SOC Project – SSH Brute Force Detection

1. Objective

Detect and analyze SSH brute-force login attempts against a Windows 11 host using Windows
Security Event Logs and controlled attack simulation from Kali Linux.

2. Environment

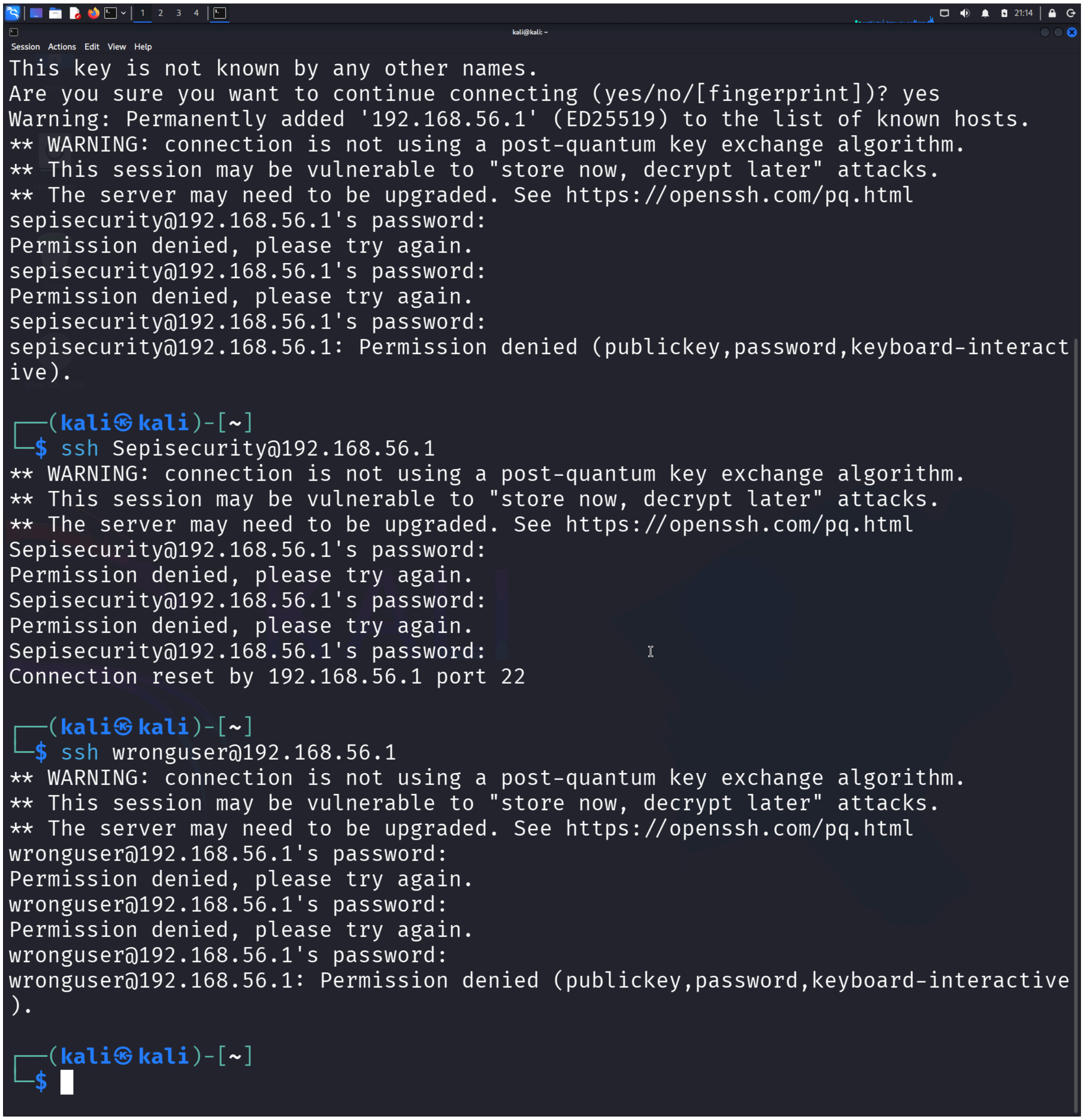
1 Attacker: Kali Linux
2 Victim: Windows 11 (OpenSSH Server enabled)
3 Service: SSH (Port 22)
4 Log Source: Windows Security Event Log
5 Tools Used: PowerShell, Nmap, SSH

3. Attack Simulation

Multiple SSH login attempts were executed from Kali Linux using invalid credentials. This simulated
a brute-force authentication attempt against the Windows host.

4. Detection

Repeated failed login events were detected in the Windows Security Log. Event ID 4625 (An account failed to log on) was observed multiple times from the same source IP address within a short time period. The repeated Event ID 4625 failures from the same source IP within seconds indicate brute-force behavior rather than normal user mistyping.

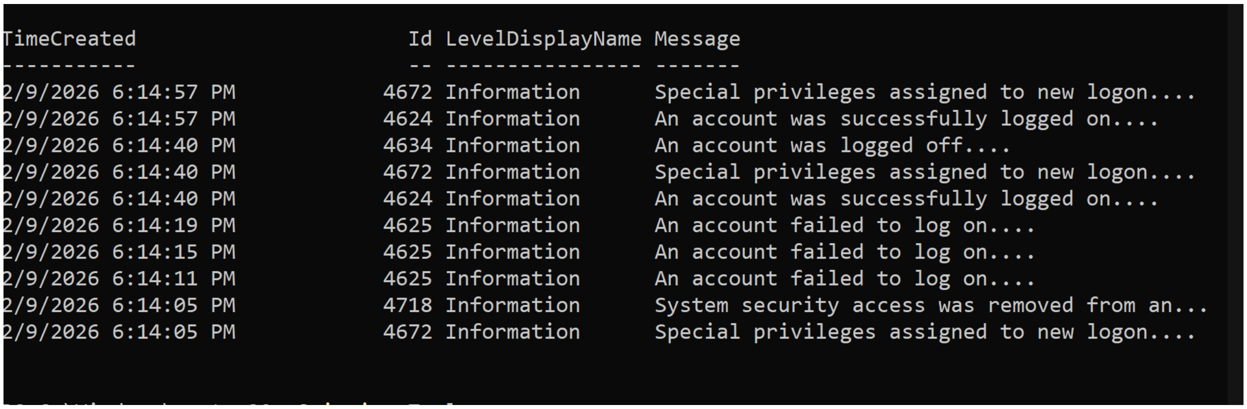


```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.1' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
sepisecurity@192.168.56.1's password:
Permission denied, please try again.
sepisecurity@192.168.56.1's password:
Permission denied, please try again.
sepisecurity@192.168.56.1's password:
sepisecurity@192.168.56.1: Permission denied (publickey,password,keyboard-interact
ive).

┌──(kali㉿kali)-[~]
└─$ ssh Sepisecurity@192.168.56.1
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Sepisecurity@192.168.56.1's password:
Permission denied, please try again.
Sepisecurity@192.168.56.1's password:
Permission denied, please try again.
Sepisecurity@192.168.56.1's password:
Connection reset by 192.168.56.1 port 22

┌──(kali㉿kali)-[~]
└─$ ssh wronguser@192.168.56.1
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
wronguser@192.168.56.1's password:
Permission denied, please try again.
wronguser@192.168.56.1's password:
Permission denied, please try again.
wronguser@192.168.56.1's password:
wronguser@192.168.56.1: Permission denied (publickey,password,keyboard-interactive
).

┌──(kali㉿kali)-[~]
└─$ 
```



```
TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
2/9/2026 6:14:57 PM           4672 Information      Special privileges assigned to new logon....
2/9/2026 6:14:57 PM           4624 Information      An account was successfully logged on....
2/9/2026 6:14:40 PM           4634 Information      An account was logged off....
2/9/2026 6:14:40 PM           4672 Information      Special privileges assigned to new logon....
2/9/2026 6:14:40 PM           4624 Information      An account was successfully logged on....
2/9/2026 6:14:19 PM           4625 Information      An account failed to log on....
2/9/2026 6:14:15 PM           4625 Information      An account failed to log on....
2/9/2026 6:14:11 PM           4625 Information      An account failed to log on....
2/9/2026 6:14:05 PM           4718 Information      System security access was removed from an...
2/9/2026 6:14:05 PM           4672 Information      Special privileges assigned to new logon....
```

5. Timeline (Sample)

1 6:14:11 PM – Failed login (Event ID 4625)
2 6:14:15 PM – Failed login (Event ID 4625)
3 6:14:19 PM – Failed login (Event ID 4625)
4 6:14:40 PM – Successful login (Event ID 4624)

6. Indicators of Compromise (IoCs)

1 Source IP: 192.168.56.1 (Kali Linux)
2 Event ID: 4625 (Failed Logon)
3 Target Account: Windows local user account
4 Protocol: SSH
5 Port: 22

7. Severity Assessment

Severity: Medium. Although no confirmed account compromise was observed, the repeated
authentication attempts indicate malicious intent and require monitoring.

8. Response & Mitigation Recommendations

1 Block suspicious IP addresses via firewall rules.
2 Enable account lockout policies.
3 Implement multi-factor authentication (MFA).
4 Continue monitoring authentication logs for abnormal activity.

9. Lessons Learned

This project demonstrates how SSH brute-force attacks can be identified through log analysis. Even basic monitoring of Windows Security Event Logs provides sufficient visibility to detect suspicious authentication behavior.