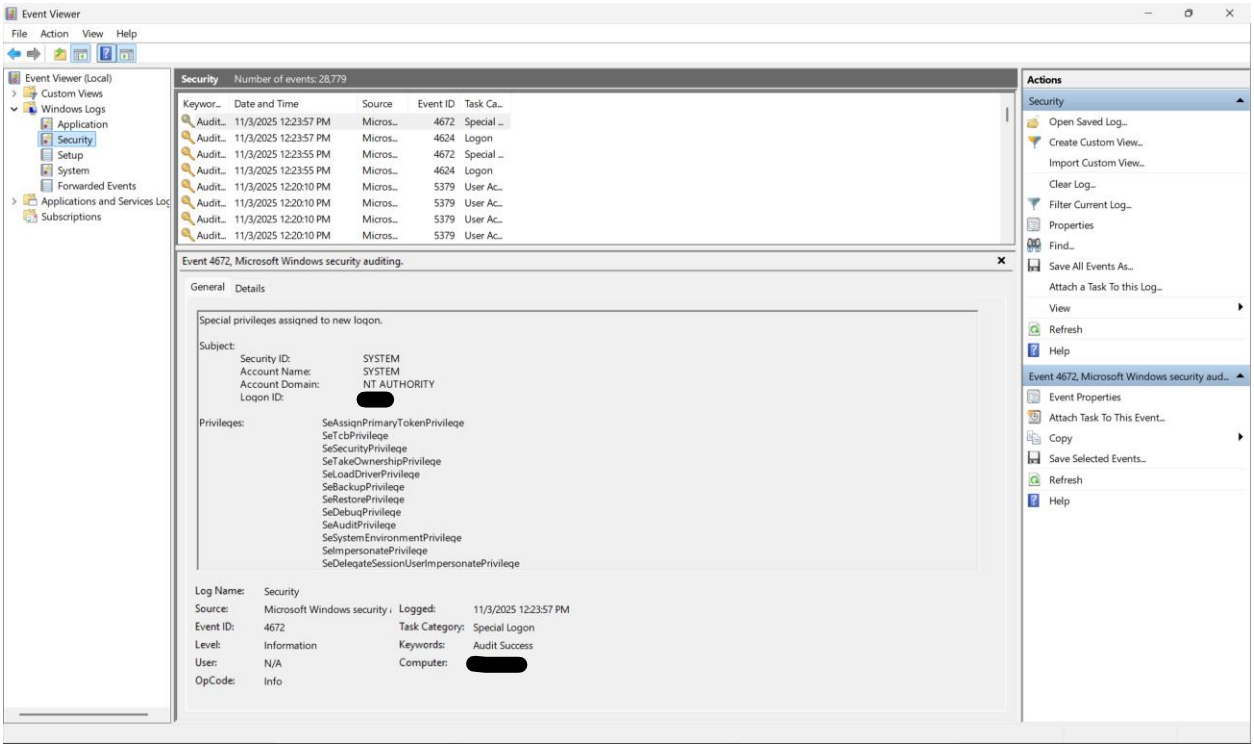
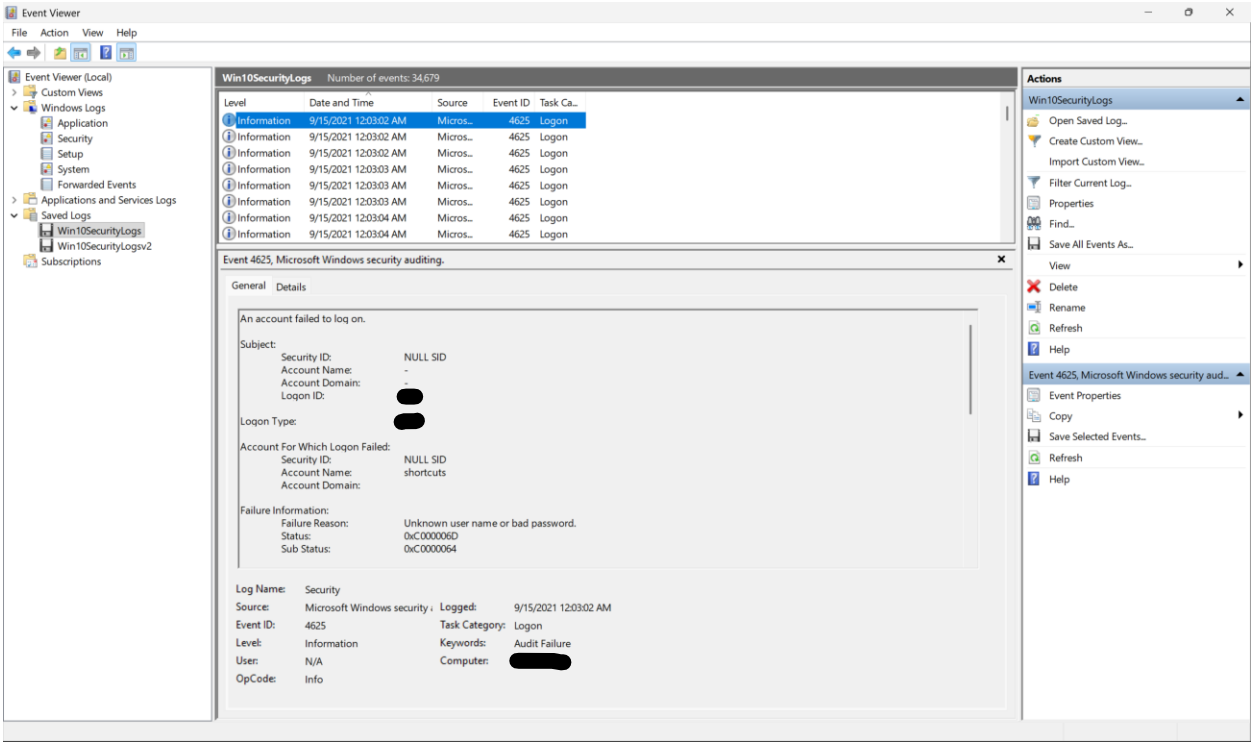
1. **Which built-in Windows utility/tool is used to view the log files? (1 point)**
   The Windows Event Viewer tool is used to view log files.

