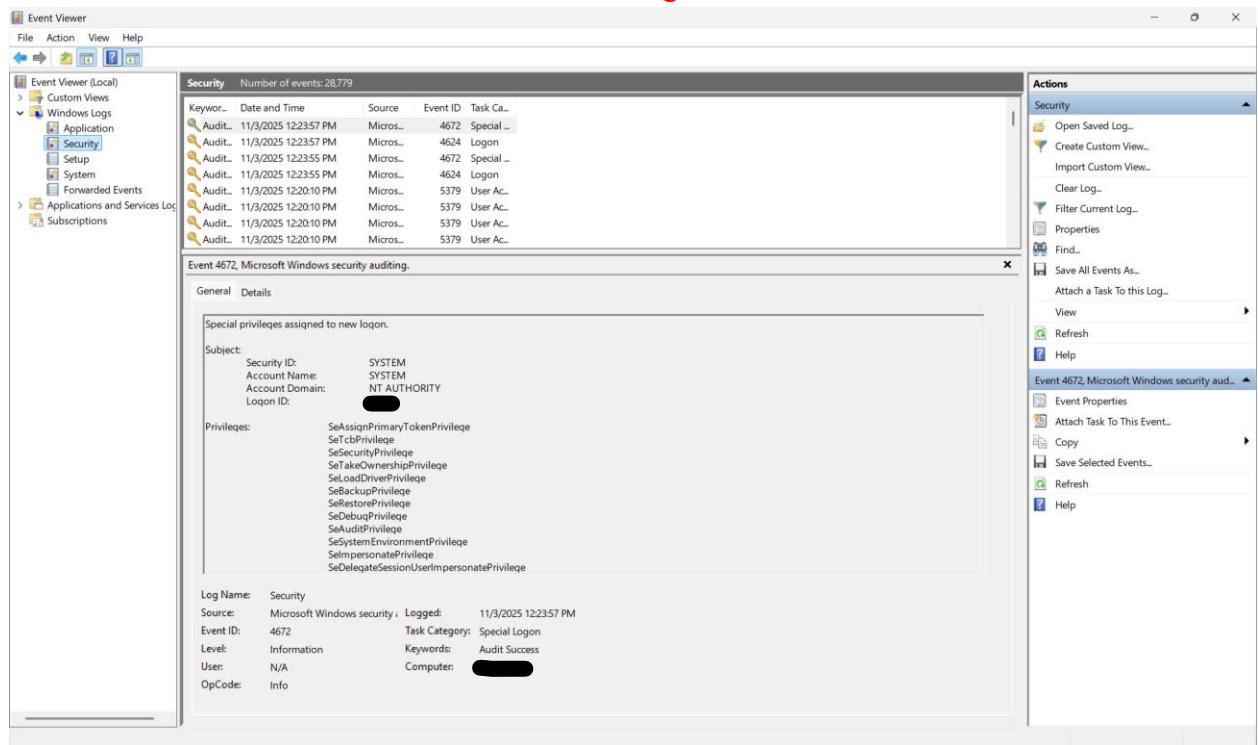


1. Which built-in Windows utility/tool is used to view the log files? (1 point)

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

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: [REDACTED]

Logon Type:

Account For Which Logon Failed:

- Security ID: NULL SID
- Account Name: shortcuts
- Account Domain: -

Failure Information:

- Failure Reason: Unknown user name or bad password.
- Status: 0xC000006D
- Sub Status: 0xC0000064

Log Name: Security
Source: Microsoft Windows security
Event ID: 4625
Level: Information
User: N/A
OpCode: Info

Task Category: Logon
Keywords: Audit Failure

Actions

- Win10SecurityLogs
 - Open Saved Log...
 - Create Custom View...
 - Import Custom View...
 - Filter Current Log...
 - Properties
 - Find...
 - Save All Events As...
 - View
- Event 4625, Microsoft Windows security aud...
 - Event Properties
 - Copy
 - Save Selected Events...
 - Refresh
 - Help

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

Event 4798, Microsoft Windows security auditing.

General Details

A user's local group membership was enumerated.

