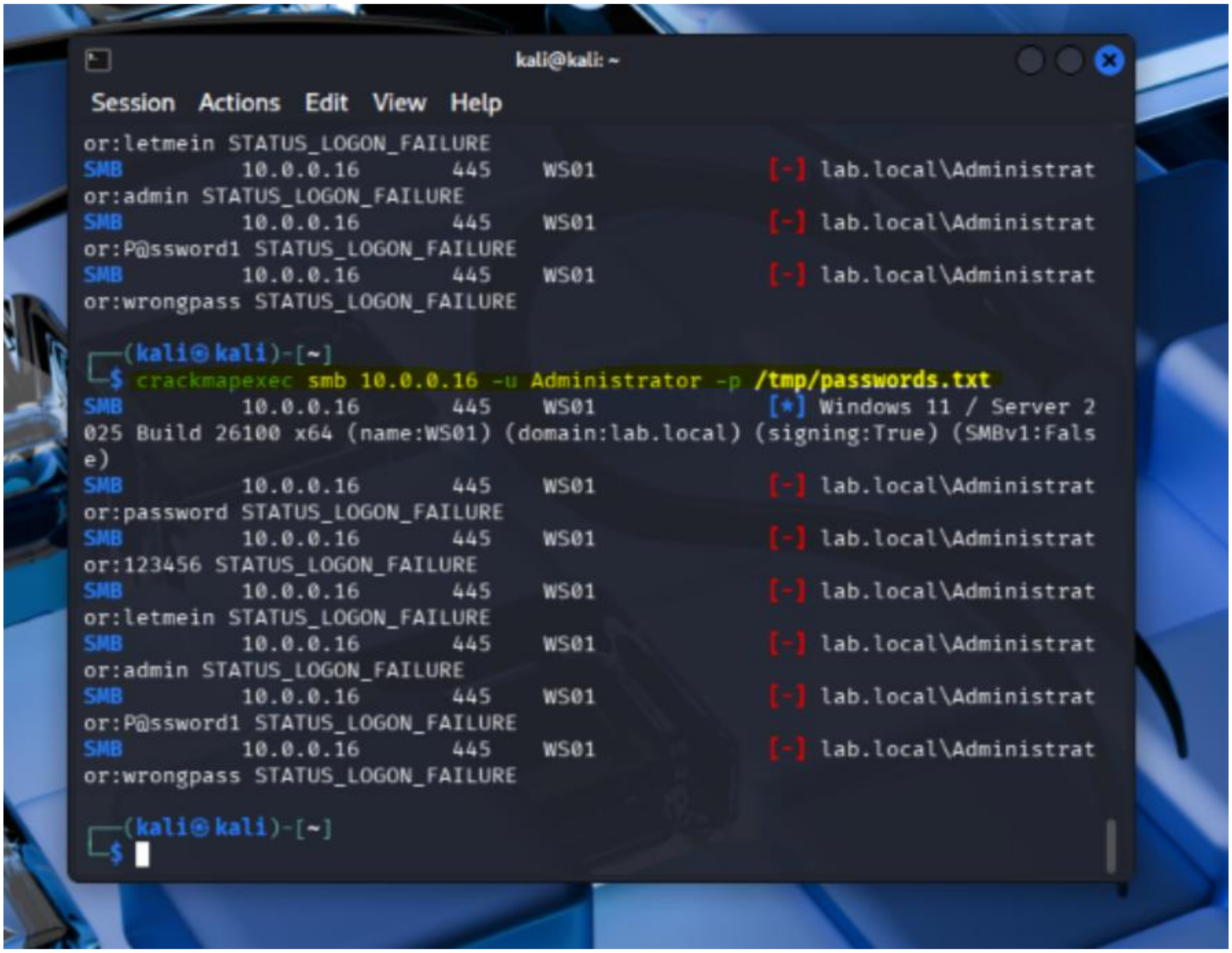
1/20/2026

Portfolio Document – Brute force attack attempt

Kali VM using crackmapexec smb 10.0.0.16 command to run a brute force attack on target

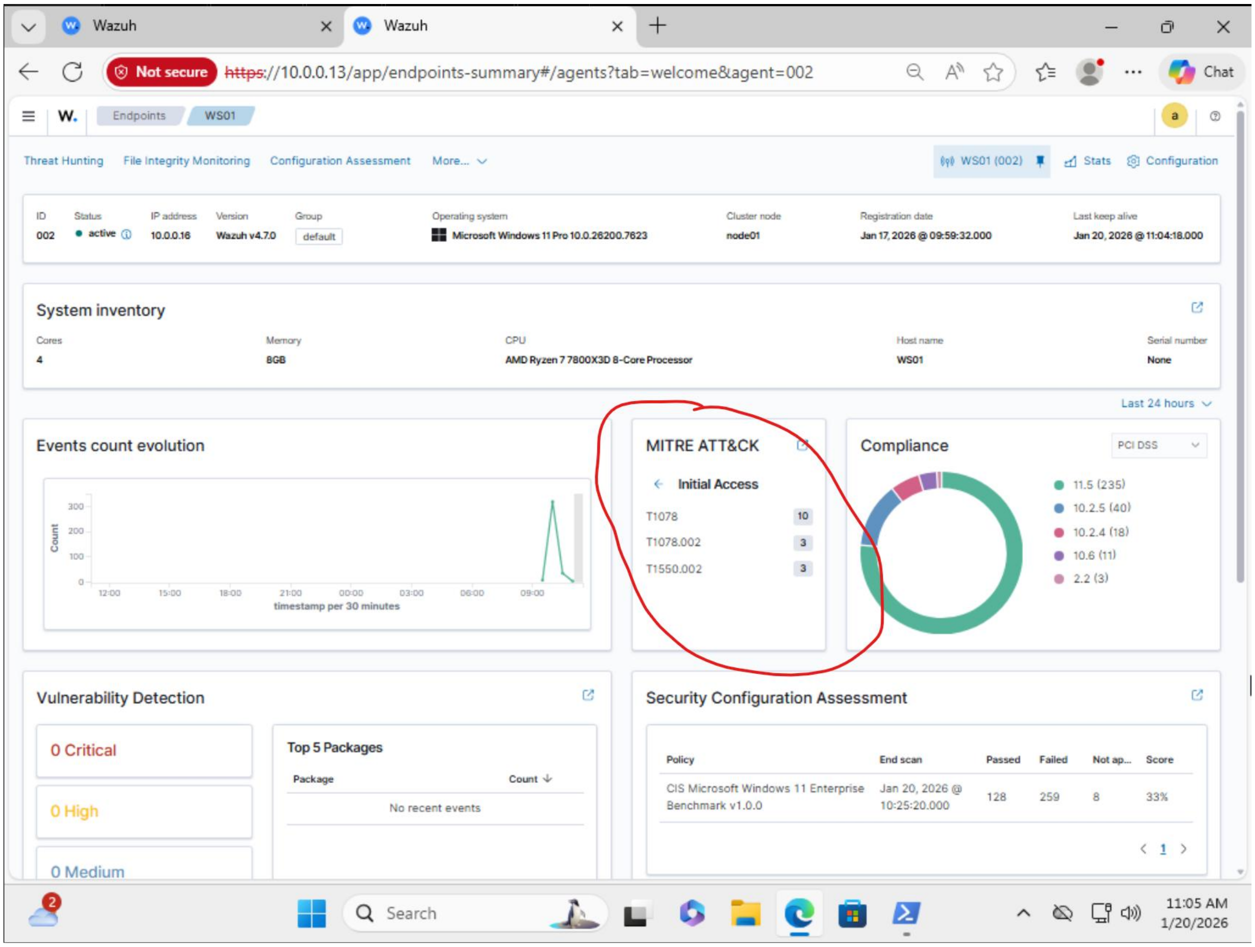


```
or:letmein STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:admin STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:P@ssword1 STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:wrongpass STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.0.0.16 -u Administrator -p /tmp/passwords.txt
SMB         10.0.0.16       445    WS01             [*] Windows 11 / Server 2
025 Build 26100 x64 (name:WS01) (domain:lab.local) (signing:True) (SMBv1:Fals
e)
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:password STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:123456 STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:letmein STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:admin STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:P@ssword1 STATUS_LOGON_FAILURE
SMB         10.0.0.16       445    WS01             [-] lab.local\Administrat
or:wrongpass STATUS_LOGON_FAILURE

┌──(kali㉿kali)-[~]
└─$ 
```

