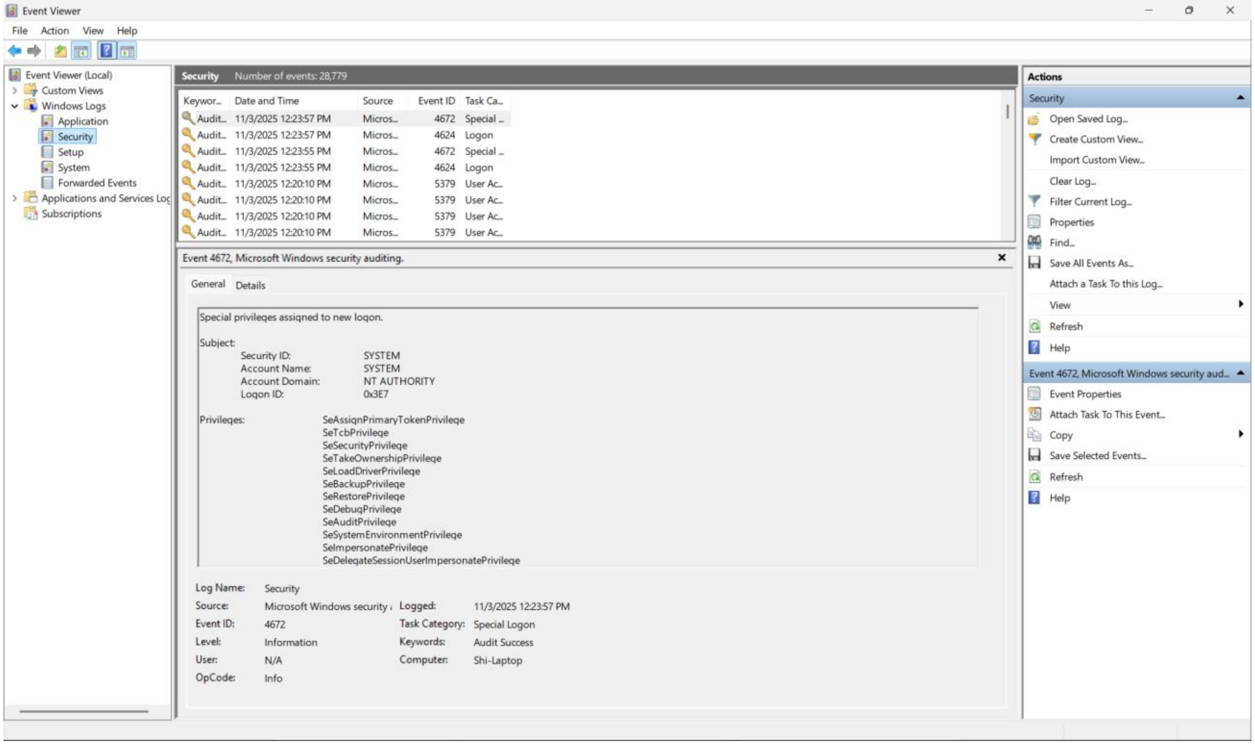
1. **Which built-in Windows utility/tool is used to view the log files? (1 point)**
   The Windows Event Viewer tool is used to view log files.



Security Number of events: 28,779

| Keywor... | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Audit... | 11/3/2025 12:23:57 PM | Micros... | 4672 | Special ... |
| Audit... | 11/3/2025 12:23:57 PM | Micros... | 4624 | Logon |
| Audit... | 11/3/2025 12:23:55 PM | Micros... | 4672 | Special ... |
| Audit... | 11/3/2025 12:23:55 PM | Micros... | 4624 | Logon |
| Audit... | 11/3/2025 12:20:10 PM | Micros... | 5379 | User Ac... |
| Audit... | 11/3/2025 12:20:10 PM | Micros... | 5379 | User Ac... |
| Audit... | 11/3/2025 12:20:10 PM | Micros... | 5379 | User Ac... |
| Audit... | 11/3/2025 12:20:10 PM | Micros... | 5379 | User Ac... |

Event 4672, Microsoft Windows security auditing.

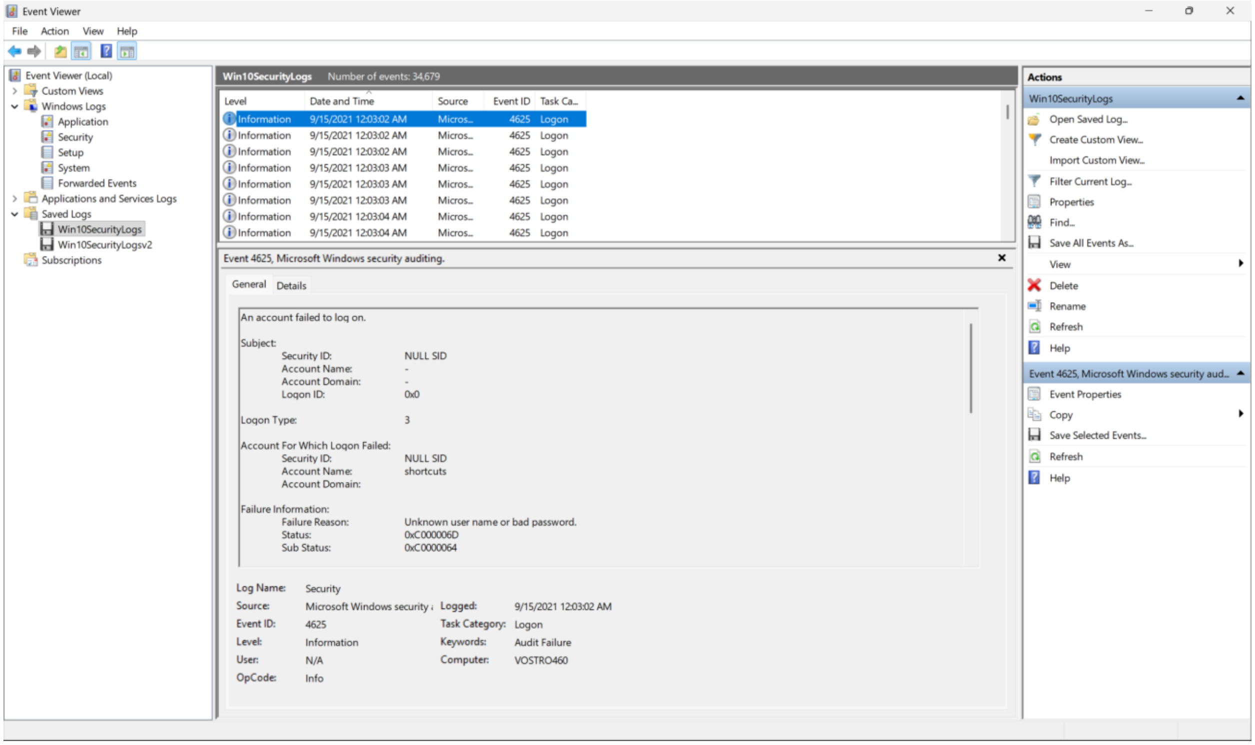
General Details

```
Special privileges assigned to new logon.

Subject:
        Security ID:        SYSTEM
        Account Name:       SYSTEM
        Account Domain:     NT AUTHORITY
        Logon ID:           0x3E7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
                        SeSystemEnvironmentPrivilege
                        SeImpersonatePrivilege
                        SeDelegateSessionUserImpersonatePrivilege
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:          11/3/2025 12:23:57 PM
Event ID:   4672                           Task Category:   Special Logon
Level:      Information                    Keywords:        Audit Success
User:       N/A                            Computer:        Shi-Laptop
OpCode:     Info
```

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

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



Win10SecurityLogs Number of events: 34,679

| Level | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Information | 9/15/2021 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:04 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:04 AM | Micros... | 4625 | Logon |