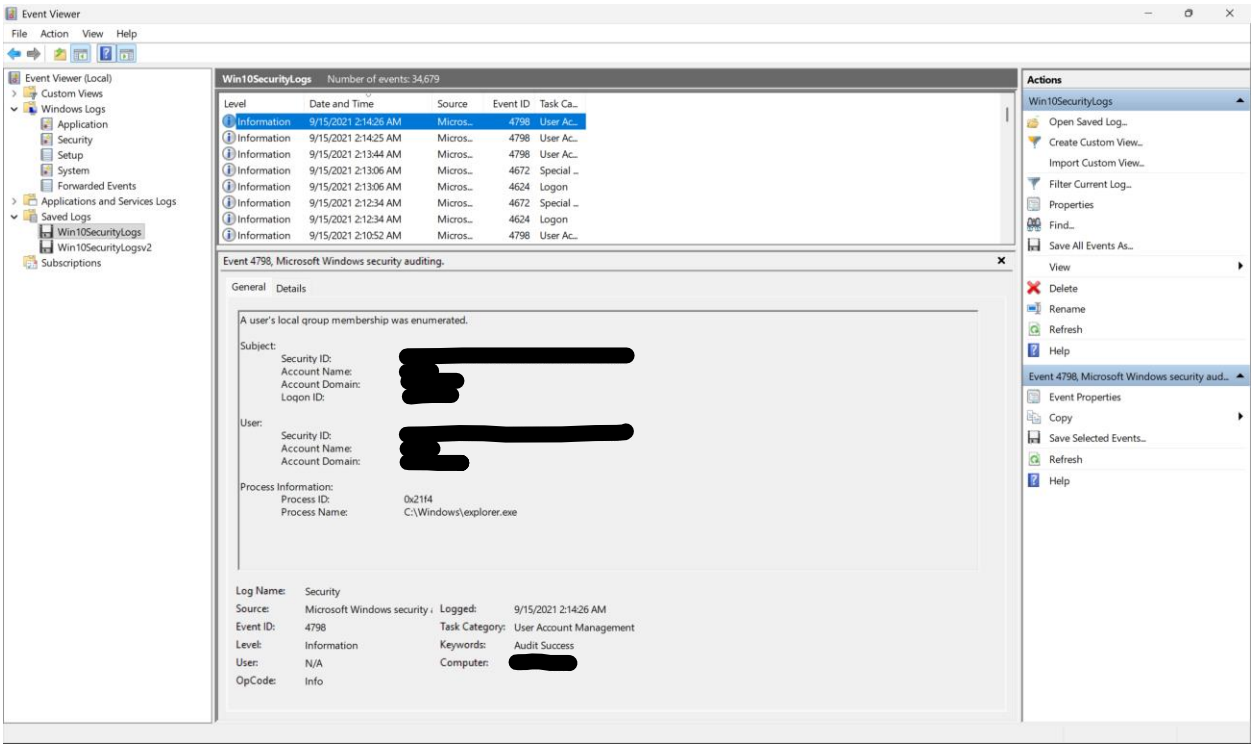


2. **What is the date/time for: (2 points):**

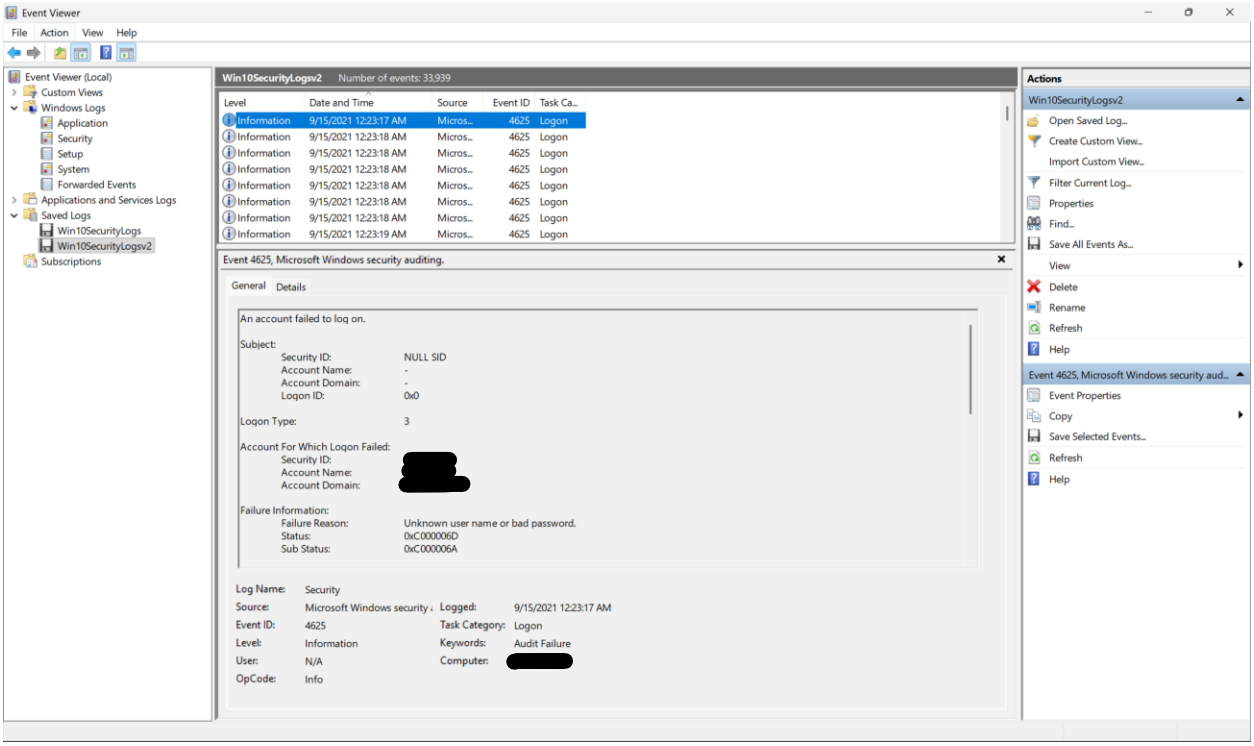
   First log in Win10SecurityLogs.evtx: 9/15/2021 12:03:02 AM



