Detecting Ghouls & Ghosts in the Wires

Michael Edie
BSIDES Augusta 2023

print('imaohw'[::-1])

USARMY Veteran (24 Years)

- Senior Security Engineer
- Data Engineer
- Tank Mechanic

SmashTheStack.org (Software Vuln Challenges)

- Principal Engineer & Co-Founder

Pluralsight Author

Adjunct Instructor – UCF

CyberPatriot Mentor – RCTC Magnet School

AGENDA

- Attacker Dwell Time
- Detective Controls
- Ghost-Busting*
- Demo
- Review & Conclusion

Attacker Dwell Time

Dwell Time: Definition

The amount of time an adversary remains within a network or system *undetected* after initial intrusion.

Attacker Dwell Time: Reporting

"According to the M-Trends 2023 report, the global median dwell time – which is calculated as the median number of days an attacker is present in a target's environment before being detected – **continues to drop year-over-year down to 16 days in 2022**."

MANDIANT®
NOW PART OF Google Cloud

Attacker Dwell Time: Reporting

"… We saw the most improvement in non-ransomware dwell times, down more than 23 days from 34 days to 11 days. (There were, however, some outliers, with one victim hosting **attackers in their network for more than 2.5 years**.)"

Sophos X-Ops

Detective Controls

Detective Controls: Vendors

GRR RAPID RESPONSE

Microsoft Security

zeek

elastic

VMware Carbon Black™

CROWDSTRIKE

TREND MICRO

Security Onion

Trellix

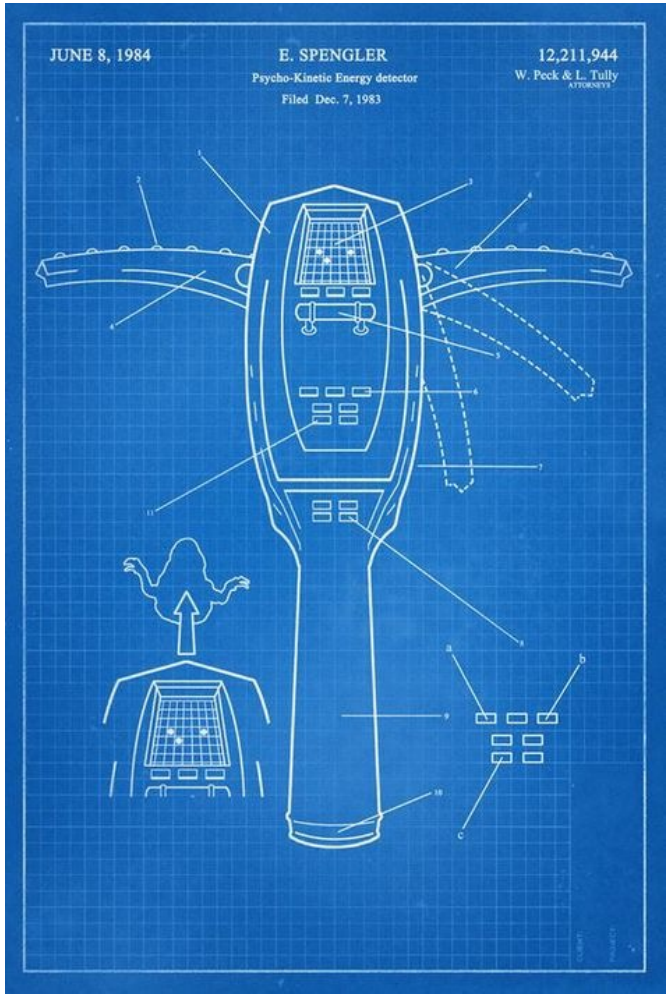
SURICATA

Detective Controls: Implementation

- Endpoint Detection & Response (EDR / XDR)
- Security Incident & Event Management (SIEM)
- Intrusion Detection System (IDS / IPS)
- File Integrity Monitoring (FIM)
- Honeypots / Honeytokens