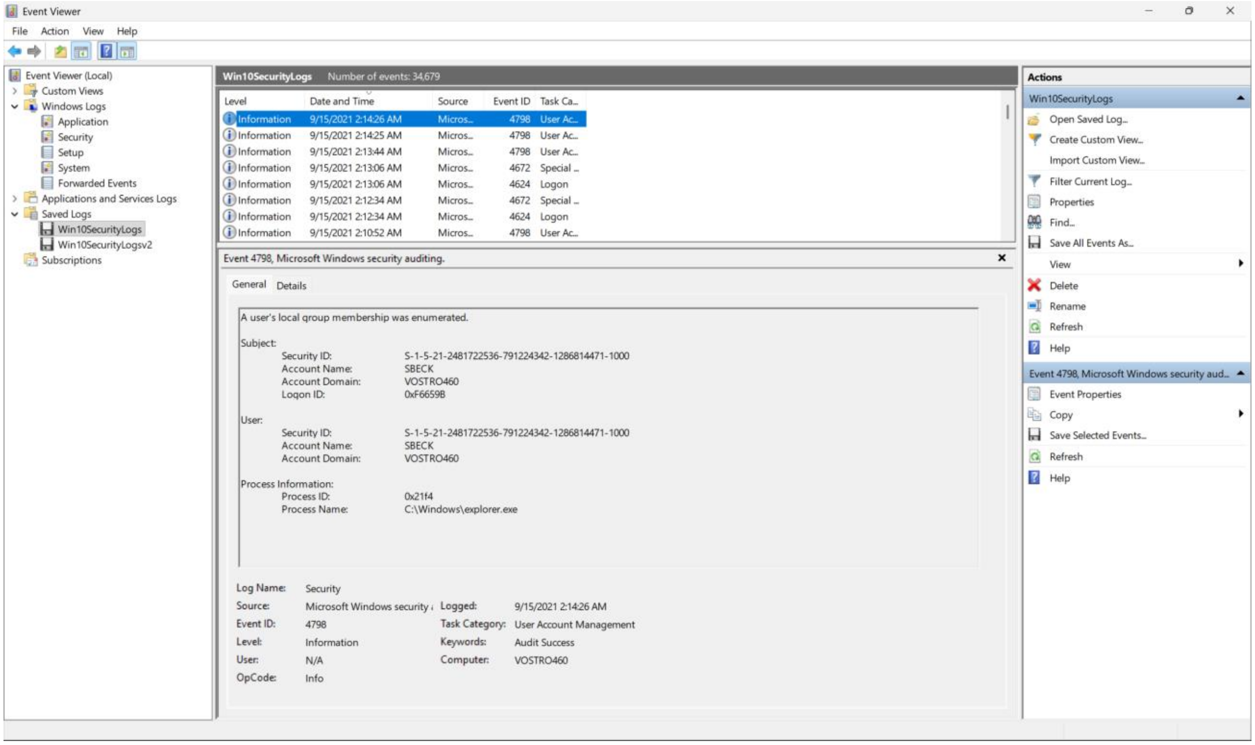
Event 4625, Microsoft Windows security auditing.

General Details

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

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 a  Logged:         9/15/2021 12:03:02 AM
Event ID:   4625                          Task Category:  Logon
Level:      Information                   Keywords:       Audit Failure
User:       N/A                           Computer:       VOSTRO460
OpCode:     Info
```

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



Win10SecurityLogs Number of events: 34,679

| Level | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Information | 9/15/2021 2:14:26 AM | Micros... | 4798 | User Ac... |
| Information | 9/15/2021 2:14:25 AM | Micros... | 4798 | User Ac... |
| Information | 9/15/2021 2:13:44 AM | Micros... | 4798 | User Ac... |
| Information | 9/15/2021 2:13:06 AM | Micros... | 4672 | Special ... |
| Information | 9/15/2021 2:13:06 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 2:12:34 AM | Micros... | 4672 | Special ... |
| Information | 9/15/2021 2:12:34 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 2:10:52 AM | Micros... | 4798 | User Ac... |

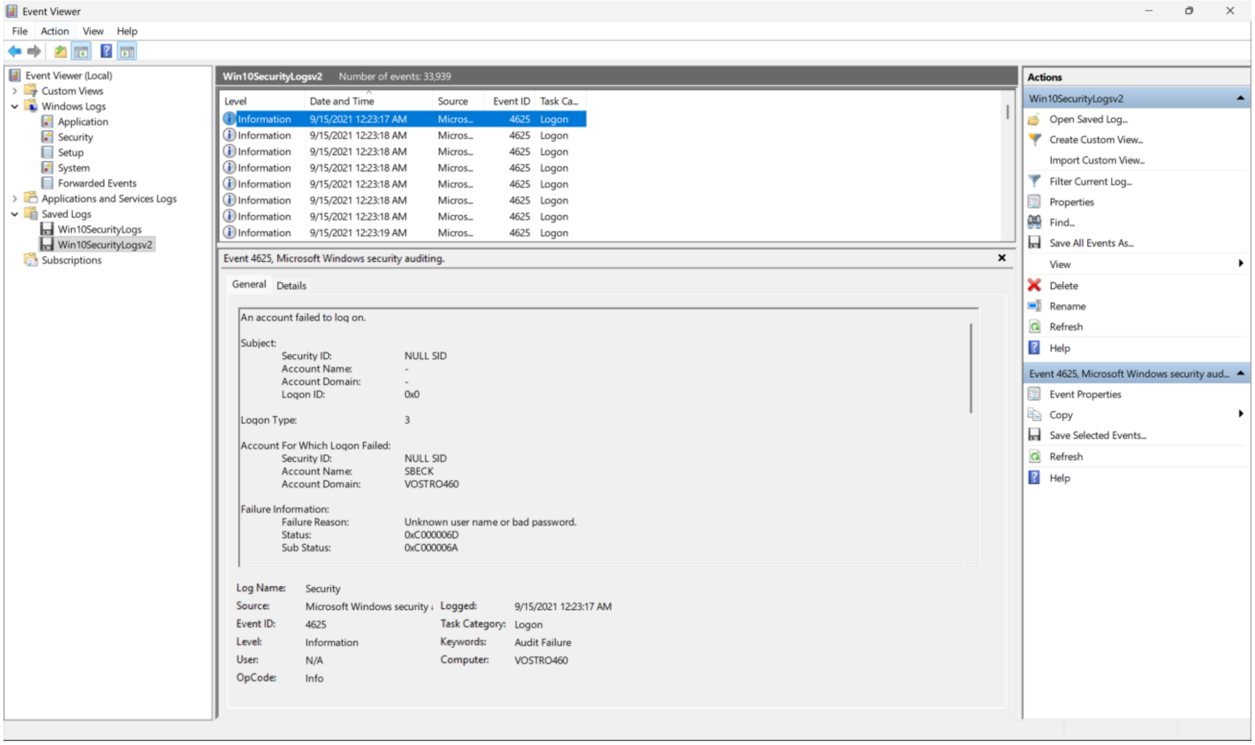
Event 4798, Microsoft Windows security auditing.

General Details

```
A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460
        Logon ID:               0xF6659B

User:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460

Process Information:
        Process ID:             0x21f4
        Process Name:           C:\Windows\explorer.exe
```

