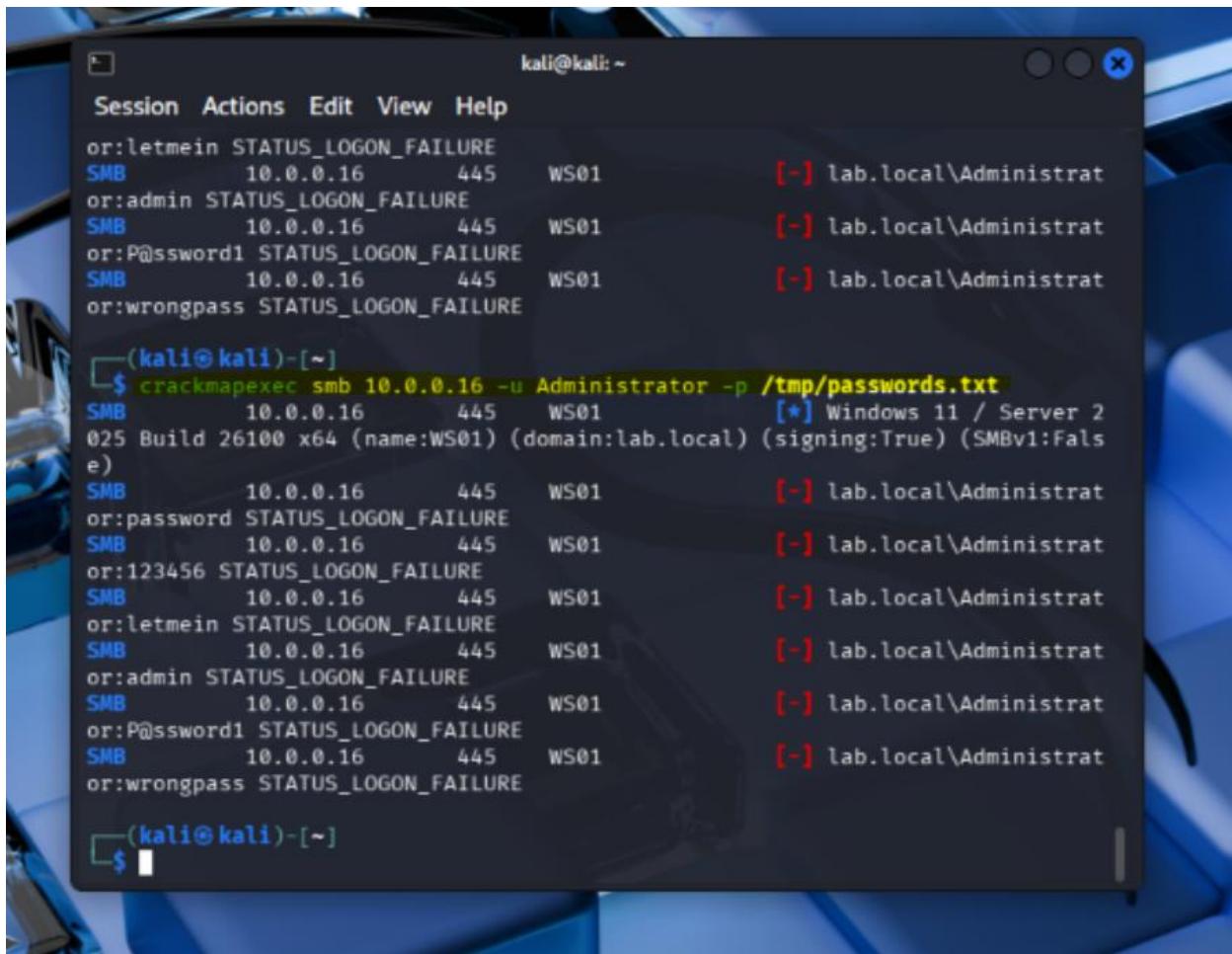


1/20/2026

## Portfolio Document – Brute force attack attempt

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



The screenshot shows a terminal window titled "kali@kali: ~". The terminal displays a series of failed logon attempts against a Windows 11/Server 2025 target (IP 10.0.0.16, port 445, domain lab.local). The attacks are listed under the "Session" tab. The user "Administrator" is being targeted. A password file "/tmp/passwords.txt" is being used. The terminal also shows the command being run: \$ crackmapexec smb 10.0.0.16 -u Administrator -p /tmp/passwords.txt.