Ghost-Busting

Spector Detector



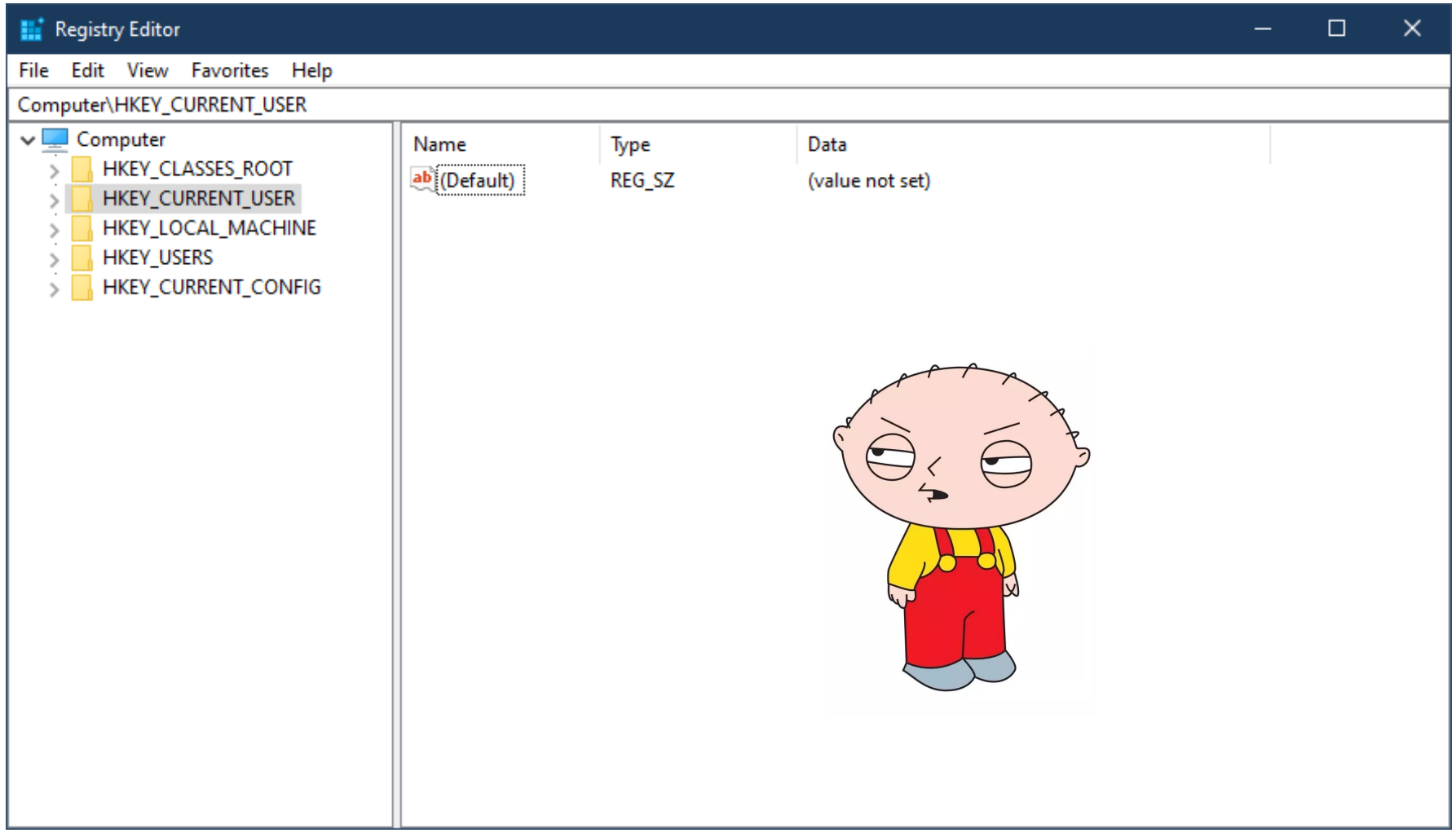
Security Event ID 4663

Ghost-Busting: Object Access Auditing

Ghost-Busting: Object Access Auditing

Tracks who accessed what and when on the filesystem.

Object Access Auditing: Registry



Object Access Auditing: Files & Folders

Trickbot

To grab VNC credentials, the pwgrab module ***searches for files*** *using the* "*.vnc.lnk" *affix that are in the following directories:*

- `%APPDATA%\Microsoft\Windows\Recent`
- `%USERPROFILE%\Documents`
- `%USERPROFILE%\Downloads`

Reference: https://bit.ly/3PCkE9l

Operation Wocao

6.7.3 File and Directory Discovery

The following command is executed to identify the contents of a (KeePass configuration) file:

```
/Q /c type c:\users\<username>\appdata\Roaming\keepass\KeePass.config.xml
```

The following command is executed to list all files in a specific directory with the kdbx (KeePass database) extension:

```
/Q /c dir *.kdbx
```

FOX IT

Reference: https://bit.ly/3EFTj00

Machete: Cyberespionage Toolset

```
#Do nothing for these folders
if list_subfolders[1] == 'Program Files' or app == 'AppData' or list_subfolders[1] == 'Program Files (x86)' or
list_subfolders[1] == 'Windows.old' or list_subfolders[1] == 'ProgramData' or list_subfolders[1] == 'Windows' o
list_subfolders[1] == 'Archivos de programa' or list_subfolders[1] == 'WINDOWS':
    pass
else:
    file_name, file_ext = os.path.splitext(file)

    if file_ext == '.doc' or file_ext == '.docx' or file_ext == '.xls' or file_ext == '.xlsx' or file_ext ==
    '.ppt' or file_ext == '.pptx' or file_ext == '.jpg' or file_ext == '.db' or file_ext == '.mdb' or file_ext
    '.pgp' or file_ext == '.skr' or file_ext == '.pkr' or file_ext == '.asc' or file_ext == '.gpg' or file_ext
    '.drw' or file_ext == '.lpt' or file_ext == '.shp' or file_ext == '.rte' or file_ext == '.sda' or file_ext
    '.odp' or file_ext == '.sxi' or file_ext == '.odt' or file_ext == '.sxw' or file_ext == '.ods' or file_ext
    '.sxc' or file_ext == '.odg' or file_ext == '.sxd' or file_ext == '.odb' or file_ext == '.odf' or file_ext
    '.sxm':
```

