

## # Detecting SMB Brute Force Attacks with Wazuh SIEM

**\*\*Author:\*\*** Benjamin Mangus

**\*\*Date:\*\*** January 20, 2026

**\*\*Lab Environment:\*\*** SEC\_LAB Home Lab

### ## Executive Summary

Simulated an SMB brute force attack against a domain-joined Windows 11 workstation using CrackMapExec from a Kali Linux attack box. The attack was successfully detected by Wazuh SIEM through Windows Security Event ID 4625 (failed logon) correlation. This exercise demonstrates detection engineering skills, SIEM operation, and understanding of the MITRE ATT&CK framework.

### \*\*Key Results:\*\*

- 18 failed logon attempts detected within a 2-minute window
- Attacker source IP (10.0.0.10) identified in event logs
- MITRE ATT&CK techniques T1110 (Brute Force) and T1078.002 (Valid Accounts: Domain Accounts) mapped

### ## Lab Environment

Host   IP Address   Role   OS
DC01   10.0.0.5   Domain Controller   Windows Server 2022
WS01   10.0.0.16   Target Workstation   Windows 11 Pro
Kali   10.0.0.10   Attack Box   Kali Linux
Wazuh   10.0.0.13   SIEM / Log Collector   Ubuntu 22.04

**\*\*Network:\*\*** VMware NAT (10.0.0.0/24)

**\*\*Domain:\*\*** lab.local

**\*\*SIEM:\*\*** Wazuh 4.14.2 with Windows agent on WS01

## **## Attack Methodology**

### **### Objective**

Simulate a credential brute force attack targeting the domain Administrator account via SMB (port 445).

### **### Tools Used**

- **CrackMapExec** - SMB authentication testing tool
- **Custom password list** - 6 common passwords for testing

### **### Attack Execution**

```
```bash
```

```
# Create password list
```

```
echo -e "password\n123456\nletmein\nadmin\nP@ssword1\nwrongpass" >
/tmp/passwords.txt
```

```
# Execute brute force attack
```

```
crackmapexec smb 10.0.0.16 -u Administrator -p /tmp/passwords.txt
```

```
```
```

### **### Attack Output**

```

SMB 10.0.0.16 445 WS01 [\*] Windows 11 / Server 2022 Build 26100 x64 (name:WS01)  
(domain:lab.local)

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:password STATUS\_LOGON\_FAILURE

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:123456 STATUS\_LOGON\_FAILURE

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:letmein STATUS\_LOGON\_FAILURE

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:admin STATUS\_LOGON\_FAILURE

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:P@ssword1  
STATUS\_LOGON\_FAILURE

SMB 10.0.0.16 445 WS01 [-] lab.local\Administrator:wrongpass  
STATUS\_LOGON\_FAILURE

### **## Detection Analysis**

#### **### Prerequisites for Detection**

Before events were visible in Wazuh, the following had to be configured:

1. **Windows Audit Policy** - Enable failed logon auditing:

``` powershell

```
auditpol /set /subcategory:"Logon" /failure:enable
```

```

2. **Wazuh Agent** - Configured to collect Windows Security logs via eventchannel

3. **Firewall Rules** - SMB (port 445) accessible for attack simulation

### ### Wazuh Detection

**\*\*Primary Detection Rule:\*\*** 60122 - "Logon Failure - Unknown user or bad password"

**\*\*Aggregation Rule:\*\*** 60204 - "Multiple Windows Logon Failures" (triggered after threshold exceeded)

### ### Event Details (Windows Event ID 4625)

Field	Value	Significance
----- ----- -----		
` data.win.system.eventID`   4625   Failed logon attempt		
` data.win.eventdata.ipAddress`   10.0.0.10   <b>**Attacker source IP**</b>		
` data.win.eventdata.targetUserName`   Administrator   Targeted account		
` data.win.eventdata.logonType`   3   Network logon (SMB)		
` data.win.eventdata.failureReason`   %%2313   Unknown username or bad password		
` data.win.eventdata.authenticationPackageName`   NTLM   Authentication protocol used		
` data.win.eventdata.logonProcessName`   NtLmSsp   NTLM Security Support Provider		

### ### MITRE ATT&CK Mapping

Technique ID	Name	Tactic	Description
----- ----- ----- -----			
T1110   Brute Force   Credential Access   Attempting multiple passwords against an account			
T1078.002   Valid Accounts: Domain Accounts   Initial Access   Attempting to use domain credentials			
T1550.002   Use Alternate Authentication Material   Lateral Movement   SMB authentication attempts			

## **## Key Findings**

1. **Attack Timeline:** 18 failed logon events within approximately 2 minutes
2. **Source Identification:** Attacker IP (10.0.0.10) clearly visible in event logs
3. **Target Account:** Domain Administrator account was targeted
4. **Authentication Method:** NTLM over SMB (Logon Type 3)
5. **Detection Latency:** Events appeared in Wazuh within seconds of attack execution

## **### Indicators of Compromise (IOCs)**

IOC Type	Value	Context
Source IP	10.0.0.10	Attack origin
Target Port	445/TCP	SMB service
Event Pattern	Multiple 4625 events	Rapid succession from single source
Target Account	Administrator	High-value account targeted

## **## Recommendations**

### **### Immediate Mitigations**

#### **1. Account Lockout Policy\*\***

- Configure via Group Policy: Lock account after 5 failed attempts
- Lockout duration: 30 minutes
- Reset counter after: 30 minutes

#### **2. Network Segmentation\*\***

- Restrict SMB access to authorized hosts only
- Use Windows Firewall to limit inbound SMB connections

### 3. **Monitoring & Alerting**

- Create Wazuh active response to block IPs with >10 failed logins
- Set up email/Slack alerts for rule 60204 (Multiple Logon Failures)

## **### Long-term Recommendations**

1. **Disable NTLM** where possible, use Kerberos authentication
2. **Implement MFA** for privileged accounts
3. **Deploy honeypot accounts** to detect credential stuffing
4. **Regular password audits** against common password lists

## **## Wazuh Query Reference**

```
# Find all failed logons from WS01  
agent.name:WS01 AND data.win.system.eventID:4625
```

```
# Find brute force alerts  
rule.id:60204 OR rule.description:*brute*
```

```
# Find events from specific attacker IP  
data.win.eventdata.ipAddress:10.0.0.10
```

## ## Lessons Learned

1. **Audit policies matter** - Without enabling failed logon auditing, no events would be generated
2. **SIEM visibility requires configuration** - Agent must be configured to collect the right logs
3. **Correlation is key** - Single failed logins are noise; patterns indicate attacks
4. **Source IP attribution** - Network logons (Type 3) include source IP, unlike interactive logons

## ## Screenshots

1. CrackMapExec attack execution from Kali

The screenshot shows a terminal window titled "kali@kali: ~". The window contains a session log and a command-line interface. The session log lists several failed logon attempts (STATUS\_LOGON\_FAILURE) for the "Administrator" account on a target host at 10.0.0.16, with the domain being "lab.local". The command-line interface shows the user running the "crackmapexec" command to perform a password cracking attack against the SMB service on the target host.

```
kali@kali: ~
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
or:(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
or:(kali㉿kali)-[~]
└─$
```

## 2. Wazuh MITRE ATT&CK dashboard showing Initial Access detections

The screenshot shows the Wazuh MITRE ATT&CK dashboard for endpoint WS01 (agent ID 002). A red circle highlights the 'Initial Access' section of the dashboard.

**System inventory:**

Cores: 4	Memory: 8GB	Operating system: Microsoft Windows 11 Pro 10.0.26200.7623	Cluster node: node01	Registration date: Jan 17, 2026 @ 09:59:32.000	Last keep alive: Jan 20, 2026 @ 11:04:18.000
Host name: WS01 Serial number: 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 donut chart showing the distribution of Initial Access techniques. The legend indicates:

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

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

**Top 5 Packages:** No recent events.

**Security Configuration Assessment:** Policy: CIS Microsoft Windows 11 Enterprise Benchmark v1.0.0. End scan: Jan 20, 2026 @ 10:25:20.000. Score: 33%.

Bottom navigation bar: Cloud icon, Search icon, Home icon, File icon, Database icon, Network icon, Application icon, User icon, Help icon.

### 3. Event list filtered by Event ID 4625

The screenshot displays two browser windows showing Wazuh MITRE ATT&CK analysis results.

**Top Window (Dashboard View):**

- Alerts evolution over time:** A line chart showing the count of alerts over time (timestamp per 30 minutes) from 12:00 to 09:00. The count remains at 0 until approximately 03:00, then rises sharply to about 10 by 09:00.
- Top tactics:** A donut chart showing the distribution of tactics. The legend indicates Impact (red) and Credential Access (pink).
- Rule level by attack:** A donut chart showing the distribution of rule levels by attack type. The legend includes Account Access Remote (pink), Brute Force (yellow), 5 (orange), and 10 (light yellow).
- MITRE attacks by tactic:** A bar chart showing the count of MITRE attacks by tactic. The legend indicates Account Access Remote (pink) and Brute Force (yellow). The chart shows a single bar for Impact with a count of 15, and a small bar for Credential Access with a count of approximately 2.
- Rule level by tactic:** A donut chart showing the distribution of rule levels by tactic. The legend indicates Impact (red), Credential Access (pink), 5 (orange), and 10 (light yellow).

**Bottom Window (Event List View):**

- Event Count:** Shows a bar chart with a total count of 18 hits.
- Table:** Displays a list of 18 log entries. Each entry includes timestamp, agent.name (WS01), rule.mitre.id (T1531), rule.mitre.tactic (Impact), rule.description (Logon Failure - Unknown user or bad password), rule.level (5), and rule.id (60122). The log entries show multiple instances of Logon Failure due to unknown users or bad passwords between Jan 19, 2026, and Jan 20, 2026.
- Page Information:** The bottom status bar shows the date (1/20/2026), time (11:08 AM), and a file icon with a '2'.

#### 4. Detailed event view showing attacker IP (10.0.0.10)

The screenshot shows a web browser window with three tabs, all titled "Wazuh". The active tab displays a log entry from "wazuh-alerts-4.x-2026.01.20#nKe\_3JsBiz2QX-Ik1Bap".

The log entry details:

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	NtLmSp
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: 0x0

## **## References**

- [MITRE ATT&CK T1110 - Brute Force](<https://attack.mitre.org/techniques/T1110/>)
- [Windows Event ID 4625](<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625>)
- [Wazuh Documentation](<https://documentation.wazuh.com/>)
- [CrackMapExec Wiki](<https://wiki.porchetta.industries/>)