 # 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	**Attacker source IP**
`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

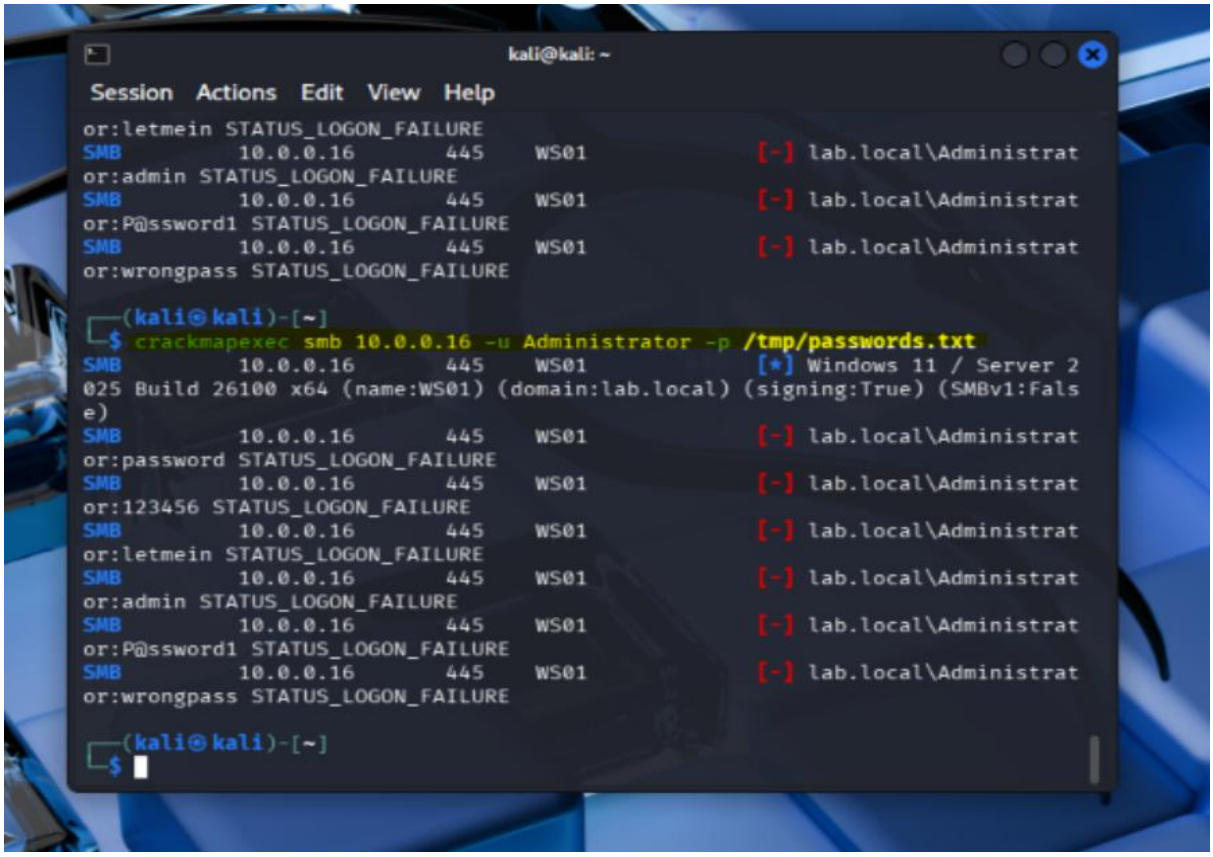
2. **SIEM visibility requires configuration** - Agent must be configured to collect the right logs

3. **Correlation is key** - Single failed logins are noise; patterns indicate attacks