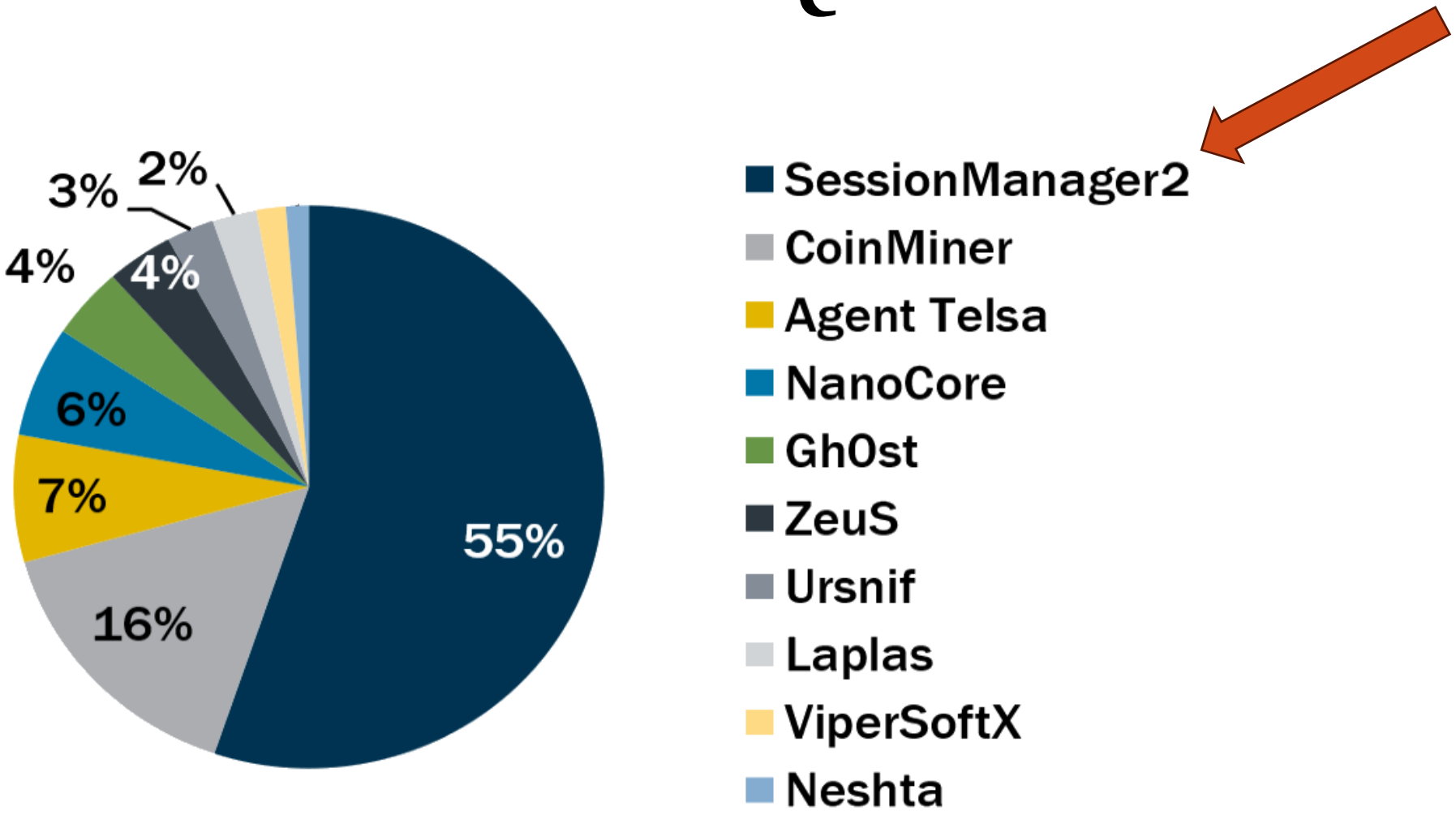
Reference: https://bit.ly/44THe1y

Machete: Cyberespionage Toolset

```
#Do nothing for these folders
if list_subfolders[1] == 'Program Files' or app == 'AppData' or list_subfolders[1] == 'Program Files (x86)' or
list_subfolders[1] == 'Windows.old' or list_subfolders[1] == 'ProgramData' or list_subfolders[1] == 'Windows' o
list_subfolders[1] == 'Archivos de programa' or list_subfolders[1] == 'WINDOWS':
    pass
else:
    file_name, file_ext = os.path.splitext(file)

    if file_ext == '.doc' or file_ext == '.docx' or file_ext == '.xls' or file_ext == '.xlsx' or file_ext ==
    '.ppt' or file_ext == '.pptx' or file_ext == '.jpg' or file_ext == '.db' or file_ext == '.mdb' or file_ext
    '.pgp' or file_ext == '.skr' or file_ext == '.pkr' or file_ext == '.asc' or file_ext == '.gpg' or file_ext
    '.drw' or file_ext == '.lpt' or file_ext == '.shp' or file_ext == '.rte' or file_ext == '.sda' or file_ext
    '.odp' or file_ext == '.sxi' or file_ext == '.odt' or file_ext == '.sxw' or file_ext == '.ods' or file_ext
    '.sxc' or file_ext == '.odg' or file_ext == '.sxd' or file_ext == '.odb' or file_ext == '.odf' or file_ext
    '.sxm':
```

Reference: https://bit.ly/44THe1y

TOP 10 Malware: Q1 2023



CIS Center for Internet Security®

Reference: https://bit.ly/45SMFiJ

SessionManager 2

```
Cookie: SM_SESSION=GETFILE;FILEPATH=private_file.txt;
```

Uber Hack

ok so basically uber had a network share \\[redacted]pts. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite

8:05 PM

on an uber IP range? or [redacted] on like GCP or AWS (*.uberinternal)

edited 8:06 PM

in Uber intranet 8:07 PM

*.corp.uber.com edited 8:07 PM

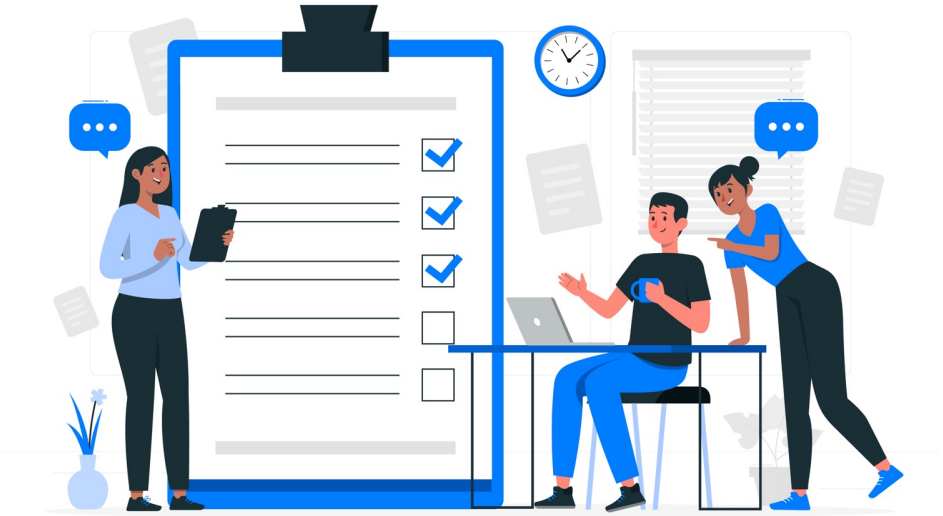
Image credit goes to @hacker_

Ghost-Busting: Discovery Tactic

File and Directory Discovery (T1083)

