Usecase 2: Multiple Failed Physical Logon Attempts

Objective: Detect and create an alert when physical brute force logon attempts occur

Log Source: Windows Security Event Logs

Event ID: 4625- “an account failed to log on”

Example Target Log From Event Viewer:

An account failed to log on.

Subject:
- Security ID: SYSTEM
- Account Name: <system name>
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Type: 2

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

Failure Information:
- Failure Reason: An Error occured during Logon.
- Status: 0xC000006D
- Sub Status: 0xC0000380

Process Information:
- Caller Process ID: 0xbd4
- Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:
- Workstation Name: -
- Source Network Address: 127.0.0.1
- Source Port: 0

Detailed Authentication Information:
- Logon Process: User32
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

Logon type 2 refers to physical, keyboard logon attempts

Pre-configuration: N/A

Custom Wazuh Rule:

```
<group name="windows, windows_security,">
    <rule id="100112" level="13" frequency="4" timeframe="300">
    <if_matched_sid>60122</if_matched_sid>
    <field name="win.system.eventID">^4625$</field>
    <field name="win.eventdata.logonType">^2$</field>
    <description>Multiple failed physical access attempts detected</description>
    </rule>
</group>
```

Frequency 4+timeframe 300 means there must be 4 attempts within 5 minutes for the alert to trigger

If_matched_sid is used for custom rules with frequency/time requirements, the specific if_sid is 60122: Logon failure with incorrect details, seen below:

```
<rule id="60122" level="5">
  <if_sid>60105</if_sid>
  <field name="win.system.eventID">^529$|^4625$</field>
  <description>Logon Failure - Unknown user or bad password</description>
  <options>no_full_log</options>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.1,gdpr_IV_35.7.d,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14
      ,nist_800_53_AC.7,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  <mitre>
    <id>T1531</id>
  </mitre>
</rule>
```

win.system.eventID=^4625$ filters for 60122 logs that have the exact match of ID 4625

win.eventdata.logonType=^2$ further filters these logs for events that have logon Typw 2

Example Alerts:

	timestamp	agent.name	rule.description	rule.id	data.win.eventdata.log...	data.win.system.eventID
	Jun 23, 2025 @ 15:30:52.575	W11-VM_agent	Multiple failed physical acc...	100112	2	4625
	Jun 23, 2025 @ 15:30:52.575	W11-VM_agent	Multiple failed physical acc...	100112	2	4625
	May 8, 2025 @ 11:53:29.847	W11-VM_agent	Multiple failed physical acc...	100112	2	4625

Verification of fields: