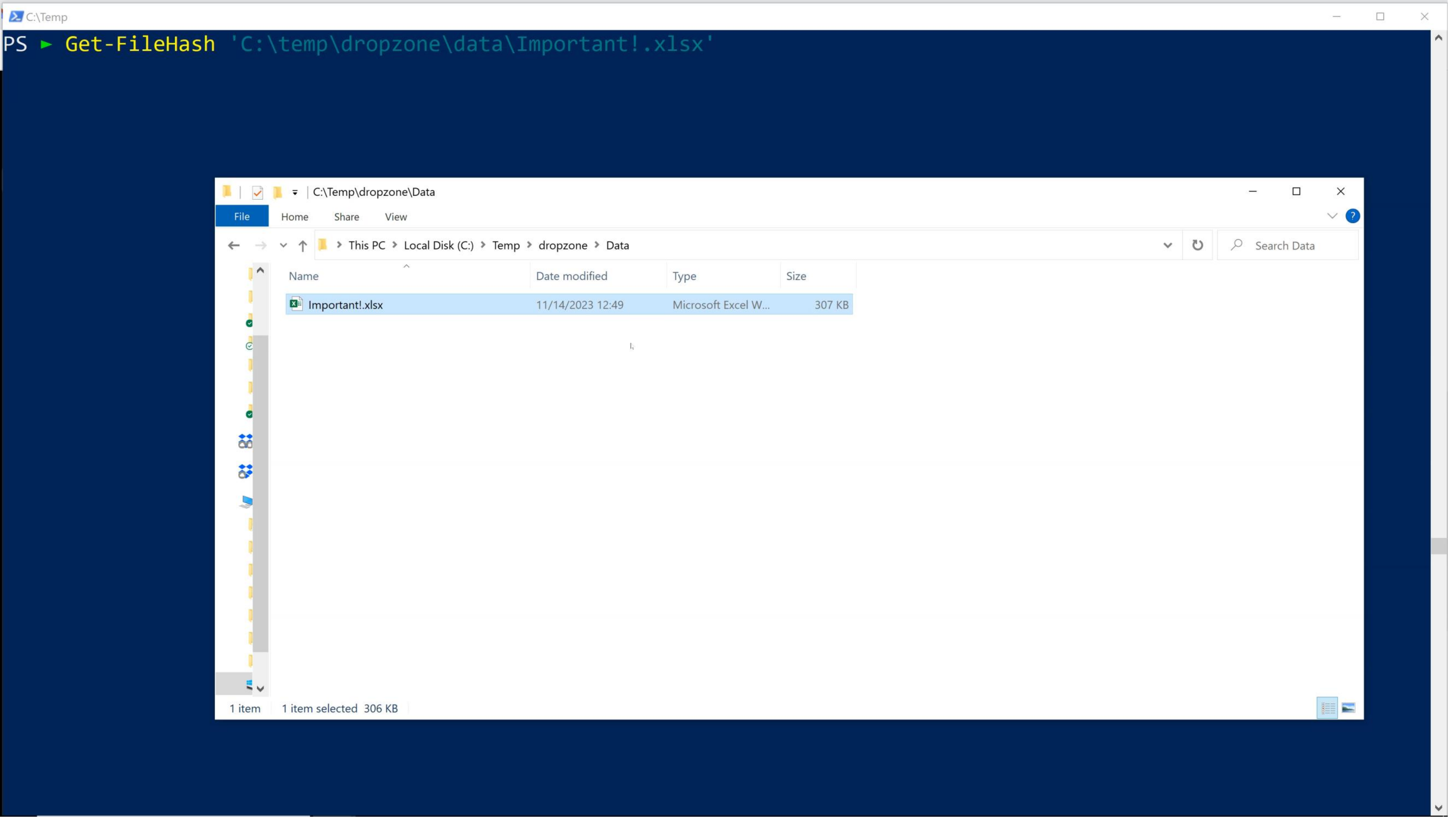
Nakatomi Space

Systems were intended for all their pathways to be traversed ☺

Our Connected World –

What does technology ‘do’?

-> Manipulates Time & Space



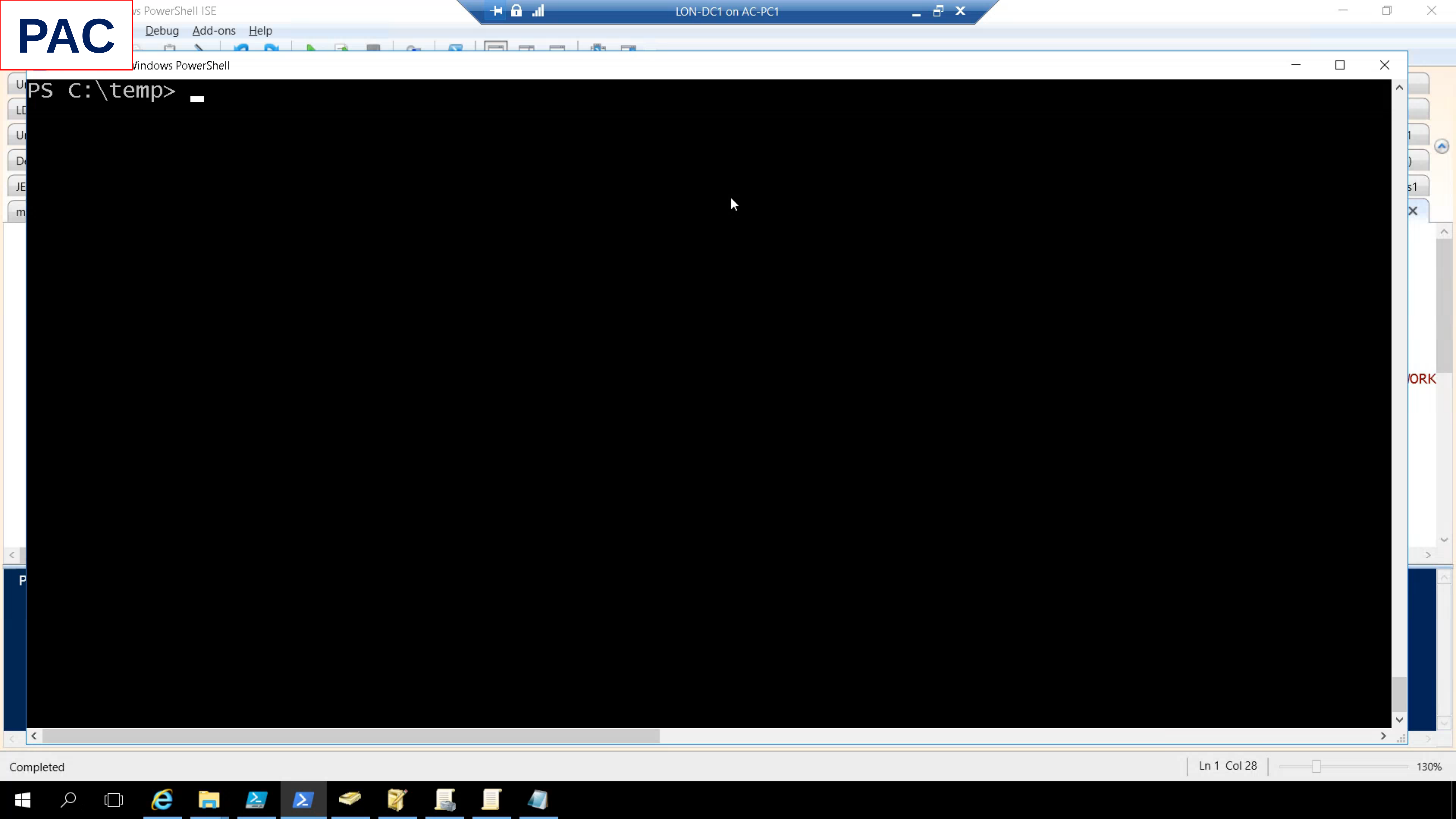
```
PS ► Get-FileHash 'C:\temp\dropzone\data\Important!.xlsx'
```

Name	Date modified	Type	Size
Important!.xlsx	11/14/2023 12:49	Microsoft Excel W...	307 KB

1 item   1 item selected 306 KB

Attacker Mindset: Concepts

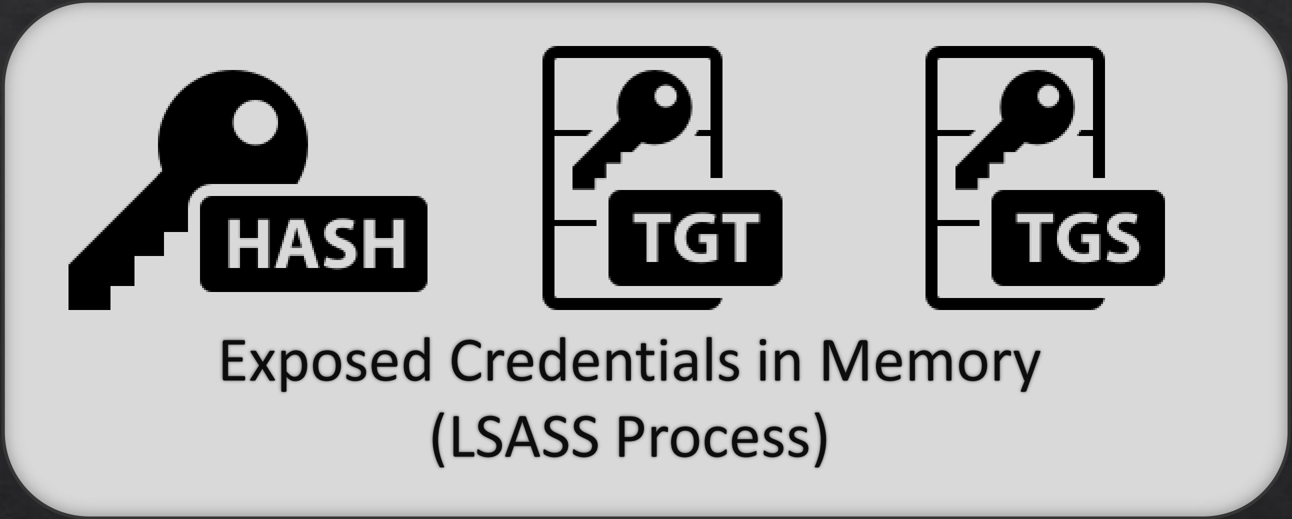
Concept / characteristics	Example defense considerations
Curiosity, Exploration, Obsession for ‘winning’	**No info=no attack, Decoys**
Adaptability, Creativity, Resourcefulness	**Monitoring TTPs, multi-layered defense controls**
Exploitation of Human Psychology, focus on High Value targets with Weak Points	**raising awareness (beyond phishing), handling Legacy, un-patched & misconfigurations**
Anonymity, Stealth, Persistence, Evade detection, Cover Tracks	**Apply relevant sensors, behavioral analysis**
Deep System Architecture knowledge, Continuous Learning	**Foster an ongoing learning culture, strive for constant improvement**



s PowerShell ISE
Debug
Add-ons
Help
LON-DC1 on AC-PC1
Windows PowerShell
Completed
Ln 1 Col 28
130%

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

In memory credentials



Exposed Credentials in Memory
(LSASS Process)

Password or Hashes are valid until
password enroll

Tickets are valid for 10H

Practical Examples
for Defense & Offense

Tools in a ‘Living off the land’ mindset

- Using resources already available
- Built-in tools/APIs abuse (e.g. powershell)
- Load code in context of legitimate process

Remote Management or Lateral Movement?

‘Living off the land’ defense example - RDP

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

*** 39484** Failed RDP logon events in less than 5 hours(!)

* 17458 events - user name does not exist (most tried ADMINISTRATOR, then Admin, then TEMP)

*** 22026** events - user name is correct (administrator) but the password is wrong

- *After* renaming the administrator account:

40156 Failed logon events in less than ~5 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

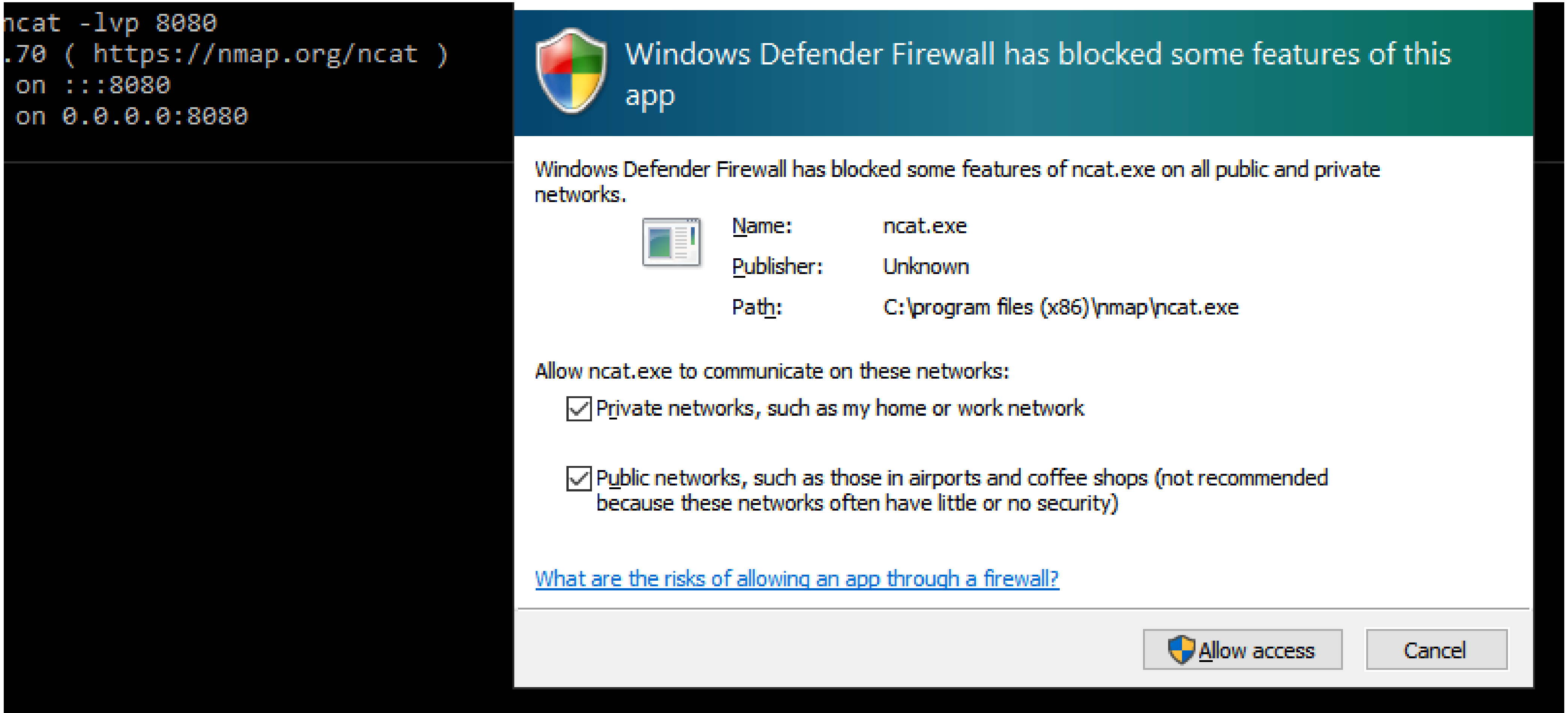
Inter-Process Communications (IPC)

- 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 ☺



```
ncat -lvp 8080
.70 ( https://nmap.org/ncat )
 on :::8080
 on 0.0.0.0:8080
```

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of ncat.exe on all public and private networks.

Name: ncat.exe

Publisher: Unknown

Path: C:\program files (x86)\nmap\ncat.exe

Allow ncat.exe to communicate on these networks:

☑ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

Named-Pipe/SMB One-liner

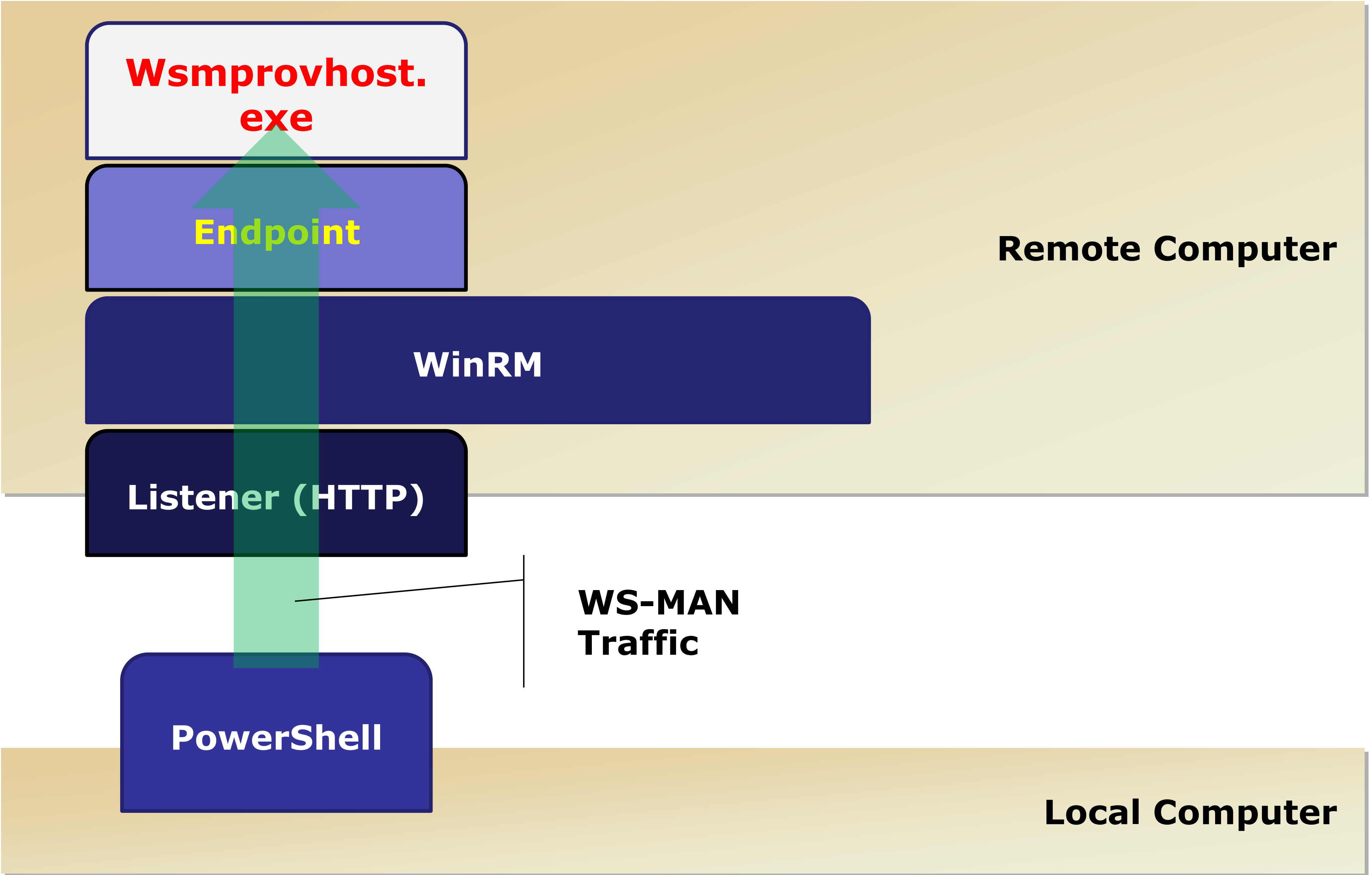
(Exfiltrate data/C2 with No socket bind)

IPC C2

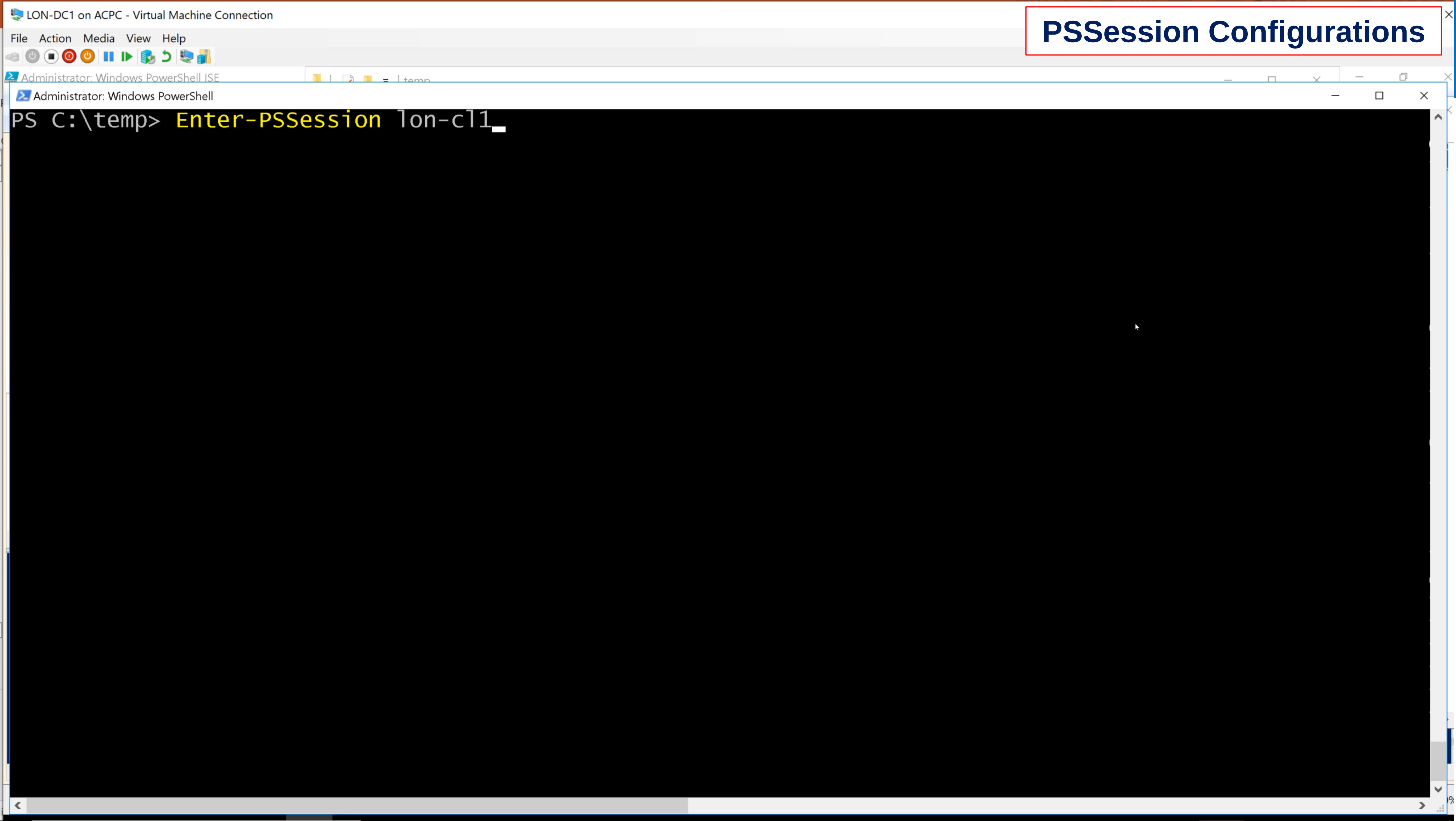
LON-CL1 on ACPC - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
PowerShell

```
PS C:\>
```

PSRemoting Architecture



PSSession Configurations

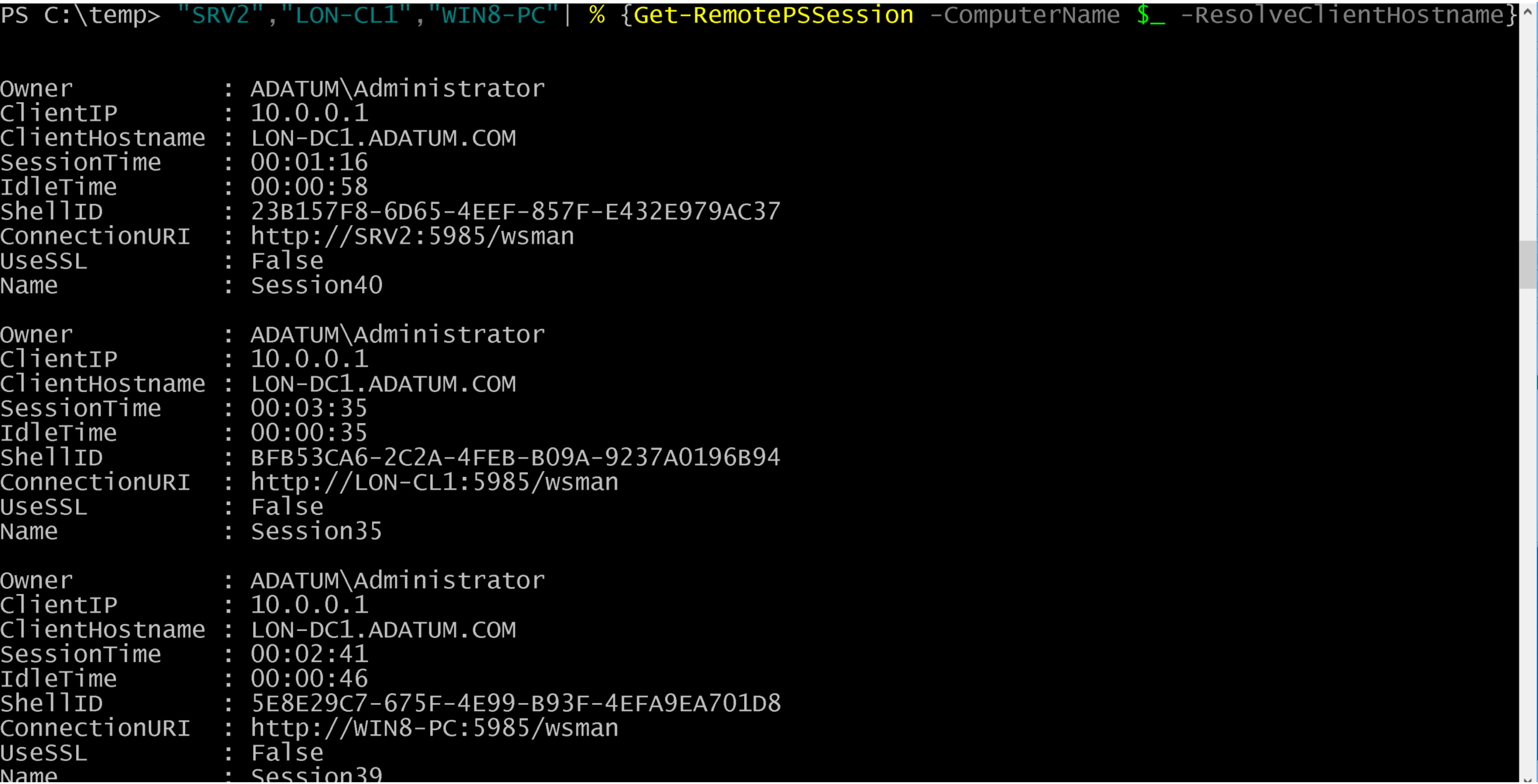

LON-DC1 on ACPC - Virtual Machine Connection
File
Action
Media
View
Help
Administrator: Windows PowerShell ISE
Administrator: Windows PowerShell

```
PS C:\temp> Enter-PSSession lon-cl1
```