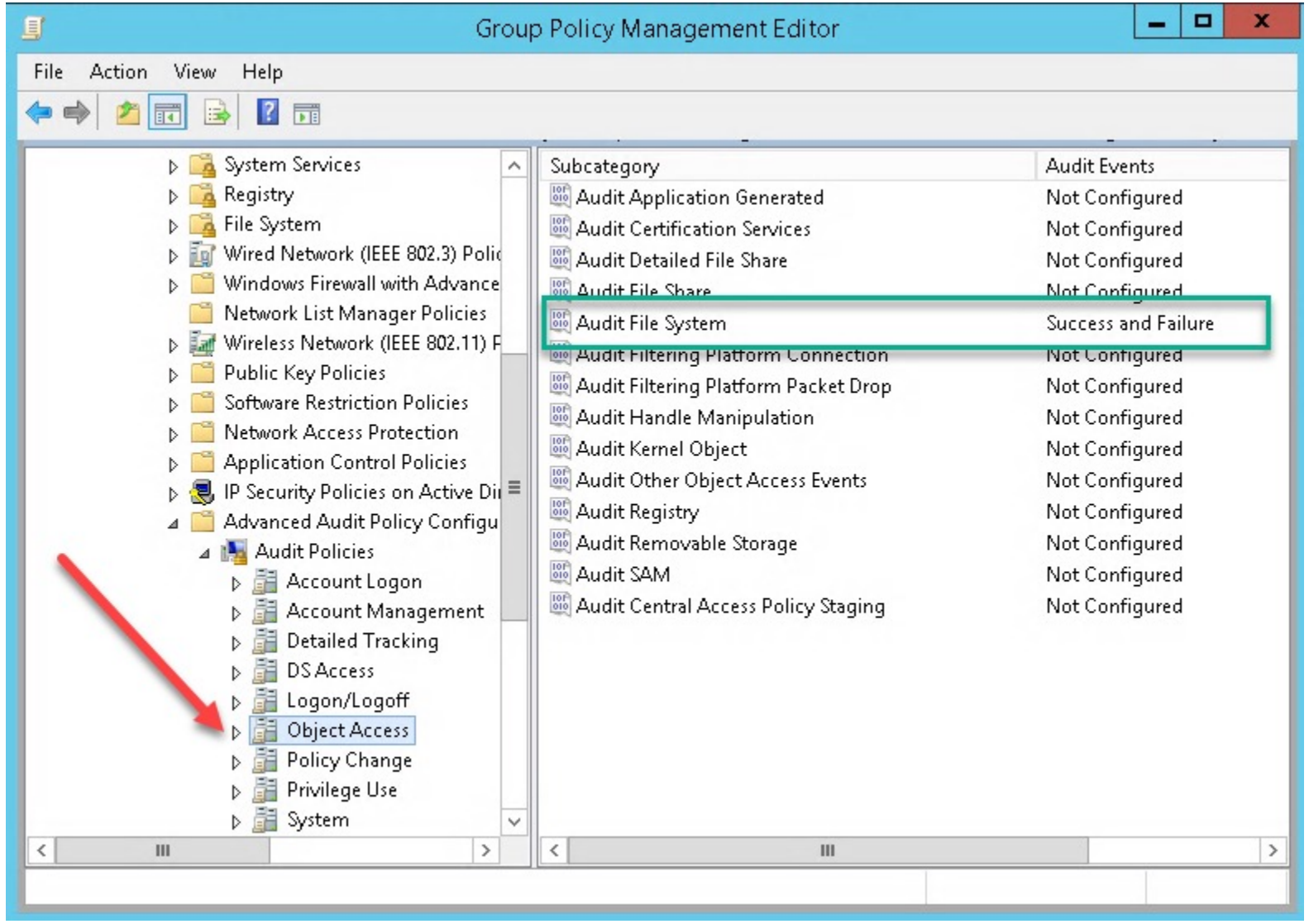
Ghost-Busting: Steps

1. Create Object Access GPO
2. Create Decoys
3. Deploy Files
4. Apply Audit ACL



Credit: Image by storyset on Freepik

Creating the Object Access GPO



Computer Configuration\Policies\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Ghost-Busting: Create Decoys

- **servers.kdbx** (KeePass database)
- **id_rsa.key** (ssh private key)
- **cloud_vps.ovpn** (VPN config with pseudo-credentials)
- **backup.zip** (password-protected zip with enticing contents)
- **%UserProfile%\.aws** (AWS CLI configuration directory)