```
Session Actions Edit View Help
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
[*] Windows 11 / Server 2025 Build 26100 x64 (name:WS01) (domain:lab.local) (signing:True) (SMBv1:False)
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"

The screenshot shows the Wazuh endpoint summary interface for an agent named WS01. The main header includes tabs for Threat Hunting, File Integrity Monitoring, Configuration Assessment, and More... A red circle highlights the MITRE ATT&CK section.

**System inventory:**

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

**Events count evolution:** A line chart showing event counts over the last 24 hours, with a sharp peak around 09:00.

**MITRE ATT&CK:** A section titled "Initial Access" showing three tactics: T1078, T1078.002, and T1550.002, each with a count of 10, 3, and 3 respectively.

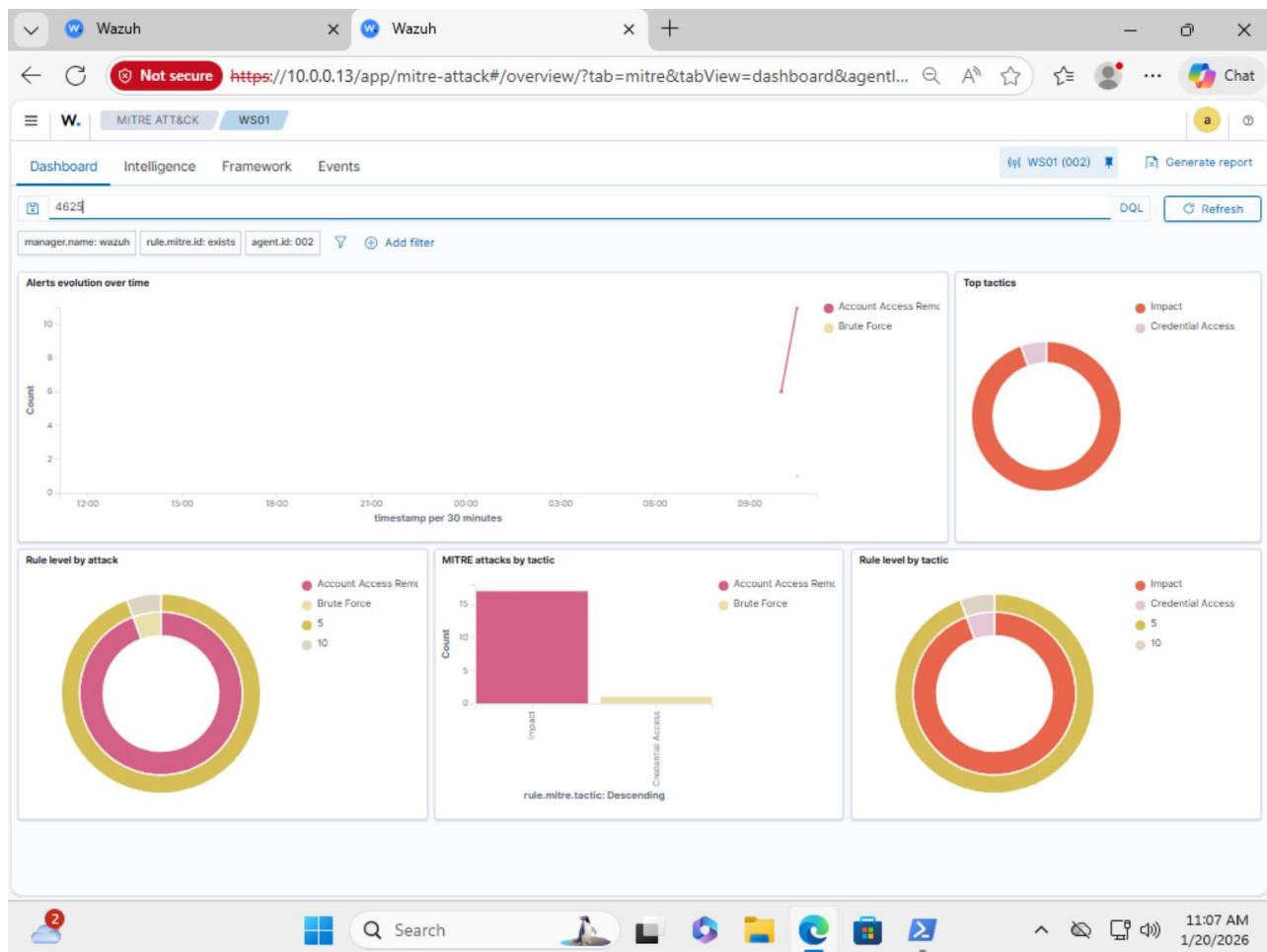
**Compliance:** A donut chart showing PCI DSS compliance status across five categories: 11.5 (235), 10.2.5 (40), 10.2.4 (18), 10.6 (11), and 2.2 (3).

**Vulnerability Detection:** Shows 0 Critical, 0 High, and 0 Medium vulnerabilities.

**Security Configuration Assessment:** Shows a single CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0 scan with 128 Passed, 259 Failed, and 8 Not applicable items, resulting in a 33% score.

The bottom navigation bar includes icons for Cloud, Search, and various system utilities, along with the timestamp 11:05 AM 1/20/2026.

## Screenshot of the filtered 4625 events list



## Event List showing failed logon attempts

The screenshot shows the Wazuh MITRE ATT&CK interface. At the top, there are two browser tabs both titled "Wazuh". The active tab shows a histogram with the y-axis labeled "Count" ranging from 0 to 10 and the x-axis labeled "timestamp per 30 minutes" with time markers from 12:00 to 09:00. Two bars are