Screenshot of the MITRE ATT&CK showing "Initial Access: 13”



ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
002	● active	10.0.0.16	Wazuh v4.7.0	default	Microsoft Windows 11 Pro 10.0.26200.7623	node01	Jan 17, 2026 @ 09:59:32.000	Jan 20, 2026 @ 11:04:18.000

System inventory

Cores	Memory	CPU	Host name	Serial number
4	8GB	AMD Ryzen 7 7800X3D 8-Core Processor	WS01	None

Events count evolution

MITRE ATT&CK

Initial Access

T1078	10
T1078.002	3
T1550.002	3

Compliance

PCI DSS

- ● 11.5 (235)
- ● 10.2.5 (40)
- ● 10.2.4 (18)
- ● 10.6 (11)
- ● 2.2 (3)

Vulnerability Detection

0 Critical

0 High

0 Medium

Top 5 Packages

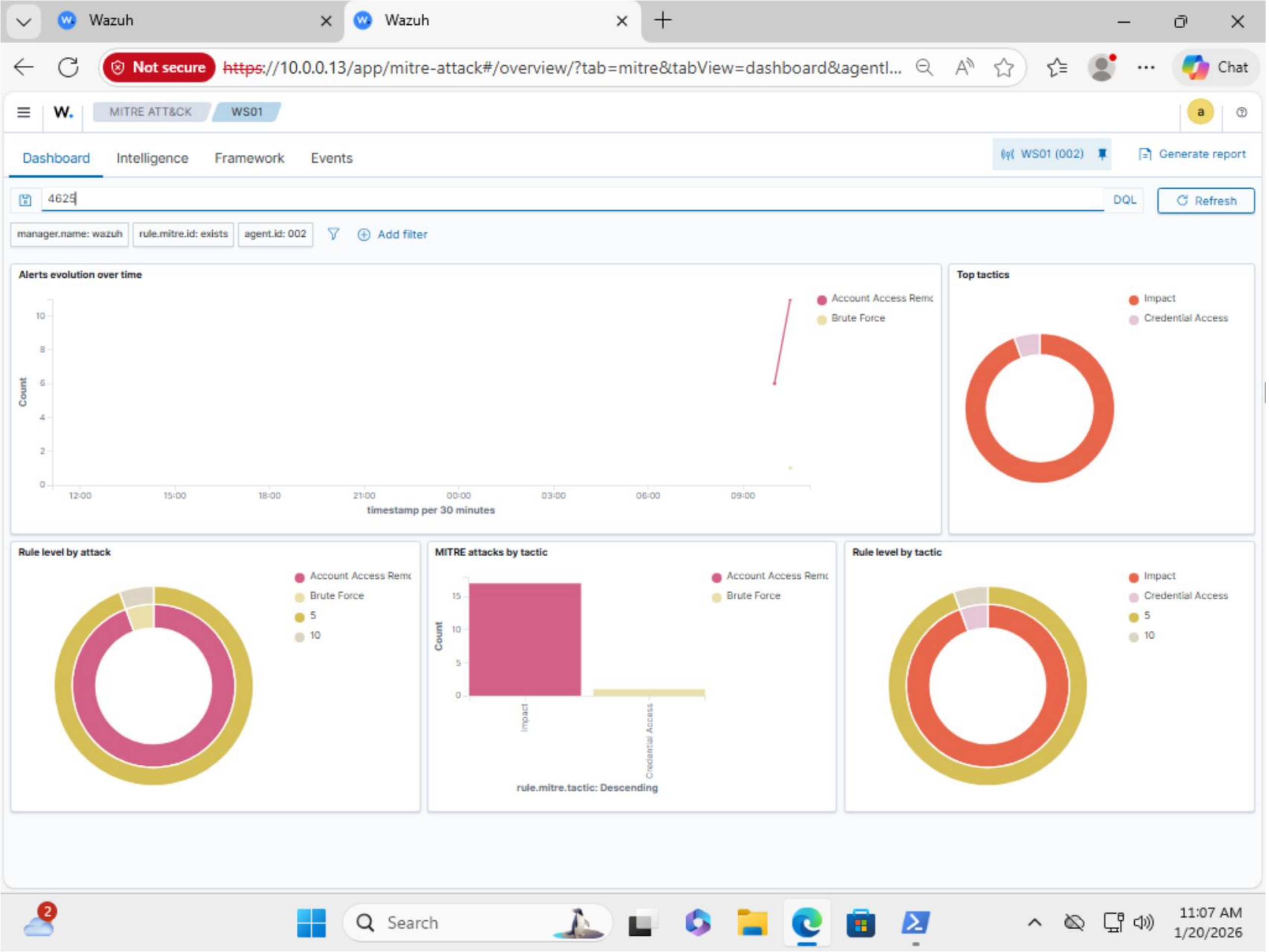
Package	Count ↓
No recent events	

Security Configuration Assessment

Policy	End scan	Passed	Failed	Not ap...	Score
CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0	Jan 20, 2026 @ 10:25:20.000	128	259	8	33%

‹ 1 ›

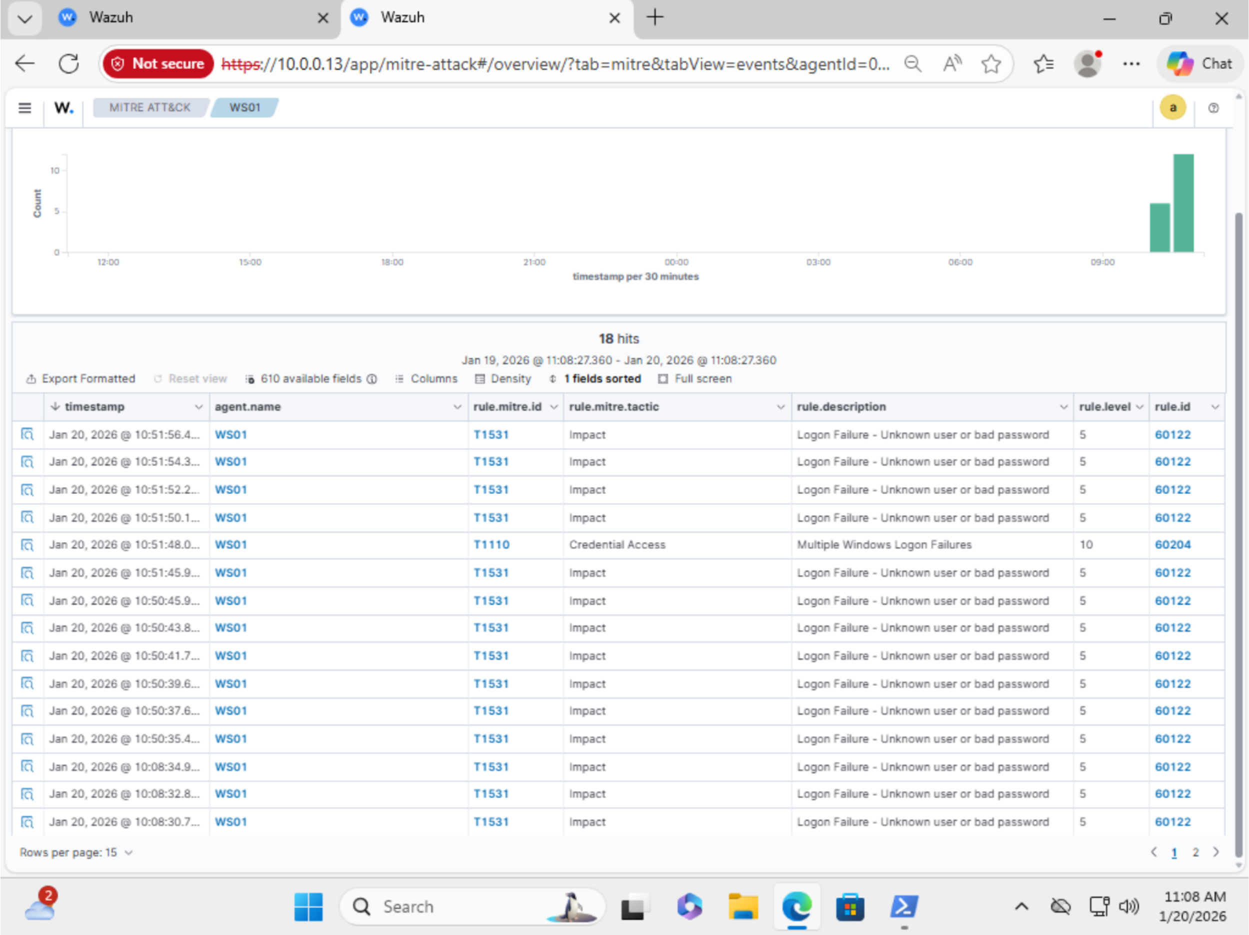
Screenshot of the filtered 4625 events list



Search: 4625

Filters: manager.name: wazuh | rule.mitre.id: exists | agent.id: 002

Event List showing failed logon attempts



18 hits

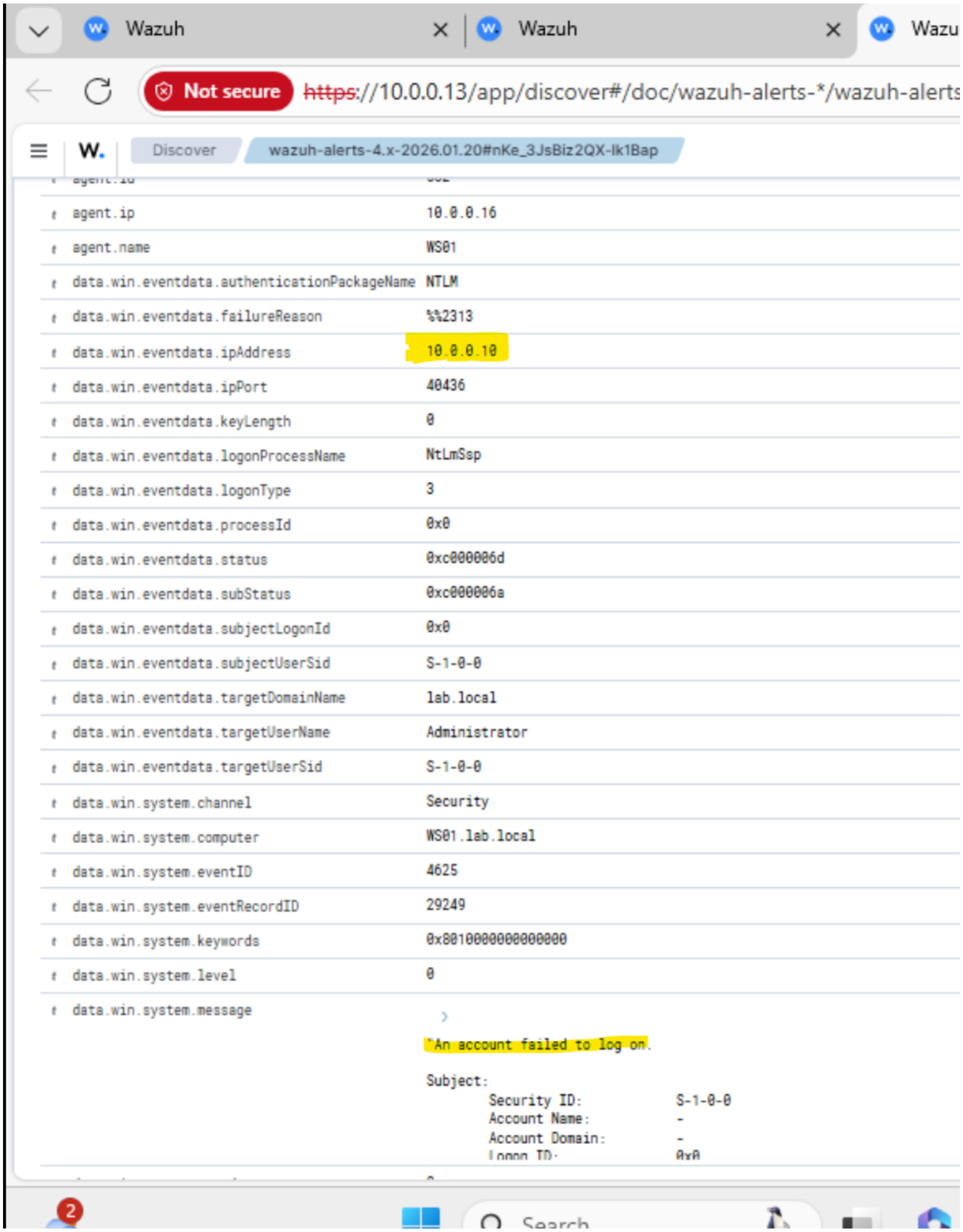
Jan 19, 2026 @ 11:08:27.360 - Jan 20, 2026 @ 11:08:27.360