Subject:

- Security ID: [REDACTED]
- Account Name: [REDACTED]
- Account Domain: [REDACTED]
- Logon ID: [REDACTED]

User:

- Security ID: [REDACTED]
- Account Name: [REDACTED]
- Account Domain: [REDACTED]

Process Information:

- Process ID: 0x2114
- Process Name: C:\Windows\explorer.exe

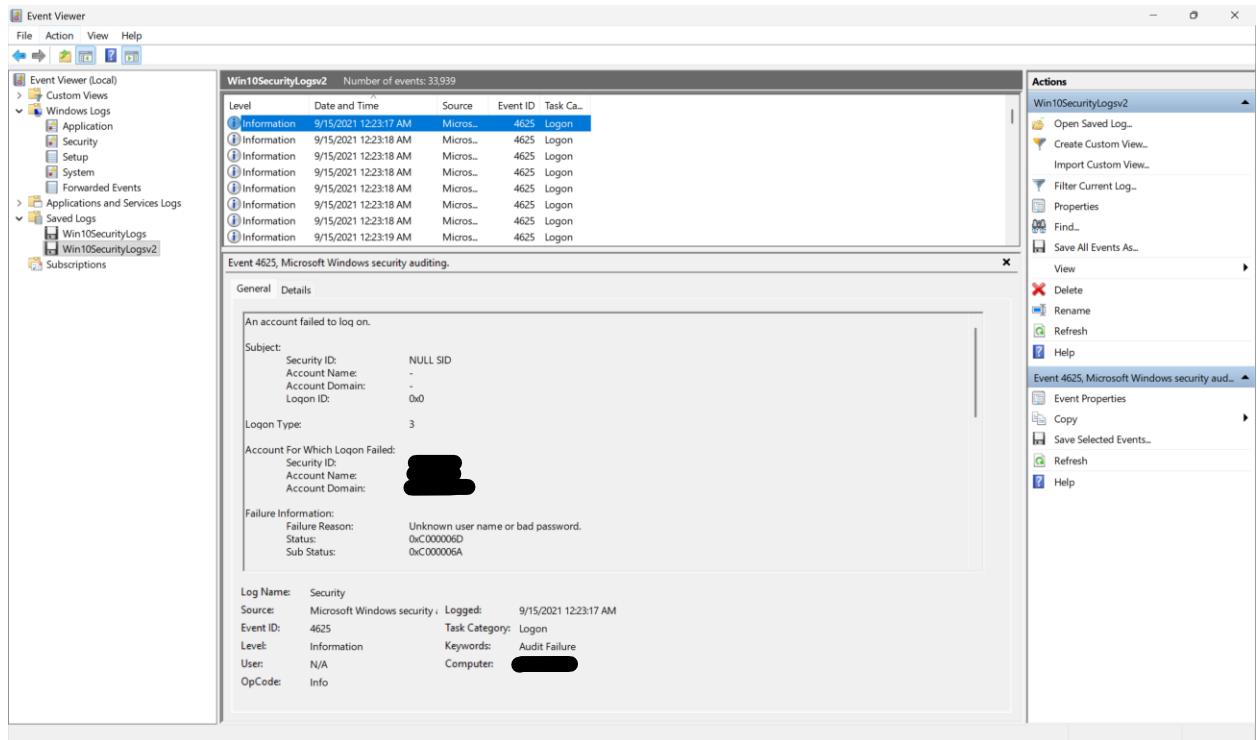
Log Name: Security
Source: Microsoft Windows security
Event ID: 4798
Level: Information
User: N/A
OpCode: Info

