Usecase 4- Failed Remote Logon Attempt

Objective: Create an alert when a remote logon attempt fails

Log Source: Windows Security Event Logs

Event ID: 4625- “Account failed to logon”

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: 8

Account For Which Logon Failed:
Security ID: NULL SID
Account Name: <account name>
Account Domain: <system name>

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

Process Information:
Caller Process ID: 0x2638
Caller Process Name: C:\Windows\System32\OpenSSH\sshd.exe

Network Information:
Workstation Name: <system name>
Source Network Address: -
Source Port: -

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

Pre-configuration: configuration of OpenSSH: run on powershell with admin privileges “Add-WindowsCapability -Online -Name OpenSSH.Server”> enable SSH connection through firewall with this “New-NetFirewallRule -Name sshd -DisplayName "OpenSSH Server (sshd)" -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22”> start the SSH server with Start-Service sshd> run the command Start-Service sshd <host username>@<host ip address> <host password> on the machine you want to establish the connecion with

Custom Wazuh Rule:

```
<group name="windows, windows_security,">
    <rule id="100115" level="13">
    <if_sid>60122</if_sid>
    <field name="win.system.eventID">^4625$</field>
        <field name="win.eventdata.logonType">^3$|^8$|^10$</field>
    <description>Failed Remote Login Attempt Detected</description>
    </rule>
</group>
```

Sid 60122 is for unsuccessful logon attempts

```
<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>
```

Of these unsuccessful logon logs, win.system.eventID is event ID 4625 along with win.eventdata.logonType is 3 (network logon), 8 (network cleartext, meaning network logon without authentication) or 10 (RDP/terminal services) filters for the logs with the relevant logon types related to remote logons.

Example Alerts:

timestamp	agent.name	rule.description	rule.id	data.win.system.eventID	data.win.eventdata.log...
May 8, 2025 @ 11:54:36.822	W11-VM_agent	Failed Remote Login Attem...	100115	4625	8
May 8, 2025 @ 10:58:29.435	W11-VM_agent	Failed Remote Login Attem...	100115	4625	8
May 8, 2025 @ 10:58:29.435	W11-VM_agent	Failed Remote Login Attem...	100115	4625	8
May 8, 2025 @ 10:58:12.983	W11-VM_agent	Failed Remote Login Attem...	100115	4625	8

Verification of fields: