Windows Log Output

Alert ID	Description	Source IP	Priority	Status
60122	Failed Login (Event ID 4625)	10.14.228.46	Medium	Open

- Alert ID = 60122 → this is the real Wazuh rule from your JSON
- Description = Failed Login (4625) → matches your real EVTX logs
- Source IP = 10.14.228.46 → your Kali machine
- Priority = Medium → real Wazuh level 5
- Status = Open → alert still active

generated real brute-force attempts

Source machine: 10.14.228.46 (your Kali VM)
Target machine: Your Windows host
Method: Evil-WinRM + wrong passwords

Windows created real Security logs (Event ID 4625)

Multiple entries with:

- Target User: mrhac
- Logon Type: 3 (network – remote login)
- Auth Package: NTLM
- Process: NtLmSsp
- Status: 0xC000006D
- SubStatus: 0xC000006A
- Source IP: 10.14.228.46
- Ports: changing values (normal for brute-force)

TimeCreated	Username	Source IP	Source Port	Logon Type	Status
13:47:00	mrhac	10.14.228.46	56113	3	0xC000006D
13:47:00	mrhac	10.14.228.46	56111	3	0xC000006D
13:46:59	mrhac	10.14.228.46	56109	3	0xC000006D
13:46:49	mrhac	10.14.228.46	56106	3	0xC000006D

TimeCreated	Username	Source IP	Source Port	Logon Type	Status
13:46:39	mrhac	10.14.228.46	56101	3	0xC000006D
13:46:39	mrhac	10.14.228.46	56099	3	0xC000006D
13:44:51	mrhac	10.14.228.46	57751	3	0xC000006D
13:44:41	mrhac	10.14.228.46	57748	3	0xC000006D
13:44:31	mrhac	10.14.228.46	57745	3	0xC000006D
13:44:31	mrhac	10.14.228.46	57743	3	0xC000006D

These events all correspond to Event ID 4625 – Failed Logon Attempts.

Field	Actual Value
Rule	Windows Security Event 4625
Level	5 (Authentication Failure)
Timestamp	19–20 Nov 2025 (multiple)
Source IPs	10.14.228.46, 127.0.0.1, ::1
Target Username	mrhac, administrator, -
Logon Type	3 (network), 2 (interactive)
Status	0xC000006D (Bad username/password)
Sub-Status	0xC000006A (Bad password), 0xC0000380 (Internal logon error)

JSON Log Output


```
[
 {
   "EventID": 4625,
   "Timestamp": "2025-11-20T13:47:00Z",
   "LogonType": 3,
   "TargetUser": "mrhac",
   "SourceIP": "10.14.228.46",
   "SourcePort": "56113",
   "Status": "0xC000006D",
   "SubStatus": "0xC000006A",
   "AuthPackage": "NTLM"
 },

{
   "EventID": 4625,
   "Timestamp": "2025-11-20T13:46:59Z",
```

```
    "LogonType": 3,
    "TargetUser": "mrhac",
    "SourceIP": "10.14.228.46",
    "SourcePort": "56109",
    "Status": "0xC000006D",
    "SubStatus": "0xC000006A",
    "AuthPackage": "NTLM"
  },
  {
    "EventID": 4625,
    "Timestamp": "2025-11-20T13:46:49Z",
    "LogonType": 3,
    "TargetUser": "mrhac",
    "SourceIP": "10.14.228.46",
    "SourcePort": "56106",
    "Status": "0xC000006D",
    "SubStatus": "0xC000006A",
    "AuthPackage": "NTLM"
  },
  {
    "EventID": 4625,
    "Timestamp": "2025-11-19T22:21:18Z",
    "LogonType": 2,
    "TargetUser": "administrator",
    "SourceIP": "::1",
    "SourcePort": "0",
    "Status": "0xC000006D",
    "SubStatus": "0xC000006A",
    "AuthPackage": "Negotiate"
}
]
```

Alert Triage Report – Failed Authentication Attempts (Event ID 4625)

Analyst: chandan prasad
Tooling: Wazuh, Windows Event Logs, VirusTotal, AlienVault OTX
Date: 20 Nov 2025

Executive Summary

Multiple failed authentication attempts were observed on the Windows host *Mr-Chandan-Prasad-indian*. The attempts originated from both local system processes and a remote machine (10.14.228.46).
The log data suggests brute-force or repeated incorrect password attempts, matching your Evil-WinRM testing.
No malware indicators found.

---

1. Alert Details

Alert ID	Event ID	Description	Target User	Source IP	Logon Type	Status	Sub-status
4625-A	4625	Failed login	mrhac	10.14.228.46	3	0xC000006D	0xC000006A
4625-B	4625	Failed login	mrhac	10.14.228.46	3	0xC000006D	0xC000006A
4625-C	4625	Failed login	administrator	::1	2	0xC000006D	0xC000006A
4625-D	4625	Failed login	-	127.0.0.1	2	0xC000006D	0xC0000380

---

2. Root Cause Analysis

The logs clearly map to your pentesting actions:

- Logon Type 3 = Network logon → triggered by your Evil-WinRM attempts.
- Source IP 10.14.228.46 = Kali machine.
- Status 0xC000006D + Sub-status 0xC000006A → Wrong password every attempt.
- Multiple attempts in sequence → typical brute-force pattern.

Required Summary

The source IP (10.14.228.46) is an internal address and does not appear in AlienVault OTX or VirusTotal. No malicious reputation is associated with it. Wazuh logs show repeated failed logons from this host during a controlled brute-force test. This activity is an intentional false positive for training.