

# Day 2: Windows Security Logs Analysis — Event IDs 4624, 4625, 4740, 4732, and 4672

## Objective

The goal of this lab is to learn how to use Windows Security Logs to detect and investigate authentication and account-management activity. I set up a controlled lab environment, enable auditing, and perform specific actions so I can observe the corresponding Security events. The lab teaches me how to:

- identify successful and failed logons,
- detect account lockouts,
- track group membership changes, and
- recognize when special privileges are assigned to a logon.

These skills help me perform baseline SOC analyst tasks: monitoring, triage, and basic incident investigation using Windows Event Viewer.

**Step 1:** A local user is created. This ensures the account exists **locally**, is visible to the `net user`, and logs all events on this VM.

```
PS C:\Windows\system32> net user jsmith 1234567 /add
The account already exists.

More help is available by typing NET HELPMSG 2224.

PS C:\Windows\system32> # try correct password (should produce a successful 4624)
PS C:\Windows\system32> net use \\127.0.0.1\IPC$ /user:jsmith 1234567
The command completed successfully.
```

**Step 2:** Enable auditing

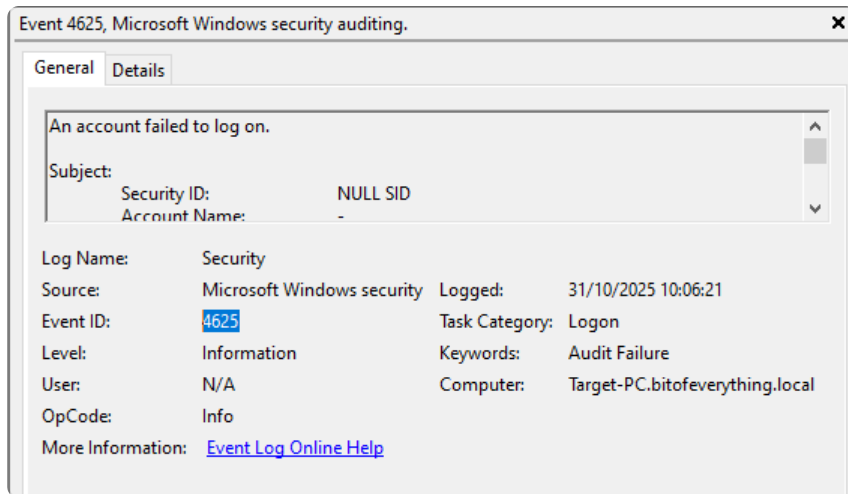
```
Administrator: Windows PowerShell

PS C:\Windows\system32> # logon auditing
PS C:\Windows\system32> auditpol /set /subcategory:"Logon" /success:enable /failure:enable
The command was successfully executed.
PS C:\Windows\system32>
PS C:\Windows\system32> # User account management auditing
PS C:\Windows\system32> auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
The command was successfully executed.
PS C:\Windows\system32>
PS C:\Windows\system32> # Special logon (for privilege escalation)
PS C:\Windows\system32> auditpol /set /subcategory:"Special Logon" /success:enable
The command was successfully executed.
PS C:\Windows\system32>
```

**Step 3:** Generate security events and analyze them using Event Viewer.

- **Event ID 4625:** Failed Logon.

This event indicates an authentication failure. In the screenshot, I show the attempted Account Name, Failure Status/SubStatus, Logon Type, and Source Network Address so I can determine why and where the failure occurs.



- **Event ID 4740:** Account Lockout.

This event indicates that the account exceeds the lockout threshold and becomes locked. In the screenshot, I show the Target Account and Caller Computer to attribute the lockout.



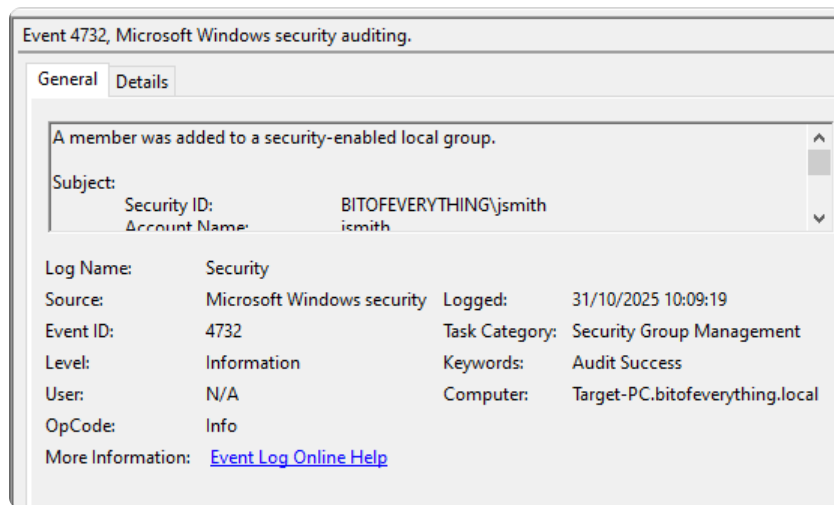
- **Event ID 4624:** Successful Logon.

This event indicates that the account was authenticated successfully. In the screenshot, I show the Account Name, Logon Type, Source Network Address, and Subject fields to verify the logon context.



- **Event ID 4732:** A user was added to a security-enabled local group.

This event indicates a change in group membership. In the screenshot, I show the Group Name, New Member, and the Subject (who made the change).



**Event ID 4672:** Special privileges assigned to a new logon (Privilege escalation)

This event indicates that a privileged account or a logon with elevated rights occurs. In the screenshot, I show the Account Name and the list of assigned privileges to confirm the escalation context.



## Conclusion

In this lab, I validate that Windows Security Logs capture the key authentication and account-management events a SOC analyst needs to monitor. I create a local test account and enable auditing so that all relevant events land on the VM. I generate failed and successful logons, an account lockout, a group membership change, and a privileged logon. I review each event in Event Viewer and document the important fields (Account Name, Logon Type, Source Network Address, Failure codes, Group Name, and Privileges). These actions allow me to detect suspicious patterns (multiple failed logons, unexpected privilege assignments, or unauthorized group changes) and support basic incident triage and reporting.