Mapping / Hunting for WSMan sessions

- EDR/Sysmon etc. (**wsmprovhost.exe**)
- WinRM / PowerShell-operational logs
- Try **Get-RemotePSSession.ps1** script

Query PSRemoting Sessions

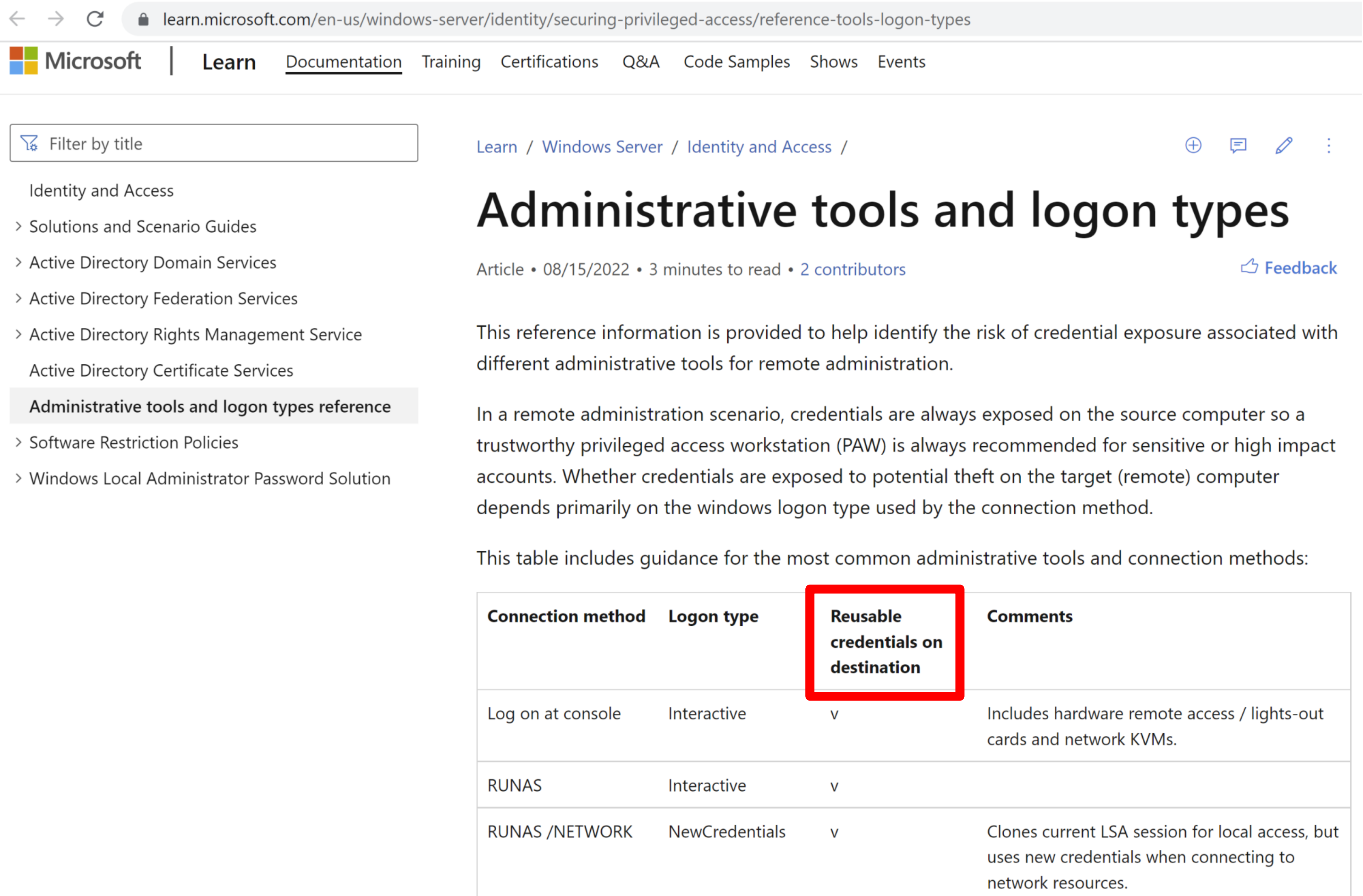


```
PS C:\temp> "SRV2","LON-CL1","WIN8-PC"| % {Get-RemotePSSession -ComputerName $_ -ResolveClientHostname}


Owner          : ADATUM\Administrator
ClientIP       : 10.0.0.1
ClientHostname : LON-DC1.ADATUM.COM
SessionTime    : 00:01:16
IdleTime       : 00:00:58
ShellID        : 23B157F8-6D65-4EEF-857F-E432E979AC37
ConnectionURI  : http://SRV2:5985/wsman
UseSSL         : False
Name           : Session40

Owner          : ADATUM\Administrator
ClientIP       : 10.0.0.1
ClientHostname : LON-DC1.ADATUM.COM
SessionTime    : 00:03:35
IdleTime       : 00:00:35
ShellID        : BFB53CA6-2C2A-4FEB-B09A-9237A0196B94
ConnectionURI  : http://LON-CL1:5985/wsman
UseSSL         : False
Name           : Session35

Owner          : ADATUM\Administrator
ClientIP       : 10.0.0.1
ClientHostname : LON-DC1.ADATUM.COM
SessionTime    : 00:02:41
IdleTime       : 00:00:46
ShellID        : 5E8E29C7-675F-4E99-B93F-4EFA9EA701D8
ConnectionURI  : http://WIN8-PC:5985/wsman
UseSSL         : False
Name           : Session39
```

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

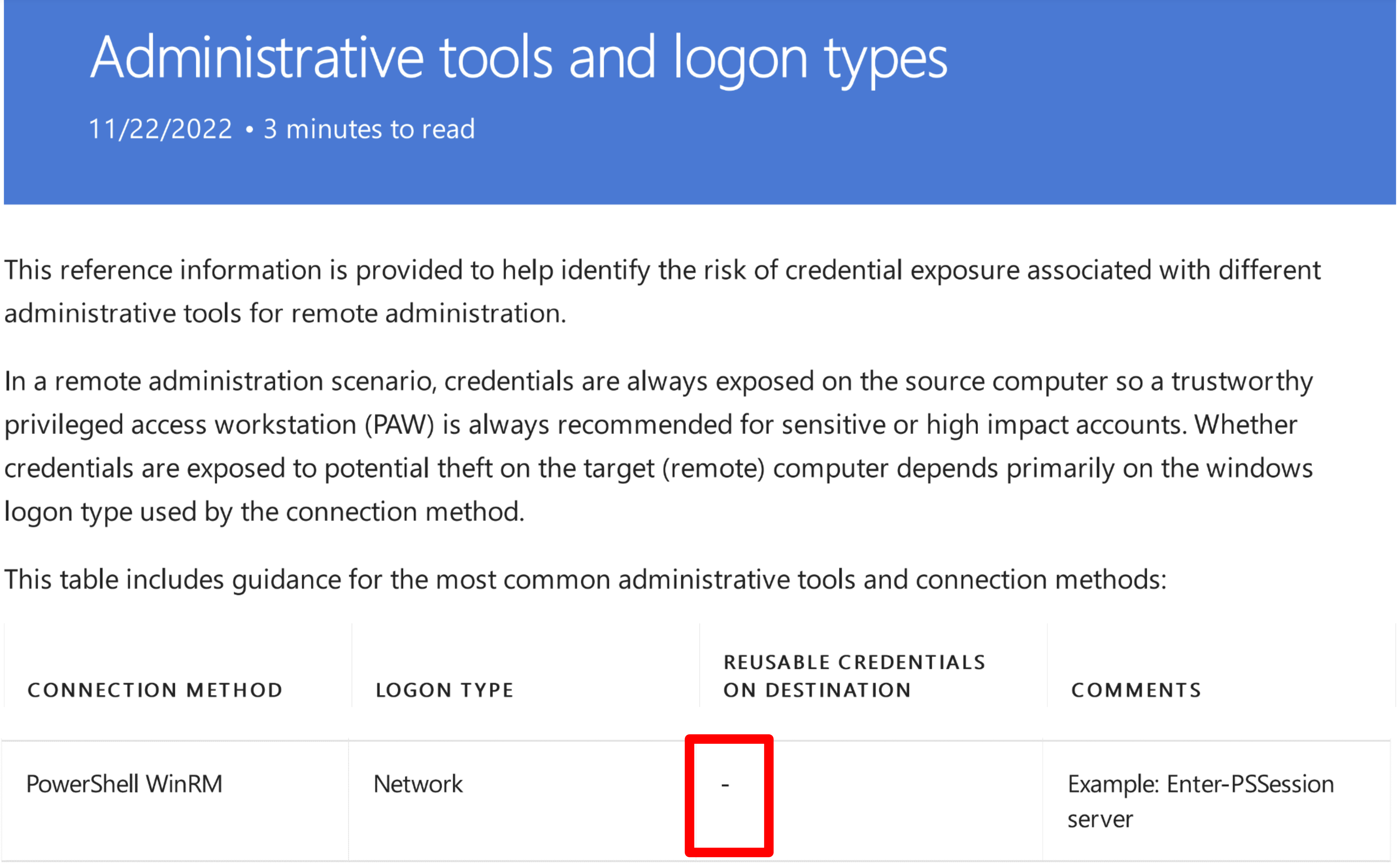
Feedback

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.