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
Jan 20, 2026 @ 10:51:56.4...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:51:54.3...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:51:52.2...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:51:50.1...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:51:48.0...	WS01	T1110	Credential Access	Multiple Windows Logon Failures	10	60204
Jan 20, 2026 @ 10:51:45.9...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:45.9...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:43.8...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:41.7...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:39.6...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:37.6...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:50:35.4...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:08:34.9...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:08:32.8...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122
Jan 20, 2026 @ 10:08:30.7...	WS01	T1531	Impact	Logon Failure - Unknown user or bad password	5	60122

Rows per page: 15

< 1 2 >

Source attacker IP address for specific Failed Logon Attempt event


Wazuh
Wazuh
Wazu
Not secure
~~https~~://10.0.0.13/app/discover#/doc/wazuh-alerts-*/wazuh-alerts
W.
Discover
wazuh-alerts-4.x-2026.01.20#nKe_3JsBiz2QX-Ik1Bap
2
Search

```
t agent.id                                      [illegible]
t agent.ip                                      10.0.0.16
t agent.name                                    WS01
t data.win.eventdata.authenticationPackageName  NTLM
t data.win.eventdata.failureReason              %%2313
t data.win.eventdata.ipAddress                  10.0.0.10
t data.win.eventdata.ipPort                     40436
t data.win.eventdata.keyLength                  0
t data.win.eventdata.logonProcessName           NtLmSsp
t data.win.eventdata.logonType                  3
t data.win.eventdata.processId                  0x0
t data.win.eventdata.status                     0xc000006d
t data.win.eventdata.subStatus                  0xc000006a
t data.win.eventdata.subjectLogonId             0x0
t data.win.eventdata.subjectUserSid             S-1-0-0
t data.win.eventdata.targetDomainName           lab.local
t data.win.eventdata.targetUserName             Administrator
t data.win.eventdata.targetUserSid              S-1-0-0
t data.win.system.channel                       Security
t data.win.system.computer                      WS01.lab.local
t data.win.system.eventID                       4625
t data.win.system.eventRecordID                 29249
t data.win.system.keywords                      0x8010000000000000
t data.win.system.level                         0
t data.win.system.message
                                                 >
                                                "An account failed to log on.

                                                Subject:
                                                        Security ID:            S-1-0-0
                                                        Account Name:           -
                                                        Account Domain:         -
                                                        Logon ID:               0x0
```