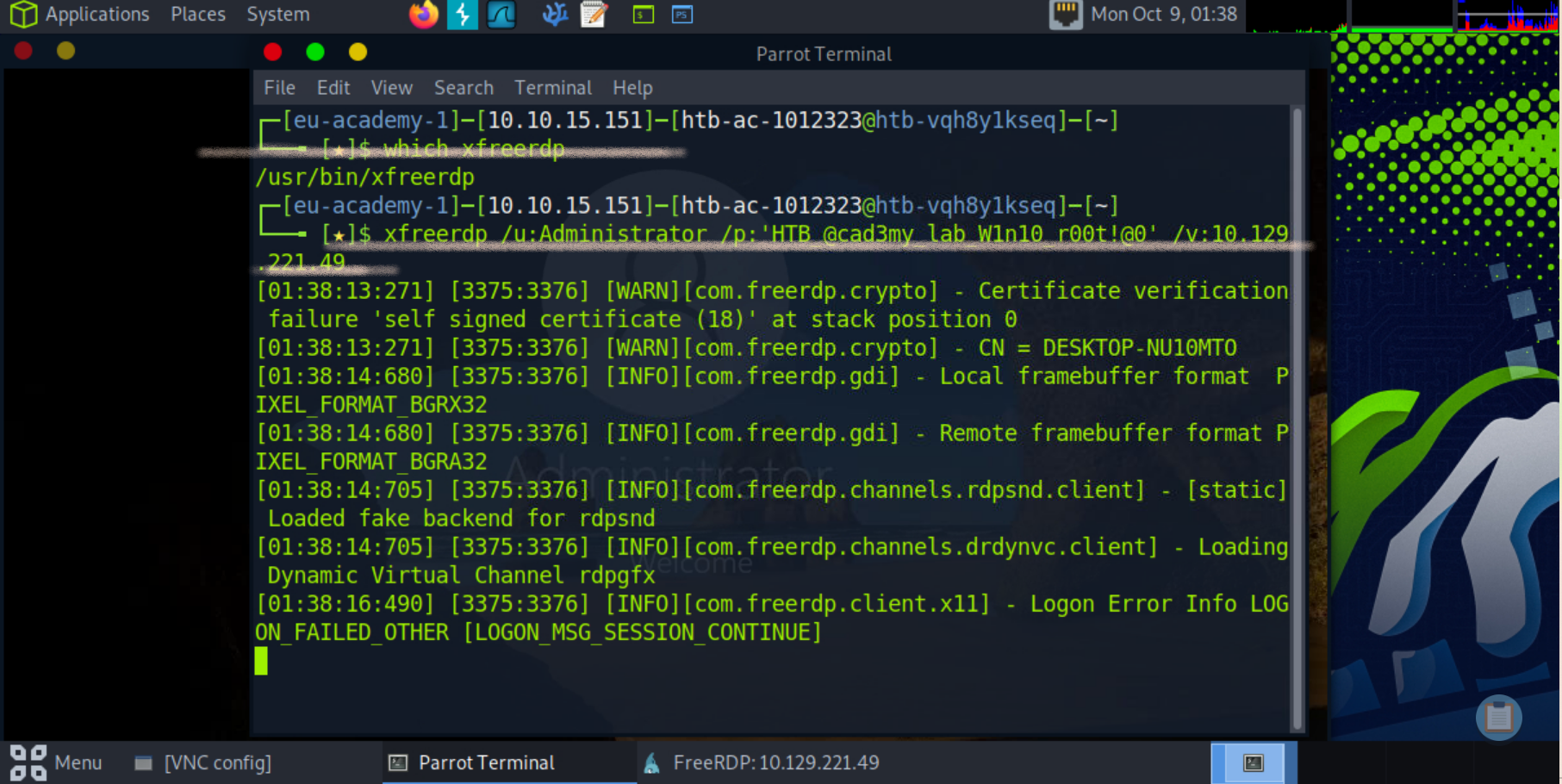
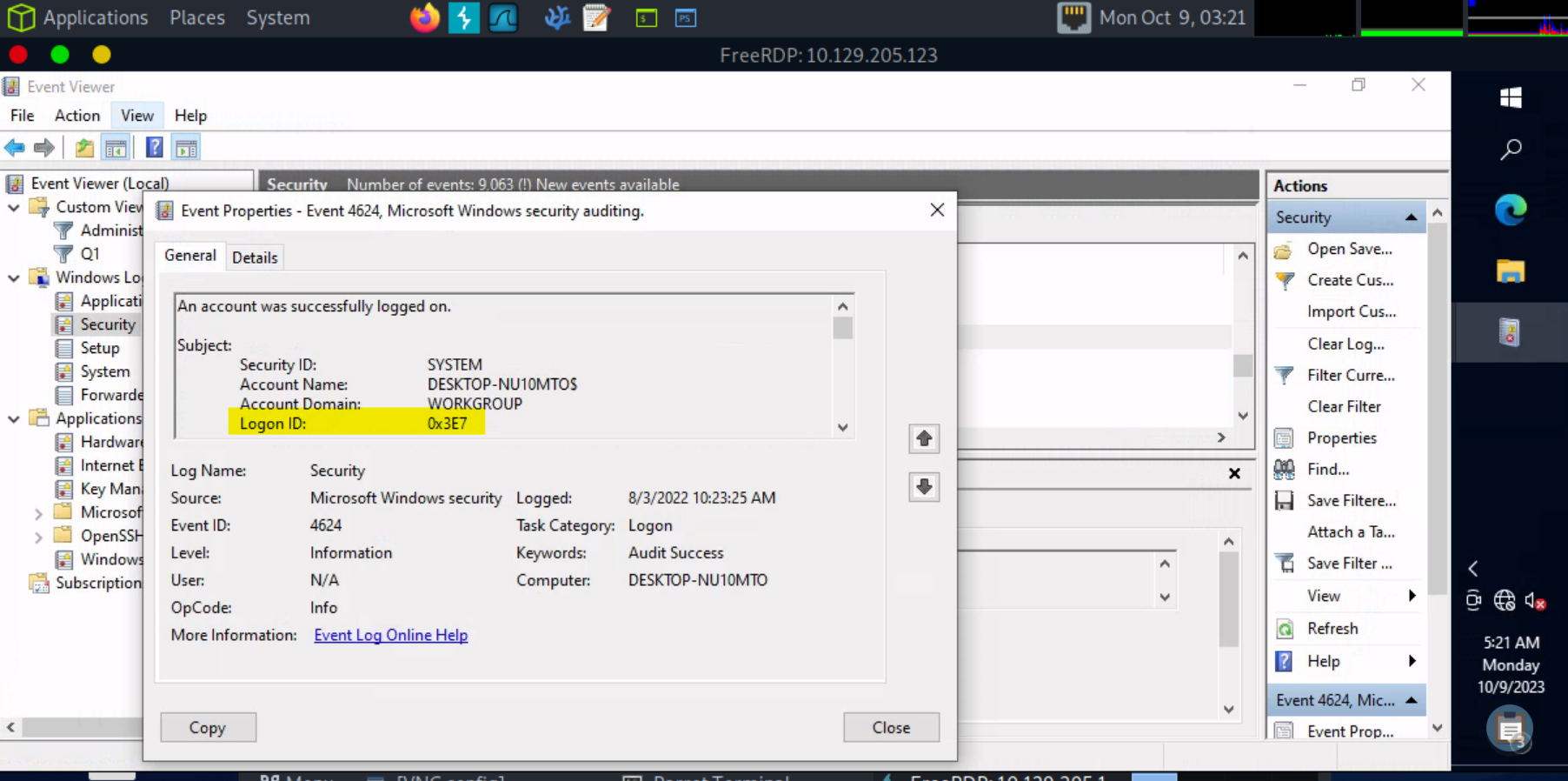
**Practical Exercises in Parrort**

Analyze the event with ID 4624, that took place on 8/3/2022 at 10:23:25. Conduct a similar investigation as outlined in this section and provide the name of the executable responsible for the modification of the auditing settings as your answer. Answer format: T\_W\_\_\_\_\_.exe

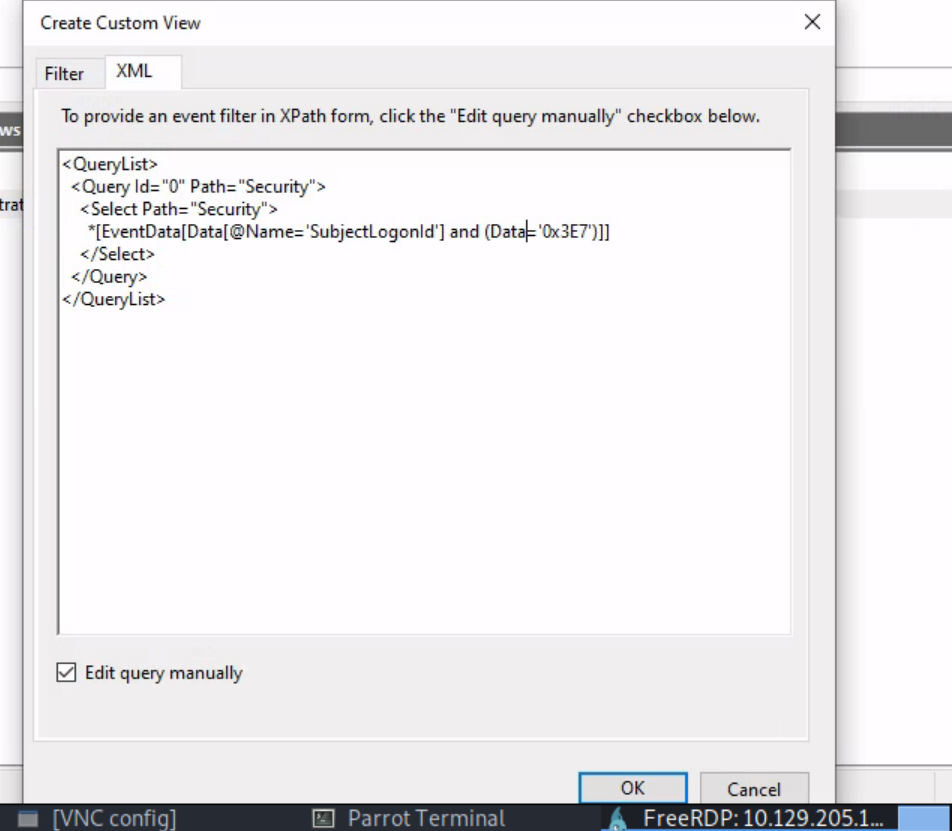
This question is so vague, go back to the investigation mentioned here, what I need to do here is investigating a security-related event (Event ID 4624) and using custom XML queries to narrow down the focus on specific logon activities associated with a particular Logon ID. And involves exploring events related to an audit policy change and identifying the process responsible for the change.