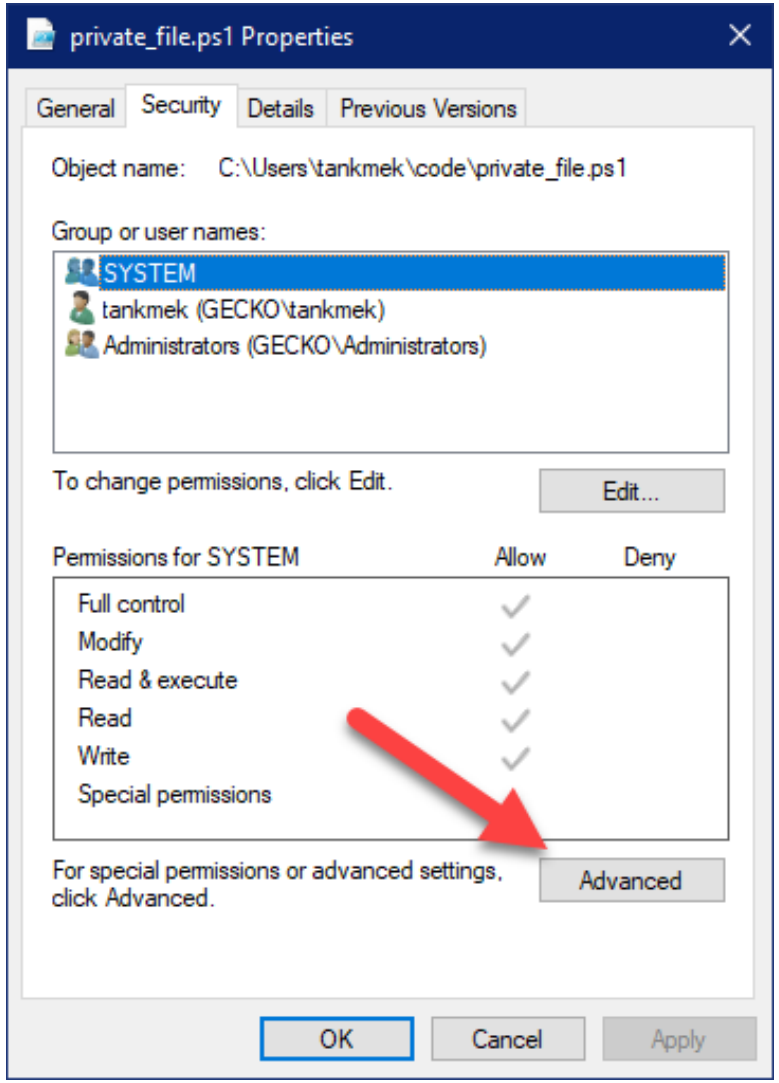
Ghost-Busting: Deploy Decoys

Ghost-Busting: Deploy Decoys

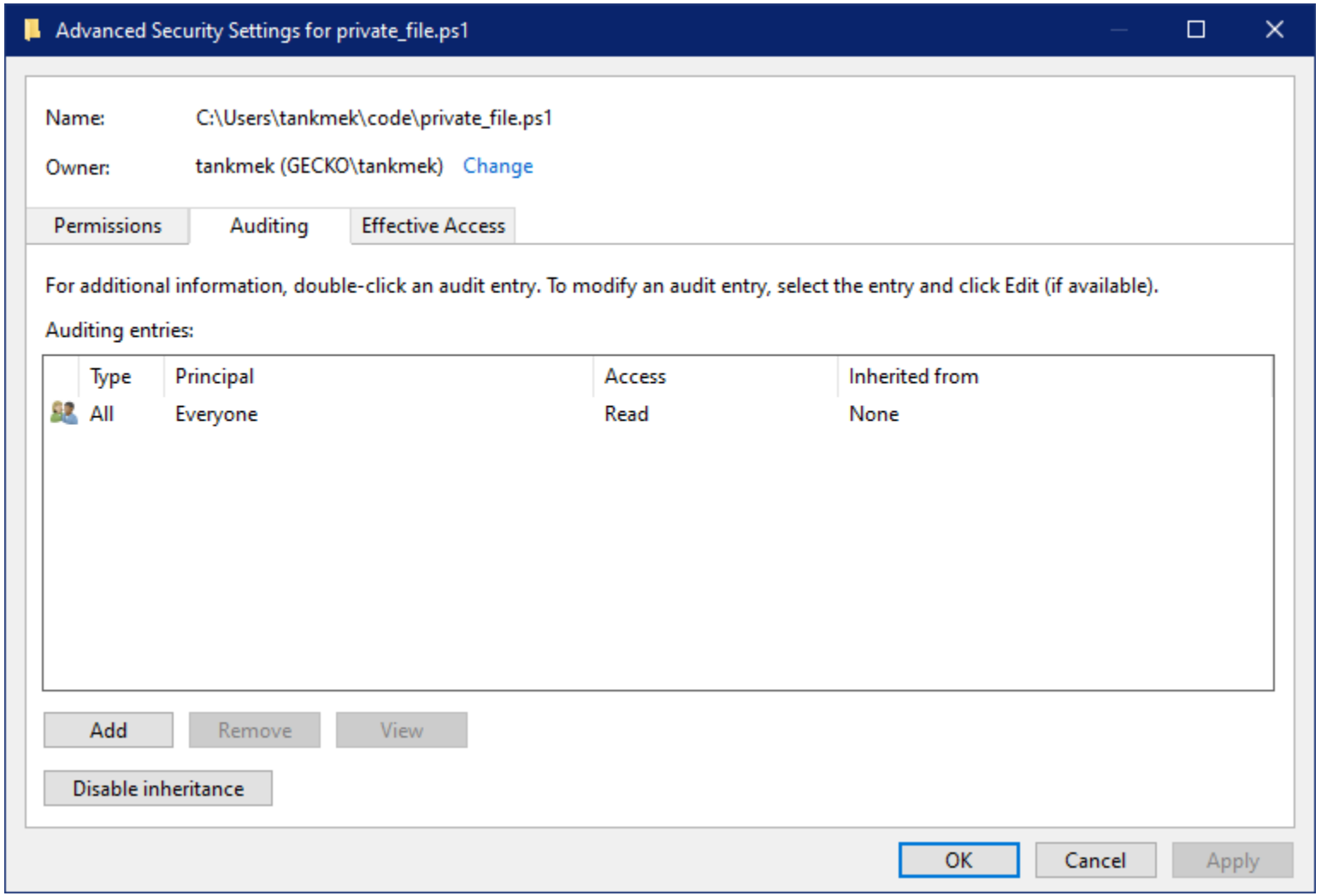
```
$session = (New-PSSession -ComputerName $computer -Credential $auth)
```

```
Copy-Item -Path $decoy_file -Destination $dest_file -ToSession $session
```

Ghost-Busting: Apply Audit ACL



Ghost-Busting: Apply Audit ACL



Ghost-Busting: Apply Audit ACL

```
-> $acl = Get-Acl -Path .\private_file.txt -Audit
-> $acl | FL

Path   : Path : Microsoft.PowerShell.Core\FileSystem::C:\tokens\private_file.txt
Owner  : FAKELABS\mechanic
Group  : FAKELABS\Domain Users
Access : BUILTIN\Administrators Allow FullControl
         NT AUTHORITY\SYSTEM Allow FullControl
         BUILTIN\Users Allow ReadAndExecute, Synchronize
         NT AUTHORITY\Authenticated Users Allow Modify, Synchronize
Audit :
```

True Coders only use Vim

Noo, VS is the best IDE

Programmer Humor

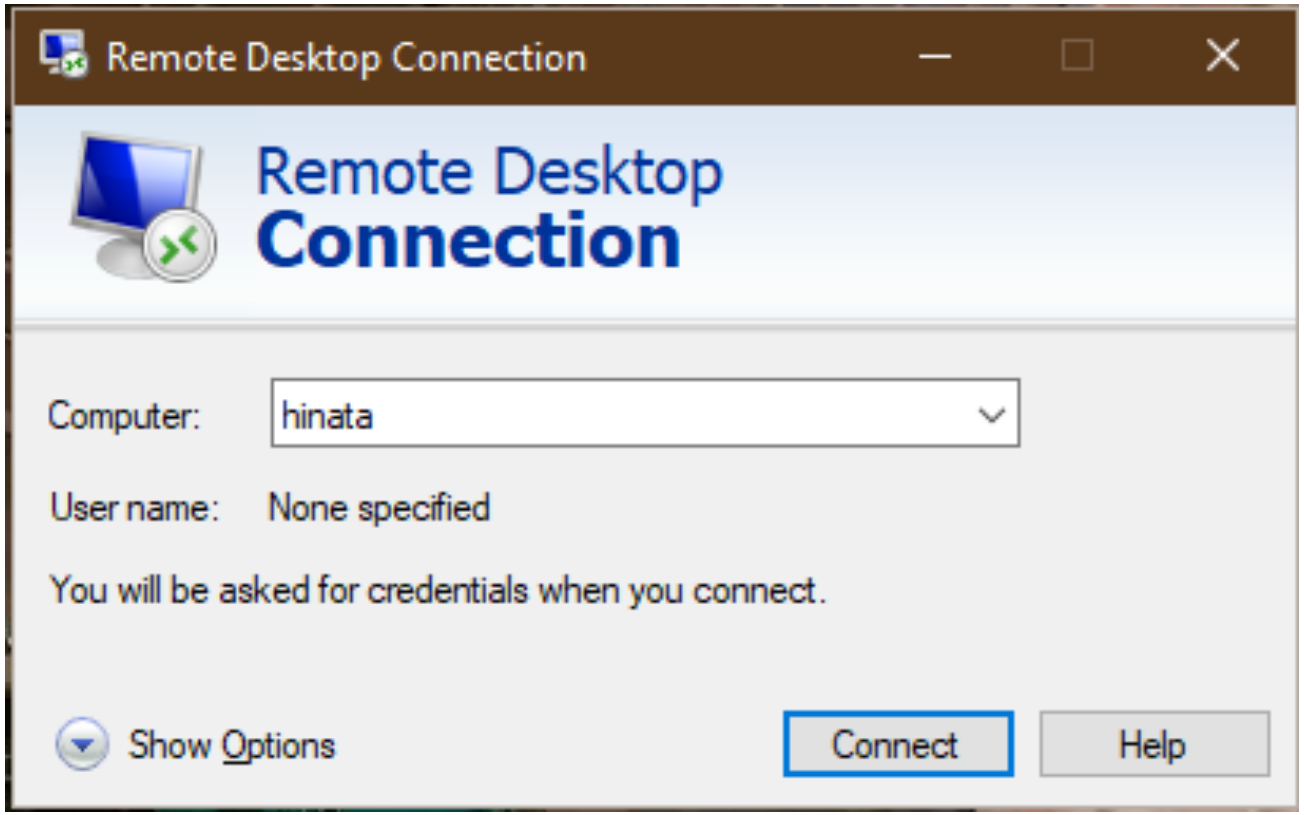
Ghost-Busting: Apply Audit ACL

```
# Retrieve the current ACL
$acl = Get-Acl -Path .\private_file.txt

# Define the audit rule for Everyone with Success and Failure auditing for Read
$auditRule = New-Object System.Security.AccessControl.FileSystemAuditRule("Everyone", "Read", "Success,Failure")

# Add the audit rule to the ACL
$acl.AddAuditRule($auditRule)

# Apply the modified ACL to the file
Set-Acl -Path .\private_file.txt -AclObject $acl
```