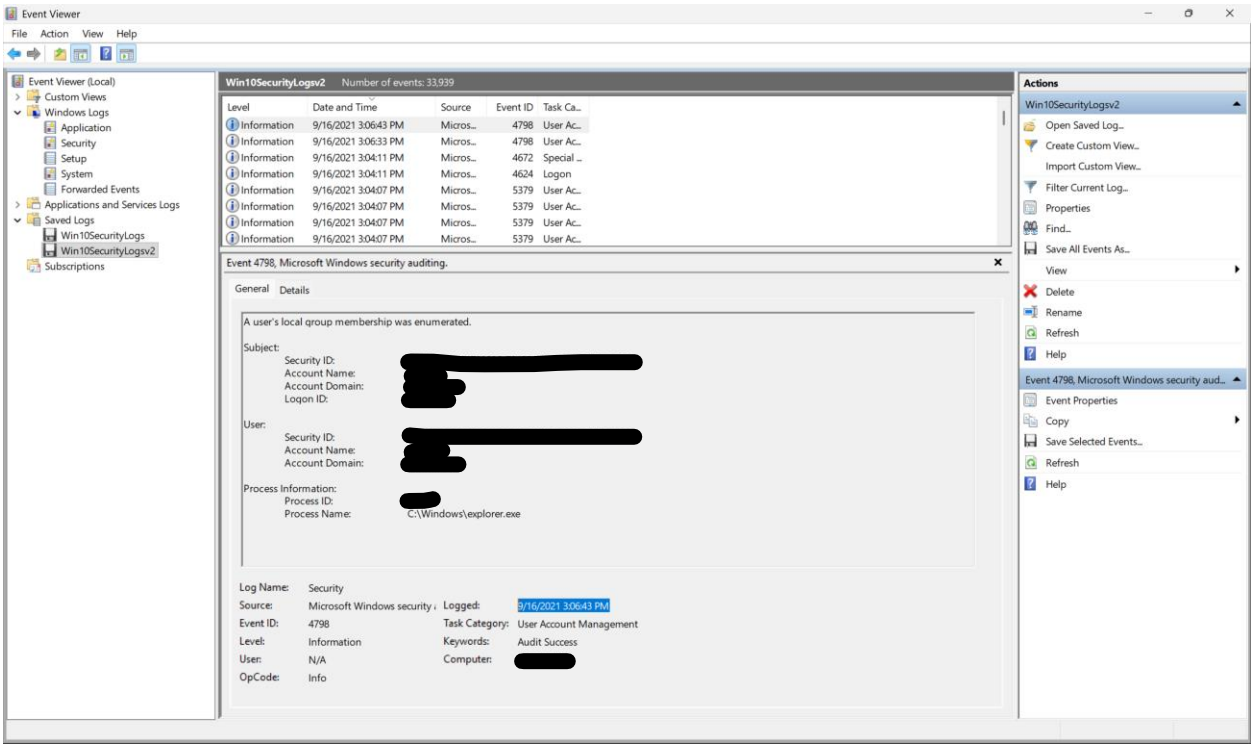
Last log in Win10SecurityLogs.evtx: 9/15/2021 12:14:26 AM



