1. Windows Event Viewer – Failed Logon Analysis (Event ID 4625)
Objective:

Use Windows Event Viewer to identify failed interactive logon attempts (Event ID 4625) and assess whether the pattern of activity indicates possible brute-force behavior.

Procedure:

Opened Event Viewer and navigated to:
Windows Logs → Security

Applied a filter to the Security log for Event ID 4625 (failed logon events).

Reviewed the resulting events in the upper pane and examined details in the lower pane.

Focused on key fields:

Status

SubStatus

LogonType

SubjectDomainName

TargetUserName

FailureReason

Observations:

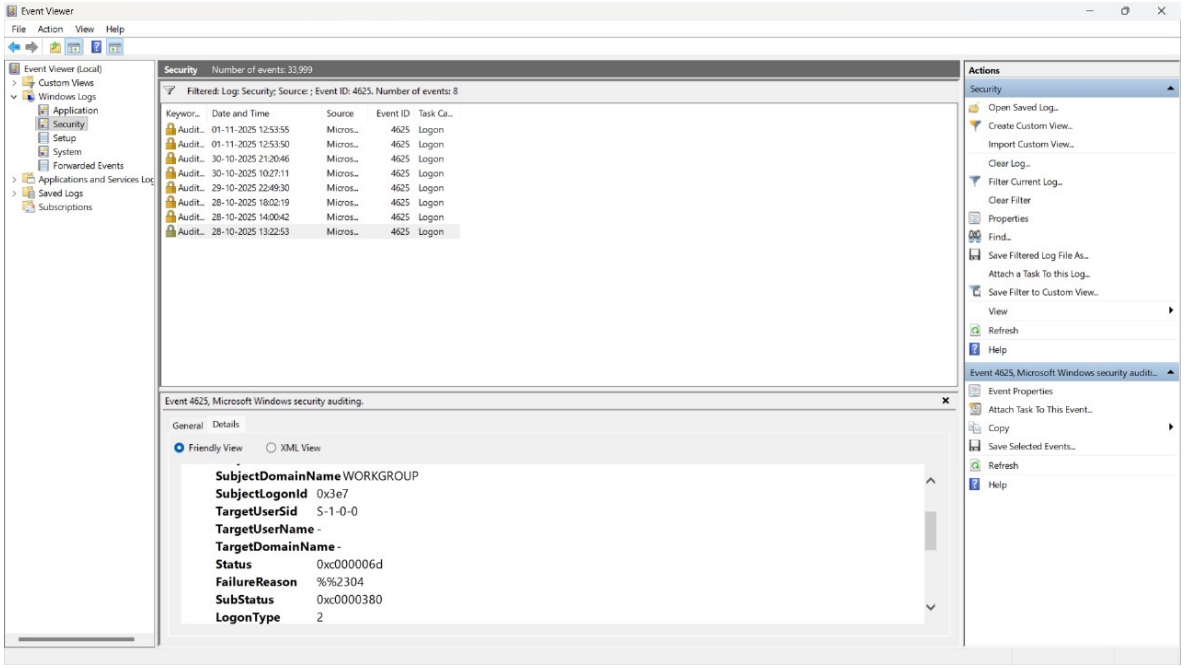
The Security log contained over 33,000 events, with filtered results showing multiple 4625 logon failures.

The recorded timestamps show failed logons across several days.

LogonType = 2 indicates interactive logons at the local console.

Status = 0xC000006D and SubStatus = 0xC0000380 indicate failed logon attempts due to incorrect username or authentication.

The SubjectDomainName = WORKGROUP, indicating a standalone workstation rather than a domain-joined environment.


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Saved Logs
Subscriptions
Security Number of events: 33,999
Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 8
Keywor... Date and Time Source Event ID Task Ca...
Audit... 01-11-2025 12:53:55 Micros... 4625 Logon
Audit... 01-11-2025 12:53:50 Micros... 4625 Logon
Audit... 30-10-2025 21:20:46 Micros... 4625 Logon
Audit... 30-10-2025 10:27:11 Micros... 4625 Logon
Audit... 29-10-2025 22:49:30 Micros... 4625 Logon
Audit... 28-10-2025 18:02:19 Micros... 4625 Logon
Audit... 28-10-2025 14:00:42 Micros... 4625 Logon
Audit... 28-10-2025 13:22:53 Micros... 4625 Logon
Event 4625, Microsoft Windows security auditing.
General Details
Friendly View
XML View
SubjectDomainName WORKGROUP
SubjectLogonId 0x3e7
TargetUserSid S-1-0-0
TargetUserName -
TargetDomainName -
Status 0xc000006d
FailureReason %%2304
SubStatus 0xc0000380
LogonType 2
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Event 4625, Microsoft Windows security auditi...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