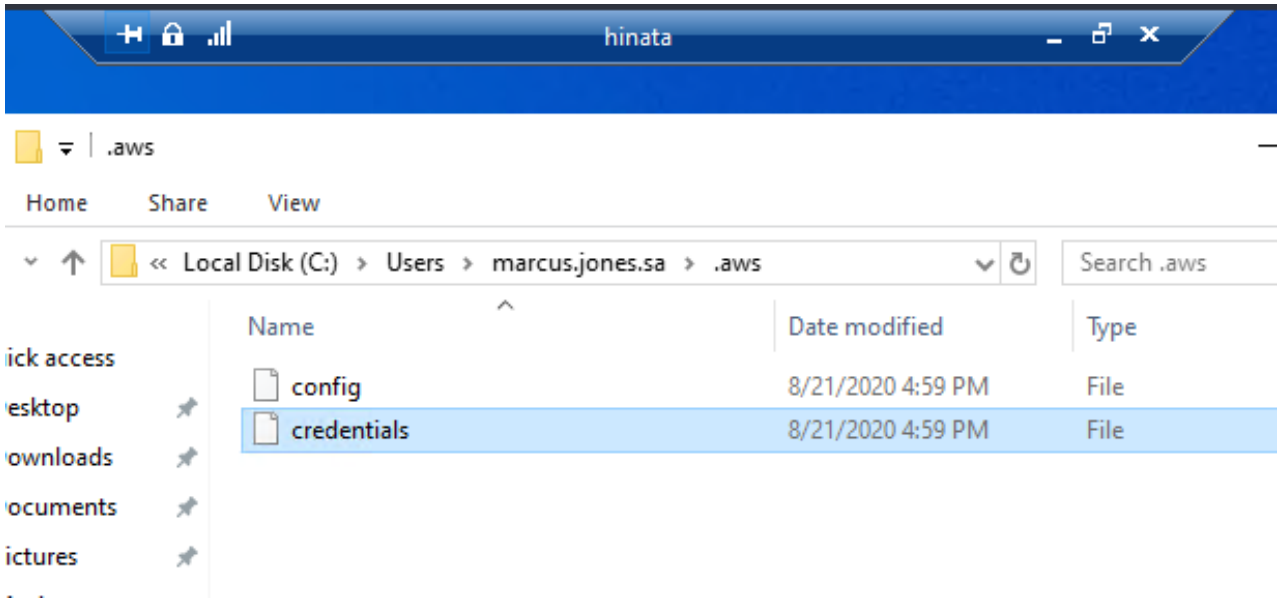
Ghost-Busting: Apply Audit ACL

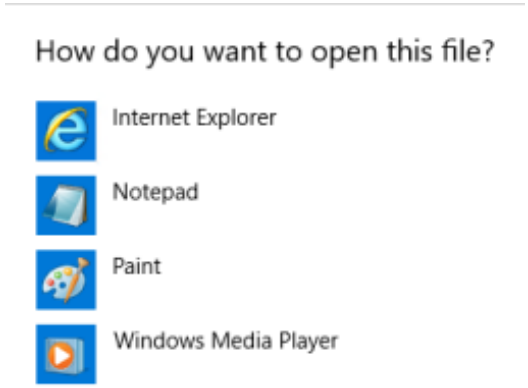
```
-> $acl = Get-Acl -Path .\private_file.txt -Audit
-> $acl | FL

Path   : Path : Microsoft.PowerShell.Core\FileSystem::C:\tokens\private_file.txt
Owner  : FAKELABS\mechanic
Group  : FAKELABS\Domain Users
Access : BUILTIN\Administrators Allow FullControl
         NT AUTHORITY\SYSTEM Allow FullControl
         BUILTIN\Users Allow ReadAndExecute, Synchronize
         NT AUTHORITY\Authenticated Users Allow Modify, Synchronize
Audit : Everyone Success, Failure Read
```

Remote Desktop



Remote Desktop





Remote Desktop

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x4A04796

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Users\marcus.jones.sa\.aws\credentials
Handle ID:	0x39c
Resource Attributes:	S:AI

Process Information:

Process ID:	0x11e4
Process Name:	C:\Windows\System32\notepad.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Remote Desktop

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x4A04796

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Users\marcus.jones.sa\.aws\credentials
Handle ID:	0x39c
Resource Attributes:	S:AI

Process Information:

Process ID:	0x11e4
Process Name:	C:\Windows\System32\notepad.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Remote Desktop

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x4A04796

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Users\marcus.jones.sa\.aws\credentials
Handle ID:	0x39c
Resource Attributes:	S:AI

Process Information:

Process ID:	0x11e4
Process Name:	C:\Windows\System32\notepad.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Remote Desktop

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x4A04796

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\Users\marcus.jones.sa\.aws\credentials
Handle ID:	0x39c
Resource Attributes:	S:AI

Process Information:

Process ID:	0x11e4
Process Name:	C:\Windows\System32\notepad.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Metasploit

Metasploit: Injected Process

```
meterpreter > search -d c:/ -f *.kdbx
Found 1 result...
    c:\admin_tools\keepass\servers.kdbx (20480 bytes)
meterpreter >
```

Metasploit: Injected Process

```
meterpreter > cd c:/
meterpreter > cd admin_tools
meterpreter > cd keepass
meterpreter > ls
Listing: c:\admin_tools\keepass
================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  20480  fil   2020-08-21 19:59:36 -0400  servers.kdbx

meterpreter > download servers.kdbx
[*] Downloading: servers.kdbx → servers.kdbx
[*] Downloaded 20.00 KiB of 20.00 KiB (100.0%): servers.kdbx → servers.kdbx
[*] download   : servers.kdbx → servers.kdbx
meterpreter >
```

Metasploit: Injected Process

```
meterpreter > cd c:/
meterpreter > cd admin_tools
meterpreter > cd keepass
meterpreter > ls
Listing: c:\admin_tools\keepass
================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  20480  fil   2020-08-21 19:59:36 -0400  servers.kdbx

meterpreter > download servers.kdbx
[*] Downloading: servers.kdbx → servers.kdbx
[*] Downloaded 20.00 KiB of 20.00 KiB (100.0%): servers.kdbx → servers.kdbx
[*] download   : servers.kdbx → servers.kdbx
meterpreter >
```

Process Injection

Event 4663, Microsoft Windows security auditing.

