Incident Title:
Suspected Brute Force Login Attempt on Windows Host

Date:
02/03/2026

Severity:
Medium

Summary:
Multiple failed authentication attempts followed by a successful login were detected on a Windows host, indicating a potential brute-force attack.

Evidence:

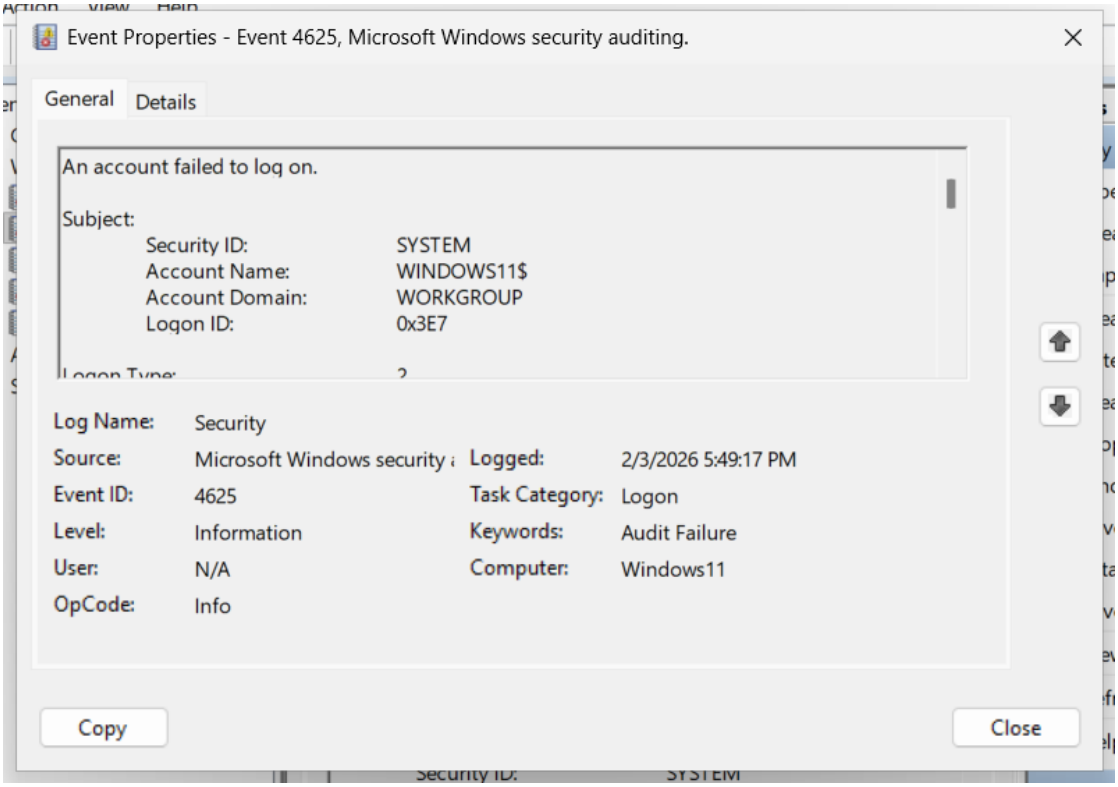
- Event ID 4625 – Failed login attempts
- Event ID 4624 – Successful login
- Event ID 4688 – Command execution