First log in Win10SecurityLogsv2.evtx: 9/15/2021 12:23:17 AM

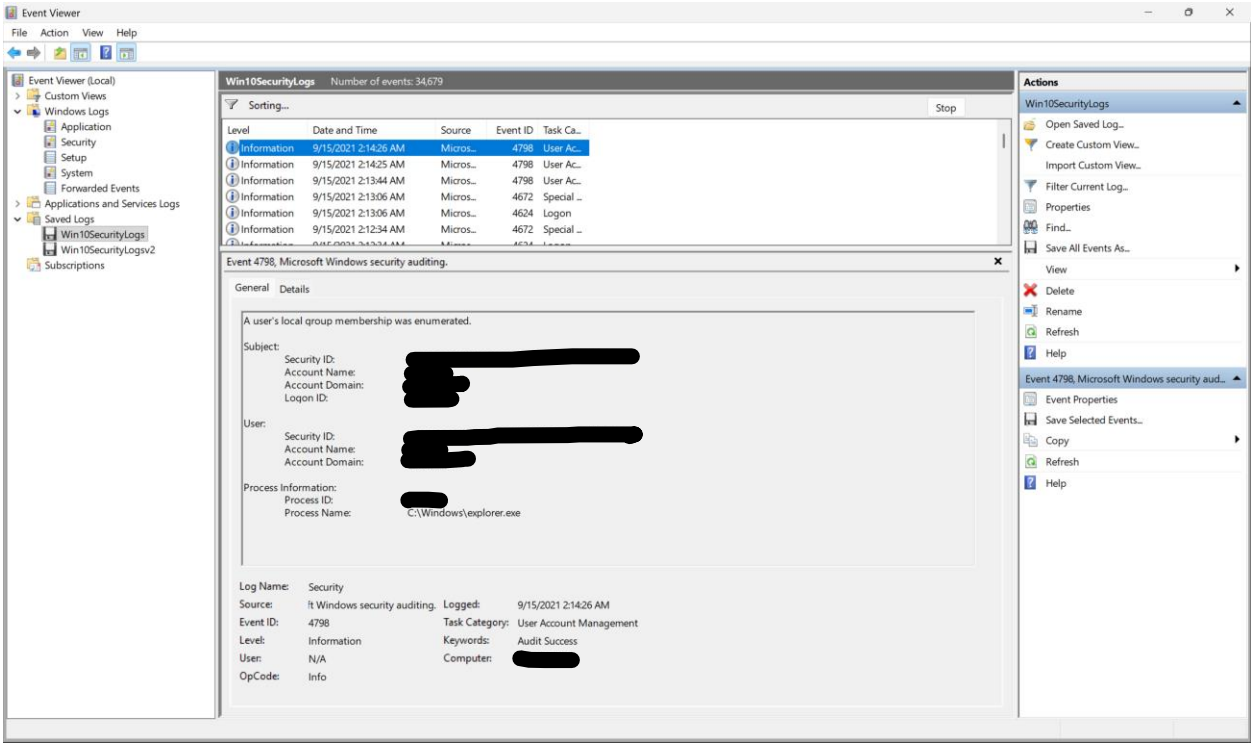


Last log in Win10SecurityLogsv2.evtx: 9/16/2021 3:06:43 PM

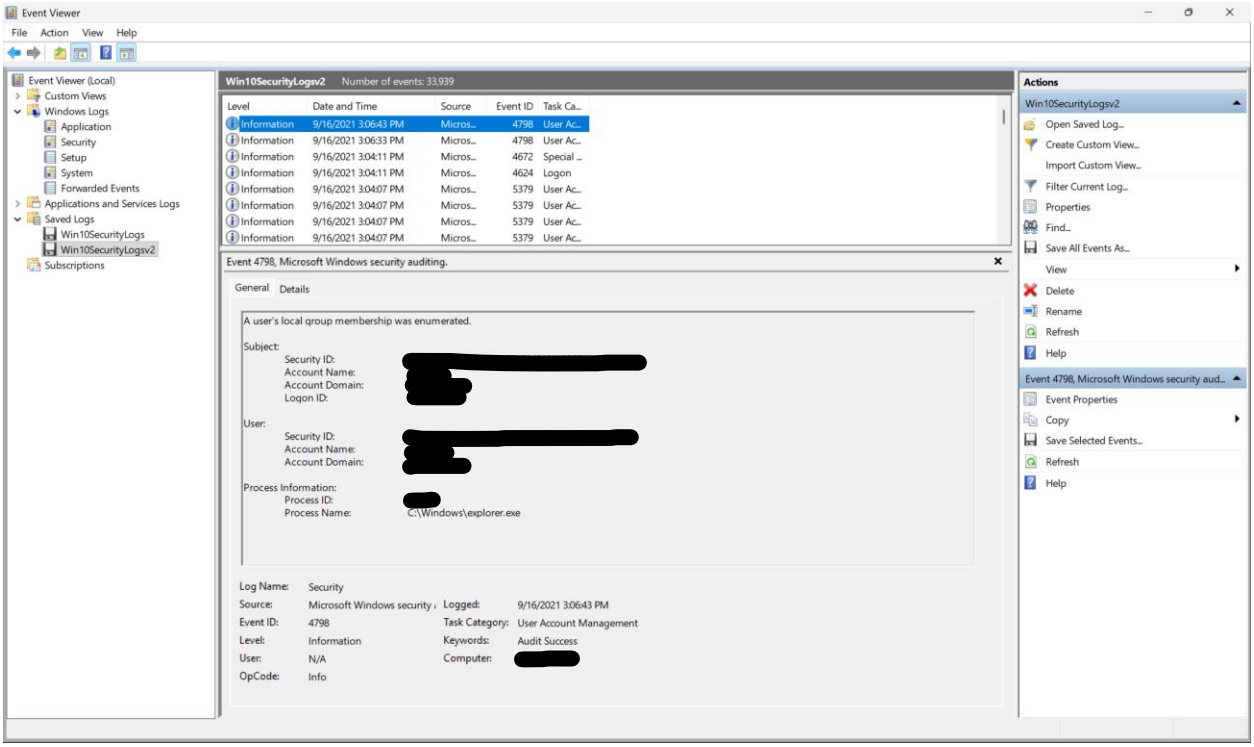


3. **Total number of events captured (1 point):**

Win10SecurityLogs.evtx: 34,679 events captured

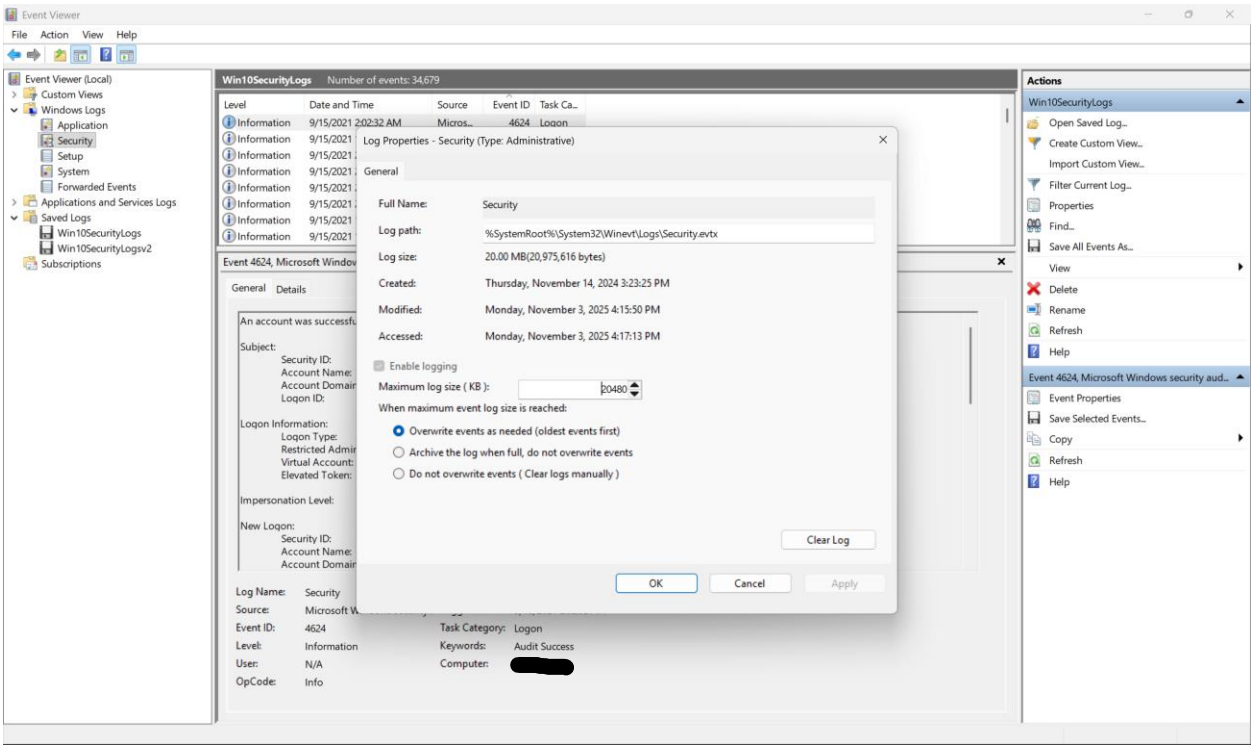


Win10SecurityLogsv2.evtx: 33,939 events captured