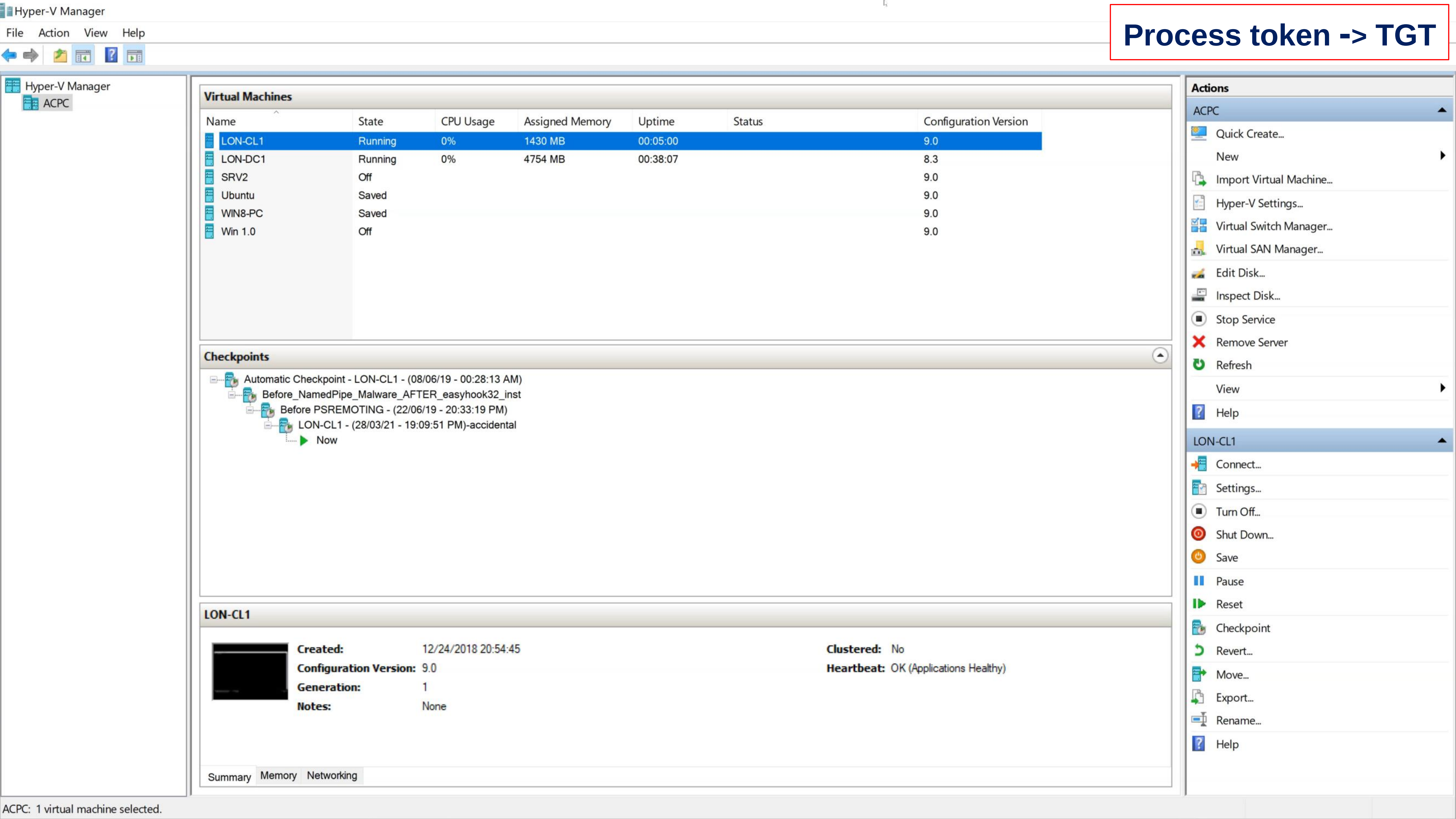
In a remote administration scenario, credentials are always exposed on the source computer so a trustworthy privileged access workstation (PAW) is always recommended for sensitive or high impact accounts. Whether credentials are exposed to potential theft on the target (remote) computer depends primarily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



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

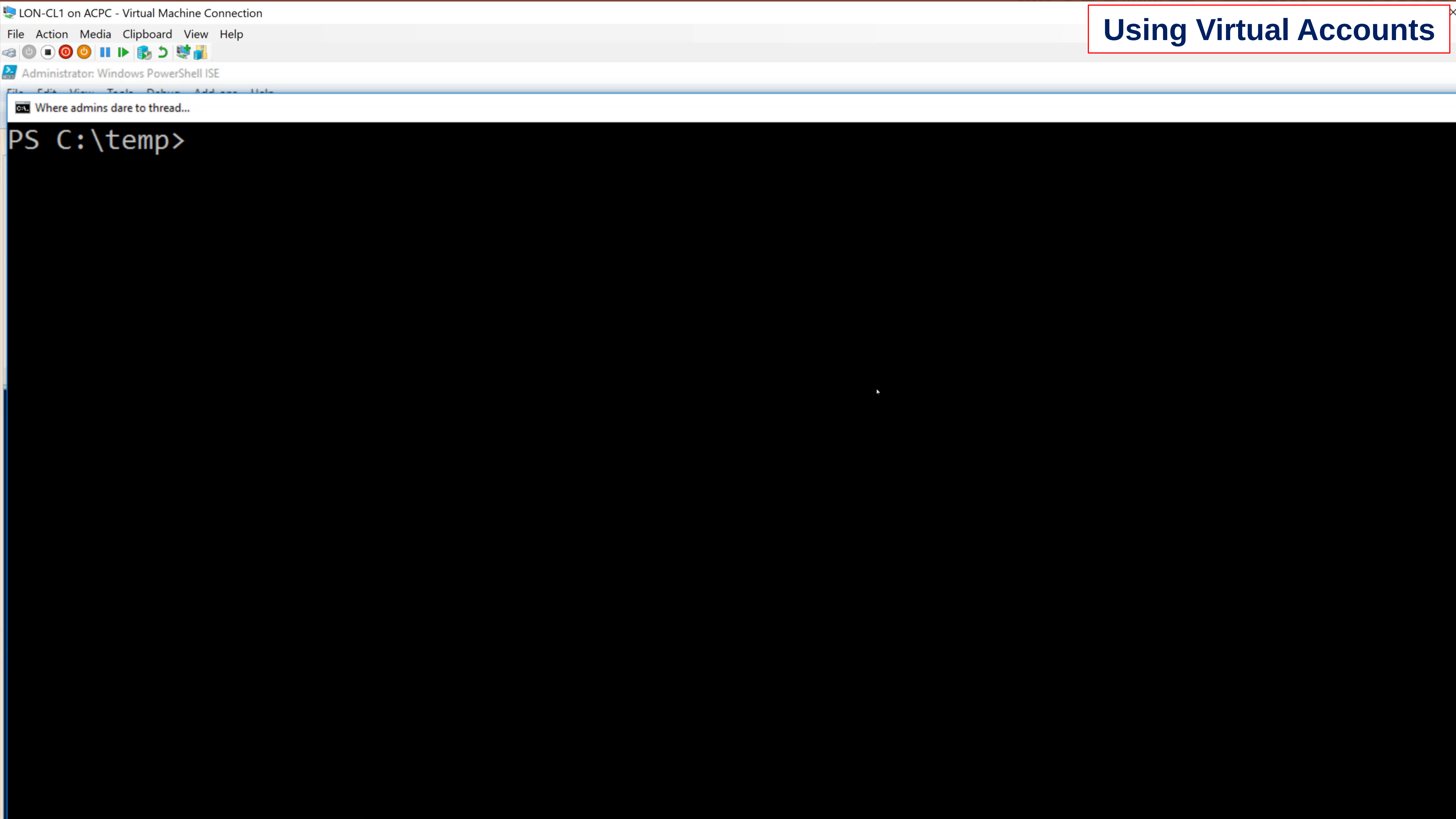
Clustered: No

Heartbeat: OK (Applications Healthy)

ACPC: 1 virtual machine selected.

