Detect Bloodhound

1. First, if you run this using the SharpHound application, it is very noisy, we can set up alerts/alarms for spikes in CPU usage,
    1. Byte transfer spikes.

==

==

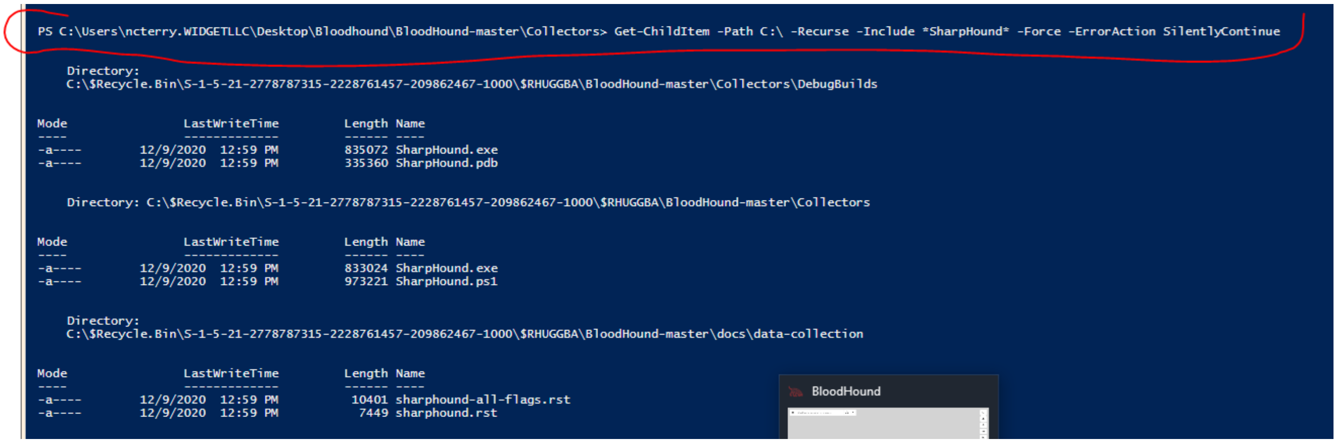
==

2. There are many keywords example:
    1. bloodhound, sharphound, neo4j, etc…..
        1. We can run a keyword sweep on the machine for a list.

Example:

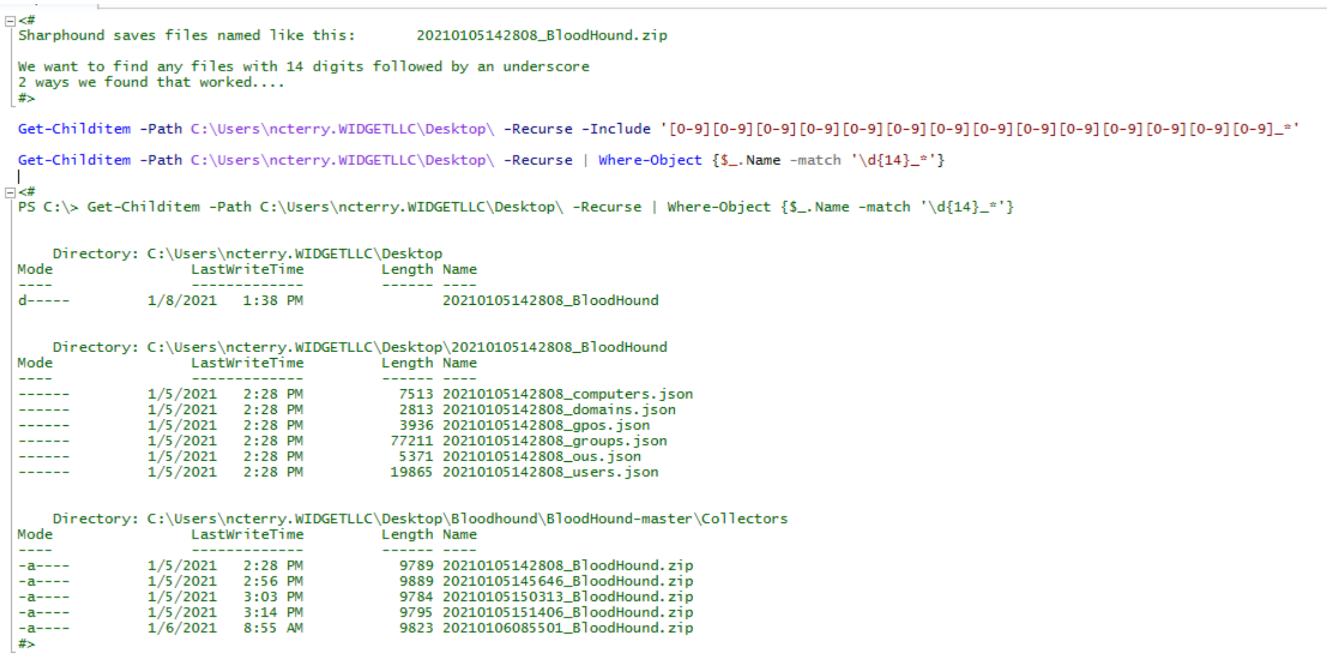
> Get-Childitem -Path C:\ -Recurse -Include *SharpHound* -Force -ErrorAction SilentlyContinue