Task Category: User Account Management
Keywords: Audit Success

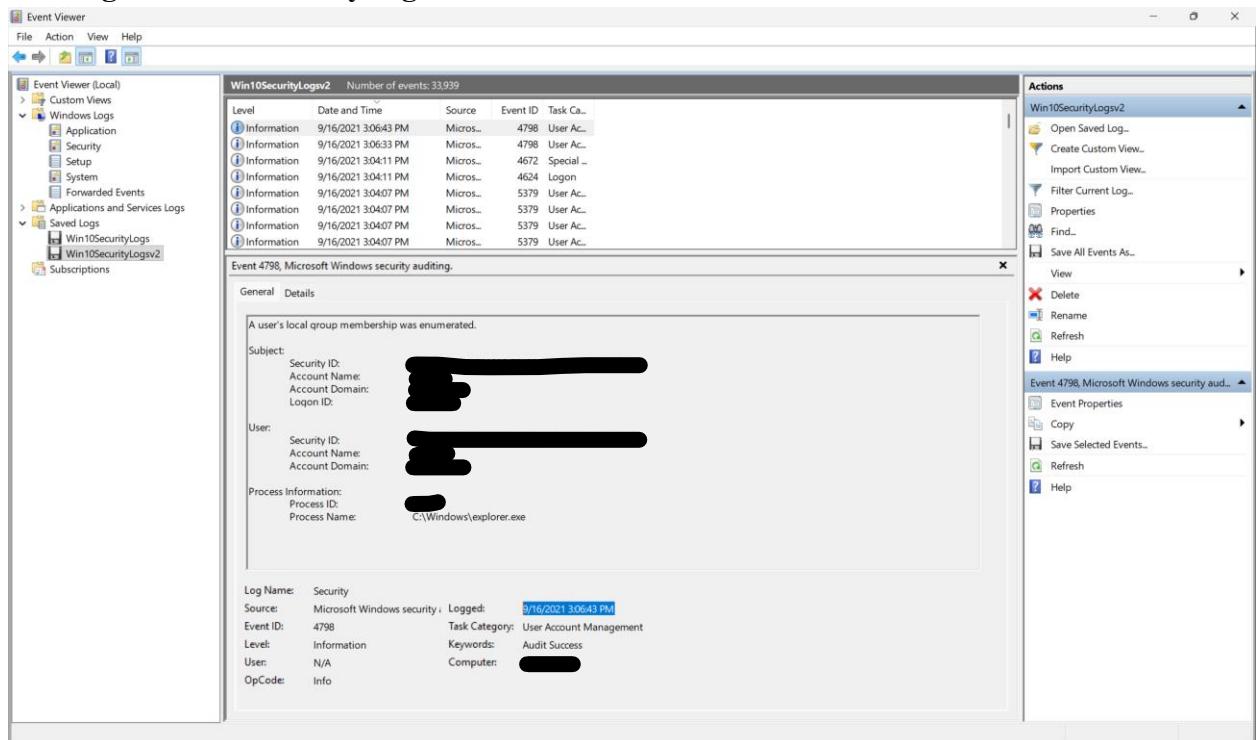
Actions

- Win10SecurityLogs
 - Open Saved Log...
 - Create Custom View...
 - Import Custom View...
 - Filter Current Log...
 - Properties
 - Find...
 - Save All Events As...
 - View
- Event 4798, Microsoft Windows security aud...
 - Event Properties
 - Copy
 - Save Selected Events...
 - Refresh
 - Help