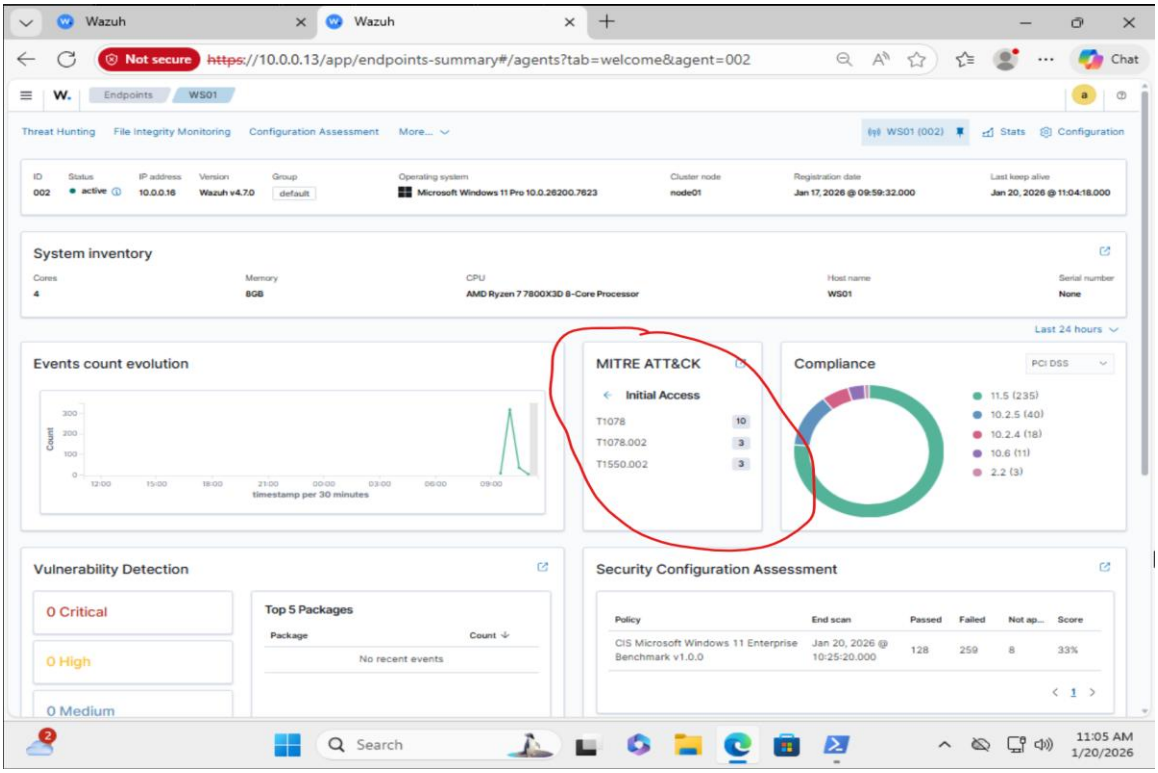
4. **Source IP attribution** - Network logons (Type 3) include source IP, unlike interactive logons

Screenshots

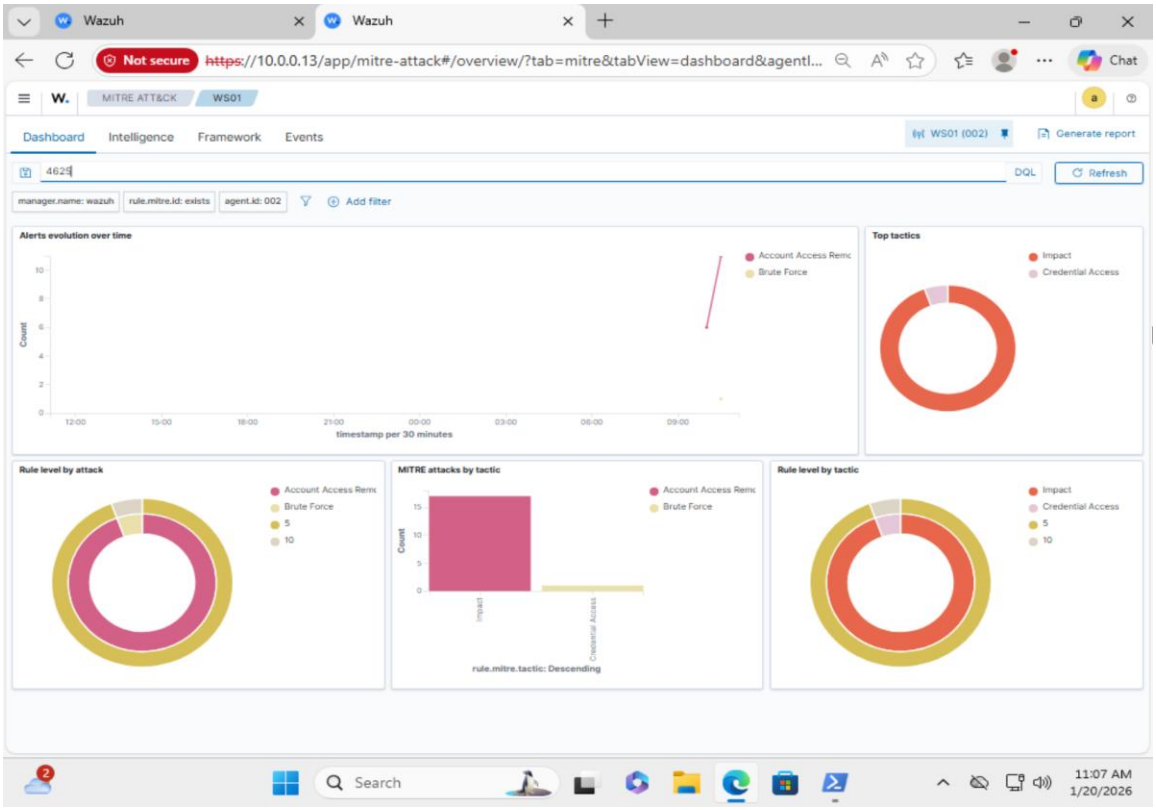
1. CrackMapExec attack execution from Kali