General | Details

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0xB95CF

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\admin_tools\keepass\servers.kdbx
Handle ID:	0x250
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1770
Process Name:	C:\Users\blueteamer\demo_malware.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Process Injection

Event 4663, Microsoft Windows security auditing.

General | Details

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0xB95CF

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\admin_tools\keepass\servers.kdbx
Handle ID:	0x250
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1770
Process Name:	C:\Users\blueteamer\demo_malware.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Process Injection

Event 4663, Microsoft Windows security auditing.

General | Details

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0xB95CF

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\admin_tools\keepass\servers.kdbx
Handle ID:	0x250
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1770
Process Name:	C:\Users\blueteamer\demo_malware.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Process Injection

Event 4663, Microsoft Windows security auditing.

General | Details

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0xB95CF

Object:

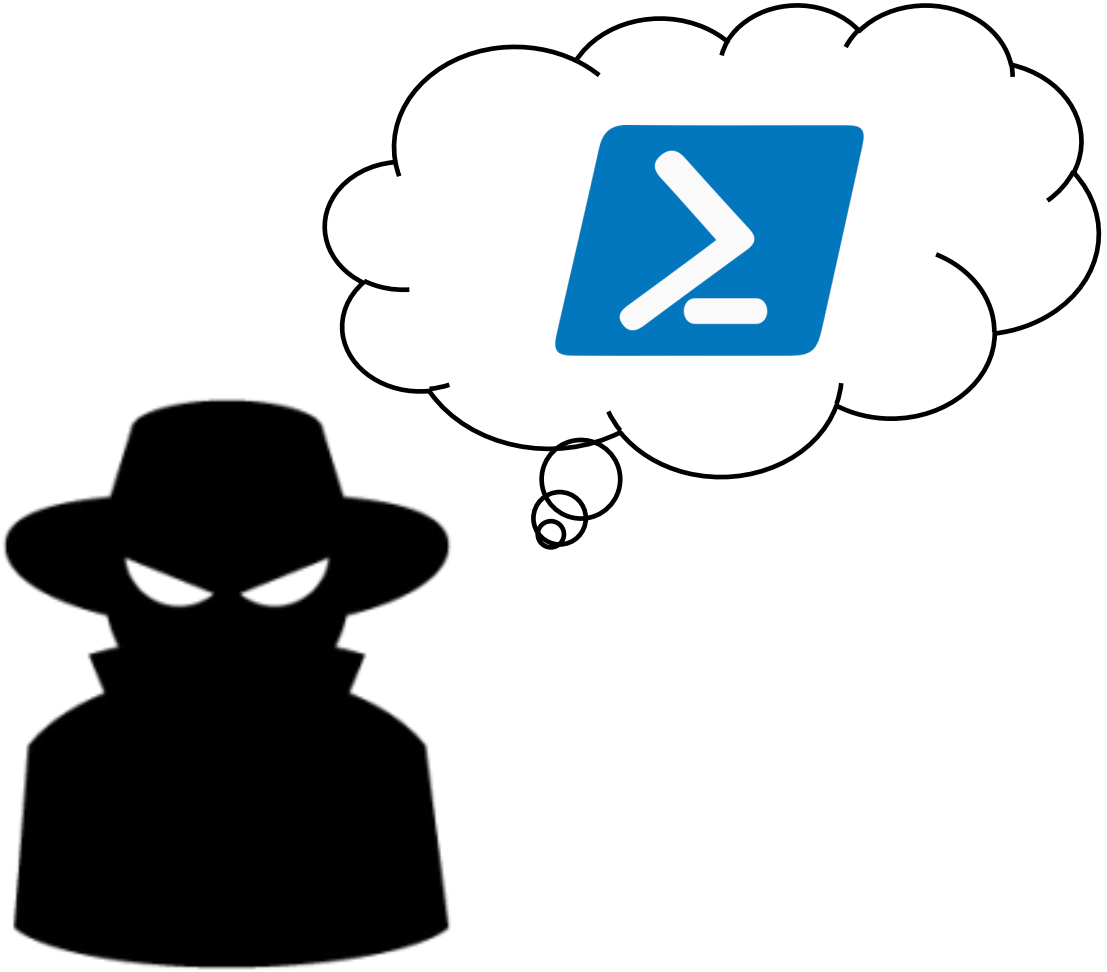
Object Server:	Security
Object Type:	File
Object Name:	C:\admin_tools\keepass\servers.kdbx
Handle ID:	0x250
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1770
Process Name:	C:\Users\blueteamer\demo_malware.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1



Ghost-Busting: WinRM

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        18-Sep-23     16:20                reports
-a----        05-Feb-23     11:14        9902745 brocade_cfgs.zip
```

```
[yagami]: PS C:\backups>
[yagami]: PS C:\backups> Expand-Archive .\brocade_cfgs.zip
```

Ghost-Busting: WinRM

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x3707037

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\backups\brocade_cfgs.zip
Handle ID:	0x1cb8
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1020
Process Name:	C:\Windows\System32\wsmprovhost.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Ghost-Busting: WinRM

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x3707037

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\backups\brocade_cfgs.zip
Handle ID:	0x1cb8
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1020
Process Name:	C:\Windows\System32\wsmprovhost.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Ghost-Busting: WinRM

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x3707037

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\backups\brocade_cfgs.zip
Handle ID:	0x1cb8
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1020
Process Name:	C:\Windows\System32\wsmprovhost.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Ghost-Busting: WinRM

An attempt was made to access an object.

Subject:

Security ID:	FAKELABS\vanya
Account Name:	vanya
Account Domain:	FAKELABS
Logon ID:	0x3707037

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\backups\brocade_cfgs.zip
Handle ID:	0x1cb8
Resource Attributes:	S:AI

Process Information:

Process ID:	0x1020
Process Name:	C:\Windows\System32\wsmprovhost.exe

Access Request Information:

Accesses:	ReadData (or ListDirectory)
Access Mask:	0x1

Ghost-Busting: WinRM

```
C:\Windows\System32\wsmprovhost.exe
```

How do we scale?

How do we scale?

SIEM Logs: Splunk