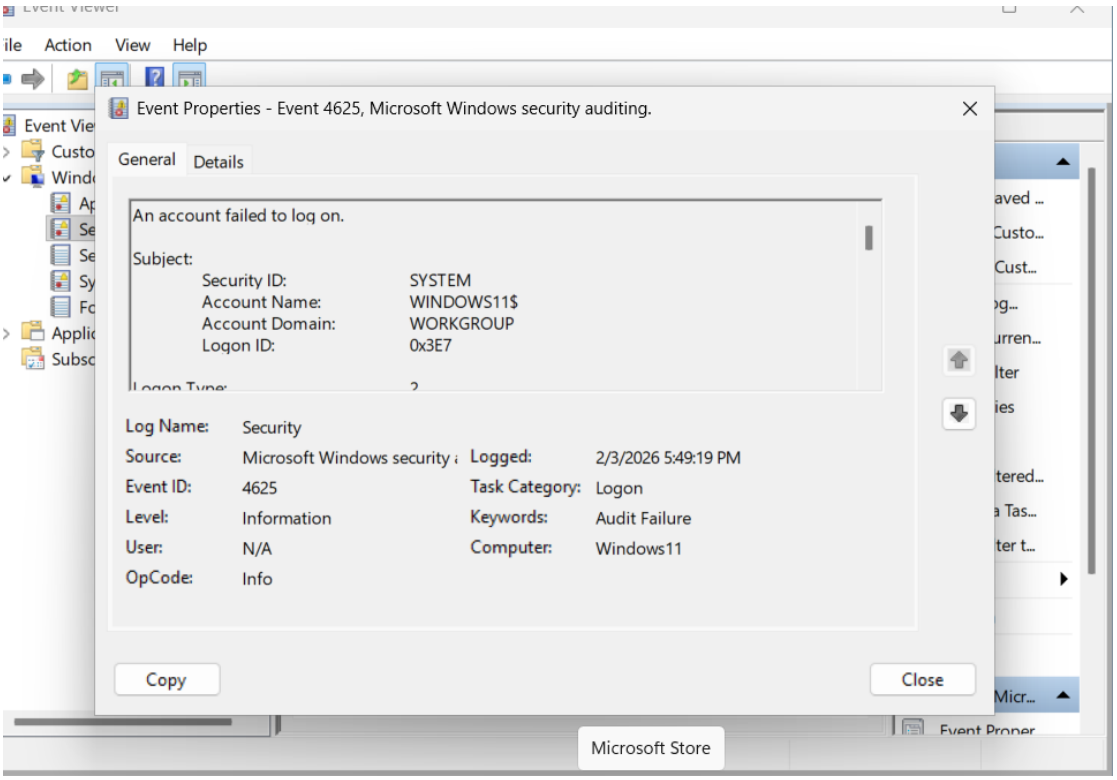
Analysis:
The same user account experienced repeated login failures followed by a successful login within a short timeframe. Post-login command execution activity was observed.

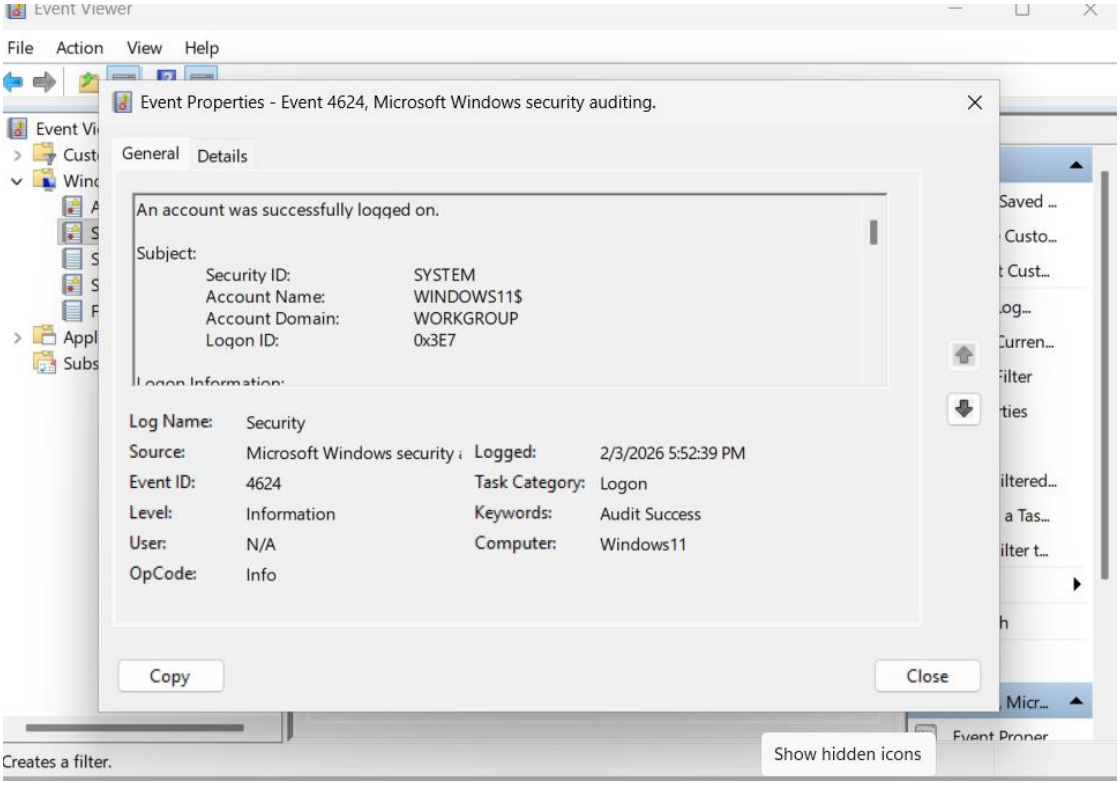
Impact:
Unauthorized access risk to the system.