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

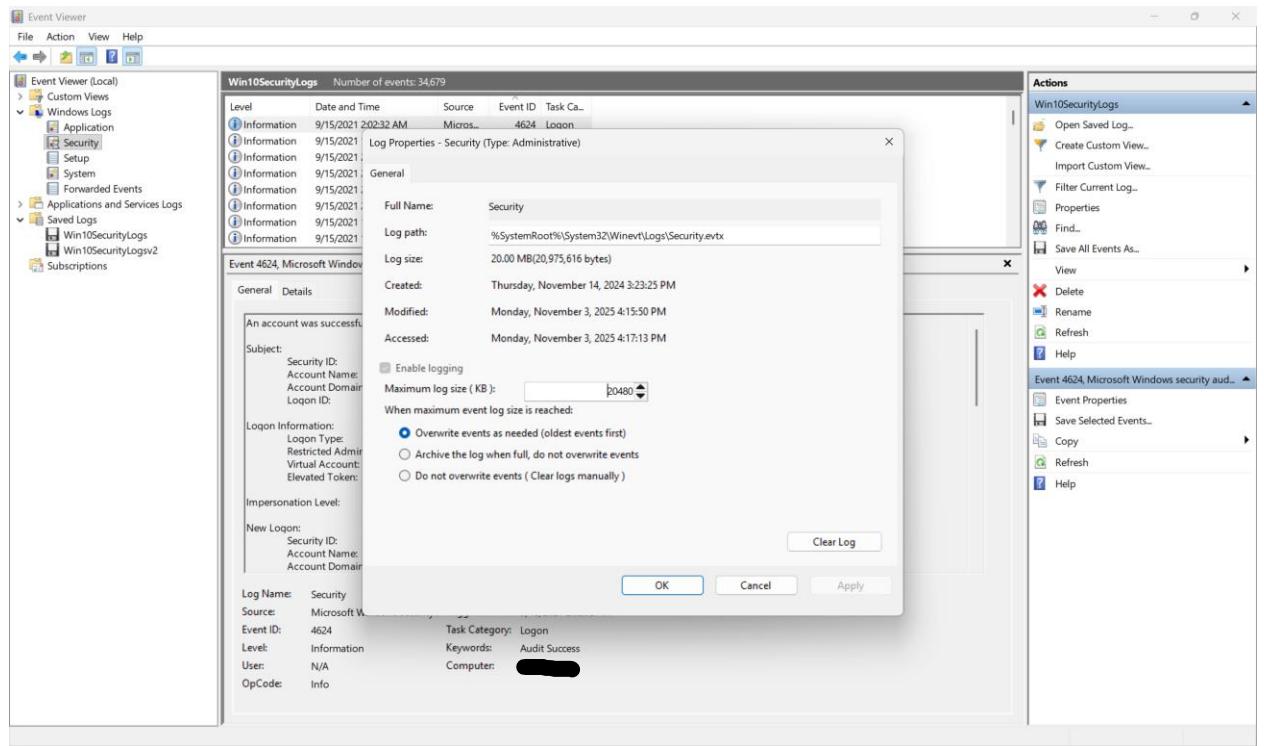
The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with 'Windows Logs' expanded to show 'Application', 'Security', 'Setup', 'System', and 'Forwarded Events'. Under 'Saved Logs', 'Win10SecurityLogs' is selected. The right pane shows a list of events for 'Win10SecurityLogs' with a total count of 34,679. One specific event is highlighted, identified as Event ID 4798, titled 'Microsoft Windows security auditing'. The details pane shows the event's properties: Log Name: Security, Source: Microsoft Windows security audit, Event ID: 4798, Task Category: User Account Management, Level: Information, Keywords: Audit Success, User: N/A, Computer: [REDACTED], and OpCode: Info. The Actions pane on the right lists various options for managing the log.

Win10SecurityLogsv2.evtx: 33,939 events captured

The screenshot shows the Windows Event Viewer interface, similar to the previous one. The left pane shows the same log structure. The right pane displays a list of events for 'Win10SecurityLogsv2' with a total count of 33,939. One specific event is highlighted, identified as Event ID 4798, titled 'Microsoft Windows security auditing'. The details pane shows the event's properties: Log Name: Security, Source: Microsoft Windows security audit, Event ID: 4798, Task Category: User Account Management, Level: Information, Keywords: Audit Success, User: N/A, Computer: [REDACTED], and OpCode: Info. The Actions pane on the right lists various options for managing the log.

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], [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...
[REDACTED]	Information	9/15/2021 12:24:16 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:16 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:17 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:17 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:17 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	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:

Account For Which Logon Failed:

Security ID:	[REDACTED]
Account Name:	[REDACTED]
Account Domain:	[REDACTED]

Failure Information:

Failure Reason: Unknown user name or bad password.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

Task Category: Logon

Keywords: Audit Failure

Computer: [REDACTED]

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...
[REDACTED]	Information	9/15/2021 12:24:16 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:16 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:17 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:17 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	Information	9/15/2021 12:24:18 AM	Micros...	4625 Logon
[REDACTED]	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:

Account For Which Logon Failed:

Security ID:	[REDACTED]
Account Name:	[REDACTED]
Account Domain:	[REDACTED]

Failure Information:

Failure Reason: Unknown user name or bad password.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

Task Category: Logon

Keywords: Audit Failure

Computer: [REDACTED]

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...