2. Document Security Events
Objective:

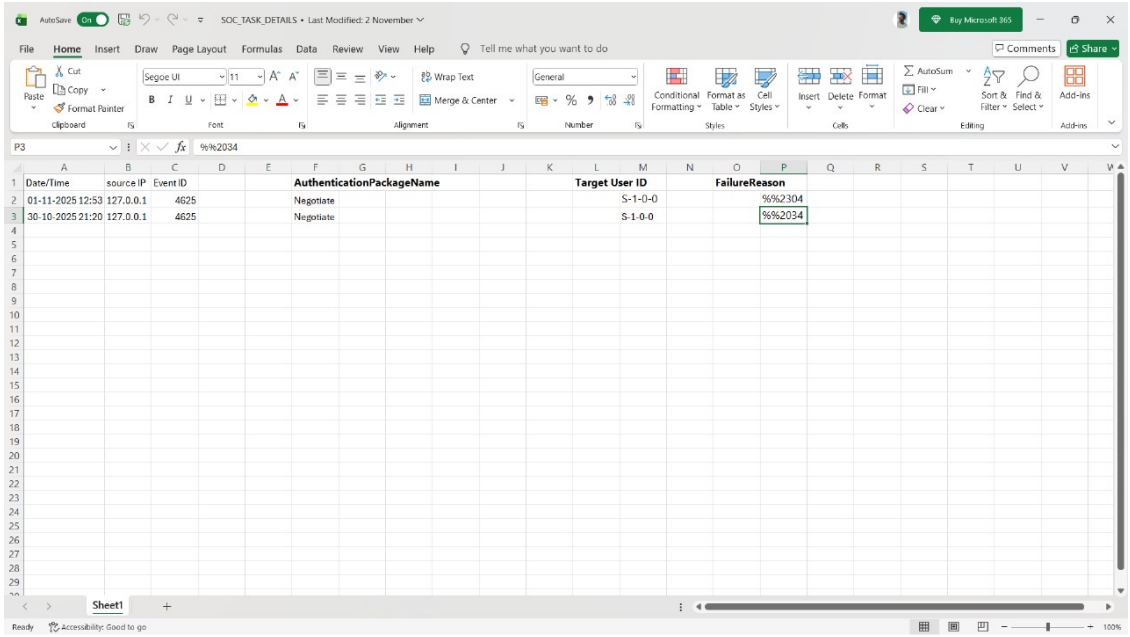
Develop proper documentation habits for security incident reporting by creating a structured and consistent log entry format.

How to Perform:

You need to create a documentation template with the following fields:

Date/Time | Source IP | Event ID | Description | Action Taken

This format is widely used in SOC, CIRT, and IR workflows. It ensures every event can be quickly understood and followed up by another analyst.



During this exercise, multiple logging and alerting mechanisms were tested to identify suspicious authentication activity within a lab-controlled environment. The focus was on examining authentication failure logs, building detection logic, and validating alert triggers in both Windows and Linux environments.

Windows Event Log Review

Accessed Windows Event Viewer

Filtered Security logs for Event ID 4625 (failed login attempts)

Extracted relevant log details into spreadsheet format

Analyzed frequency, timestamps, user context

Observation:
Multiple failed login attempts were logged, but the timing between events was spread out — indicating accidental user mistakes rather than aggressive brute-force activity.

Elastic SIEM Rule:

Designed rule to detect 5+ failed logins within 5 minutes

Purpose was to automatically identify potential brute-force attacks

Wazuh Custom Rule

Created a detection mechanism for SSH brute-force attempts by defining a rule that triggers when:

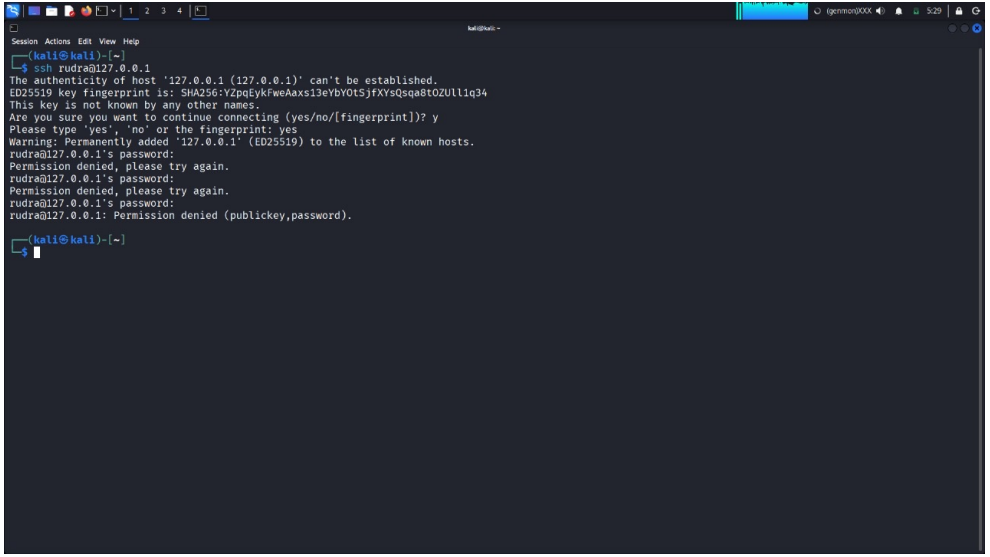
3 or more failed logins occur within 120 seconds