```
Log Name:   Security
Source:     Microsoft Windows security a  Logged:         9/15/2021 2:14:26 AM
Event ID:   4798                          Task Category:  User Account Management
Level:      Information                   Keywords:       Audit Success
User:       N/A                           Computer:       VOSTRO460
OpCode:     Info
```

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



Win10SecurityLogsv2 Number of events: 33,939

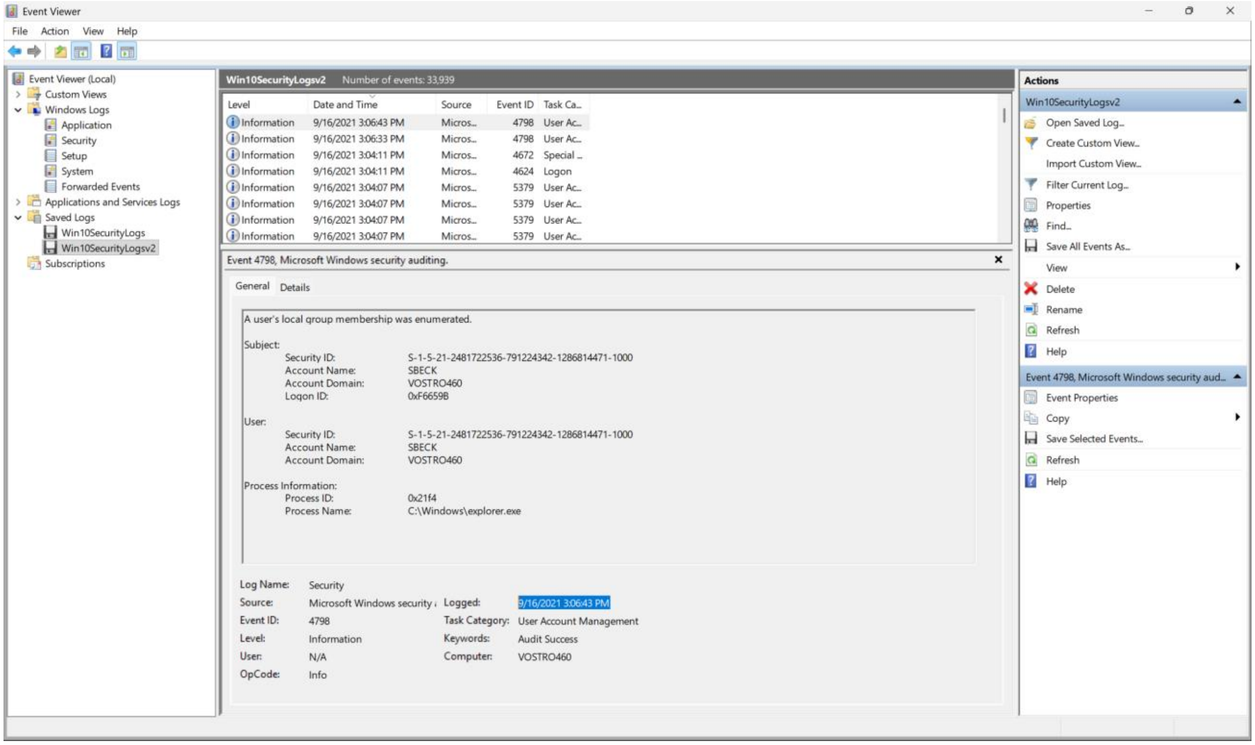
| Level | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Information | 9/15/2021 12:23:17 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:18 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:23:19 AM | Micros... | 4625 | Logon |

Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           SBECK
        Account Domain:         VOSTRO460

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:         9/15/2021 12:23:17 AM
Event ID:   4625                           Task Category:  Logon
Level:      Information                    Keywords:       Audit Failure
User:       N/A                            Computer:       VOSTRO460
OpCode:     Info
```

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



Win10SecurityLogsv2 Number of events: 33,939

| Level | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Information | 9/16/2021 3:06:43 PM | Micros... | 4798 | User Ac... |
| Information | 9/16/2021 3:06:33 PM | Micros... | 4798 | User Ac... |
| Information | 9/16/2021 3:04:11 PM | Micros... | 4672 | Special ... |
| Information | 9/16/2021 3:04:11 PM | Micros... | 4624 | Logon |
| Information | 9/16/2021 3:04:07 PM | Micros... | 5379 | User Ac... |
| Information | 9/16/2021 3:04:07 PM | Micros... | 5379 | User Ac... |
| Information | 9/16/2021 3:04:07 PM | Micros... | 5379 | User Ac... |
| Information | 9/16/2021 3:04:07 PM | Micros... | 5379 | User Ac... |

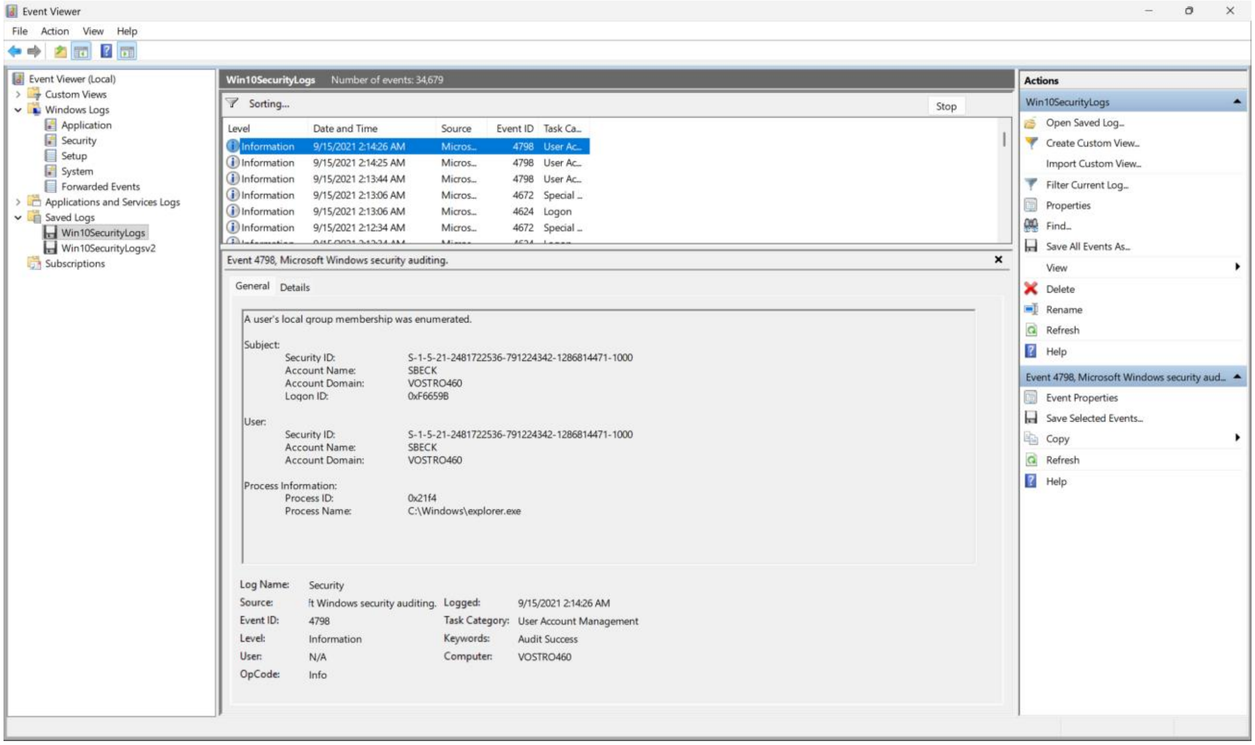
Event 4798, Microsoft Windows security auditing.

```
A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460
        Logon ID:               0xF6659B

User:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460

Process Information:
        Process ID:             0x21f4
        Process Name:           C:\Windows\explorer.exe
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:         9/16/2021 3:06:43 PM
Event ID:   4798                           Task Category:  User Account Management
Level:      Information                    Keywords:       Audit Success
User:       N/A                            Computer:       VOSTRO460
OpCode:     Info
```