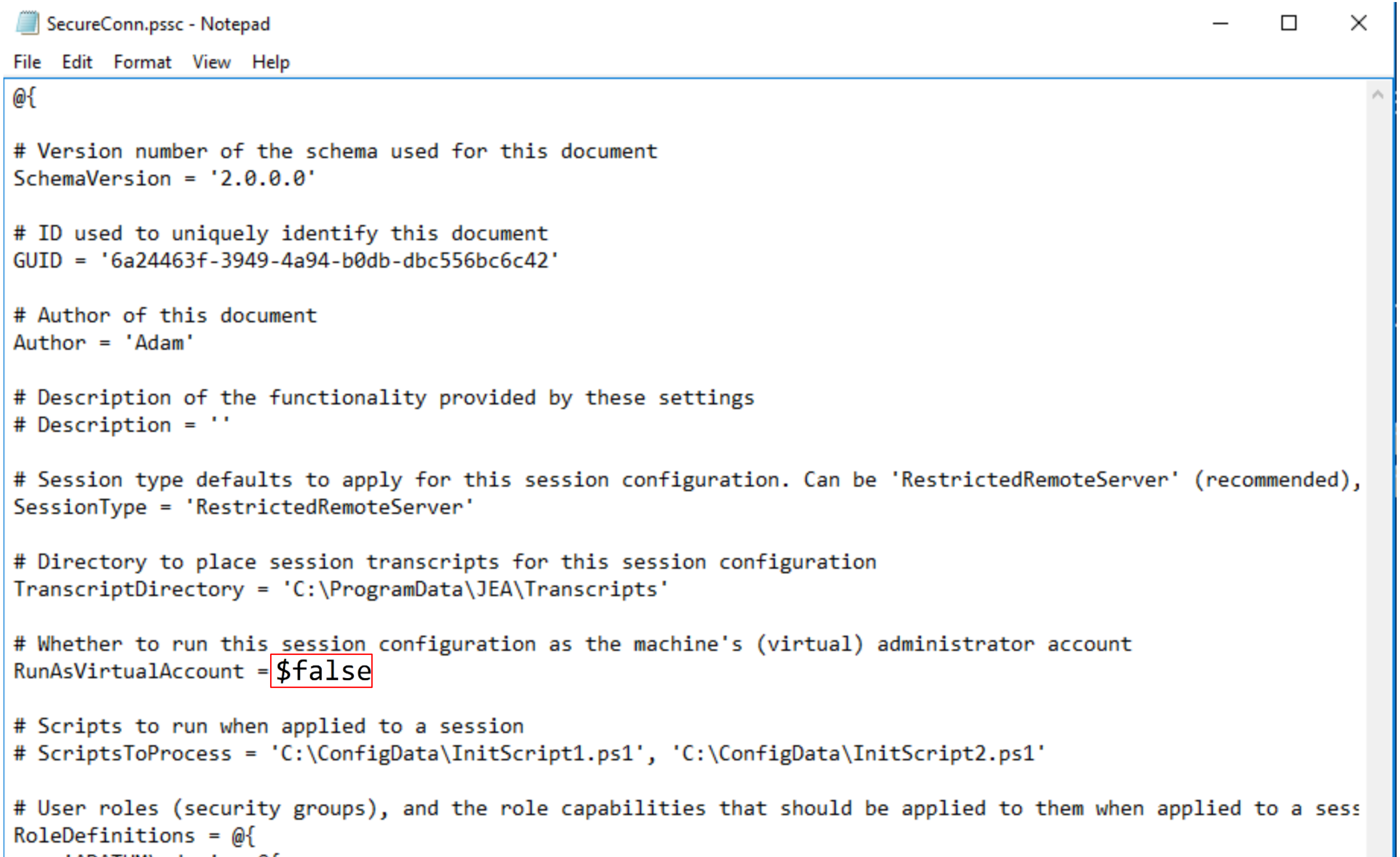
Potential Mitigation – Use Virtual accounts

Using Virtual Accounts


LON-CL1 on ACPC - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Administrator: Windows PowerShell ISE
Where admins dare to thread...

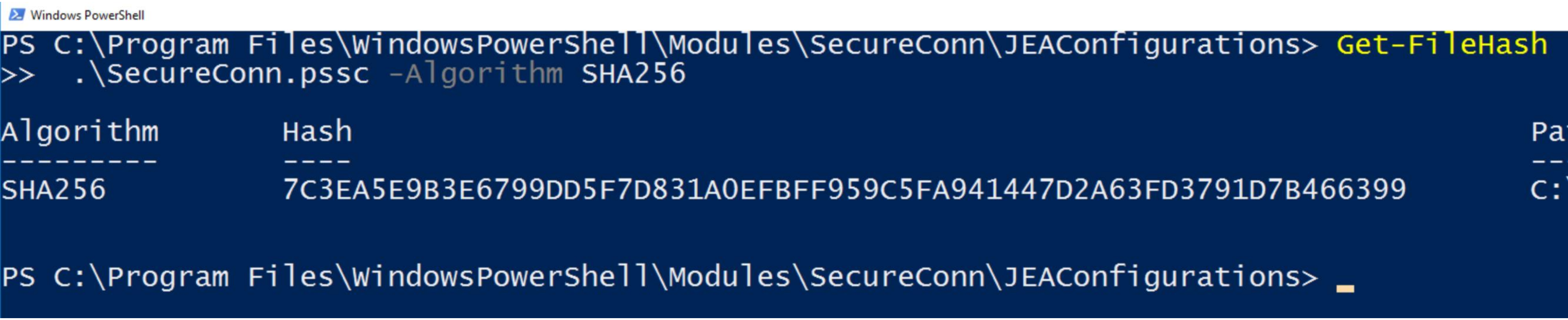
```
PS C:\temp>
```

But… the adversary can edit the Role Capabilities file ☺



```
@{

# 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)



```
PS C:\Program Files\WindowsPowerShell\Modules\SecureConn\JEAConfigurations> Get-FileHash
>>   .\SecureConn.pssc -Algorithm SHA256

Algorithm       Hash                                                                   Pa
---------       ----                                                                   --
SHA256          7C3EA5E9B3E6799DD5F7D831A0EFBFF959C5FA941447D2A63FD3791D7B466399       C:

PS C:\Program Files\WindowsPowerShell\Modules\SecureConn\JEAConfigurations> _
```

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?”

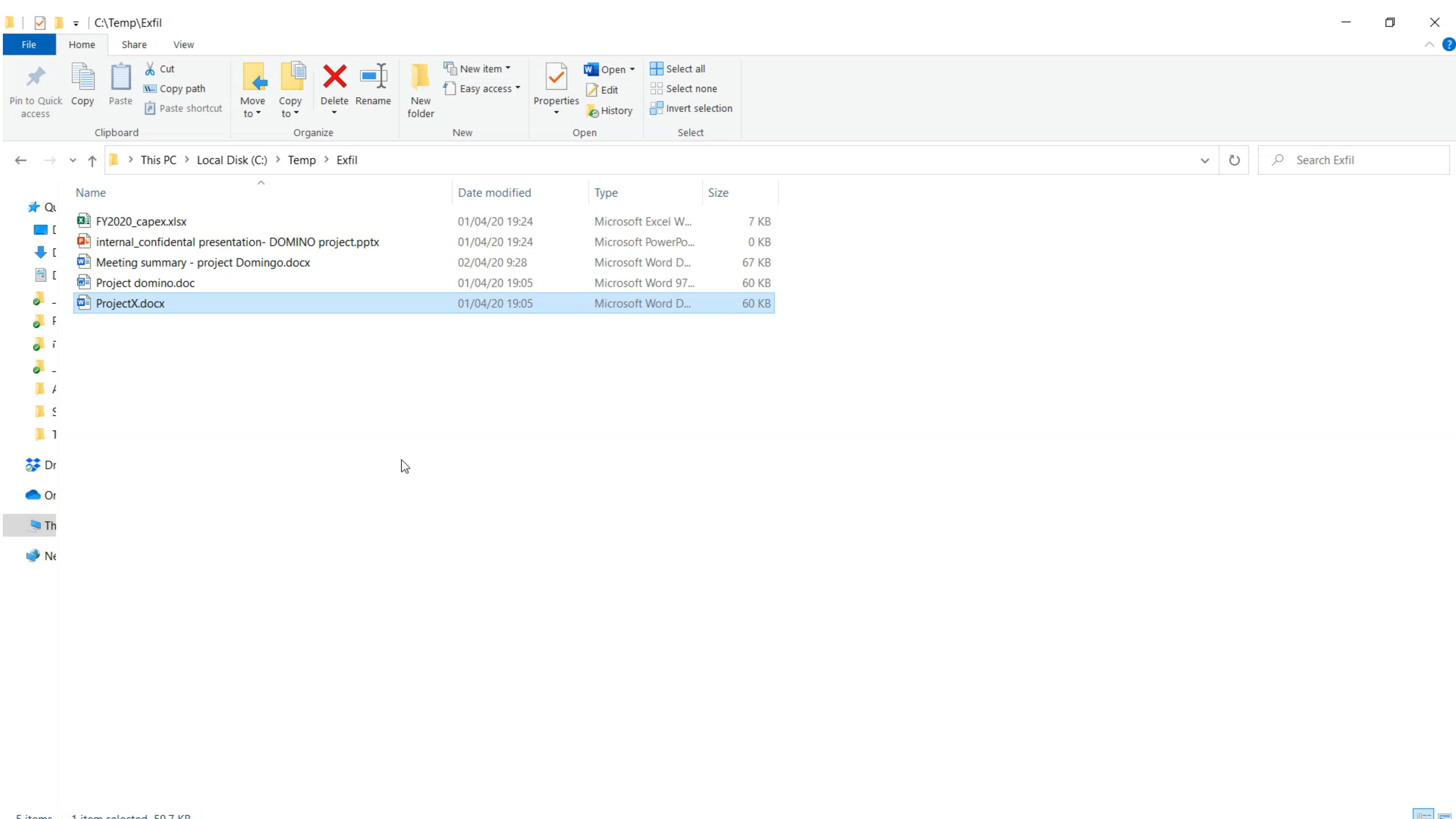
C2 is not about an established connection.

Nor TCP, or UDP.

It’s a MINDSET

How about your **email client**?

When outlook goes rouge



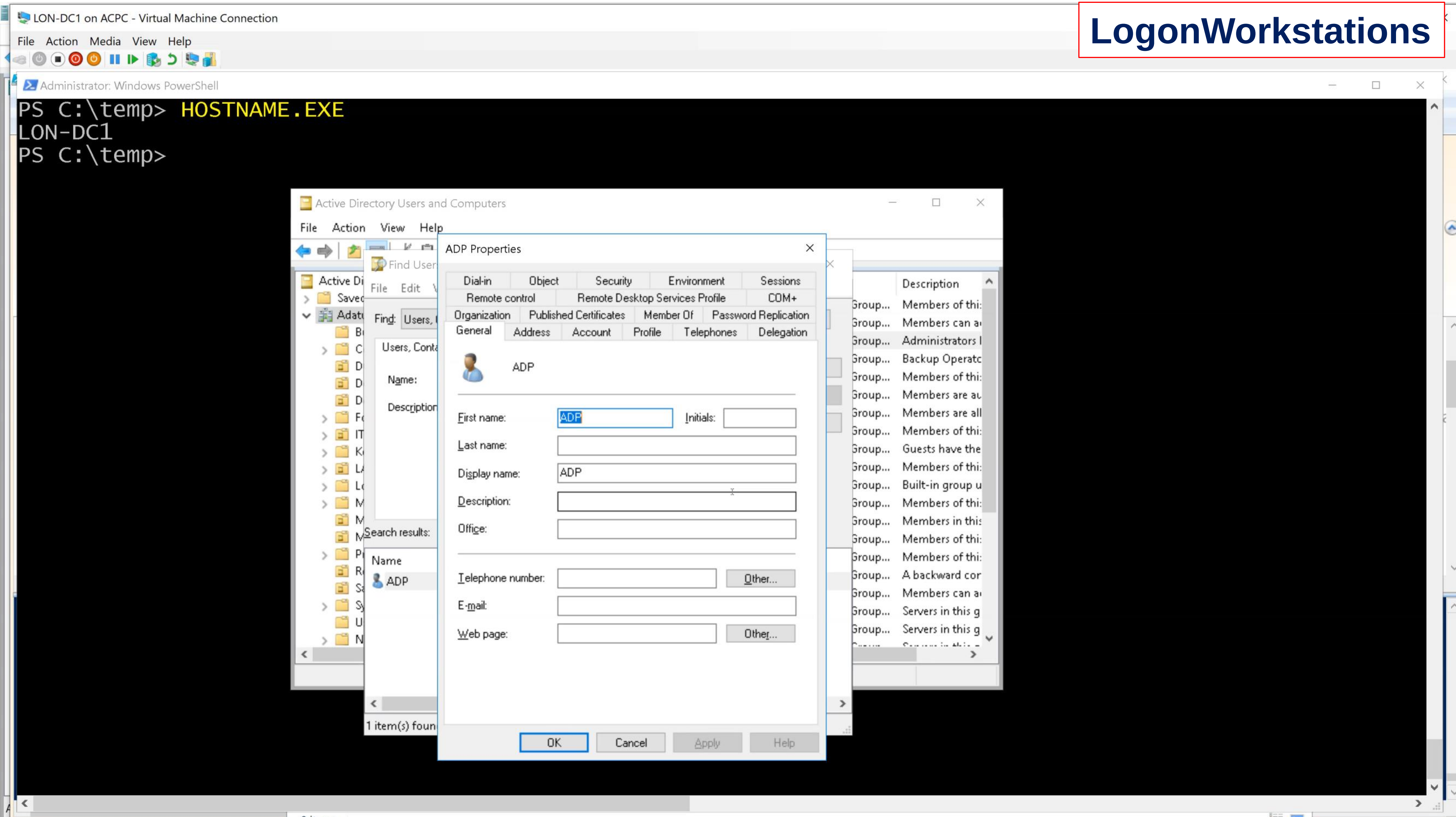
Name	Date modified	Type	Size
FY2020_capex.xlsx	01/04/20 19:24	Microsoft Excel W...	7 KB
internal_confidental presentation- DOMINO project.pptx	01/04/20 19:24	Microsoft PowerPo...	0 KB
Meeting summary - project Domingo.docx	02/04/20 9:28	Microsoft Word D...	67 KB
Project domino.doc	01/04/20 19:05	Microsoft Word 97...	60 KB
ProjectX.docx	01/04/20 19:05	Microsoft Word D...	60 KB

5 items 1 item selected 59.7 KB

HOW DO I PREVENT DOMAIN ADMINS FROM LOGON TO ENDPOINTS
... AND STOP LATERAL MOVEMENT?
imgflip.com

How do we STOP Lateral Movement?
Buy a New EDR
Firewall
Just set 'Logon Restrictions' in AD?
imgflip.com

LogonWorkstations



```
PS C:\temp> HOSTNAME.EXE
LON-DC1
PS C:\temp>
```

ADP Properties

ADP

First name: ADP

Initials:

Last name:

Display name: ADP

Description:

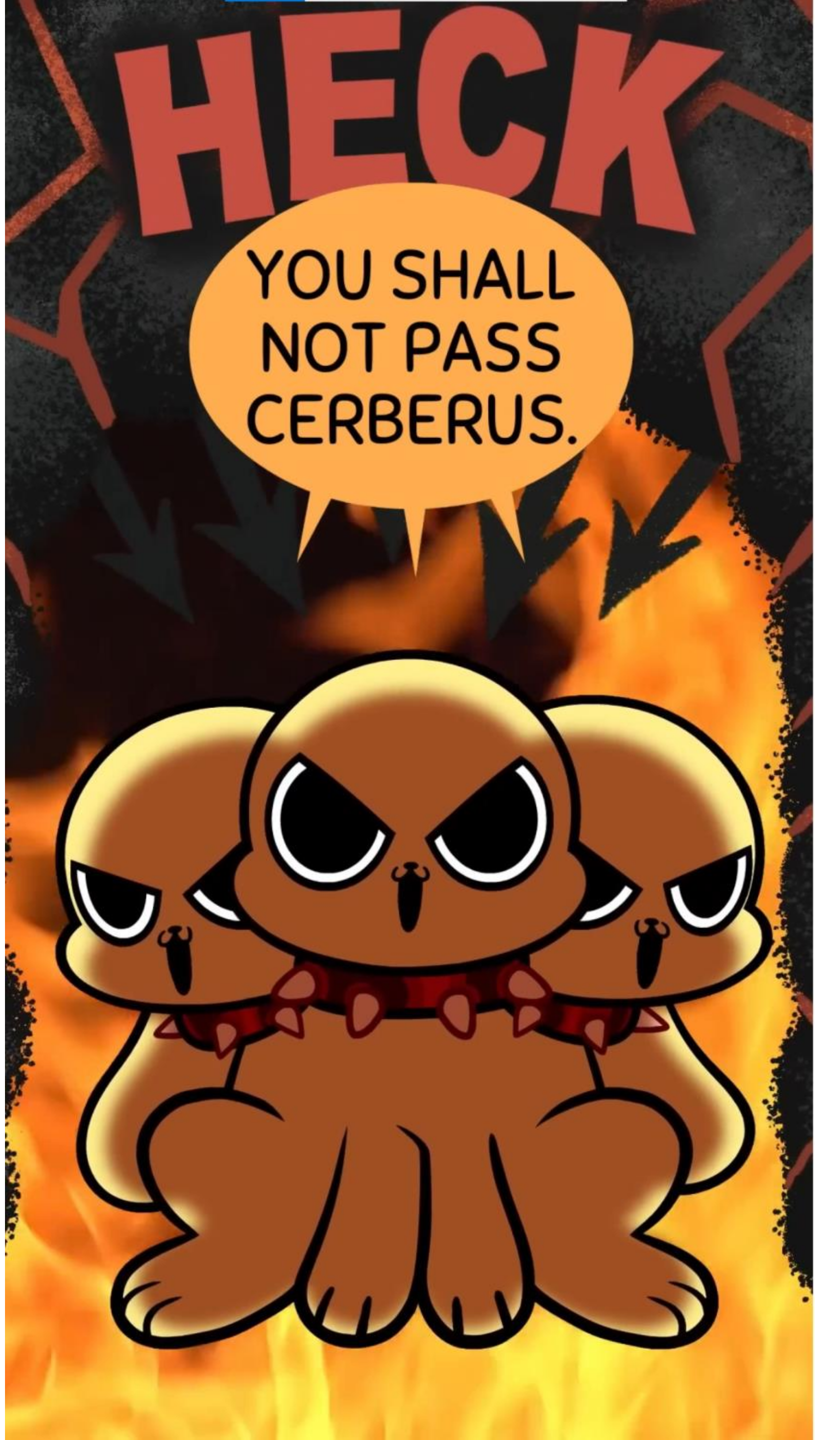
Office:

Telephone number:

E-mail:

Web page:

…But, what about crafting your TGT to *remove* LogonRestrictions? ☺

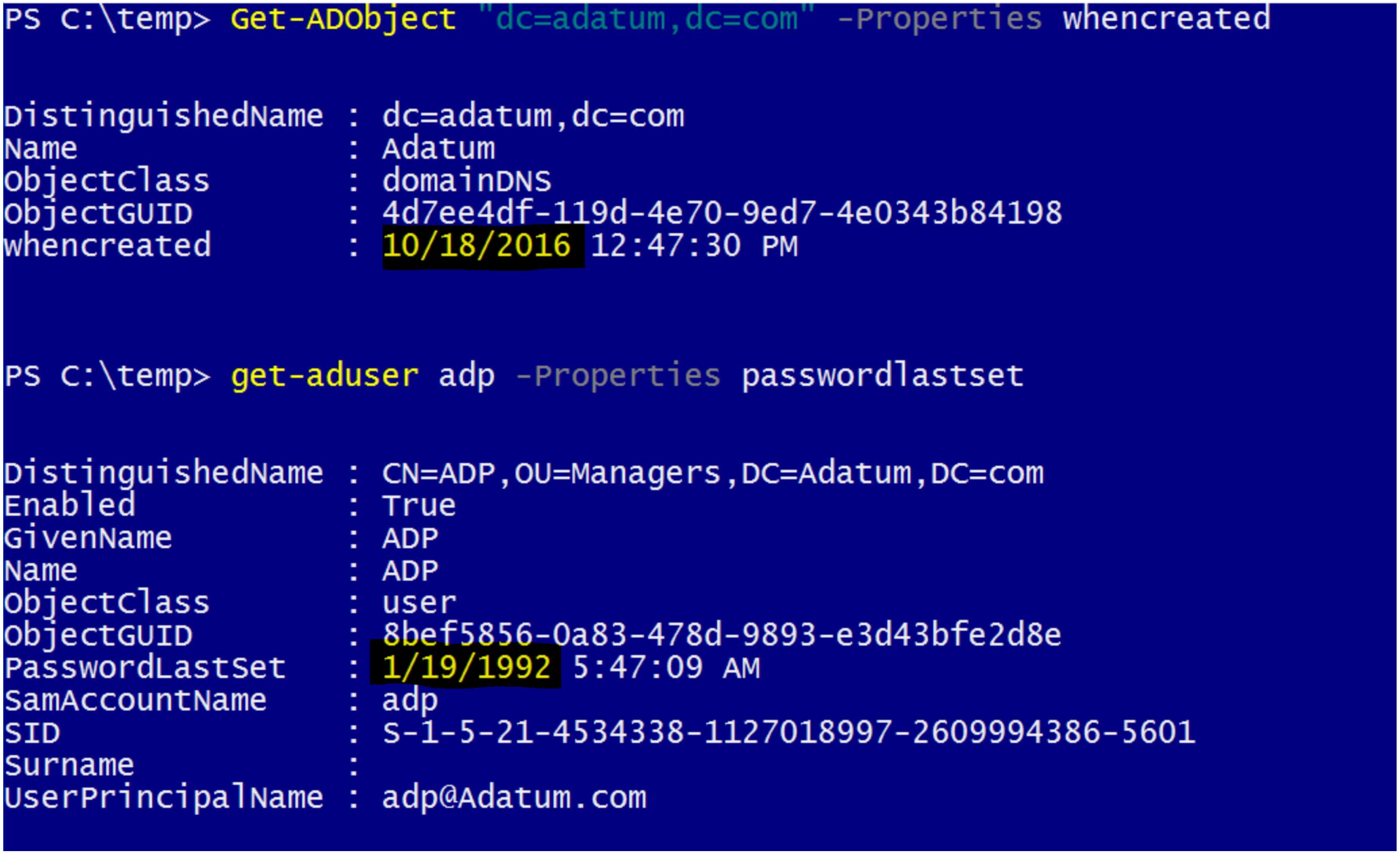


"All warfare is based on deception“

- Sun Tzu, “The Art of War”

Tips on Creating Decoy Accounts

- Account set to Pre-AuthN *not* required (vulnerable to AS-REProasting), yet with a very Longgggg password
- Privileged admin account – *tightly monitored*
  - Enabled, yet with:
    - logonHours set to none(?) - Pros/Cons
    - logonWorkstations - Same dilemma – Pros/Cons..
    - Consider adding a SPN (kerberoasting)
- Leverage ‘DCShadow attack’ to change pwdlastset to ‘appear’ as weak/old password ☺ *