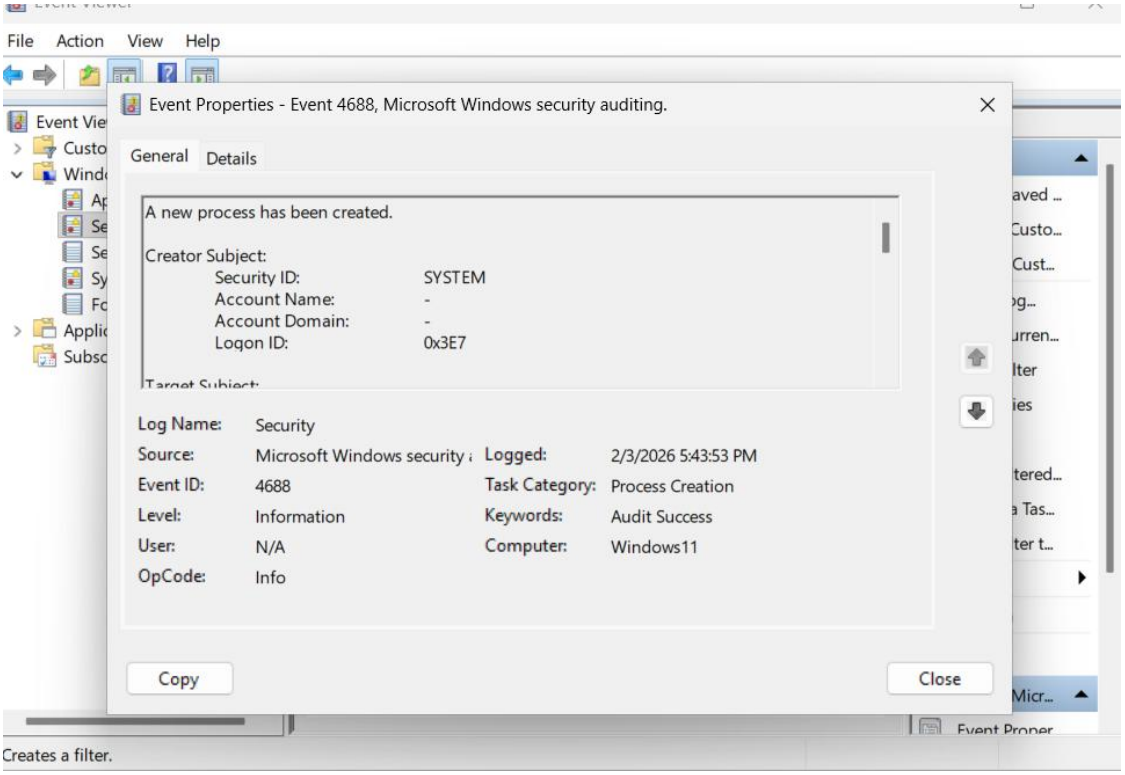
Recommendations:

- Enforce account lockout policy
- Enable MFA
- Monitor repeated authentication failures


Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
An account failed to log on.
Subject:
Security ID: SYSTEM
Account Name: WINDOWS11$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security
Logged: 2/3/2026 5:49:17 PM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: Windows11
OpCode: Info
Copy
Close


Action
View
Help
Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
An account failed to log on.
Subject:
Security ID: SYSTEM
Account Name: WINDOWS11$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security
Logged: 2/3/2026 5:49:19 PM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: Windows11
OpCode: Info
Copy
Close
Microsoft Store


Event Viewer
File Action View Help
Event Properties - Event 4624, Microsoft Windows security auditing.
General Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: WINDOWS11$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security Logged: 2/3/2026 5:52:39 PM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: Windows11
OpCode: Info
Copy
Close
Show hidden icons
Creates a filter.


File Action View Help
Event Properties - Event 4688, Microsoft Windows security auditing.
General Details
A new process has been created.
Creator Subject:
Security ID: SYSTEM
Account Name: -
Account Domain: -
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security Logged: 2/3/2026 5:43:53 PM
Event ID: 4688 Task Category: Process Creation
Level: Information Keywords: Audit Success
User: N/A Computer: Windows11
OpCode: Info
Copy
Close
Creates a filter.