- Get-Childitem = go get something
- -Path C:\ -Recurse = where to search including inside corresponding directories.
- -Include *SharpHound* -Force = go look for this anything that has this word.
    - Force it to keep looking no matter what.
    - Anything on either side of the word.
    - Can be upper or lowercase.
- -ErrorActions SilentlyContinue = There will be errors trying to access certain things no matter what. This just tells the system to ignore errors and keep looking.



```
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> Get-ChildItem -Path C:\ -Recurse -Include *SharpHound* -Force -ErrorAction SilentlyContinue

    Directory:
    C:\$Recycle.Bin\S-1-5-21-2778787315-2228761457-209862467-1000\$RHUGGBA\BloodHound-master\Collectors\DebugBuilds


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/9/2020  12:59 PM         835072 SharpHound.exe
-a----         12/9/2020  12:59 PM         335360 SharpHound.pdb


    Directory: C:\$Recycle.Bin\S-1-5-21-2778787315-2228761457-209862467-1000\$RHUGGBA\BloodHound-master\Collectors


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/9/2020  12:59 PM         833024 SharpHound.exe
-a----         12/9/2020  12:59 PM         973221 SharpHound.ps1


    Directory:
    C:\$Recycle.Bin\S-1-5-21-2778787315-2228761457-209862467-1000\$RHUGGBA\BloodHound-master\docs\data-collection


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/9/2020  12:59 PM          10401 sharphound-all-flags.rst
-a----         12/9/2020  12:59 PM           7449 sharphound.rst
```

Example2: We know that Sharphound saves it’s results



```
<#
Sharphound saves files named like this:       20210105142808_BloodHound.zip

We want to find any files with 14 digits followed by an underscore
2 ways we found that worked....
#>

Get-Childitem -Path C:\Users\ncterry.WIDGETLLC\Desktop\ -Recurse -Include '[0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]_*'

Get-Childitem -Path C:\Users\ncterry.WIDGETLLC\Desktop\ -Recurse | Where-Object {$_.Name -match '\d{14}_*'}

<#
PS C:\> Get-Childitem -Path C:\Users\ncterry.WIDGETLLC\Desktop\ -Recurse | Where-Object {$_.Name -match '\d{14}_*'}


    Directory: C:\Users\ncterry.WIDGETLLC\Desktop
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         1/8/2021   1:38 PM                20210105142808_BloodHound


    Directory: C:\Users\ncterry.WIDGETLLC\Desktop\20210105142808_BloodHound
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
------         1/5/2021   2:28 PM           7513 20210105142808_computers.json
------         1/5/2021   2:28 PM           2813 20210105142808_domains.json
------         1/5/2021   2:28 PM           3936 20210105142808_gpos.json
------         1/5/2021   2:28 PM          77211 20210105142808_groups.json
------         1/5/2021   2:28 PM           5371 20210105142808_ous.json
------         1/5/2021   2:28 PM          19865 20210105142808_users.json


    Directory: C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         1/5/2021   2:28 PM           9789 20210105142808_BloodHound.zip
-a----         1/5/2021   2:56 PM           9889 20210105145646_BloodHound.zip
-a----         1/5/2021   3:03 PM           9784 20210105150313_BloodHound.zip
-a----         1/5/2021   3:14 PM           9795 20210105151406_BloodHound.zip
-a----         1/6/2021   8:55 AM           9823 20210106085501_BloodHound.zip
#>
```