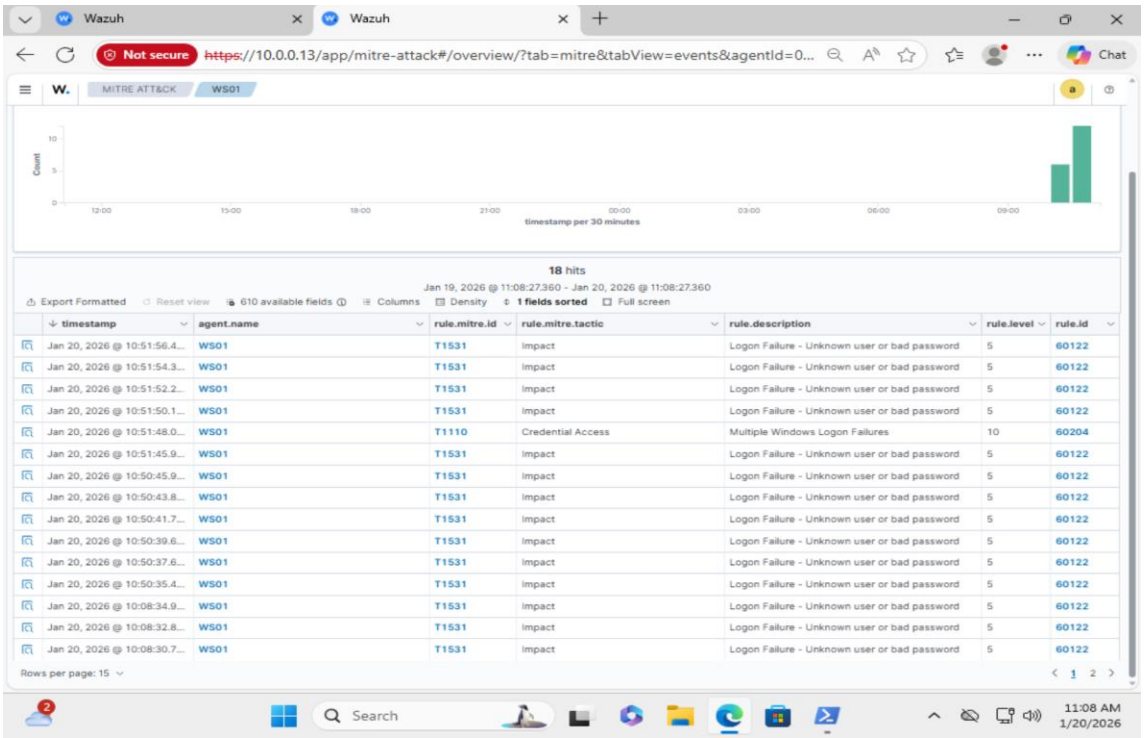


2. Wazuh MITRE ATT&CK dashboard showing Initial Access detections

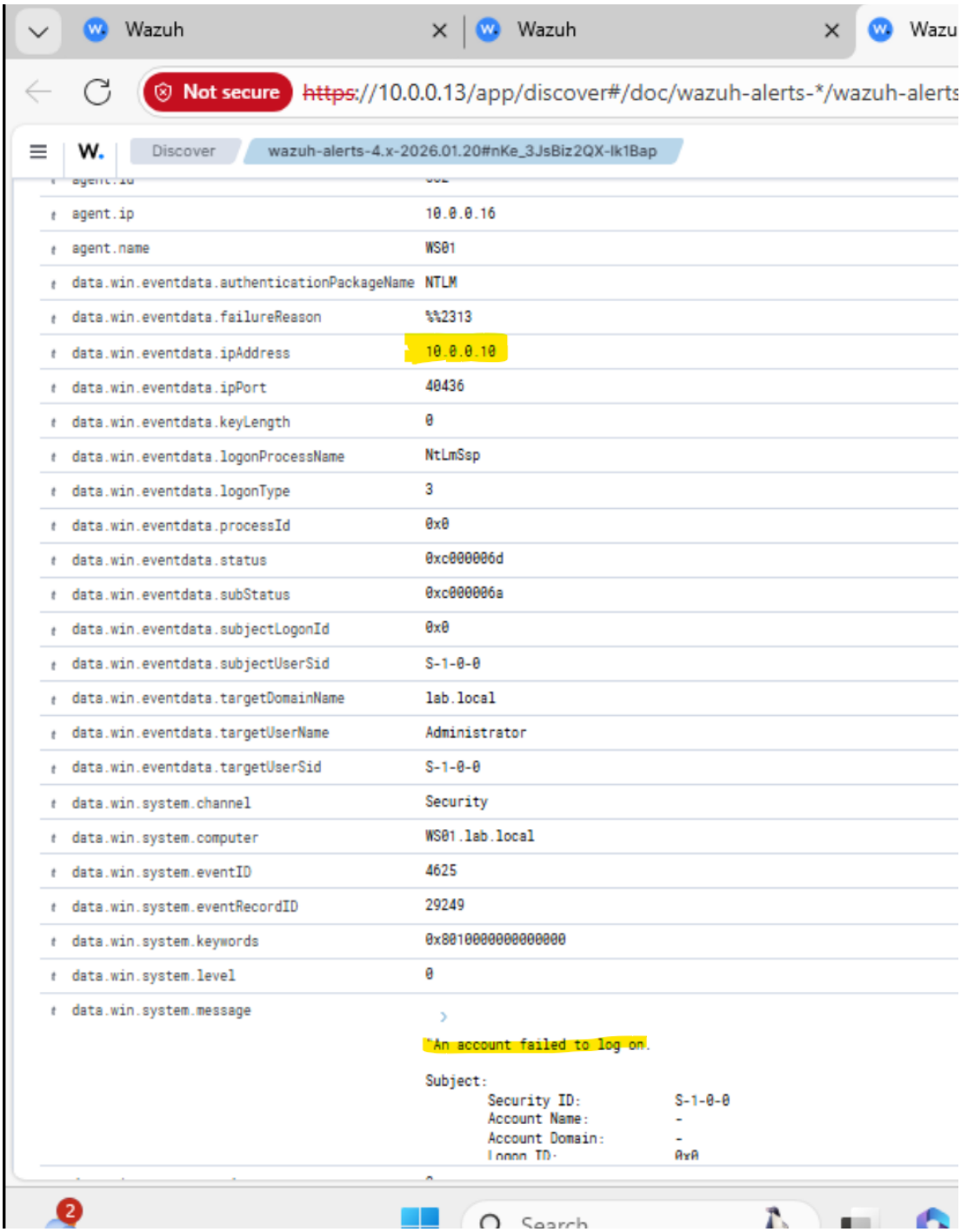


3. Event list filtered by Event ID 4625





4. Detailed event view showing attacker IP (10.0.0.10)



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/)