1. RDP with xfreerdp  
   
2. Successfully connected and opened the event viewer

Find the LogonID



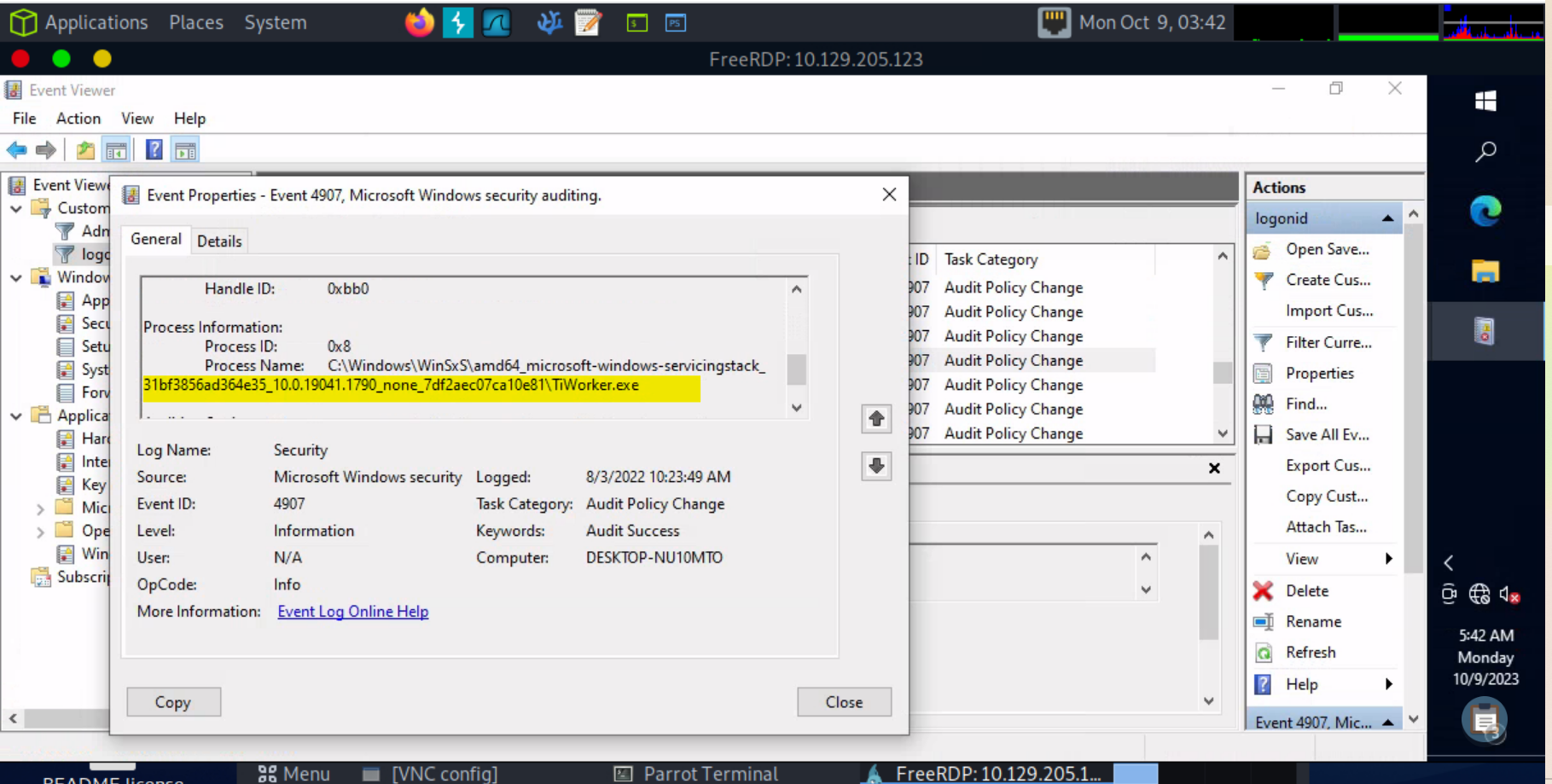
1. Narrowing Down with a Specific Logon ID