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

**Win10SecurityLogs.evtx:** 34,679 events captured



Win10SecurityLogs   Number of events: 34,679

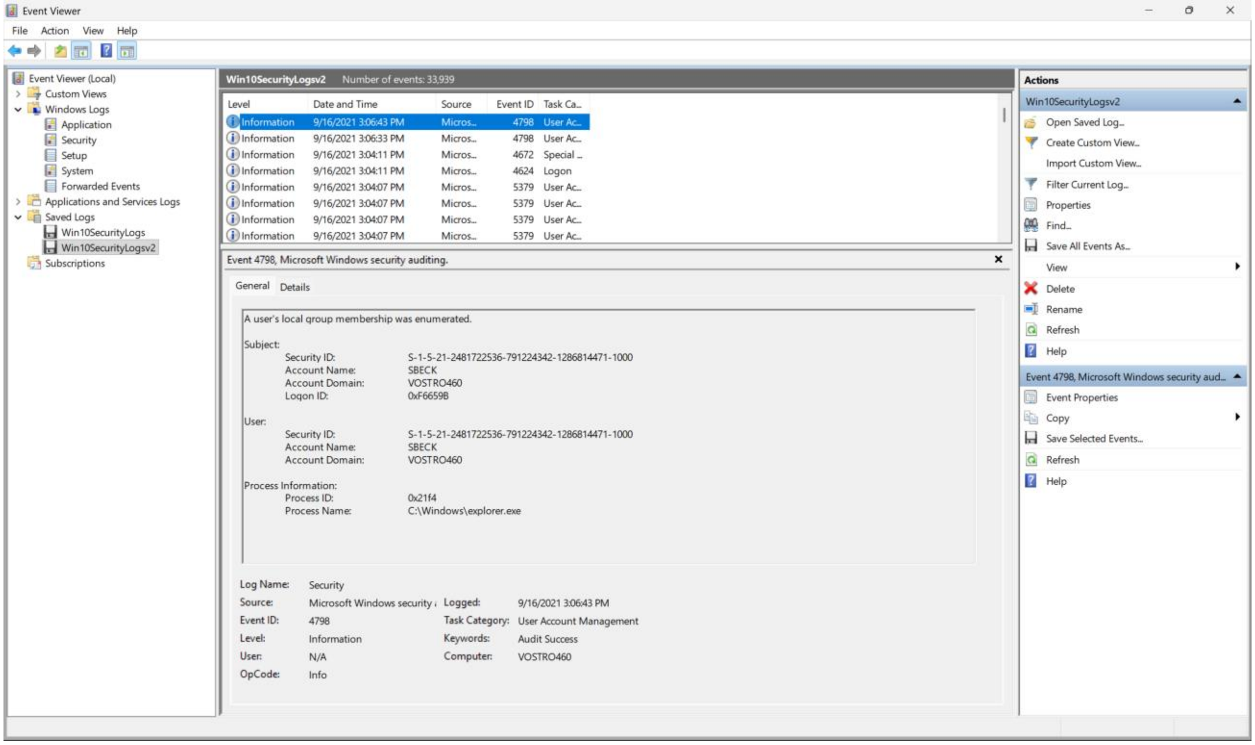
```
Level         Date and Time          Source    Event ID  Task Ca...
Information   9/15/2021 2:14:26 AM   Micros...     4798  User Ac...
Information   9/15/2021 2:14:25 AM   Micros...     4798  User Ac...
Information   9/15/2021 2:13:44 AM   Micros...     4798  User Ac...
Information   9/15/2021 2:13:06 AM   Micros...     4672  Special ...
Information   9/15/2021 2:13:06 AM   Micros...     4624  Logon
Information   9/15/2021 2:12:34 AM   Micros...     4672  Special ...
```

Event 4798, Microsoft Windows security auditing.

```
A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460
        Logon ID:               0xF6659B

User:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460

Process Information:
        Process ID:             0x21f4
        Process Name:           C:\Windows\explorer.exe
```

```
Log Name:   Security
Source:     ft Windows security auditing.   Logged:          9/15/2021 2:14:26 AM
Event ID:   4798                            Task Category:   User Account Management
Level:      Information                     Keywords:        Audit Success
User:       N/A                             Computer:        VOSTRO460
OpCode:     Info
```

**Win10SecurityLogsv2.evtx:** 33,939 events captured



Win10SecurityLogsv2   Number of events: 33,939

```
Level         Date and Time          Source    Event ID  Task Ca...
Information   9/16/2021 3:06:43 PM   Micros...     4798  User Ac...
Information   9/16/2021 3:06:33 PM   Micros...     4798  User Ac...
Information   9/16/2021 3:04:11 PM   Micros...     4672  Special ...
Information   9/16/2021 3:04:11 PM   Micros...     4624  Logon
Information   9/16/2021 3:04:07 PM   Micros...     5379  User Ac...
Information   9/16/2021 3:04:07 PM   Micros...     5379  User Ac...
Information   9/16/2021 3:04:07 PM   Micros...     5379  User Ac...
Information   9/16/2021 3:04:07 PM   Micros...     5379  User Ac...
```

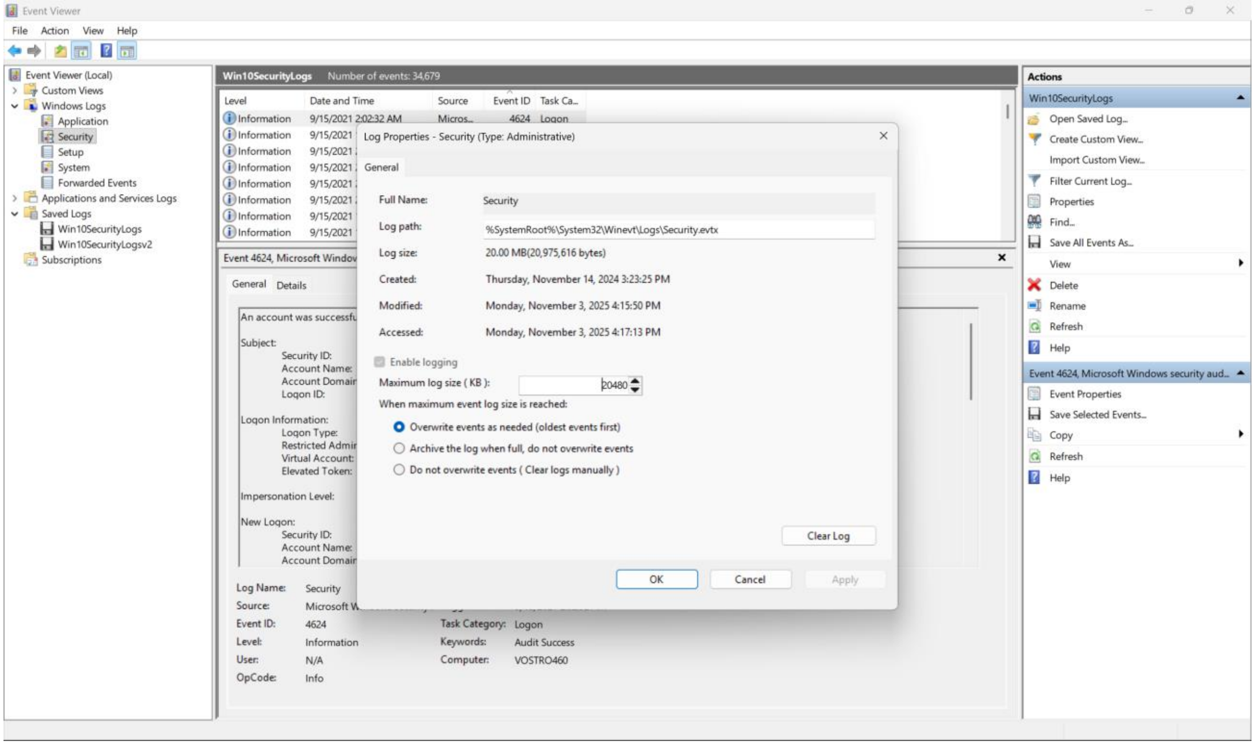
Event 4798, Microsoft Windows security auditing.

```
A user's local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460
        Logon ID:               0xF6659B

User:
        Security ID:            S-1-5-21-2481722536-791224342-1286814471-1000
        Account Name:           SBECK
        Account Domain:         VOSTRO460

Process Information:
        Process ID:             0x21f4
        Process Name:           C:\Windows\explorer.exe
```

```
Log Name:   Security
Source:     Microsoft Windows security a    Logged:          9/16/2021 3:06:43 PM
Event ID:   4798                            Task Category:   User Account Management
Level:      Information                     Keywords:        Audit Success
User:       N/A                             Computer:        VOSTRO460
OpCode:     Info
```

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.