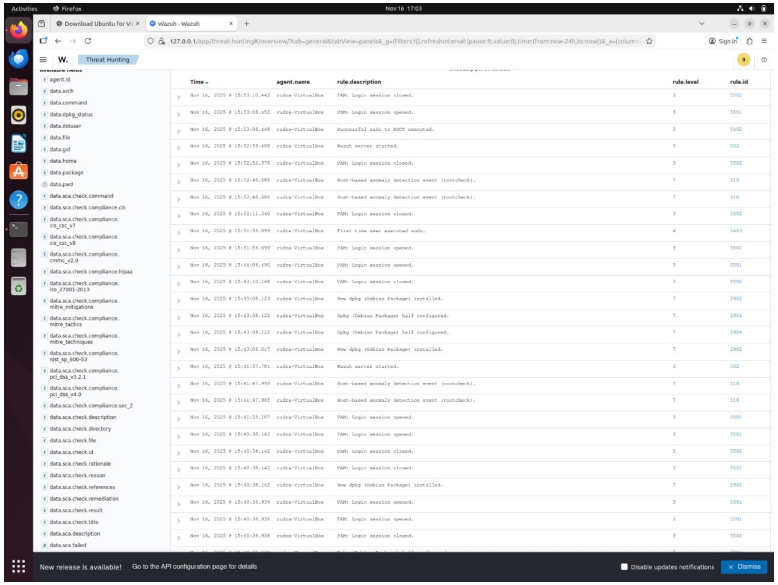
Implemented rule in:
/var/ossec/etc/rules/custom_ssh_rules.xml

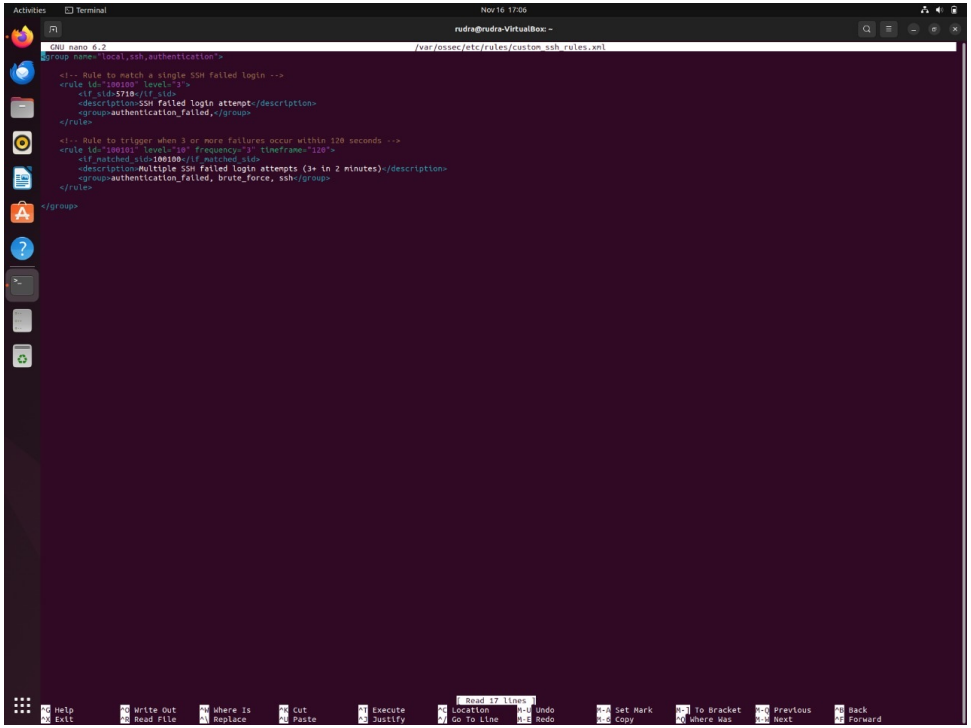
Two rules were defined:

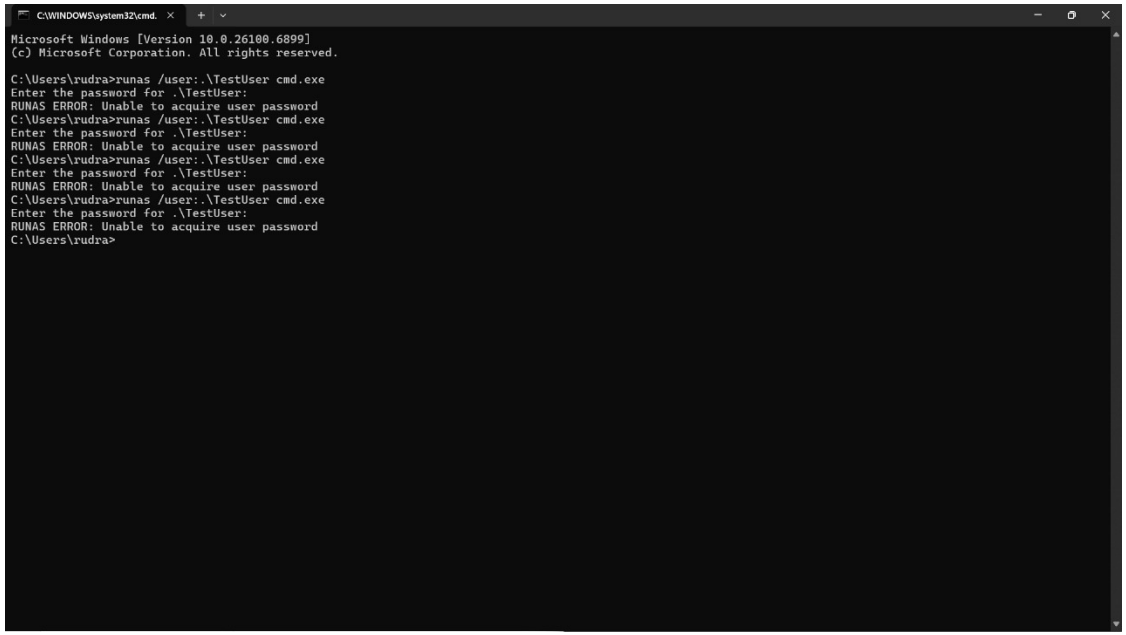
Single failed SSH login

Multiple failed SSH failures within 2 minutes


Session Actions Edit View Help
(kali㉿kali)-[~]
$ ssh rudra@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is: SHA256:YZpqEykFweAaxs13eYbYOtSjfXYsQsqa8tOZUlliq34
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.
rudra@127.0.0.1's password:
Permission denied, please try again.
rudra@127.0.0.1's password:
Permission denied, please try again.
rudra@127.0.0.1's password:
rudra@127.0.0.1: Permission denied (publickey,password).
(kali㉿kali)-[~]
$


Threat Hunting
Time
agent.name
rule.description
rule.level
rule.id
New release is available!
Go to the API configuration page for details
Disable updates notifications
Dismiss


Activities
Terminal
Nov 16 17:06
rudra@rudra-VirtualBox: ~
GNU nano 6.2
/var/ossec/etc/rules/custom_ssh_rules.xml
<group name="local,ssh,authentication">
<!-- Rule to match a single SSH failed login -->
<rule id="100200" level="3">
<if_sid>5710</if_sid>
<description>SSH failed login attempt</description>
<group>authentication_failed,</group>
</rule>
<!-- Rule to trigger when 3 or more failures occur within 120 seconds -->
<rule id="100101" level="10" frequency="3" timeframe="120">
<if_matched_sid>100100</if_matched_sid>
<description>Multiple SSH failed login attempts (3+ in 2 minutes)</description>
<group>authentication_failed, brute_force, ssh</group>
</rule>
</group>
Read 17 lines
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^J Execute
^T Justify
^C Location
^/ Go To Line
M-U Undo
M-E Redo
M-6 Set Mark
M-^ Copy
M-] To Bracket
M-W Where Was
M-Q Previous
M-W Next
M-B Back
M-F Forward


C:\WINDOWS\system32\cmd.
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.
C:\Users\rudra>runas /user:.\TestUser cmd.exe
Enter the password for .\TestUser:
RUNAS ERROR: Unable to acquire user password
C:\Users\rudra>runas /user:.\TestUser cmd.exe
Enter the password for .\TestUser:
RUNAS ERROR: Unable to acquire user password
C:\Users\rudra>runas /user:.\TestUser cmd.exe
Enter the password for .\TestUser:
RUNAS ERROR: Unable to acquire user password
C:\Users\rudra>runas /user:.\TestUser cmd.exe
Enter the password for .\TestUser:
RUNAS ERROR: Unable to acquire user password
C:\Users\rudra>