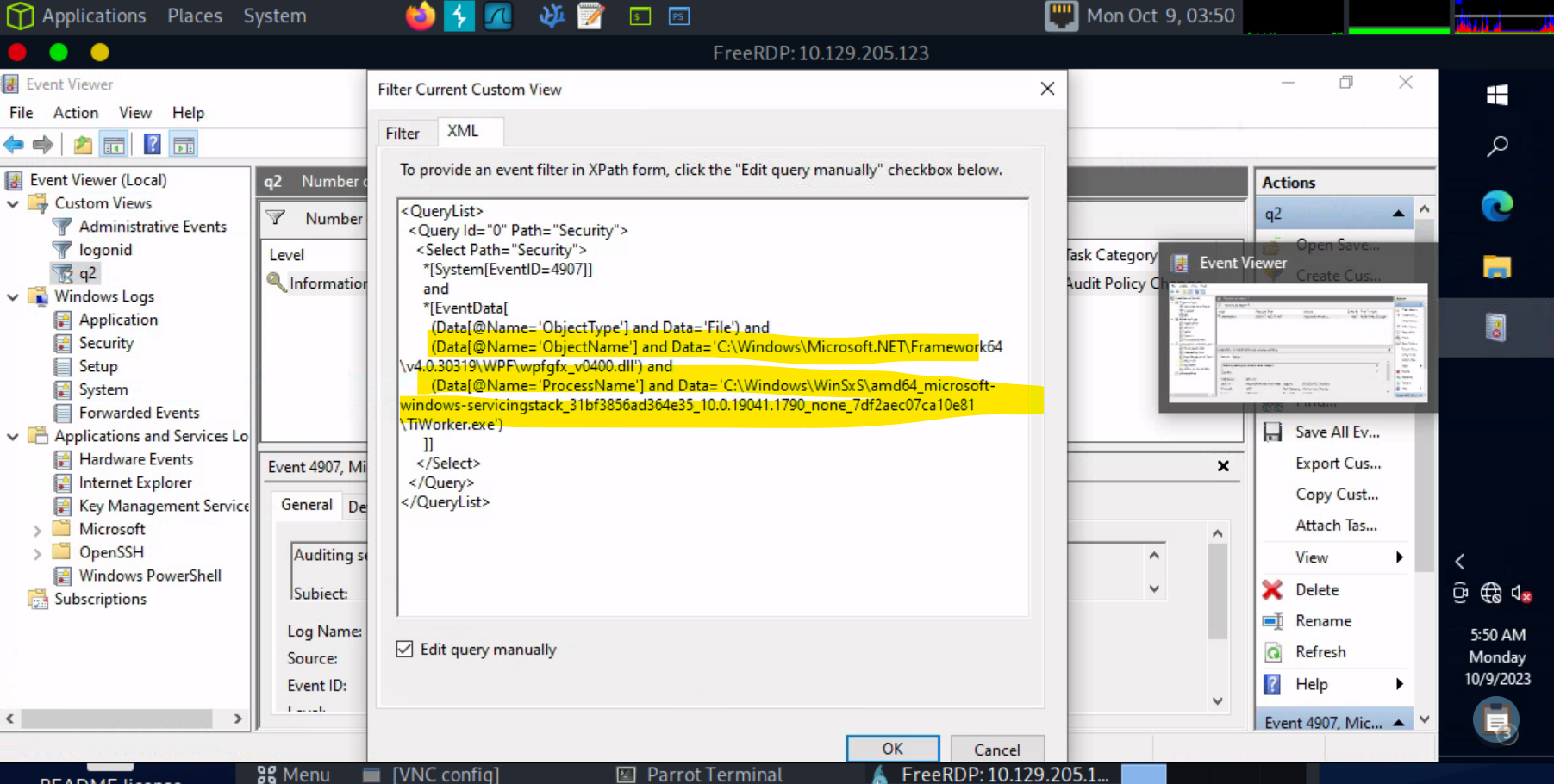
A screenshot of a computer

Description automatically generated

1. look for Event ID 4907 (Audit Policy Change)



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. Enter the time of the identified event in the format HH:MM:SS as your answer.



A screenshot of a computer

Description automatically generated