```
index=wineventlog EventCode=4663 brocade OR keepass OR .aws\\c*
| stats count by host, Object_Name, Accesses, Process_Name, Account_Name
```

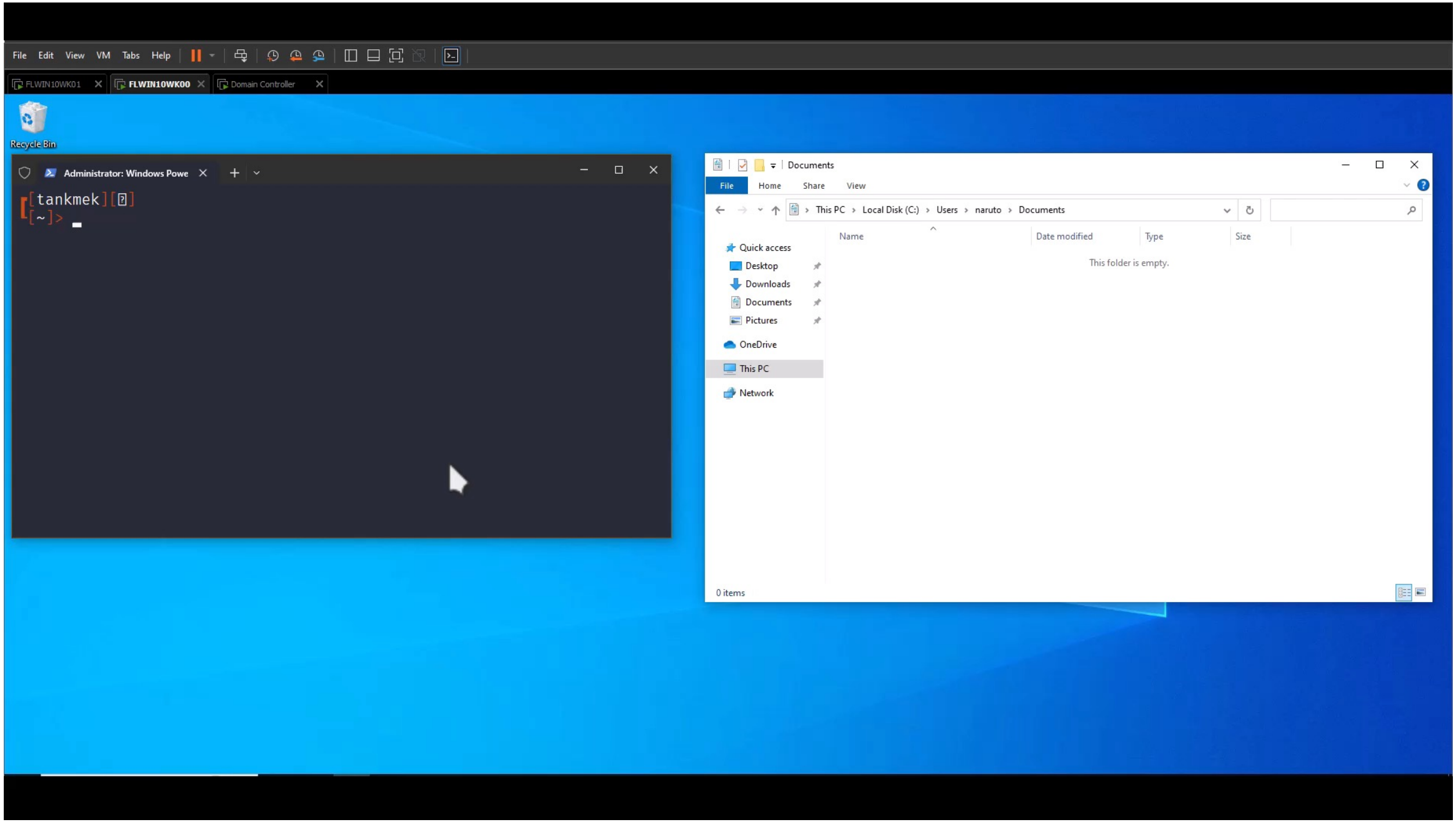
SIEM Logs: Splunk

host	Object_Name	Accesses
BRUCE	C:\admin_tools\keepass\servers.kdbx	READ_CONTROL
BRUCE	C:\admin_tools\keepass\servers.kdbx	ReadAttributes
BRUCE	C:\admin_tools\keepass\servers.kdbx	ReadData (or ListDirectory)
HINATA	C:\Users\marcus.jones.sa\.aws\credentials	READ_CONTROL
HINATA	C:\Users\marcus.jones.sa\.aws\credentials	ReadAttributes
HINATA	C:\Users\marcus.jones.sa\.aws\credentials	ReadAttributes
HINATA	C:\Users\marcus.jones.sa\.aws\credentials	ReadData (or ListDirectory)
yagami	C:\backups\brocade_cfgs.zip	ReadData (or ListDirectory)
yagami	C:\backups\brocade_cfgs.zip	ReadData (or ListDirectory)

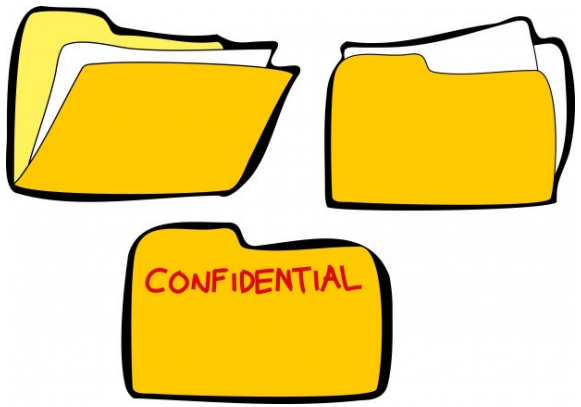
SIEM Logs: Splunk

Process_Name	Account_Name	count
C:\Windows\explorer.exe	vanya	3
C:\Windows\explorer.exe	vanya	2
C:\Windows\explorer.exe	vanya	1
C:\Windows\explorer.exe	blueteamer	2
C:\Windows\System32\notepad.exe	blueteamer	1
C:\Windows\explorer.exe	blueteamer	2
C:\Windows\System32\notepad.exe	blueteamer	2
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Administrator	1
C:\Windows\System32\wsmprovhost.exe	vanya	1

DEMO


File Edit View VM Tabs Help
FLWIN10WK01
FLWIN10WK00
Domain Controller
Recycle Bin
Administrator: Windows Powe
[tankmek][?]
[~]>
Documents
File Home Share View
This PC > Local Disk (C:) > Users > naruto > Documents
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Network
Name
Date modified
Type
Size
This folder is empty.
0 items

Review & Conclusion



Connect

@tankmek

https://www.linkedin.com/in/tankmek