==

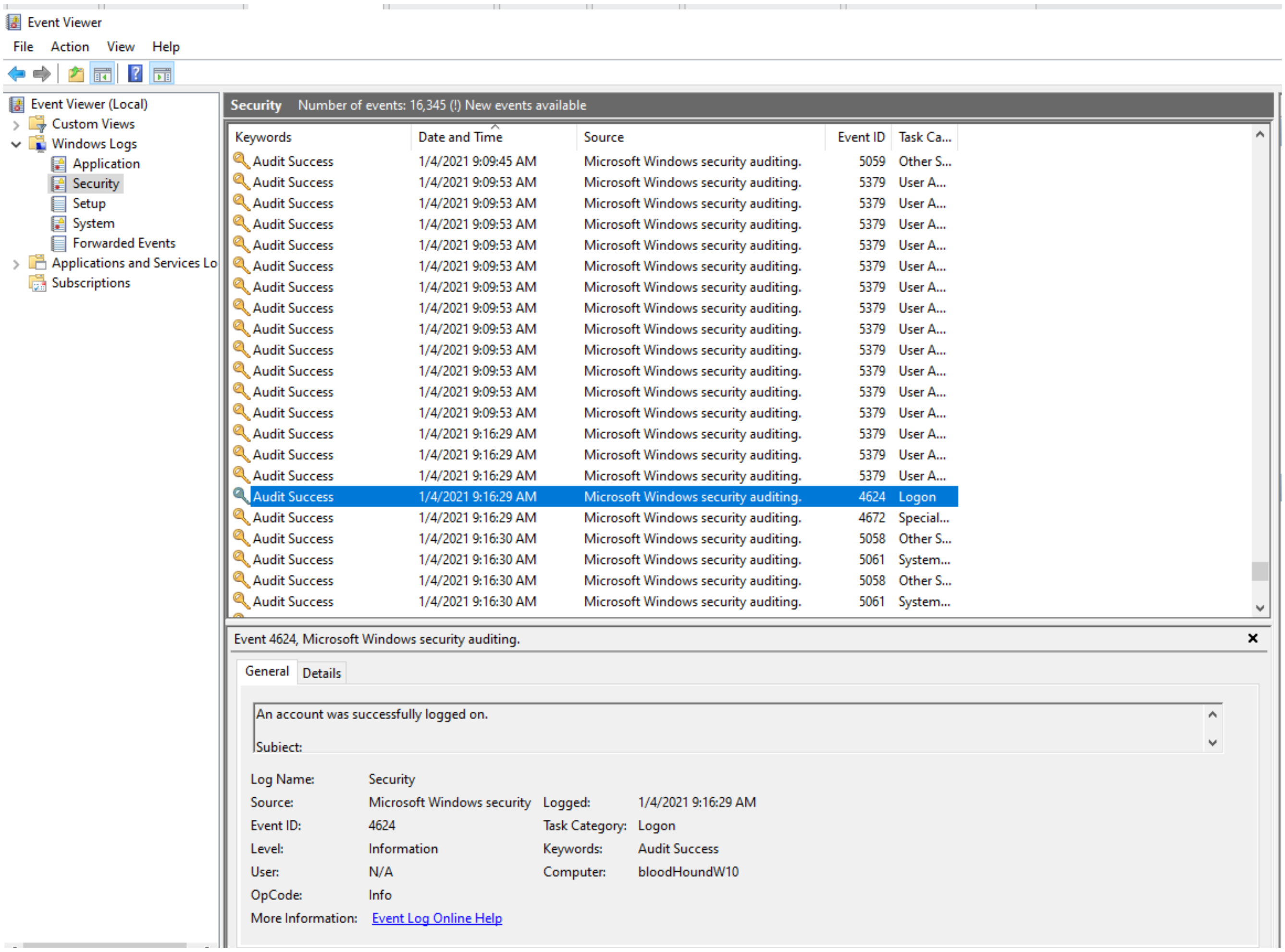
==

==

3. We see already that Windows Defender is strongly protecting against SharpHound.exe and related files. These are deleted from folders even if they are zipped.

4. If you are able to unzip them, and Windows Defender does not delete them immediately, you still cannot rename those files/folders in the interim. I do not have admin status, and because it has these questionable names, it does not allow me to make those changes.

5. Look into.
6. Queries that we run with BloodHound/SharpHound will leave 4624 and 4634 on all of the machines in the domain which can be picked up on. If you see that this log-action is left, and it is not by the normal user/s, then we see a red flag.
    1. 4624 – An account was successfully logged on. While this is normal, it is also very valuable as it documents every successful logon to the local computer, regardless of (logon type, location of user, type of account)
    2. 4634 – an account was logged off of. Tied directly to 4624
    3. You can check these logs directly by:
        1. Event Viewer >> Windows Logs >> Security



Security Number of events: 16,345 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Ca...
Audit Success	1/4/2021 9:09:45 AM	Microsoft Windows security auditing.	5059	Other S...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:16:29 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:16:29 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:16:29 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:16:29 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	1/4/2021 9:16:29 AM	Microsoft Windows security auditing.	4672	Special...
Audit Success	1/4/2021 9:16:30 AM	Microsoft Windows security auditing.	5058	Other S...
Audit Success	1/4/2021 9:16:30 AM	Microsoft Windows security auditing.	5061	System...
Audit Success	1/4/2021 9:16:30 AM	Microsoft Windows security auditing.	5058	Other S...
Audit Success	1/4/2021 9:16:30 AM	Microsoft Windows security auditing.	5061	System...

Event 4624, Microsoft Windows security auditing.

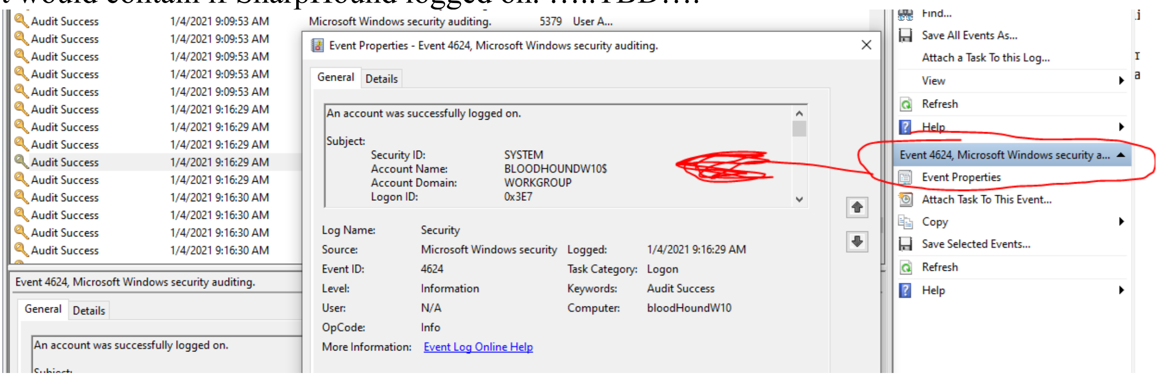
An account was successfully logged on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/4/2021 9:16:29 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	bloodHoundW10
OpCode:	Info		
More Information:	Event Log Online Help		

7. Above you can see the list of all logs, where we have highlighted the most recent 4624

8. Below, once selected the target log, and we click on the option for “Event Properties”, then we can see much more details on who logged in. We do not have SharpHound running on our VM at the moment, and cannot determine the difference between a normal log like seen below, and what it would contain if SharpHound logged on. …..TBD….



Audit Success	1/4/2021 9:09:53 AM	Microsoft Windows security auditing.	5379	User A...
Audit Success	1/4/2021 9:09:53 AM			
Audit Success	1/4/2021 9:09:53 AM			
Audit Success	1/4/2021 9:09:53 AM			
Audit Success	1/4/2021 9:09:53 AM			
Audit Success	1/4/2021 9:16:29 AM			
Audit Success	1/4/2021 9:16:29 AM			
Audit Success	1/4/2021 9:16:29 AM			
Audit Success	1/4/2021 9:16:29 AM			
Audit Success	1/4/2021 9:16:29 AM			
Audit Success	1/4/2021 9:16:30 AM			
Audit Success	1/4/2021 9:16:30 AM			
Audit Success	1/4/2021 9:16:30 AM			
Audit Success	1/4/2021 9:16:30 AM			

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Event Properties - Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

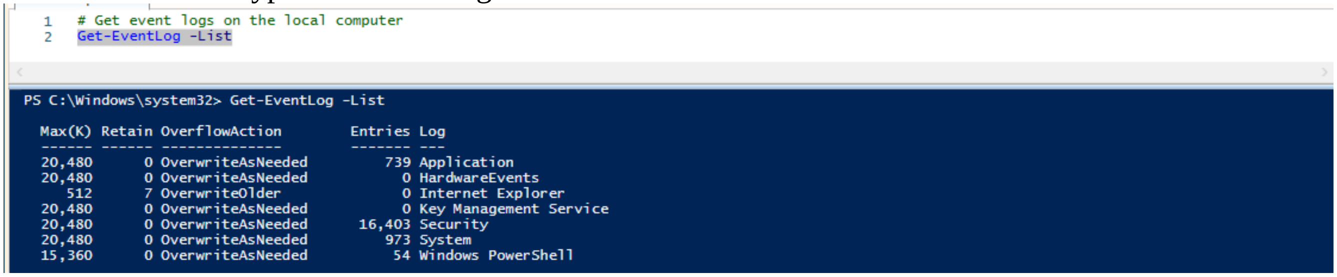
Security ID:	SYSTEM
Account Name:	BLOODHOUNDW10$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/4/2021 9:16:29 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	bloodHoundW10
OpCode:	Info		
More Information:	Event Log Online Help		

==

==

Now a list of commands with Screenshots on how to capture these event logs using PowerShell
Gather a list of all types of current logs.



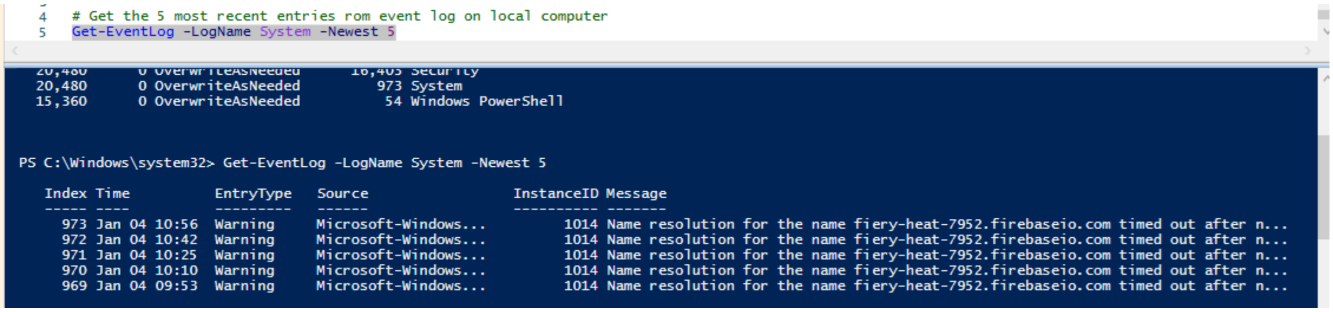
```
# Get event logs on the local computer
Get-EventLog -List
```

```
PS C:\Windows\system32> Get-EventLog -List

  Max(K) Retain OverflowAction        Entries Log
  ------ ------ --------------        ------- ---
  20,480      0 OverwriteAsNeeded         739 Application
  20,480      0 OverwriteAsNeeded           0 HardwareEvents
     512      7 OverwriteOlder              0 Internet Explorer
  20,480      0 OverwriteAsNeeded           0 Key Management Service
  20,480      0 OverwriteAsNeeded      16,403 Security
  20,480      0 OverwriteAsNeeded         973 System
  15,360      0 OverwriteAsNeeded          54 Windows PowerShell
```