```
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:
Check if Defenders are ‘tricking’ you

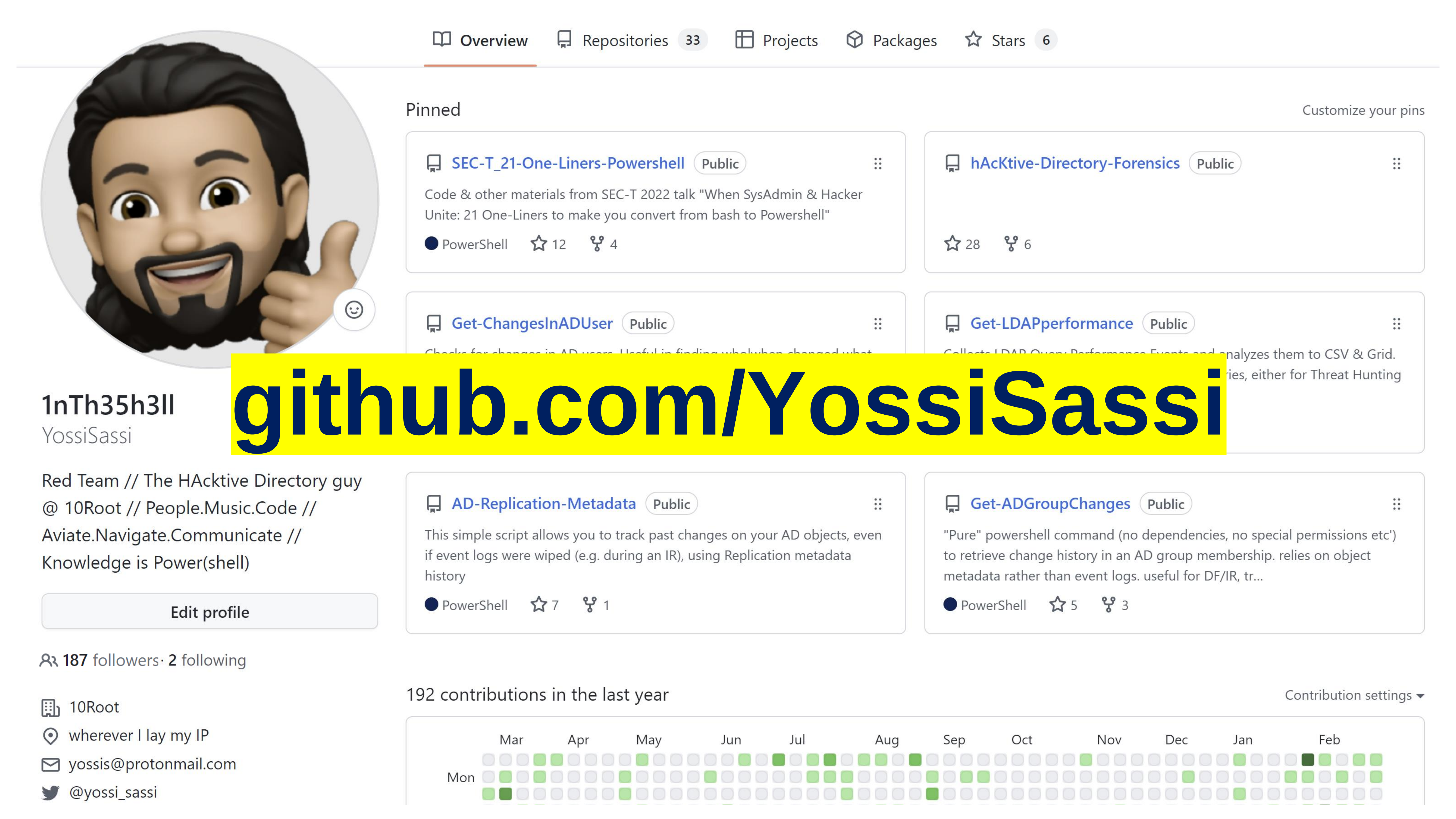
- Mmm.. Maybe, check replication metadata LastOriginatingChangeTime? ☺

Blue Team:

Ensure you ‘fix’ the metadata as well

- With mimikatz, can utilize /replOriginatingTime:**YYYY-MM-DD** , /replOriginatingUsn:**<USN>** argument

github.com/YossiSassi



Overview | Repositories 33 | Projects | Packages | Stars 6

1nTh35h3ll

YossiSassi

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

Edit profile

187 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

Checks for changes in AD users. Useful in finding who/when changed what

Get-LDAPperformance Public

Collects LDAP Query Performance Events and analyzes them to CSV & Grid.

ries, 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 ▾

Key Takeaways

- Understanding ‘The Attacker Mindset’ is crucial for both defense & offense efforts
  - Embrace ‘Living off the land’ tools mindset (Red & Blue)
  - Get practical with relevant concepts & knowledge

- ***Time*** is the only Cyber Security metric(s)
- Check out **github.com/YossiSassi** for tools & scripts

D@nk3

𝕏 Yossi_Sassi

✉ yossis@protonmail.com