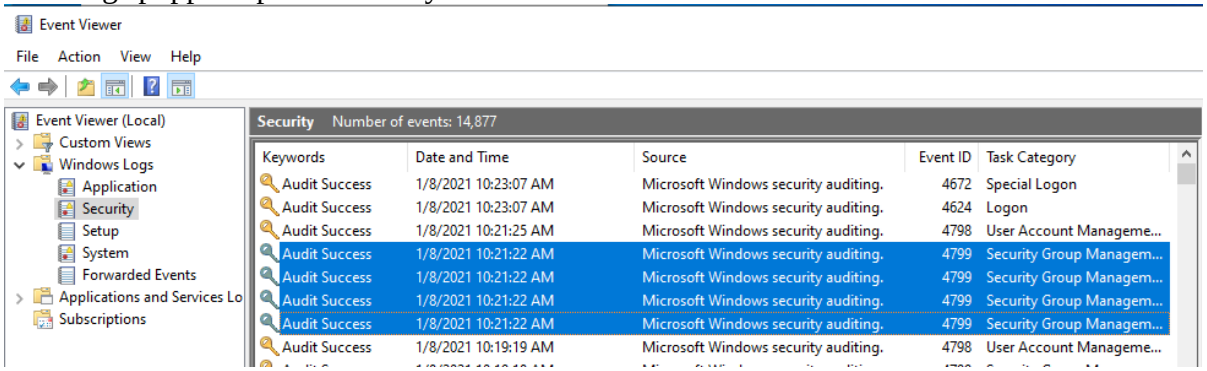
NCT_Detect_SharpHound

1. I ran a SharpHound scan on ‘client01’ which is the Windows10 machine on the Domain

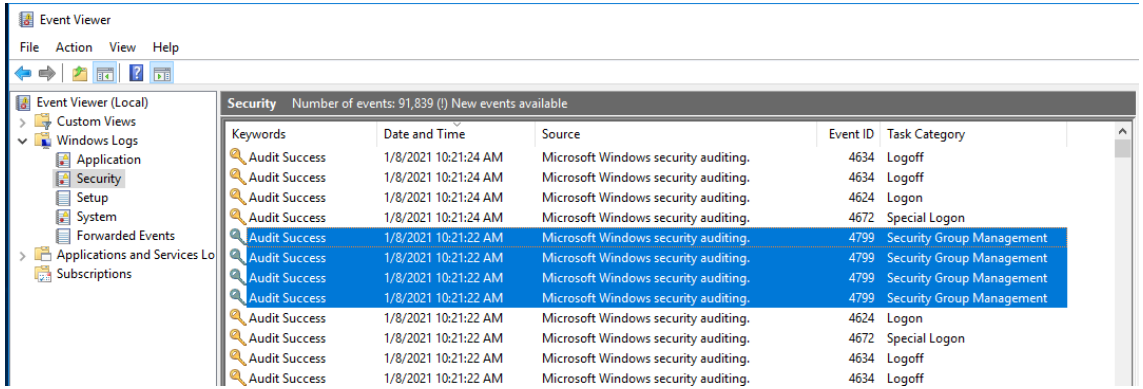
```
PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors> .\SharpHound.exe
---------------------------------------------
Initializing SharpHound at 10:21 AM on 1/8/2021
---------------------------------------------

Resolved Collection Methods: Group, Sessions, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain WIDGETLLC.INTERNAL using path CN=Schema,CN=Configuration,DC=WIDGETLLC,DC=INTERNAL
[+] Cache File Found! Loaded 116 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 22 MB RAM
Status: 73 objects finished (+73 36.5)/s -- Using 28 MB RAM
Enumeration finished in 00:00:02.1854412
Compressing data to .\20210108102122_BloodHound.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 10:21 AM on 1/8/2021! Happy Graphing!


PS C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-master\Collectors>
```

2. In the Event Viewer >> Security
3. These 4 logs popped up immediately after the scan.



4. When I went into the Domain Controller DC01 and checked the event viewer, these same for logs were there.
5. Currently we would be looking for 4 sequential 4799 logs to indicate SharpHound enumeration.

Sharphound



Source – client01

Domain Controller – DC01

Same Event log

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />
      <EventID>4799</EventID>
      <Version>0</Version>
      <Level>0</Level>
      <Task>13826</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8020000000000000</Keywords>
      <TimeCreated SystemTime="2021-01-08T15:21:22.7279819002" />
      <EventRecordID>14871</EventRecordID>
      <Correlation ActivityID="{3361b1de-e5bd-0000-a3b2-6133bde5d601}" />
      <Execution ProcessID="628" ThreadID="3096" />
      <Channel>Security</Channel>
      <Computer>Client01.WidgetLLC.Internal</Computer>
      <Security />
    </System>
  - <EventData>
      <Data Name="TargetUserName">Distributed COM Users</Data>
      <Data Name="TargetDomainName">Builtin</Data>
      <Data Name="TargetSid">S-1-5-32-562</Data>
      <Data Name="SubjectUserSid">S-1-5-21-2778787315-2228761457-209862467-500</Data>
      <Data Name="SubjectUserName">Administrator</Data>
      <Data Name="SubjectDomainName">WIDGETLLC</Data>
      <Data Name="SubjectLogonId">0x1a228a</Data>
      <Data Name="CallerProcessId">0x3c0</Data>
      <Data Name="CallerProcessName">C:\Users\ncterry.WIDGETLLC\Desktop\Bloodhound\BloodHound-
        master\Collectors\SharpHound.exe</Data>
    </EventData>
  </Event>
```

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
      <EventID>4799</EventID>
      <Version>0</Version>
      <Level>0</Level>
      <Task>13826</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8020000000000000</Keywords>
      <TimeCreated SystemTime="2021-01-08T15:21:22.7421539002" />
      <EventRecordID>91820</EventRecordID>
      <Correlation />
      <Execution ProcessID="600" ThreadID="4076" />
      <Channel>Security</Channel>
      <Computer>DC01.WidgetLLC.Internal</Computer>
      <Security />
    </System>
  - <EventData>
      <Data Name="TargetUserName">Remote Management Users</Data>
      <Data Name="TargetDomainName">Builtin</Data>
      <Data Name="TargetSid">S-1-5-32-580</Data>
      <Data Name="SubjectUserSid">S-1-5-21-2778787315-2228761457-209862467-500</Data>
      <Data Name="SubjectUserName">Administrator</Data>
      <Data Name="SubjectDomainName">WIDGETLLC</Data>
      <Data Name="SubjectLogonId">0x221c2bb</Data>
      <Data Name="CallerProcessId">0x0</Data>
      <Data Name="CallerProcessName">-</Data>
    </EventData>
  </Event>
```

Red different than client01