visible: one at approximately 08:00 with a height of about 5, and another at approximately 09:00 with a height of about 10. Below the histogram is a table titled "18 hits" showing event details. The table has columns: timestamp, agent.name, rule.mitre.id, rule.mitre.tactic, rule.description, rule.level, and rule.id. The data is as follows:

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

At the bottom of the interface, there is a toolbar with various icons and a status bar indicating "11:08 AM 1/20/2026".

## Source attacker IP address for specific Failed Logon Attempt event

The screenshot shows the Wazuh web interface with three tabs at the top: 'Discover' (selected), 'Logs', and 'Metrics'. The URL is https://10.0.0.13/app/discover#/doc/wazuh-alerts-\*?wazuh-alerts.

The main content area displays a table of event data fields:

Field	Value
agent.ip	10.0.0.16
agent.name	WS01
data.win.eventdata.authenticationPackageName	NTLM
data.win.eventdata.failureReason	%2313
data.win.eventdata.ipAddress	10.0.0.10
data.win.eventdata.ipPort	40436
data.win.eventdata.keyLength	0
data.win.eventdata.logonProcessName	NtLmSsp
data.win.eventdata.logonType	3
data.win.eventdata.processId	0x0
data.win.eventdata.status	0xc000006d
data.win.eventdata.subStatus	0xc000006a
data.win.eventdata.subjectLogonId	0x0
data.win.eventdata.subjectUserSid	S-1-0-0
data.win.eventdata.targetDomainName	lab.local
data.win.eventdata.targetUserName	Administrator
data.win.eventdata.targetUserSid	S-1-0-0
data.win.system.channel	Security
data.win.system.computer	WS01.lab.local
data.win.system.eventID	4625
data.win.system.eventRecordID	29249
data.win.system.keywords	0x8010000000000000
data.win.system.level	0
data.win.system.message	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: AxA

At the bottom left, there is a red circle with the number '2' indicating new notifications.