==

==

Get the most recent 5 events from the “System” log



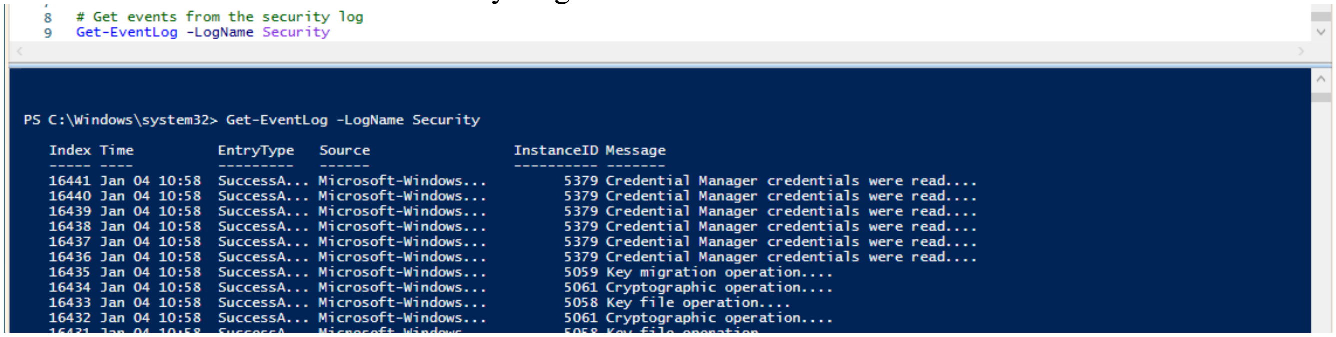
```
# Get the 5 most recent entries rom event log on local computer
Get-EventLog -LogName System -Newest 5
```

```
  20,480      0 OverwriteAsNeeded      16,403 Security
  20,480      0 OverwriteAsNeeded         973 System
  15,360      0 OverwriteAsNeeded          54 Windows PowerShell


PS C:\Windows\system32> Get-EventLog -LogName System -Newest 5

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
     973 Jan 04 10:56  Warning     Microsoft-Windows...         1014 Name resolution for the name fiery-heat-7952.firebaseio.com timed out after n...
     972 Jan 04 10:42  Warning     Microsoft-Windows...         1014 Name resolution for the name fiery-heat-7952.firebaseio.com timed out after n...
     971 Jan 04 10:25  Warning     Microsoft-Windows...         1014 Name resolution for the name fiery-heat-7952.firebaseio.com timed out after n...
     970 Jan 04 10:10  Warning     Microsoft-Windows...         1014 Name resolution for the name fiery-heat-7952.firebaseio.com timed out after n...
     969 Jan 04 09:53  Warning     Microsoft-Windows...         1014 Name resolution for the name fiery-heat-7952.firebaseio.com timed out after n...
```

==

==

Get all of the events from the “Security” log. This is where we would find the 4624 InstanceId at.



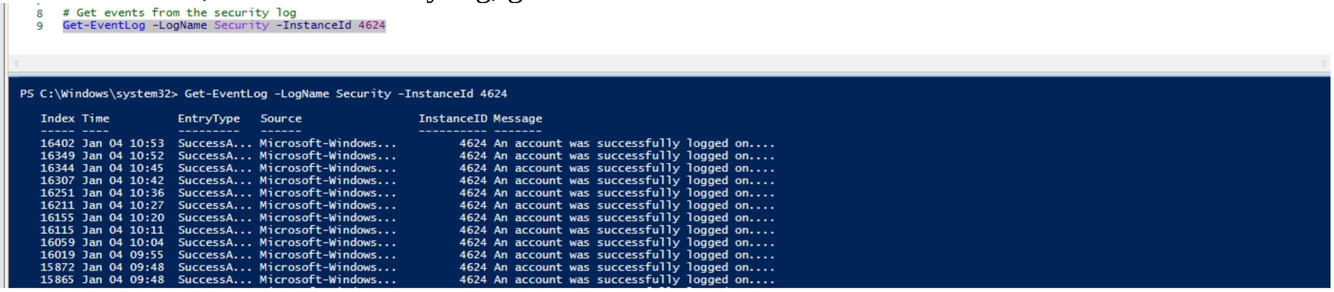
```
# Get events from the security log
Get-EventLog -LogName Security
```

```
PS C:\Windows\system32> Get-EventLog -LogName Security

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   16441 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16440 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16439 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16438 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16437 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16436 Jan 04 10:58  SuccessA... Microsoft-Windows...         5379 Credential Manager credentials were read....
   16435 Jan 04 10:58  SuccessA... Microsoft-Windows...         5059 Key migration operation....
   16434 Jan 04 10:58  SuccessA... Microsoft-Windows...         5061 Cryptographic operation....
   16433 Jan 04 10:58  SuccessA... Microsoft-Windows...         5058 Key file operation....
   16432 Jan 04 10:58  SuccessA... Microsoft-Windows...         5061 Cryptographic operation....
   16431 Jan 04 10:58  SuccessA... Microsoft-Windows...         5058 Key file operation....
```

==

==

As stated above, from the Security log, get all events with the InstanceId = 4624



```
# Get events from the security log
Get-EventLog -LogName Security -InstanceId 4624
```

```
PS C:\Windows\system32> Get-EventLog -LogName Security -InstanceId 4624

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   16402 Jan 04 10:53  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16349 Jan 04 10:52  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16344 Jan 04 10:45  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16307 Jan 04 10:42  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16251 Jan 04 10:36  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16211 Jan 04 10:27  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16155 Jan 04 10:20  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16115 Jan 04 10:11  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16059 Jan 04 10:04  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16019 Jan 04 09:55  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15872 Jan 04 09:48  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15865 Jan 04 09:48  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
```