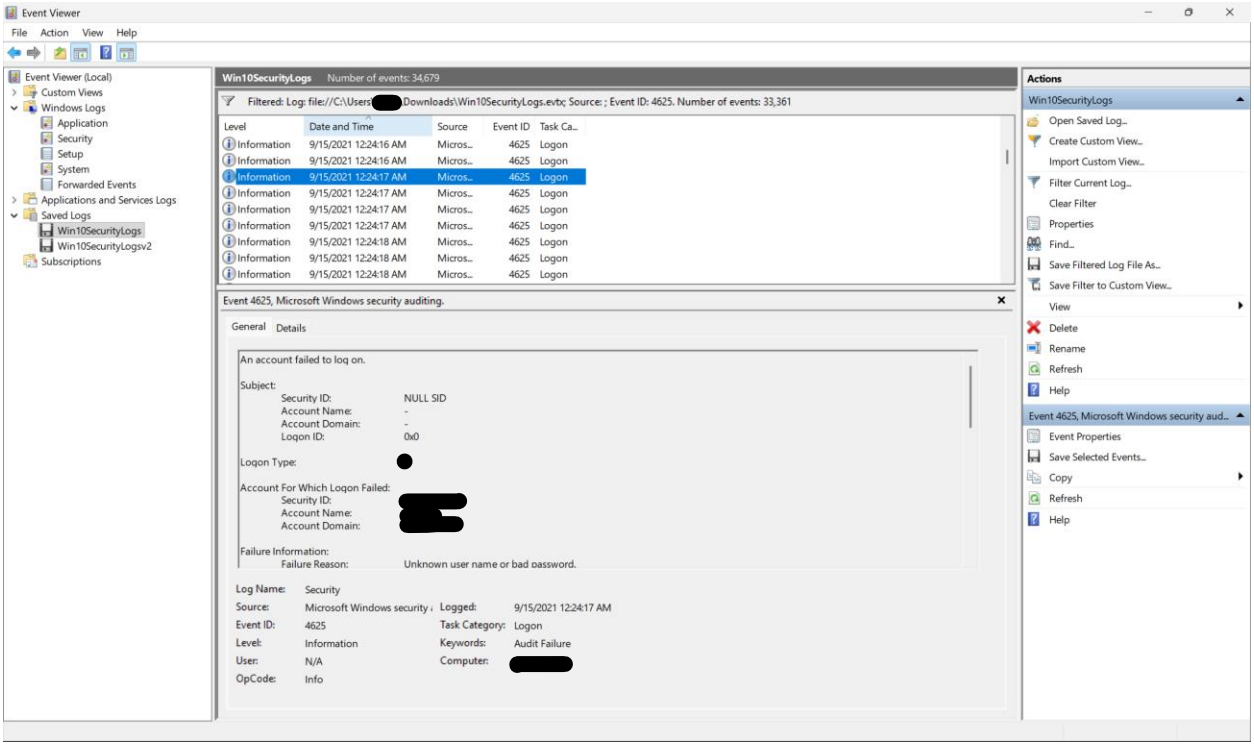
4. **Why are both log dumps approximately 20 MB in size? (5 points)**

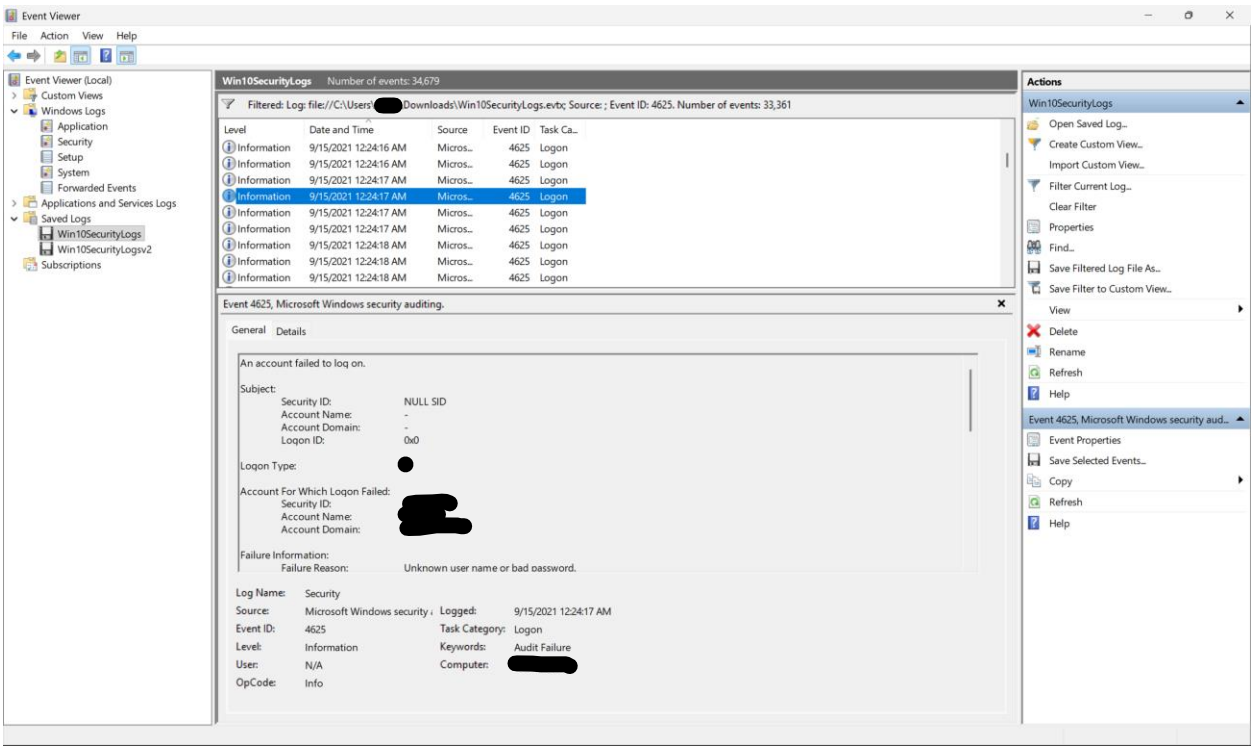
This is because the event logs have a maximum log file size configuration setting, and in this case, it's 20MB for Security logs by default. When the file size exceeds the limit, older events are overwritten by new ones.