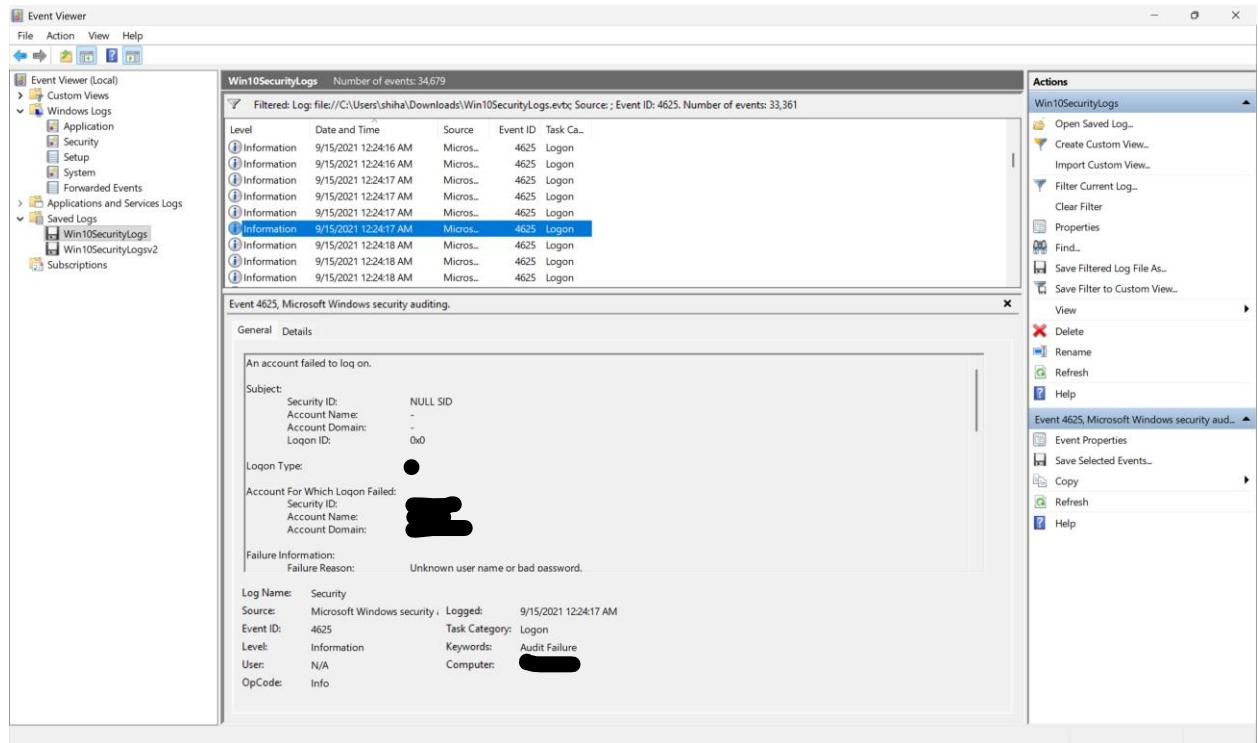
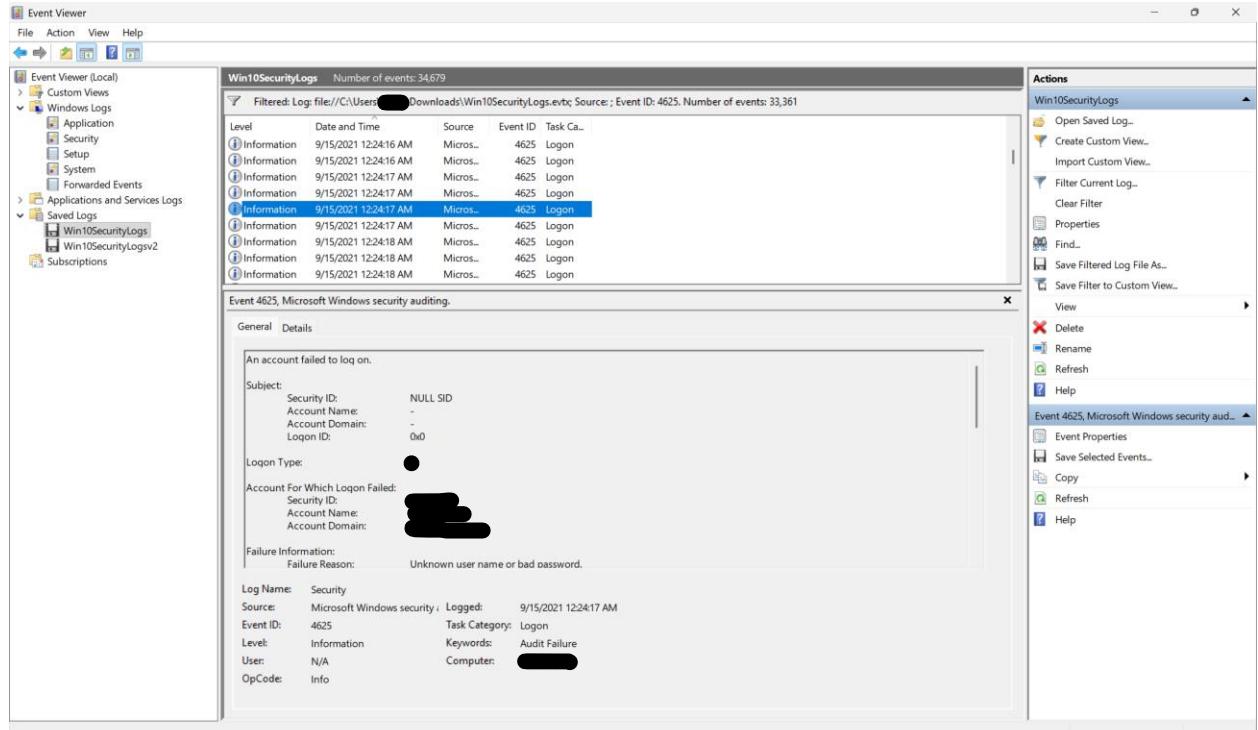
Event Properties

Save Selected Events...

Copy

Refresh

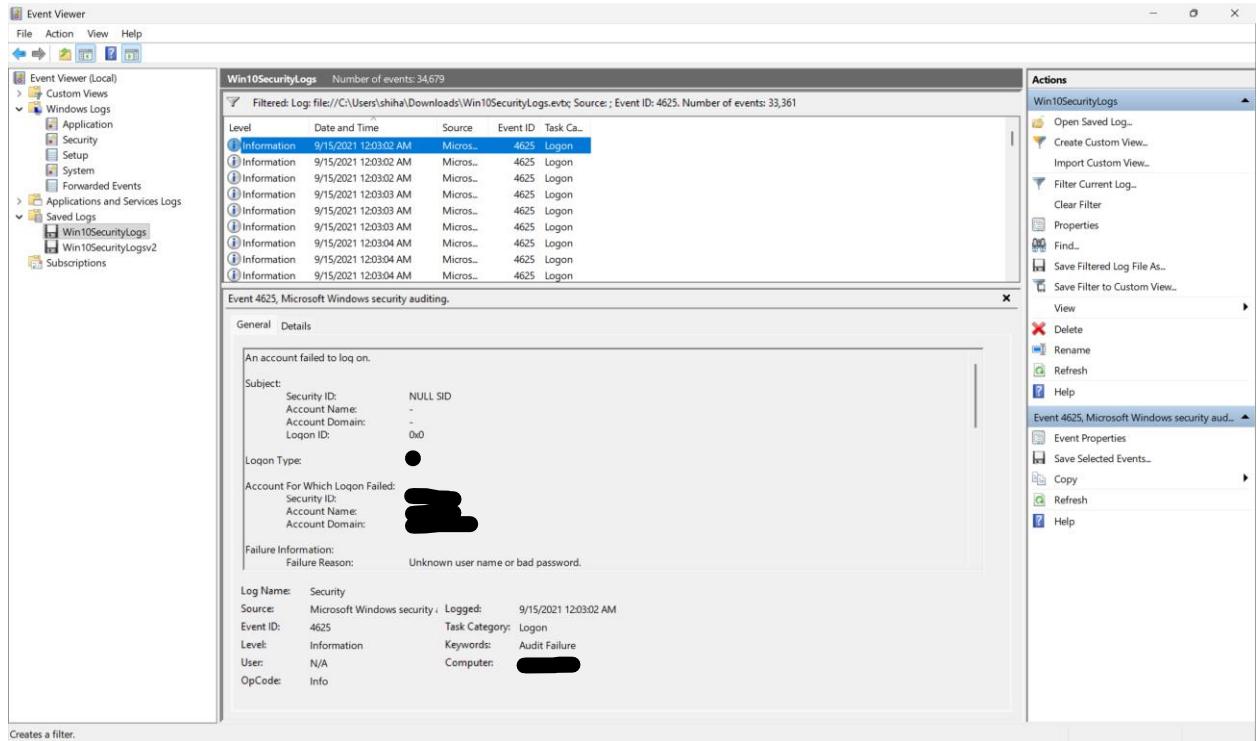
Help



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.