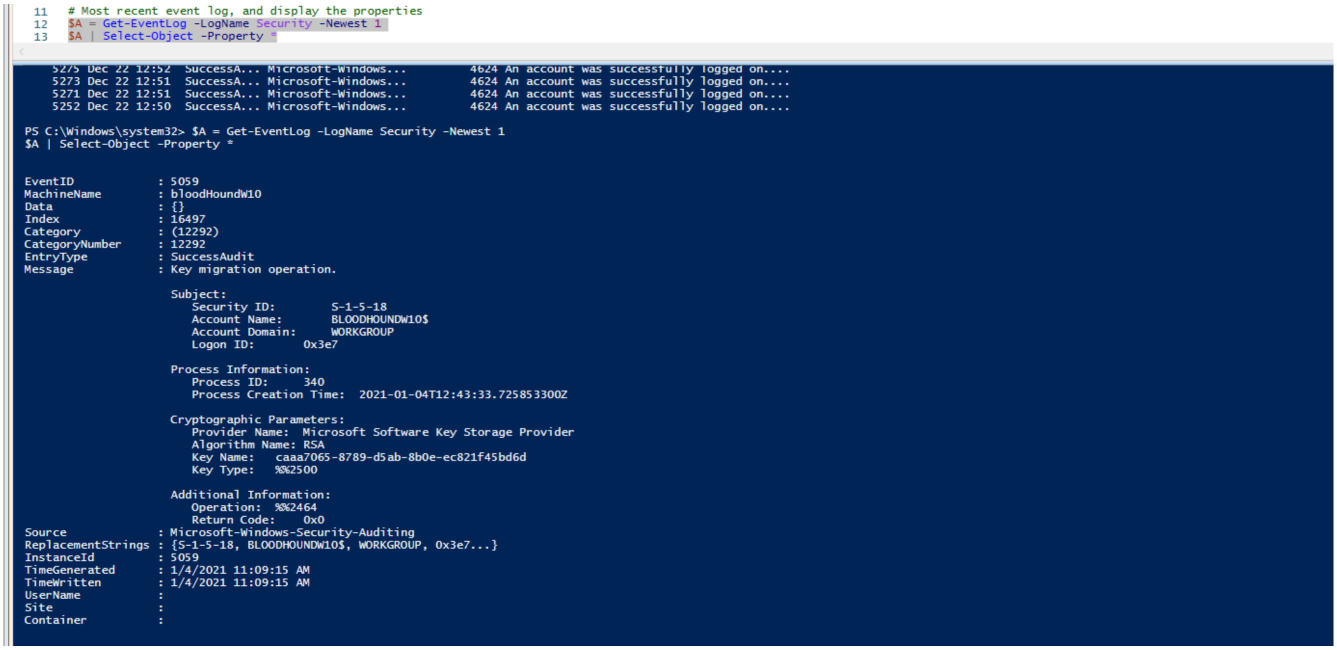
==

==

==

==

Below we gather the most current event from the Security log, and then display all properties from that event. We would probably be comparing the “UserName” when analyzing for SharpHound but this screenshot is just from is a default Windows 10 VM, not connected to Domain/AD, and is blank here.



```
# Most recent event log, and display the properties
$A = Get-EventLog -LogName Security -Newest 1
$A | Select-Object -Property *
```

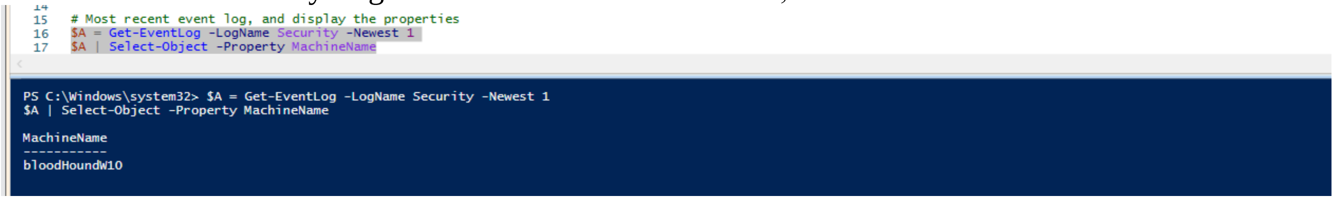
```
    5275 Dec 22 12:52  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
    5273 Dec 22 12:51  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
    5271 Dec 22 12:51  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
    5252 Dec 22 12:50  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....

PS C:\Windows\system32> $A = Get-EventLog -LogName Security -Newest 1
$A | Select-Object -Property *


EventID            : 5059
MachineName        : bloodHoundW10
Data               : {}
Index              : 16497
Category           : (12292)
CategoryNumber     : 12292
EntryType          : SuccessAudit
Message            : Key migration operation.

                     Subject:
                        Security ID:        S-1-5-18
                        Account Name:       BLOODHOUNDW10$
                        Account Domain:     WORKGROUP
                        Logon ID:       0x3e7

                     Process Information:
                        Process ID:     340
                        Process Creation Time:  2021-01-04T12:43:33.725853300Z

                     Cryptographic Parameters:
                        Provider Name:  Microsoft Software Key Storage Provider
                        Algorithm Name: RSA
                        Key Name:   caaa7065-8789-d5ab-8b0e-ec821f45bd6d
                        Key Type:   %%2500

                     Additional Information:
                        Operation:  %%2464
                        Return Code:    0x0
Source             : Microsoft-Windows-Security-Auditing
ReplacementStrings : {S-1-5-18, BLOODHOUNDW10$, WORKGROUP, 0x3e7...}
InstanceId         : 5059
TimeGenerated      : 1/4/2021 11:09:15 AM
TimeWritten        : 1/4/2021 11:09:15 AM
UserName           :
Site               :
Container          :
```

==

==

The same as above, but instead of displaying all properties from that log, we just display the ‘MachineName’. Stuff like this and ‘UserName’ would allow us to compare and find if someone other than the normal user logged in.

We are already isolating to the ‘-Newest 1’ on the security log, but we could go further, and just isolate all events on the Security Log that have the -InstanceId 4624, and don’t have the normal UserName.

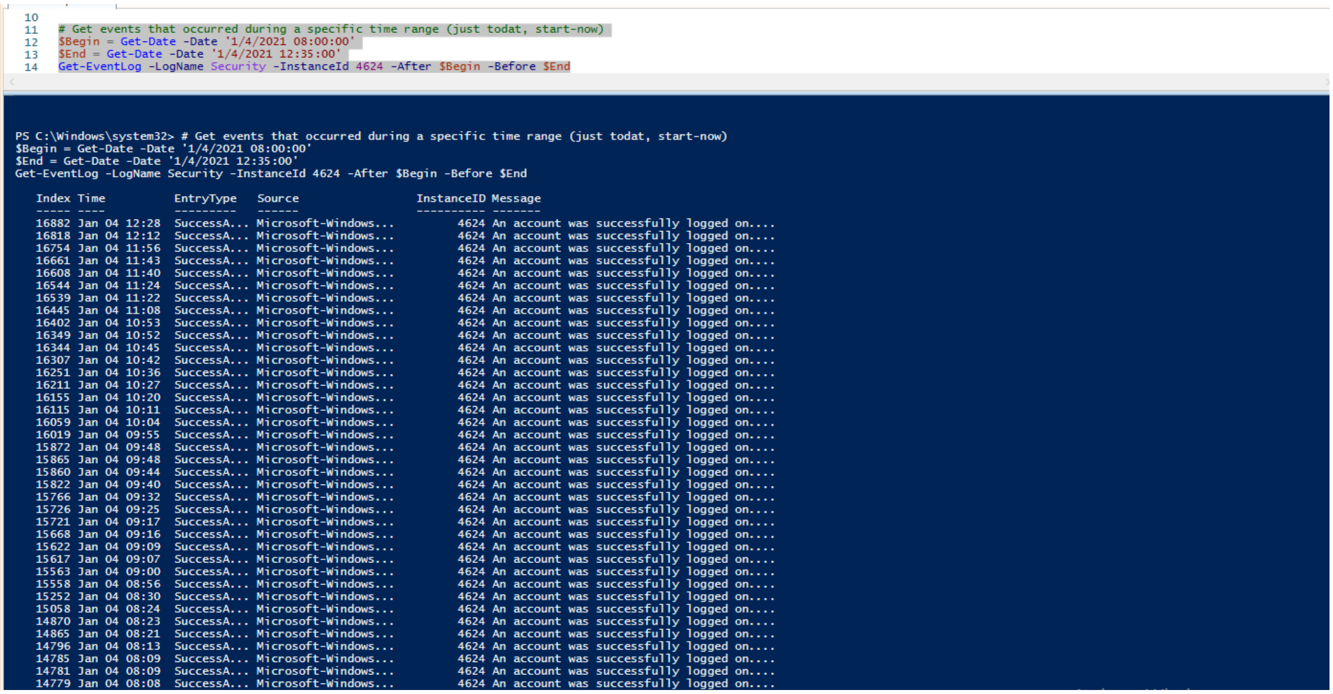


```
# Most recent event log, and display the properties
$A = Get-EventLog -LogName Security -Newest 1
$A | Select-Object -Property MachineName
```

```
PS C:\Windows\system32> $A = Get-EventLog -LogName Security -Newest 1
$A | Select-Object -Property MachineName

MachineName
-----------
bloodHoundW10
```

==
==

Below, we are setting to variables, based on today, when work started, and when we ran this.
We then get all events from the Security log, that have the -InstanceId 4624, which fall between when we started working, and now.

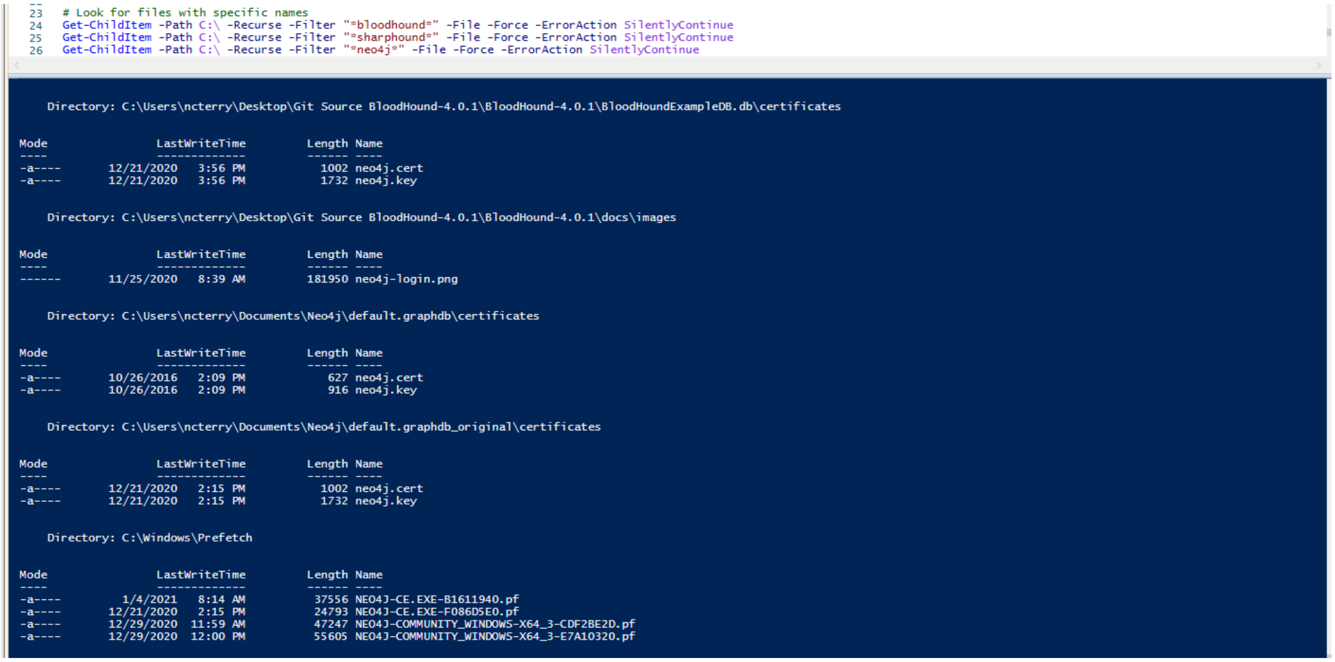


```
# Get events that occurred during a specific time range (just todat, start-now)
$Begin = Get-Date -Date '1/4/2021 08:00:00'
$End = Get-Date -Date '1/4/2021 12:35:00'
Get-EventLog -LogName Security -InstanceId 4624 -After $Begin -Before $End
```

```
PS C:\Windows\system32> # Get events that occurred during a specific time range (just todat, start-now)
$Begin = Get-Date -Date '1/4/2021 08:00:00'
$End = Get-Date -Date '1/4/2021 12:35:00'
Get-EventLog -LogName Security -InstanceId 4624 -After $Begin -Before $End

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
   16882 Jan 04 12:28  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16818 Jan 04 12:12  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16754 Jan 04 11:56  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16661 Jan 04 11:43  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16608 Jan 04 11:40  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16544 Jan 04 11:24  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16539 Jan 04 11:22  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16445 Jan 04 11:08  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16402 Jan 04 10:53  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16349 Jan 04 10:52  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16344 Jan 04 10:45  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16307 Jan 04 10:42  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16251 Jan 04 10:36  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16211 Jan 04 10:27  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16155 Jan 04 10:20  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16115 Jan 04 10:11  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16059 Jan 04 10:04  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   16019 Jan 04 09:55  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15872 Jan 04 09:48  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15865 Jan 04 09:48  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15860 Jan 04 09:44  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15822 Jan 04 09:40  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15766 Jan 04 09:32  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15726 Jan 04 09:25  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15721 Jan 04 09:17  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15668 Jan 04 09:16  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15622 Jan 04 09:09  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15617 Jan 04 09:07  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15563 Jan 04 09:00  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15558 Jan 04 08:56  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15252 Jan 04 08:30  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   15058 Jan 04 08:24  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14870 Jan 04 08:23  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14865 Jan 04 08:21  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14796 Jan 04 08:13  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14785 Jan 04 08:09  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14781 Jan 04 08:09  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
   14779 Jan 04 08:08  SuccessA... Microsoft-Windows...         4624 An account was successfully logged on....
```

==
==

Use PowerShell to search for file names:
The three commands shown in the screenshot below, are trying to find objects in the entire C:\ directory, which recursively goes through all sub folders, and filters based on 3 names. We could combine that, but we are separating them in different commands just for display. We are searching for these names as a ‘-File’, and forcing it regardless. Even with force, we will always get an error message to start that says denied, but we can overstep that error message with ‘-ErrorAction SilentlyContinue’



```
# Look for files with specific names
Get-ChildItem -Path C:\ -Recurse -Filter "*bloodhound*" -File -Force -ErrorAction SilentlyContinue
Get-ChildItem -Path C:\ -Recurse -Filter "*sharphound*" -File -Force -ErrorAction SilentlyContinue
Get-ChildItem -Path C:\ -Recurse -Filter "*neo4j*" -File -Force -ErrorAction SilentlyContinue
```

```
    Directory: C:\Users\ncterry\Desktop\Git Source BloodHound-4.0.1\BloodHound-4.0.1\BloodHoundExampleDB.db\certificates


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/21/2020   3:56 PM           1002 neo4j.cert
-a----        12/21/2020   3:56 PM           1732 neo4j.key


    Directory: C:\Users\ncterry\Desktop\Git Source BloodHound-4.0.1\BloodHound-4.0.1\docs\images


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
------        11/25/2020   8:39 AM         181950 neo4j-login.png


    Directory: C:\Users\ncterry\Documents\Neo4j\default.graphdb\certificates


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/26/2016   2:09 PM            627 neo4j.cert
-a----        10/26/2016   2:09 PM            916 neo4j.key


    Directory: C:\Users\ncterry\Documents\Neo4j\default.graphdb_original\certificates


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/21/2020   2:15 PM           1002 neo4j.cert
-a----        12/21/2020   2:15 PM           1732 neo4j.key


    Directory: C:\Windows\Prefetch


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          1/4/2021   8:14 AM          37556 NEO4J-CE.EXE-B1611940.pf
-a----        12/21/2020   2:15 PM          24793 NEO4J-CE.EXE-F086D5E0.pf
-a----        12/29/2020  11:59 AM          47247 NEO4J-COMMUNITY_WINDOWS-X64_3-CDF2BE2D.pf
-a----        12/29/2020  12:00 PM          55605 NEO4J-COMMUNITY_WINDOWS-X64_3-E7A10320.pf
```