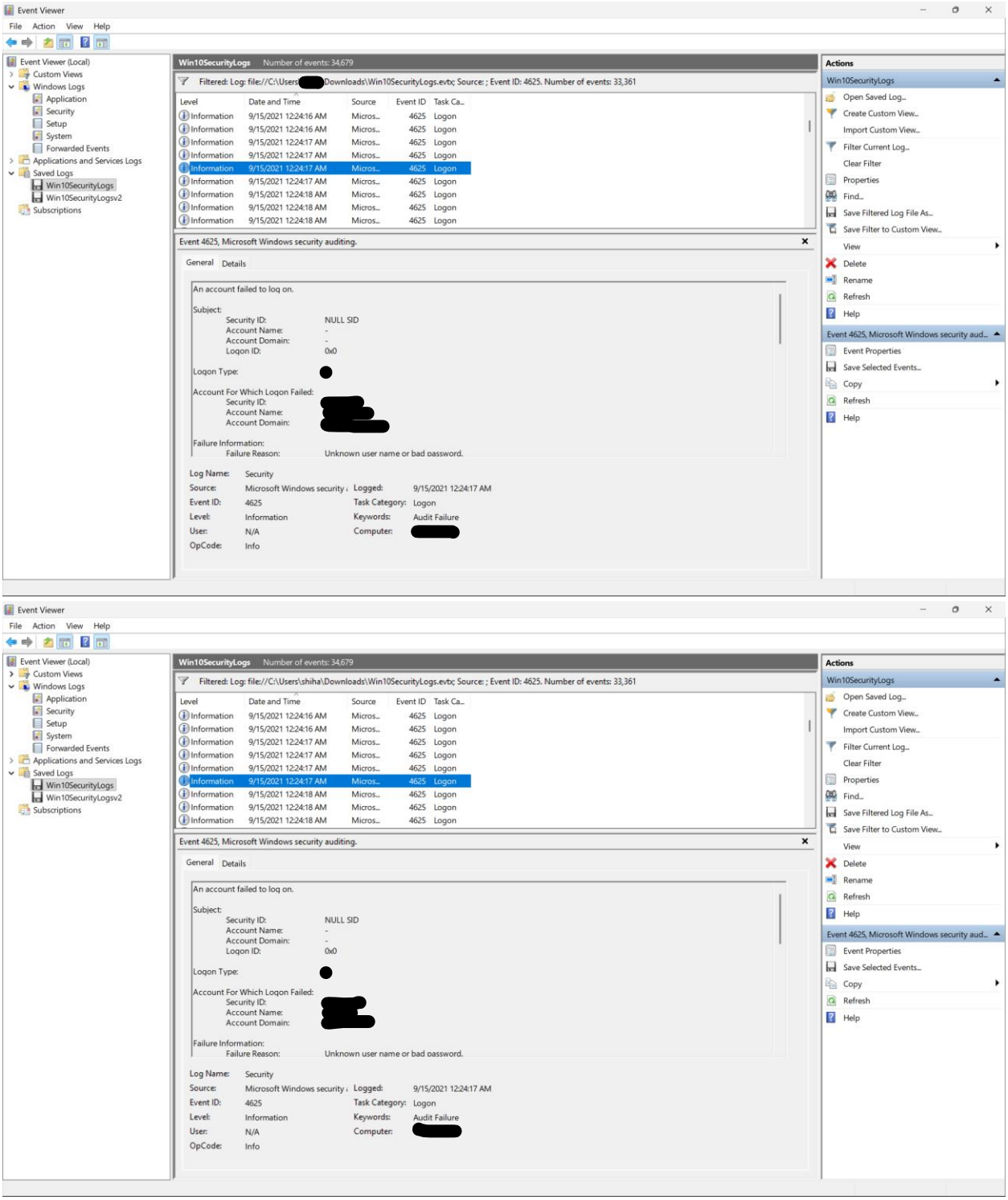


5. **Analyzing the events within Win10SecurityLogs.evtx, which user(s) attempted to log on at 9/15/2021 12:24:17 AM (Hint: 4625)? (3 points)**

   The users are [redacted], and [redacted]

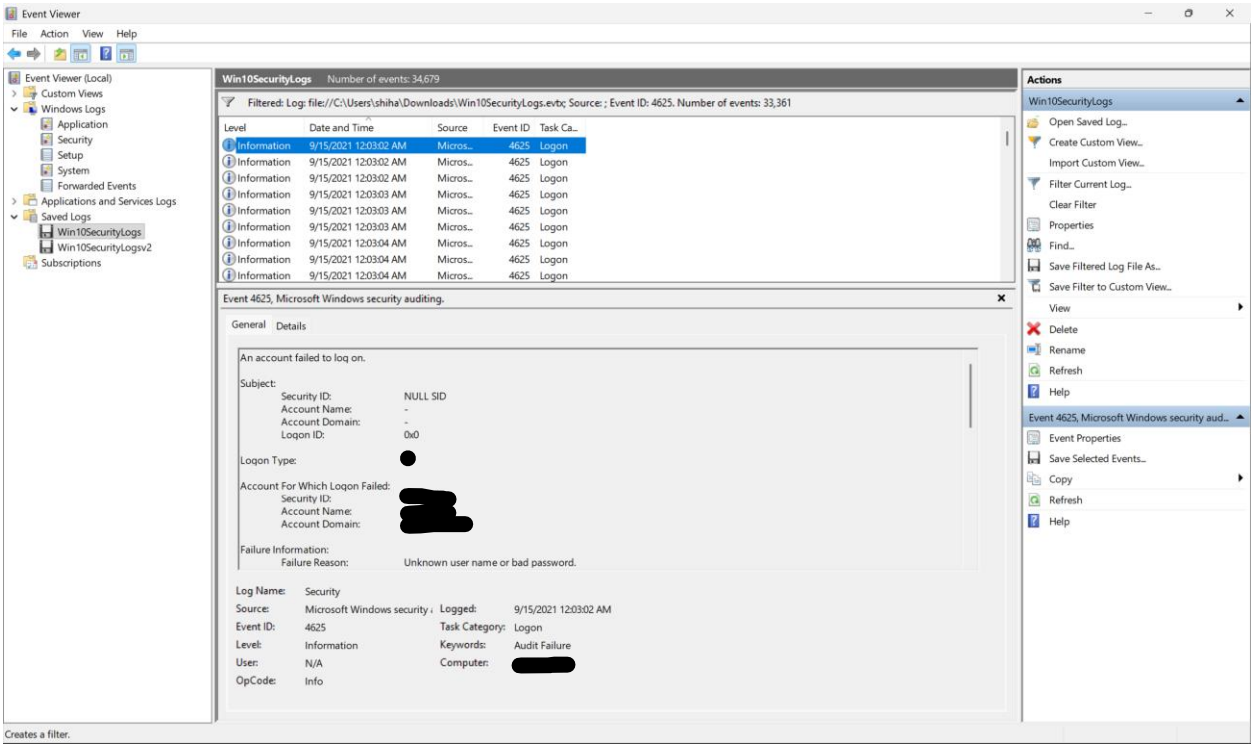

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Saved Logs
Win10SecurityLogs
Win10SecurityLogsv2
Subscriptions
Win10SecurityLogs Number of events: 34,679
Filtered: Log: file://C:\Users\[redacted]\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4625. Number of events: 33,361
Level Date and Time Source Event ID Task Ca...
Information 9/15/2021 12:24:16 AM Micros... 4625 Logon
Information 9/15/2021 12:24:16 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Event 4625, Microsoft Windows security auditing.
General Details
An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: [redacted]
Account For Which Logon Failed:
Security ID:
Account Name:
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Log Name: Security
Source: Microsoft Windows security Logged: 9/15/2021 12:24:17 AM
Event ID: 4625 Task Category: Logon
Level: Information Keywords: Audit Failure
User: N/A Computer: [redacted]
OpCode: Info
Actions
Win10SecurityLogs
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Save Filter to Custom View...
View
Delete
Rename
Refresh
Help
Event 4625, Microsoft Windows security aud...
Event Properties
Save Selected Events...
Copy
Refresh
Help


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Saved Logs
Win10SecurityLogs
Win10SecurityLogsv2
Subscriptions
Win10SecurityLogs Number of events: 34,679
Filtered: Log: file://C:\Users\[redacted]\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4625. Number of events: 33,361
Level Date and Time Source Event ID Task Ca...
Information 9/15/2021 12:24:16 AM Micros... 4625 Logon
Information 9/15/2021 12:24:16 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:17 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Information 9/15/2021 12:24:18 AM Micros... 4625 Logon
Event 4625, Microsoft Windows security auditing.
General Details
An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: [redacted]
Account For Which Logon Failed:
Security ID:
Account Name:
Account Domain:
Failure Information:
Failure Reason: Unknown user name or bad password.
Log Name: Security
Source: Microsoft Windows security Logged: 9/15/2021 12:24:17 AM
Event ID: 4625 Task Category: Logon
Level: Information Keywords: Audit Failure
User: N/A Computer: [redacted]
OpCode: Info
Actions
Win10SecurityLogs
Open Saved Log...
Create Custom View...
Import Custom View...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Save Filter to Custom View...
View
Delete
Rename
Refresh
Help
Event 4625, Microsoft Windows security aud...
Event Properties
Save Selected Events...
Copy
Refresh
Help



6. **Analyzing more log events, what type of attack happened (5 points)?**
   It looks like a brute-force privilege escalation attack has happened. There are multiple failed logons of attempts to guess passwords for the accounts. The reason for all failure is

stated as “Unknown user name or bad password,” which is Event ID 4625, and it just means the wrong password entered for a specific account in this case.

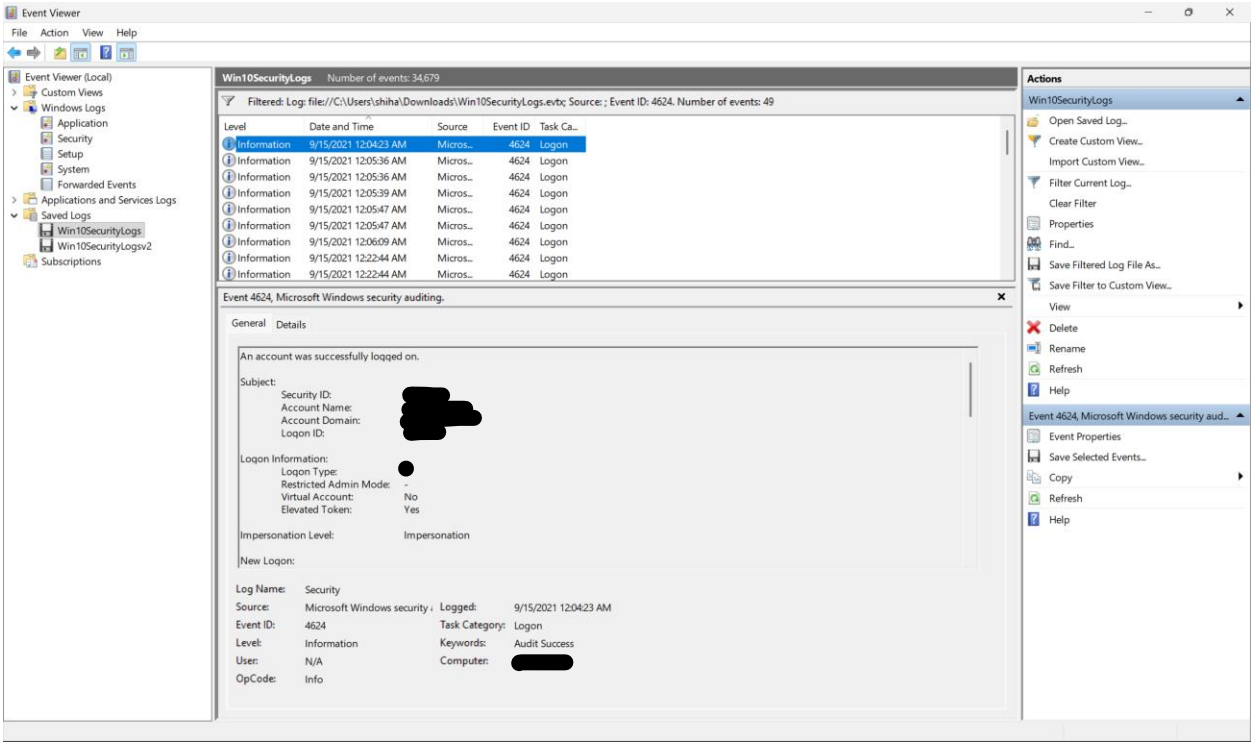


7. **What is the vulnerability(ies)? (5 points)**

   The vulnerabilities are likely to be weak passwords, didn’t set up account lockout policy, and RDP is probably open to the public. If so, the RDP was also not set up for limited failed login attempts, which can literally have infinite login attempts for treating actors to keep trying to guess passwords.

8. **Was the attack successful? (5 points)**

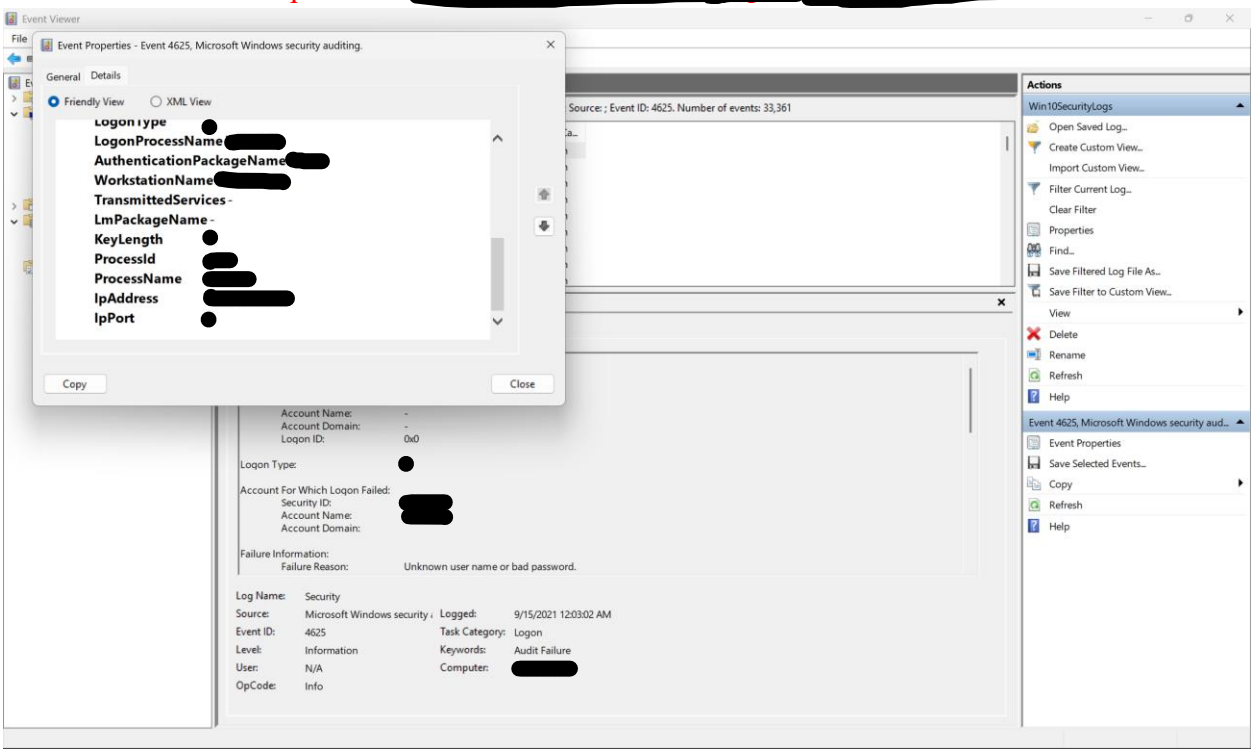
   No, the attack was not successful because the only successful login is the authorized user.

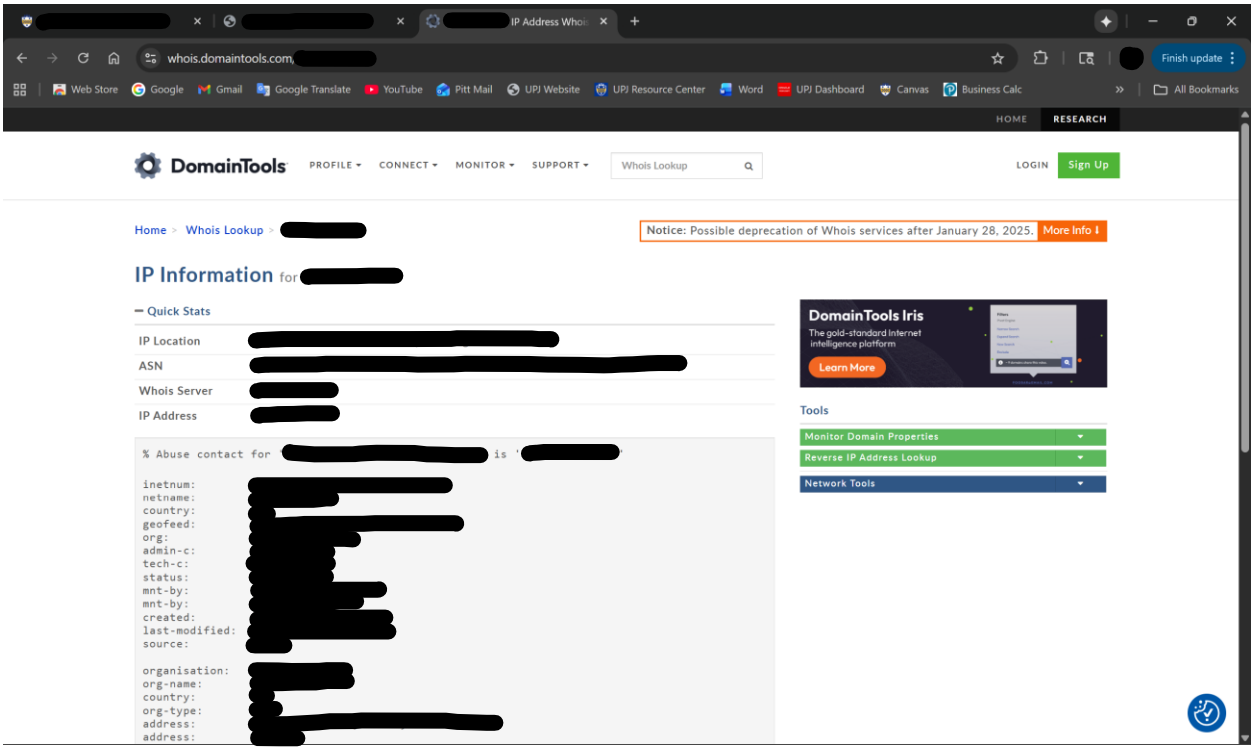


9. **What was most likely the motivation for the attack? (3 points)**
   The attacker's motivation was likely to gain unauthorized access to the system or network. By doing so, the attacker can gain remote access for further exploitation, such as information theft or using the system as a botnet.

10. **Who were the attackers (i.e. country, etc...)? (5 points)**
    I used https://whois.domaintools.com/ to look up the IP address (, and it is showing me the attack was from The IP address range from -

[redacted] and it points to [redacted]





11. How should vulnerability be remediated? (10 points)

Vulnerability should be remediated by keeping system and firewall updated, setting up strong password policies, setting up account lockout policies after several failed logon

attempts, and disable RDP access to the public internet or use secure connections such as VPN.

12. **Management wants a summary of what additional steps should be taken to ensure there is better logging (i.e. no gaps) and to ensure this vulnerability does not happen again? (15 points)**

    To improve logging and prevent similar attacks, Management should strengthen its log management system:

    1. Increase log retention size from default 20MB to somewhere 200MB+, and schedule automatic log backups to avoid gaps.
    2. Enable *Advanced Audit Policy* in the Local Security Policy, so it ensures complete tracking of user activities and possible attack attempts.
    3. Set up alerts for repeated failed logon attempts, which in this case, is Event ID 4625.
    4. Regularly review logs and automatically report suspicious activity.
    5. Set up an account lockout policy so the system will lock itself if the wrong password is entered many times.
    6. Enforce strong passwords and have expiration dates for them.
    7. Enable MFA for remote access and admin accounts.
    8. Renaming the default administrator account or disable it to reduce brute-force targets.
    9. Disable RDP access from the internet or use VPN connection.
    10. Allow only trusted IP addresses using Firewall rules.
    11. Regularly update the OS and firewall.
    12. Perform security audits to review logs, firewall, and account activity
    13. Train employees to notice phishing emails and not to interact with them and always report suspicious activities.