Windows Event Log Analysis with Filtering and XML Queries

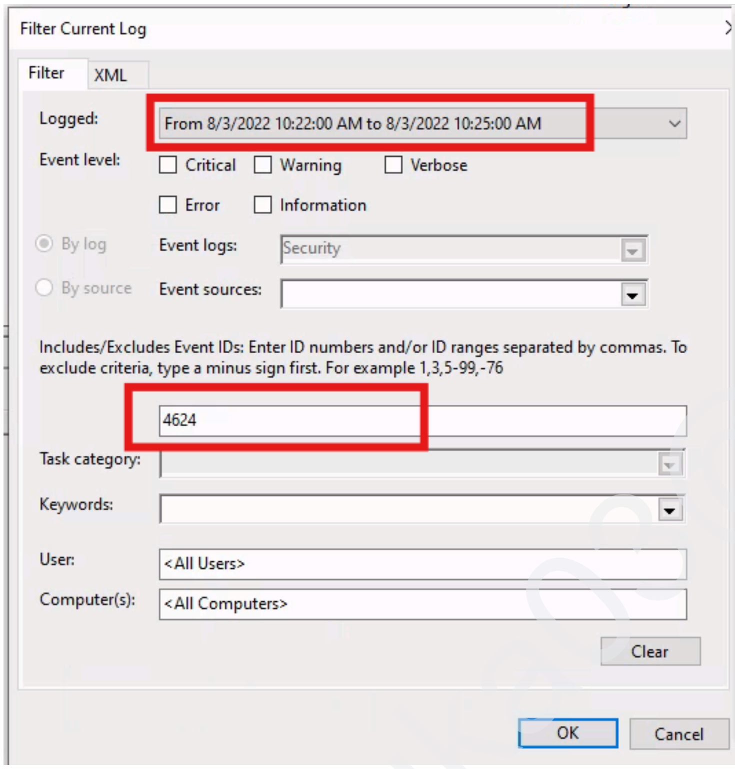
Part 1 - Analyze the event with <u>Event ID 4624 - *An account was successfully logged on*</u>, that took place on 8/3/2022 at 10:23:25. Find the name of the executable responsible for the modification of the auditing settings.

Part 2 - Build an XML query to determine if the previously mentioned executable modified the auditing settings of C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\wpfgfx_v0400.dll. Find the time of the identified event

---

Part 1

1. Set the time period and the Event ID for the Security log filter.



Filter Current Log

Logged: From 8/3/2022 10:22:00 AM to 8/3/2022 10:25:00 AM

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

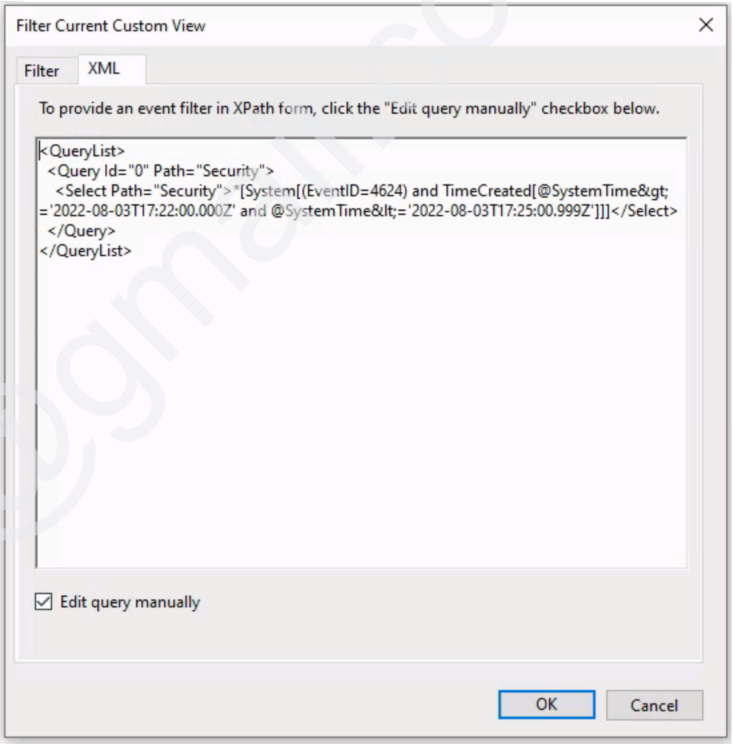
4624

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>



Filter Current Custom View

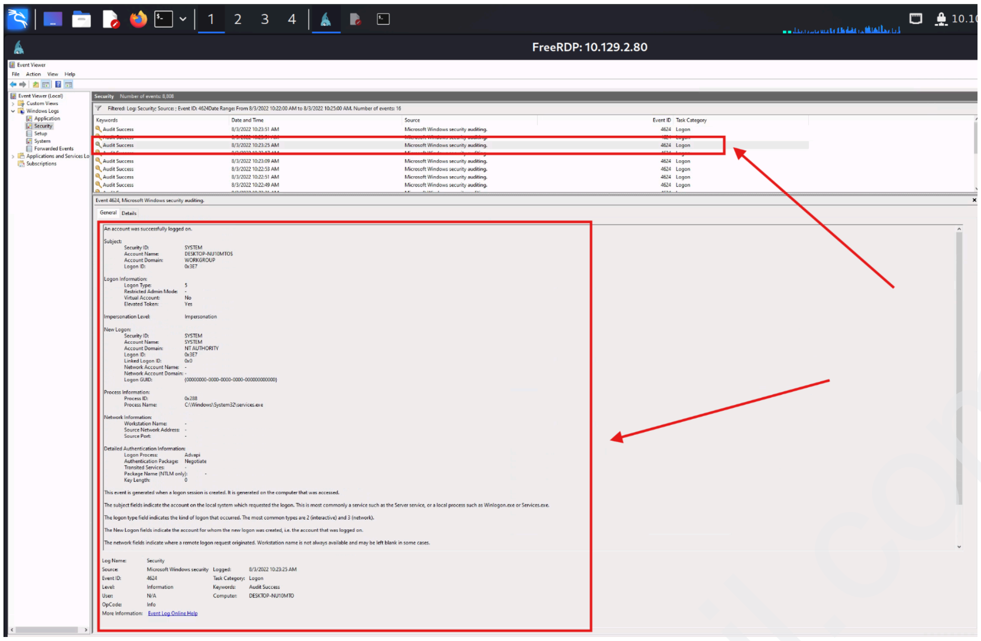
To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="Security">
   <Select Path="Security">*[System[(EventID=4624) and TimeCreated[@SystemTime&gt;
='2022-08-03T17:22:00.000Z' and @SystemTime&lt;='2022-08-03T17:25:00.999Z']]]</Select>
  </Query>
</QueryList>
```

☑ Edit query manually

Equivalent Query for the filter

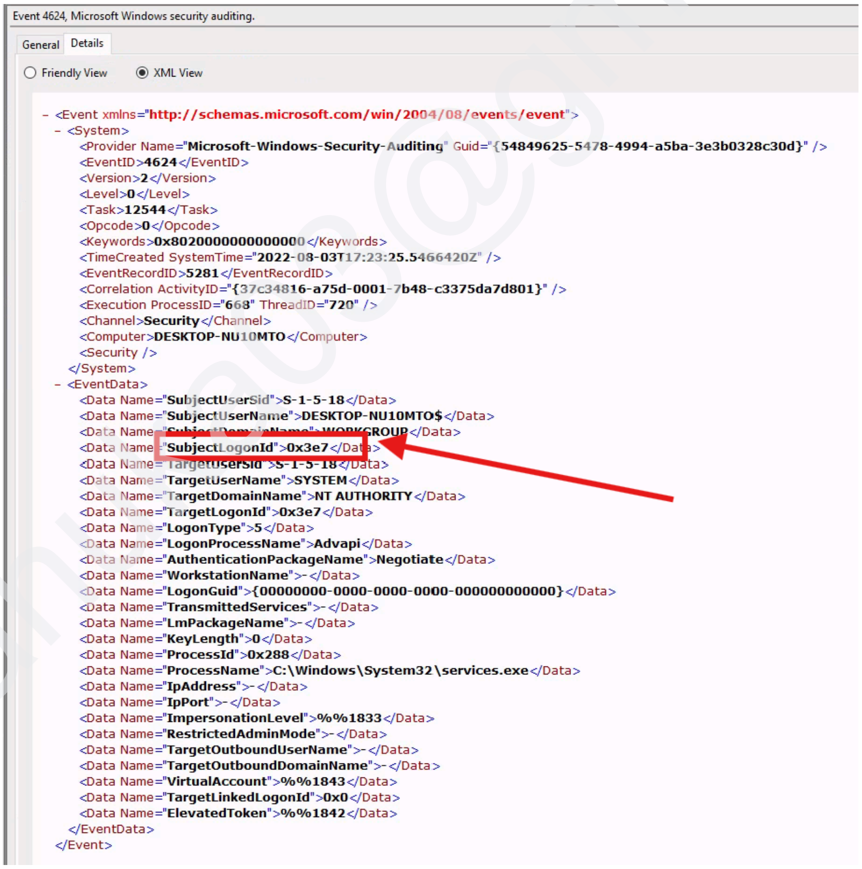
2. Find the relevant event that took place on 8/3/2022 at 10:23:25.



FreeRDP: 10.129.2.80

```
Security   Number of events: 8,808
Filtered: Log: Security; Source: ; Event ID: 4624Date Range: From 8/3/2022 10:22:00 AM to 8/3/2022 10:25:00 AM. Number of events: 16

Keywords        Date and Time            Source                                   Event ID  Task Category
Audit Success   8/3/2022 10:23:51 AM     Microsoft Windows security auditing.     4624      Logon
Audit Success   8/3/2022 10:23:25 AM     Microsoft Windows security auditing.     4624      Logon
Audit Success   8/3/2022 10:23:09 AM     Microsoft Windows security auditing.     4624      Logon
Audit Success   8/3/2022 10:22:53 AM     Microsoft Windows security auditing.     4624      Logon
Audit Success   8/3/2022 10:22:51 AM     Microsoft Windows security auditing.     4624      Logon
Audit Success   8/3/2022 10:22:49 AM     Microsoft Windows security auditing.     4624      Logon

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-NU10MTO$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x288
        Process Name:           C:\Windows\System32\services.exe

Network Information:
        Workstation Name:       -
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          Advapi
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

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 service, 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).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name:      Security
Source:        Microsoft Windows security   Logged:         8/3/2022 10:23:25 AM
Event ID:      4624                         Task Category:  Logon
Level:         Information                  Keywords:       Audit Success
User:          N/A                          Computer:       DESKTOP-NU10MTO
OpCode:        Info
More Information:  Event Log Online Help
```

3. Analyze the XML view of the event to identify the Logon ID associated with the specific event.



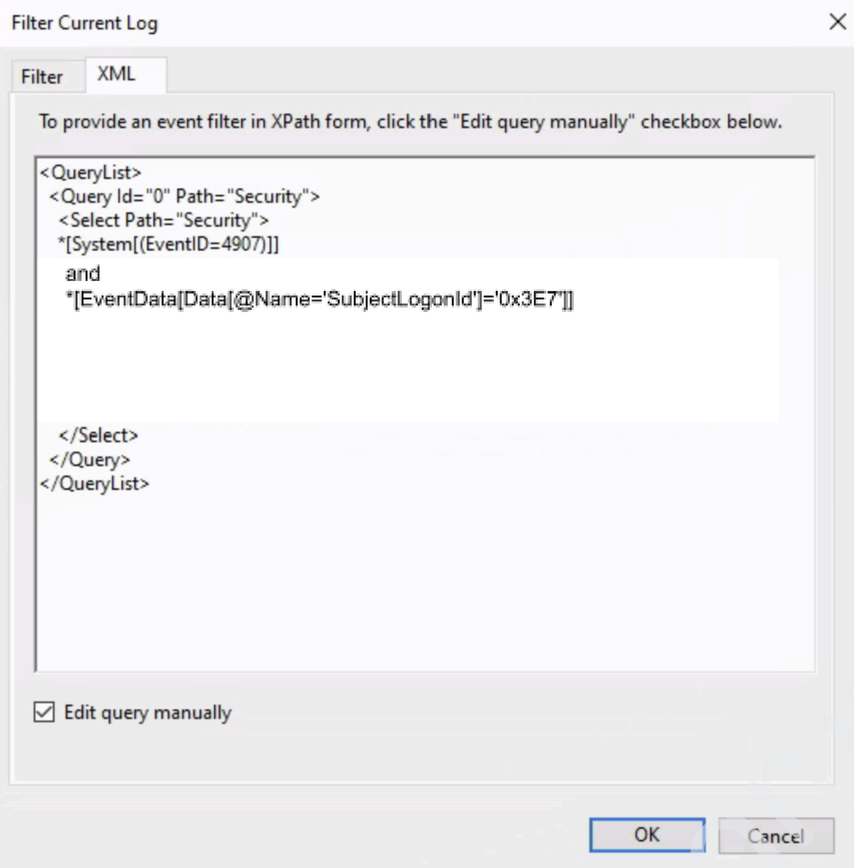
Event 4624, Microsoft Windows security auditing.

General | Details

○ Friendly View ● XML View

```
- <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>4624</EventID>
      <Version>2</Version>
      <Level>0</Level>
      <Task>12544</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8020000000000000</Keywords>
      <TimeCreated SystemTime="2022-08-03T17:23:25.5466420Z" />
      <EventRecordID>5281</EventRecordID>
      <Correlation ActivityID="{37c34816-a75d-0001-7b48-c3375da7d801}" />
      <Execution ProcessID="668" ThreadID="720" />
      <Channel>Security</Channel>
      <Computer>DESKTOP-NU10MTO</Computer>
      <Security />
    </System>
  - <EventData>
      <Data Name="SubjectUserSid">S-1-5-18</Data>
      <Data Name="SubjectUserName">DESKTOP-NU10MTO$</Data>
      <Data Name="SubjectDomainName">WORKGROUP</Data>
      <Data Name="SubjectLogonId">0x3e7</Data>
      <Data Name="TargetUserSid">S-1-5-18</Data>
      <Data Name="TargetUserName">SYSTEM</Data>
      <Data Name="TargetDomainName">NT AUTHORITY</Data>
      <Data Name="TargetLogonId">0x3e7</Data>
      <Data Name="LogonType">5</Data>
      <Data Name="LogonProcessName">Advapi</Data>
      <Data Name="AuthenticationPackageName">Negotiate</Data>
      <Data Name="WorkstationName">-</Data>
      <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
      <Data Name="TransmittedServices">-</Data>
      <Data Name="LmPackageName">-</Data>
      <Data Name="KeyLength">0</Data>
      <Data Name="ProcessId">0x288</Data>
      <Data Name="ProcessName">C:\Windows\System32\services.exe</Data>
      <Data Name="IpAddress">-</Data>
      <Data Name="IpPort">-</Data>
      <Data Name="ImpersonationLevel">%%1833</Data>
      <Data Name="RestrictedAdminMode">-</Data>
      <Data Name="TargetOutboundUserName">-</Data>
      <Data Name="TargetOutboundDomainName">-</Data>
      <Data Name="VirtualAccount">%%1843</Data>
      <Data Name="TargetLinkedLogonId">0x0</Data>
      <Data Name="ElevatedToken">%%1842</Data>
    </EventData>
  </Event>
```

4. Then, Use the following Query to filter only events with Logon ID 0x3E7 and <u>Event ID 4907- *modification of the auditing settings*</u> .

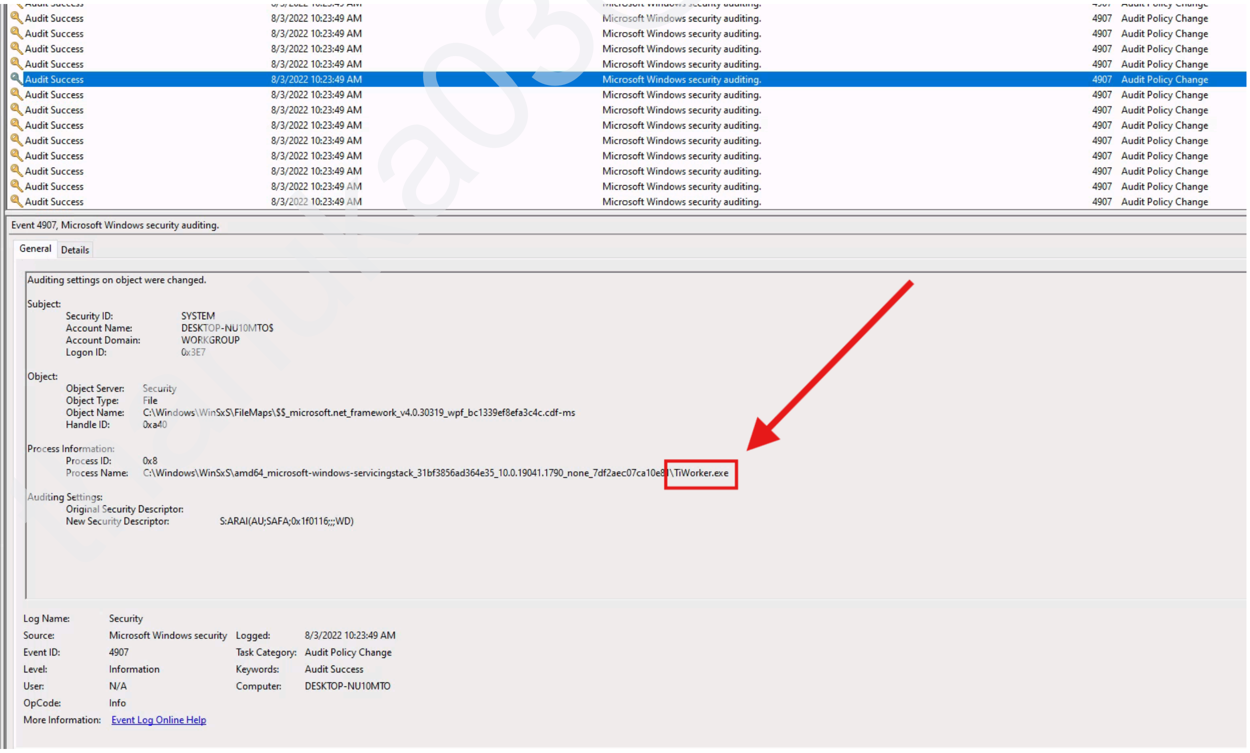


To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
 <Query Id="0" Path="Security">
  <Select Path="Security">
  *[System[(EventID=4907)]]
   and
   *[EventData[Data[@Name='SubjectLogonId']='0x3E7']]
  </Select>
 </Query>
</QueryList>
```

☑ Edit query manually

5. Analyze the 'Process Name' field in the output entries to identify the executable responsible for modifying the auditing settings.



```
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
Audit Success    8/3/2022 10:23:49 AM    Microsoft Windows security auditing.    4907    Audit Policy Change
```

Event 4907, Microsoft Windows security auditing.

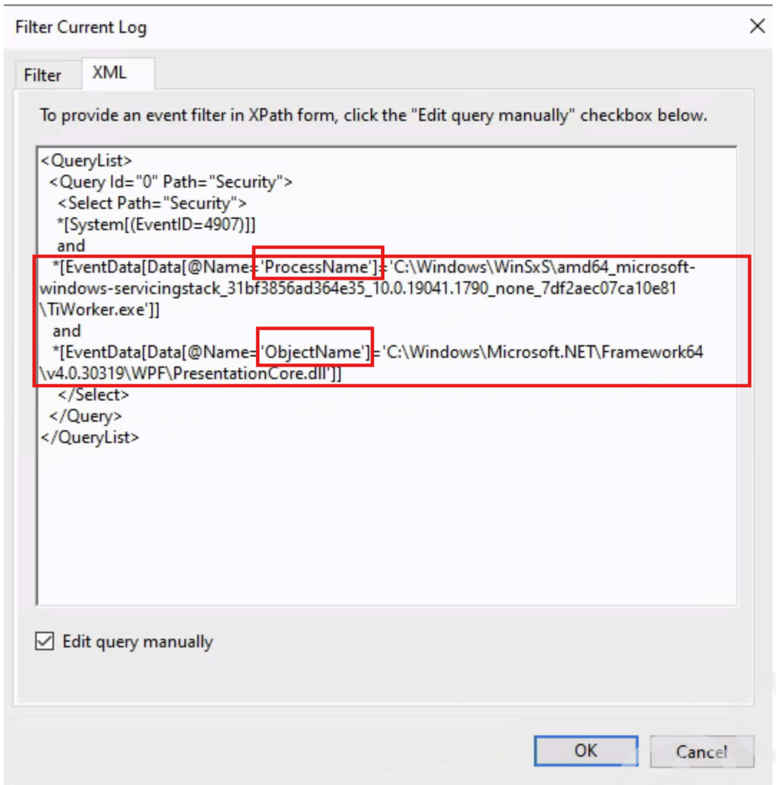
```
Auditing settings on object were changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-NU10MTO$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Object:
        Object Server:    Security
        Object Type:      File
        Object Name:      C:\Windows\WinSxS\FileMaps\$$_microsoft.net_framework_v4.0.30319_wpf_bc1339ef8efa3c4c.cdf-ms
        Handle ID:        0xa40

Process Information:
        Process ID:       0x8
        Process Name:     C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.1790_none_7df2aec07ca10e81\TiWorker.exe

Auditing Settings:
        Original Security Descriptor:
        New Security Descriptor:        S:ARAI(AU;SAFA;0x1f0116;;;WD)
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8/3/2022 10:23:49 AM
Event ID:          4907                         Task Category:   Audit Policy Change
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        DESKTOP-NU10MTO
OpCode:            Info
More Information:  Event Log Online Help
```

Name of the executable responsible for the modification of the auditing settings is **TiWorker.exe**

Part 2

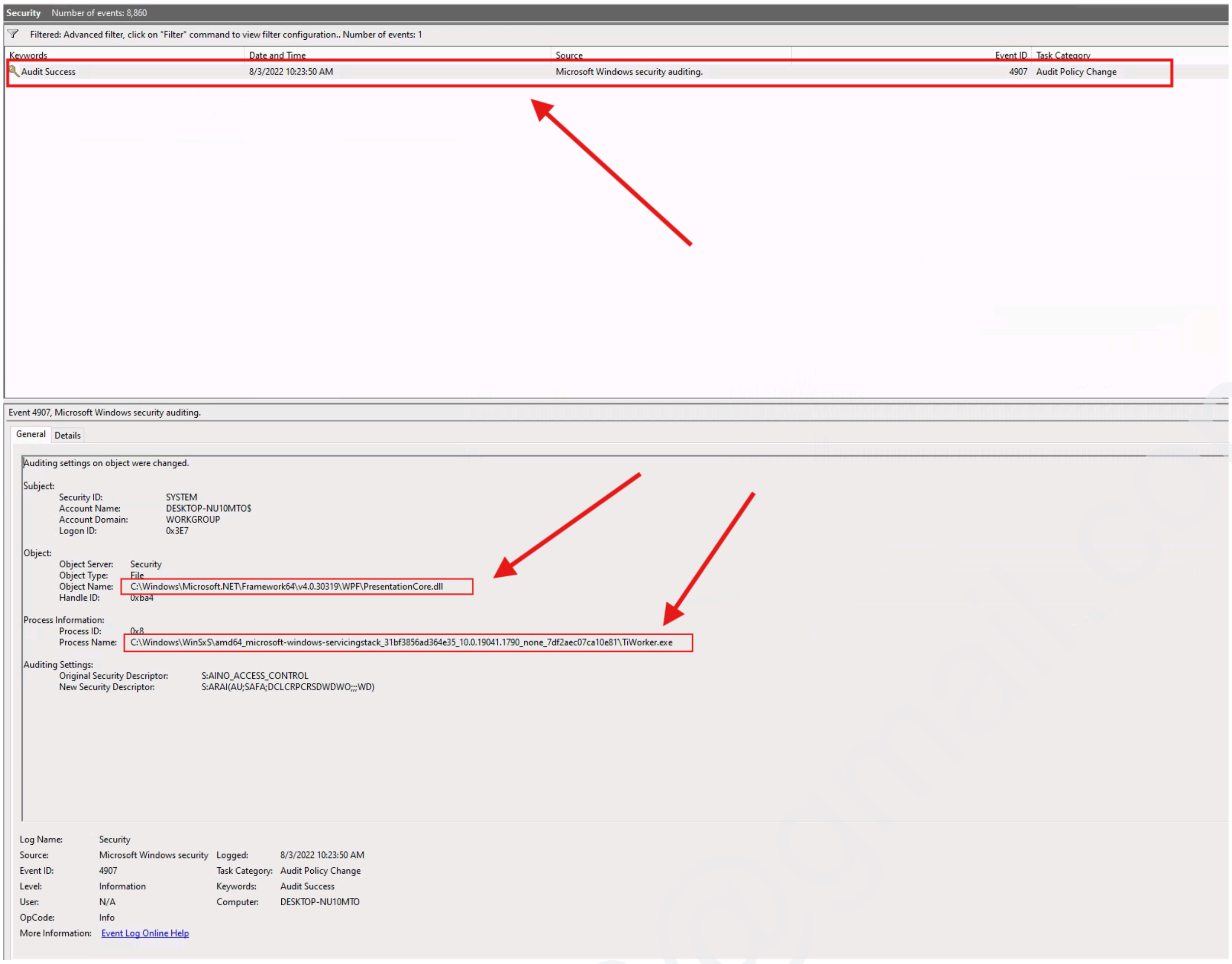
1. Execute the following query to obtain the event that corresponds to the given requirement.



To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="Security">
   <Select Path="Security">
   *[System[(EventID=4907)]]
   and
  *[EventData[Data[@Name='ProcessName']='C:\Windows\WinSxS\amd64_microsoft-
windows-servicingstack_31bf3856ad364e35_10.0.19041.1790_none_7df2aec07ca10e81
\TiWorker.exe']]
  and
  *[EventData[Data[@Name='ObjectName']='C:\Windows\Microsoft.NET\Framework64
\v4.0.30319\WPF\PresentationCore.dll']]
   </Select>
  </Query>
</QueryList>
```

☑ Edit query manually



Security Number of events: 8,860

Filtered: Advanced filter, click on "Filter" command to view filter configuration.. Number of events: 1

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/3/2022 10:23:50 AM	Microsoft Windows security auditing.	4907	Audit Policy Change

Event 4907, Microsoft Windows security auditing.

```
Auditing settings on object were changed.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-NU10MTO$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Object:
        Object Server:  Security
        Object Type:    File
        Object Name:    C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\PresentationCore.dll
        Handle ID:      0xba4

Process Information:
        Process ID:     0x8
        Process Name:   C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.1790_none_7df2aec07ca10e81\TiWorker.exe

Auditing Settings:
        Original Security Descriptor:   S:AINO_ACCESS_CONTROL
        New Security Descriptor:        S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8/3/2022 10:23:50 AM
Event ID:          4907                         Task Category:   Audit Policy Change
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        DESKTOP-NU10MTO
OpCode:            Info
More Information:  Event Log Online Help
```

*** Relevant event showing the modification of auditing settings for* C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\wpfgfx_v0400.dll by TiWorker.exe

Time of the identified event is **10:23:50 AM**

END