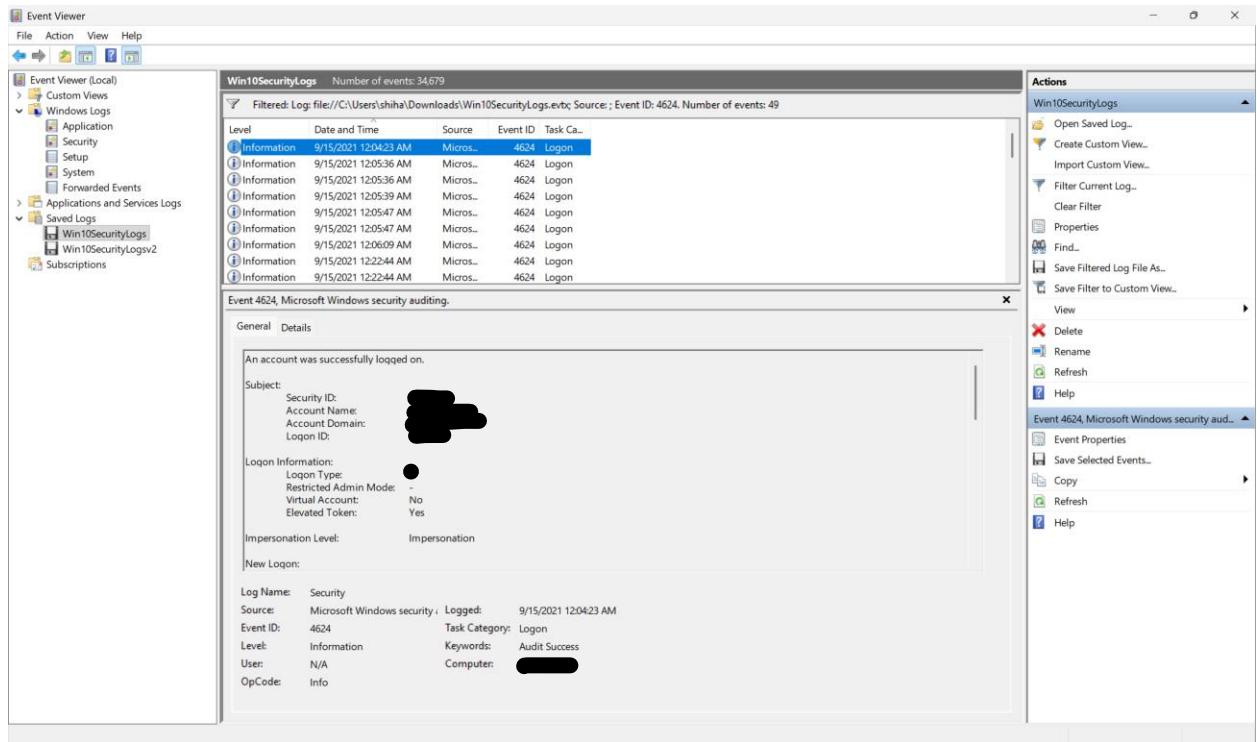


7. What is the vulnerability(ies)? (5 points)

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 [REDACTED], and it is showing me the attack was from [REDACTED]. The IP address range from [REDACTED] - [REDACTED].

[REDACTED] and it points to [REDACTED]

The screenshot shows two windows side-by-side. The left window is the Windows Event Viewer displaying an event properties dialog for Event ID 4625, Microsoft Windows security auditing. The event details show a failed logon attempt where the account name and domain are blank, and the failure reason is "Unknown user name or bad password". The right window is a web browser showing a Whois lookup for an IP address. The results include quick stats like IP location, ASN, and Whois server, followed by a large list of WHOIS metadata fields, many of which are redacted. A notice at the top of the Whois page warns of potential deprecation after January 28, 2025.

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.