Win10SecurityLogs Number of events: 34,679

```
Level        Date and Time          Source   Event ID  Task Ca...
Information  9/15/2021 2:02:32 AM   Micros...    4624  Logon
Information  9/15/2021
Information  9/15/2021
Information  9/15/2021
Information  9/15/2021
Information  9/15/2021
Information  9/15/2021
Information  9/15/2021
```

Log Properties - Security (Type: Administrative)

- Full Name: Security
- Log path: %SystemRoot%\System32\Winevt\Logs\Security.evtx
- Log size: 20.00 MB(20,975,616 bytes)
- Created: Thursday, November 14, 2024 3:23:25 PM
- Modified: Monday, November 3, 2025 4:15:50 PM
- Accessed: Monday, November 3, 2025 4:17:13 PM

☑ Enable logging

Maximum log size ( KB ): 20480

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

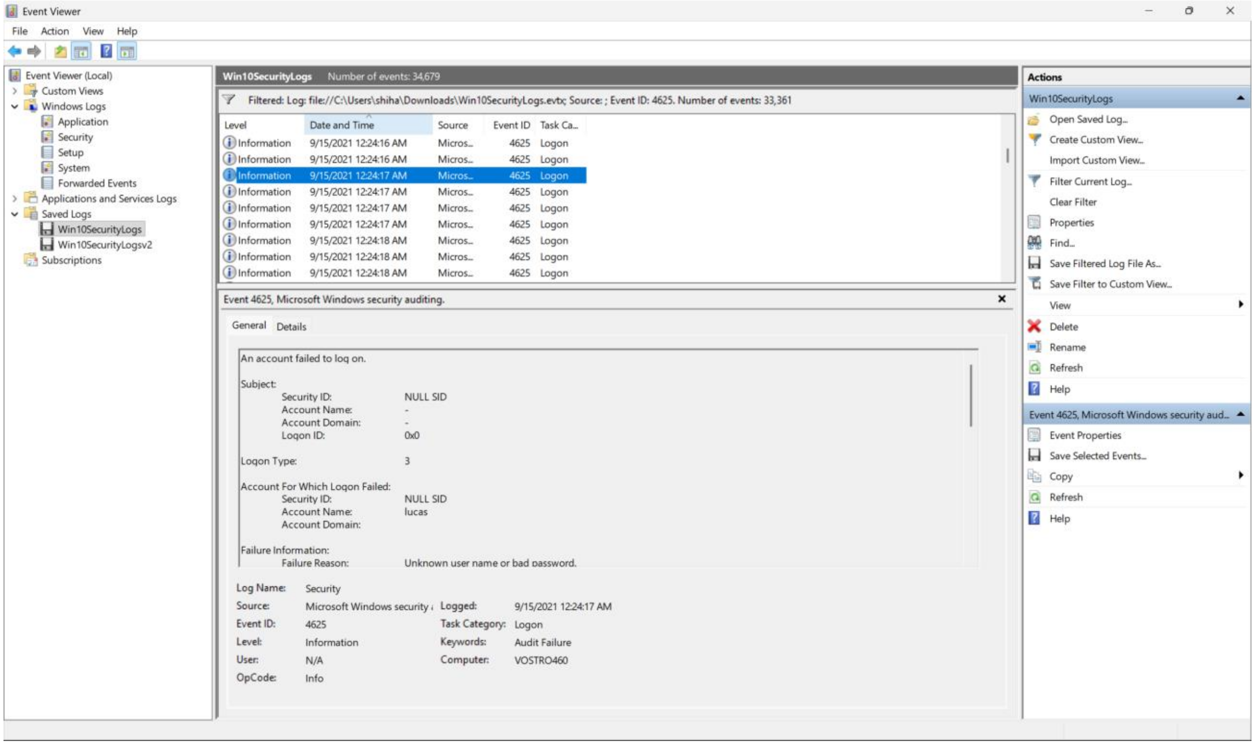
○ Do not overwrite events ( Clear logs manually )

Event 4624, Microsoft Window

```
An account was successfu

Subject:
        Security ID:
        Account Name:
        Account Domair
        Logon ID:

Logon Information:
        Logon Type:
        Restricted Admir
        Virtual Account:
        Elevated Token:

Impersonation Level:

New Logon:
        Security ID:
        Account Name:
        Account Domair
```

```
Log Name:   Security
Source:     Microsoft W
Event ID:   4624          Task Category:  Logon
Level:      Information   Keywords:       Audit Success
User:       N/A           Computer:       VOSTRO460
OpCode:     Info
```

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 lucas, SBECK, administrator, and denise.



Win10SecurityLogs Number of events: 34,679

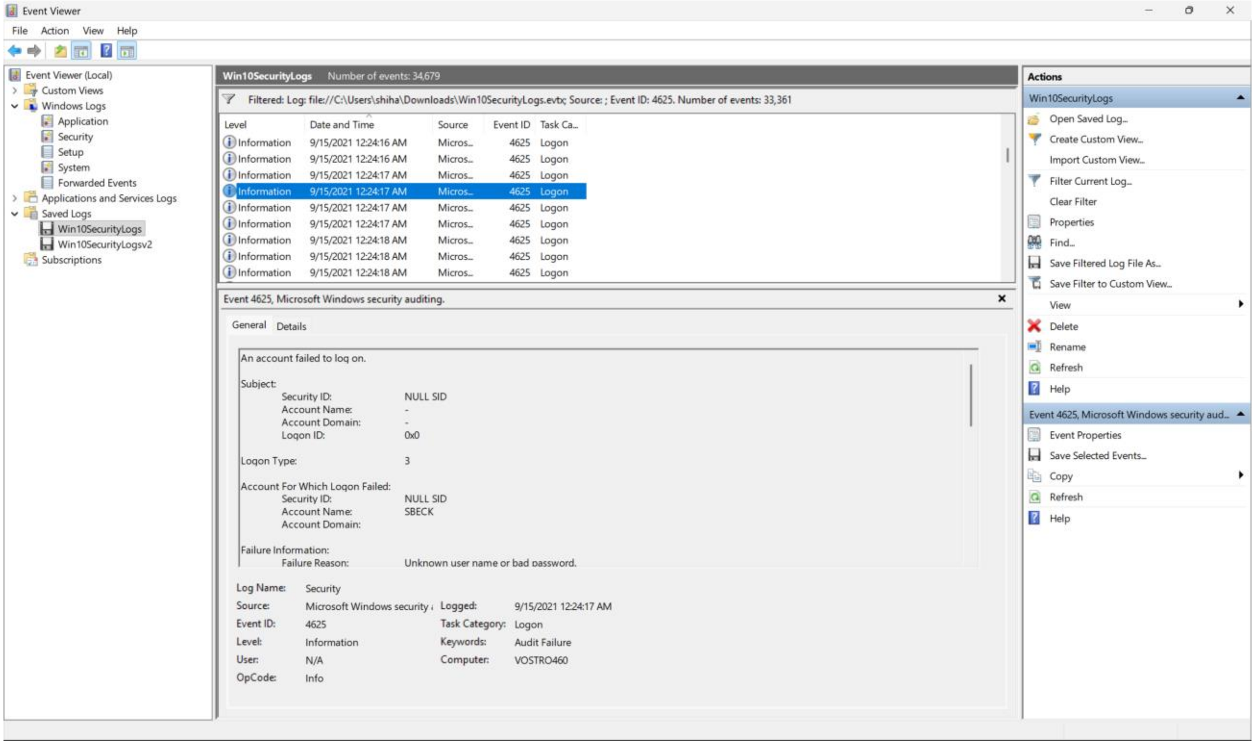
Filtered: Log: file://C:\Users\shiha\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4625. Number of events: 33,361

```
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.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           lucas
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:         9/15/2021 12:24:17 AM
Event ID:   4625                           Task Category:  Logon
Level:      Information                    Keywords:       Audit Failure
User:       N/A                            Computer:       VOSTRO460
OpCode:     Info
```



Win10SecurityLogs Number of events: 34,679

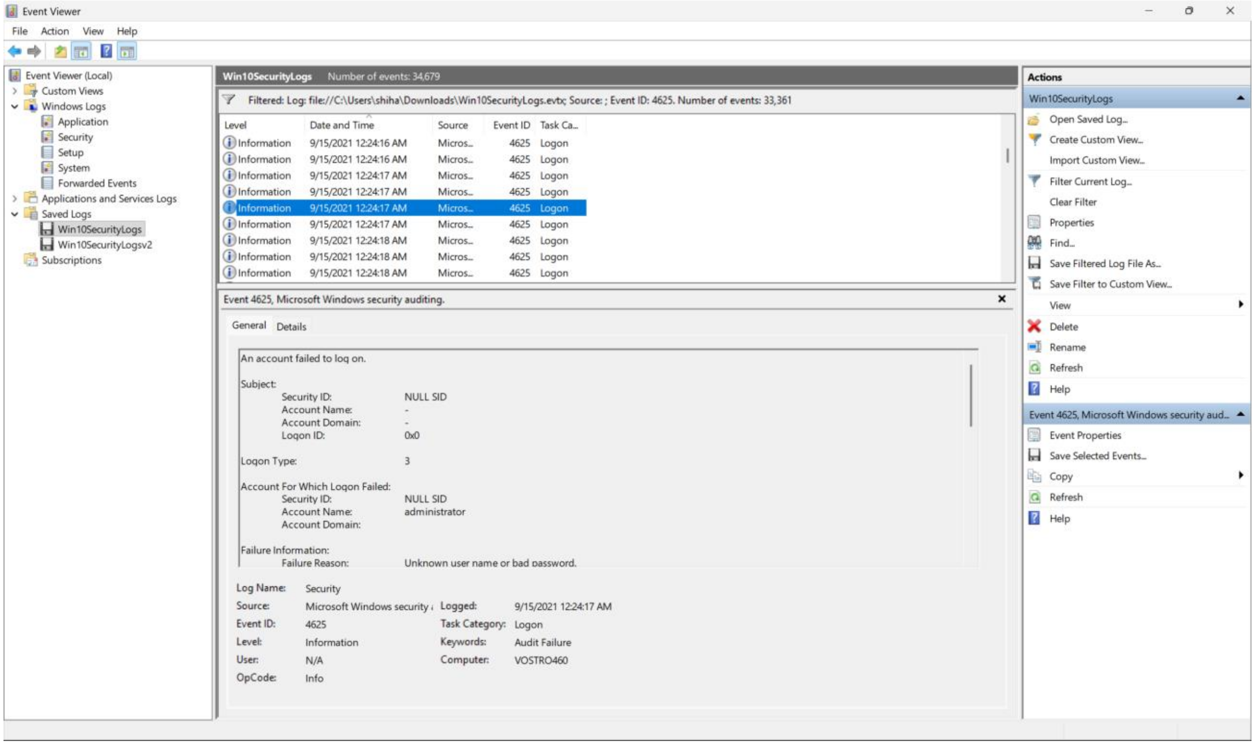
Filtered: Log: file://C:\Users\shiha\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4625. Number of events: 33,361

```
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
```

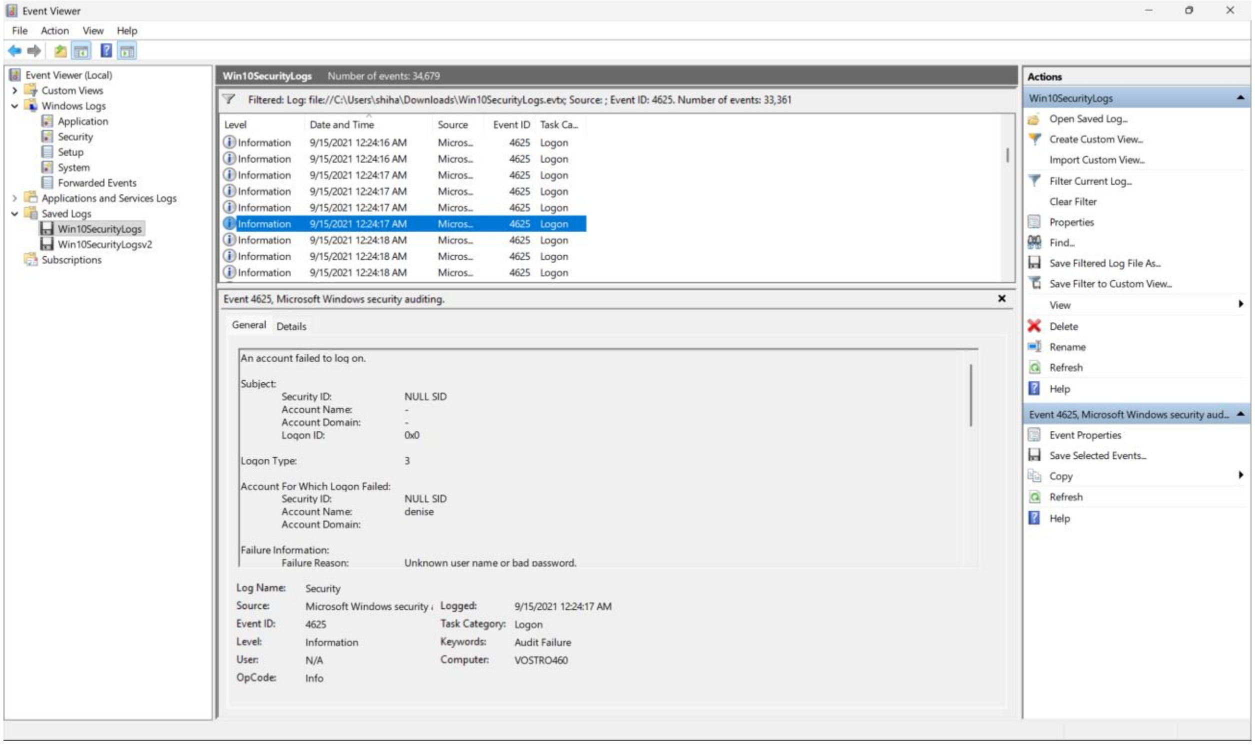
Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           SBECK
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
```

```
Log Name:   Security
Source:     Microsoft Windows security a   Logged:         9/15/2021 12:24:17 AM
Event ID:   4625                           Task Category:  Logon
Level:      Information                    Keywords:       Audit Failure
User:       N/A                            Computer:       VOSTRO460
OpCode:     Info
```



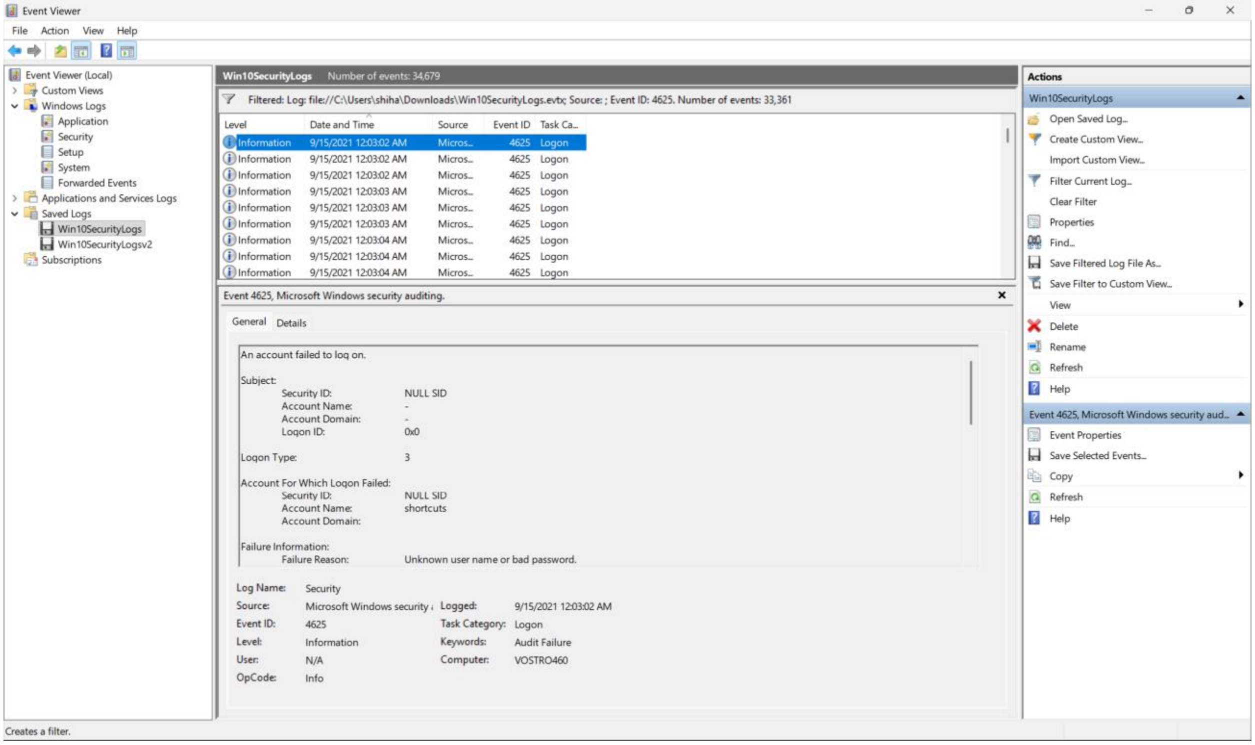
```
Win10SecurityLogs   Number of events: 34,679
Filtered: Log: file://C:\Users\shiha\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4625. Number of events: 33,361

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.

An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           administrator
        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:       VOSTRO460
OpCode:     Info
```



```
Win10SecurityLogs   Number of events: 34,679
Filtered: Log: file://C:\Users\shiha\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.

An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           denise
        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:       VOSTRO460
OpCode:     Info
```

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.



Win10SecurityLogs Number of events: 34,679

Filtered: Log: file://C:\Users\shiha\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 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:02 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:03 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:04 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:04 AM | Micros... | 4625 | Logon |
| Information | 9/15/2021 12:03:04 AM | Micros... | 4625 | Logon |

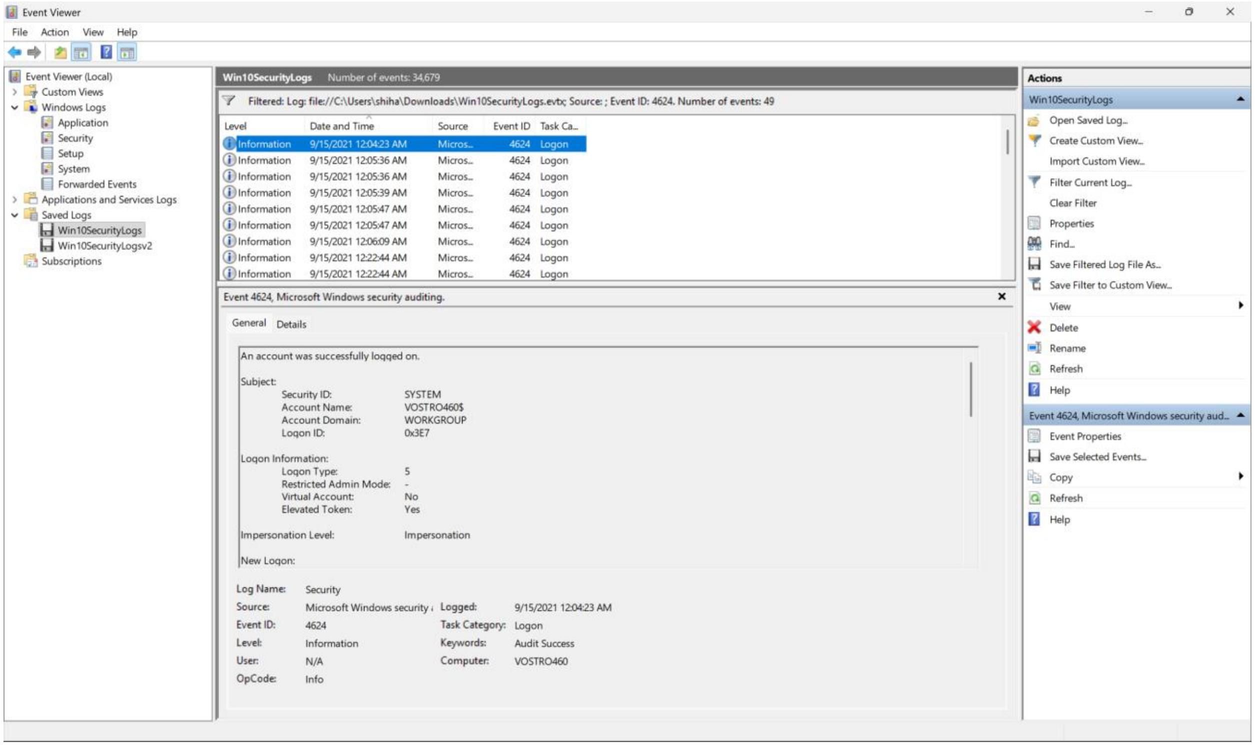
Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           shortcuts
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
```

| | | | |
|---|---|---|---|
| Log Name: | Security | | |
| Source: | Microsoft Windows security ‹ | Logged: | 9/15/2021 12:03:02 AM |
| Event ID: | 4625 | Task Category: | Logon |
| Level: | Information | Keywords: | Audit Failure |
| User: | N/A | Computer: | VOSTRO460 |
| OpCode: | Info | | |

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.



Win10SecurityLogs Number of events: 34,679

Filtered: Log: file://C:\Users\shiha\Downloads\Win10SecurityLogs.evtx; Source: ; Event ID: 4624. Number of events: 49

| Level | Date and Time | Source | Event ID | Task Ca... |
|---|---|---|---|---|
| Information | 9/15/2021 12:04:23 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:05:36 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:05:36 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:05:39 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:05:47 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:05:47 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:06:09 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:22:44 AM | Micros... | 4624 | Logon |
| Information | 9/15/2021 12:22:44 AM | Micros... | 4624 | Logon |

Event 4624, Microsoft Windows security auditing.

General Details

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           VOSTRO460$
        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:
```

```
Log Name:   Security
Source:     Microsoft Windows security    Logged:         9/15/2021 12:04:23 AM
Event ID:   4624                          Task Category:  Logon
Level:      Information                   Keywords:       Audit Success
User:       N/A                           Computer:       VOSTRO460
OpCode:     Info
```

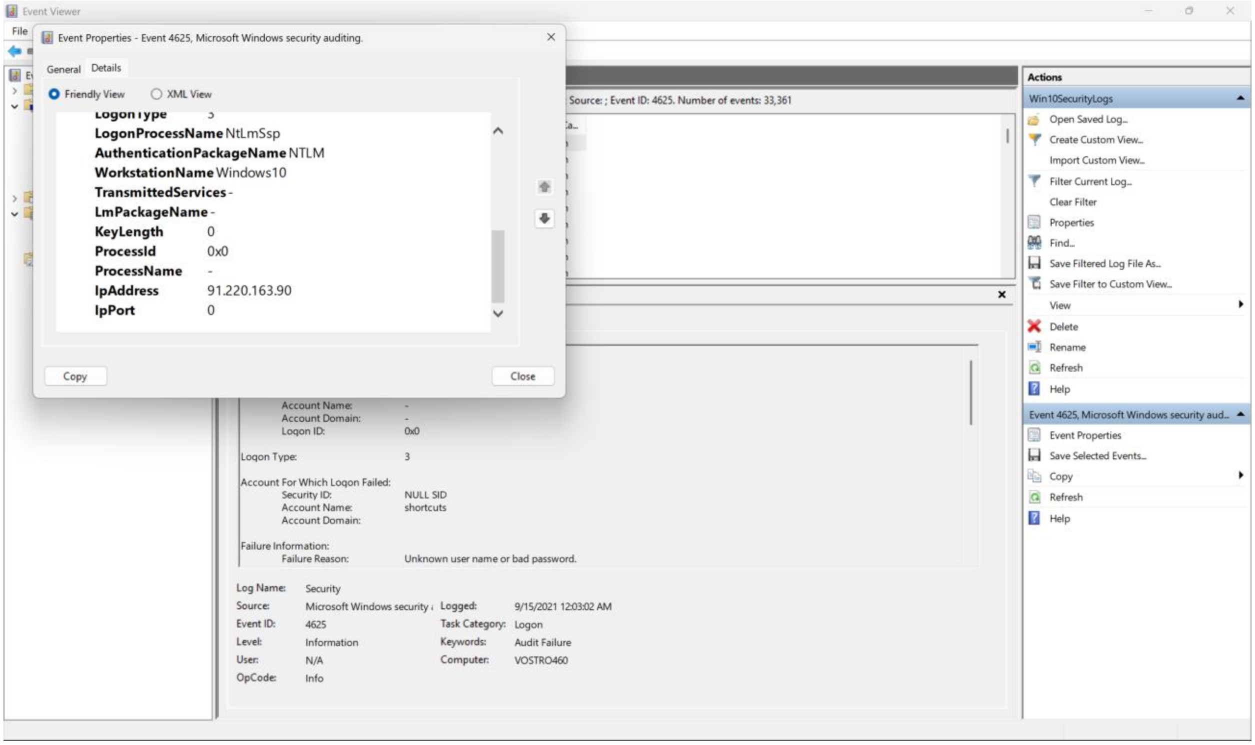
**9. What was most likely the motivation for the attack? (3 points)**

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 (91.220.163.90), and it is showing me the attack was from Russia. The IP address range from 91.220.163.0 -

91.220.163.255 and it points to *Russian Federation Sankt-peterburg Media Land LLC.*



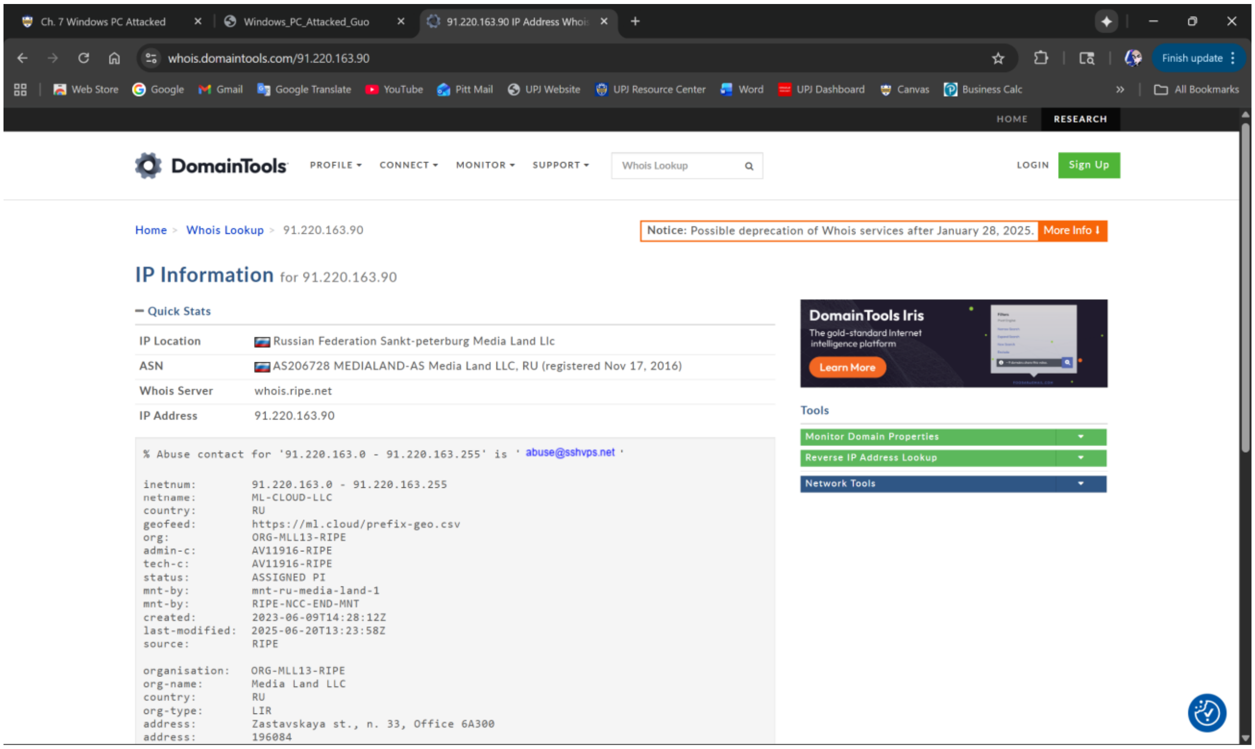
Source: ; Event ID: 4625. Number of events: 33,361

Event Properties - Event 4625, Microsoft Windows security auditing.

● Friendly View ○ XML View

```
LogonType                  3
LogonProcessName NtLmSsp
AuthenticationPackageName NTLM
WorkstationName Windows10
TransmittedServices -
LmPackageName -
KeyLength         0
ProcessId         0x0
ProcessName       -
IpAddress         91.220.163.90
IpPort            0
```

```
        Account Name:          -
        Account Domain:        -
        Logon ID:              0x0

Logon Type:                    3

Account For Which Logon Failed:
        Security ID:           NULL SID
        Account Name:          shortcuts
        Account Domain:

Failure Information:
        Failure Reason:        Unknown user name or bad password.

Log Name:   Security
Source:     Microsoft Windows security   Logged:         9/15/2021 12:03:02 AM
Event ID:   4625                         Task Category:  Logon
Level:      Information                  Keywords:       Audit Failure
User:       N/A                          Computer:       VOSTRO460
OpCode:     Info
```



Home > Whois Lookup > 91.220.163.90

Notice: Possible deprecation of Whois services after January 28, 2025. More Info

## IP Information for 91.220.163.90

Quick Stats

| | |
|---|---|
| IP Location | Russian Federation Sankt-peterburg Media Land Llc |
| ASN | AS206728 MEDIALAND-AS Media Land LLC, RU (registered Nov 17, 2016) |
| Whois Server | whois.ripe.net |
| IP Address | 91.220.163.90 |

```
% Abuse contact for '91.220.163.0 - 91.220.163.255' is ' abuse@sshvps.net '

inetnum:        91.220.163.0 - 91.220.163.255
netname:        ML-CLOUD-LLC
country:        RU
geofeed:        https://ml.cloud/prefix-geo.csv
org:            ORG-MLL13-RIPE
admin-c:        AV11916-RIPE
tech-c:         AV11916-RIPE
status:         ASSIGNED PI
mnt-by:         mnt-ru-media-land-1
mnt-by:         RIPE-NCC-END-MNT
created:        2023-06-09T14:28:12Z
last-modified:  2025-06-20T13:23:58Z
source:         RIPE

organisation:   ORG-MLL13-RIPE
org-name:       Media Land LLC
country:        RU
org-type:       LIR
address:        Zastavskaya st., n. 33, Office 6A300
address:        196084
```

**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.