Day 6: Incident Respond

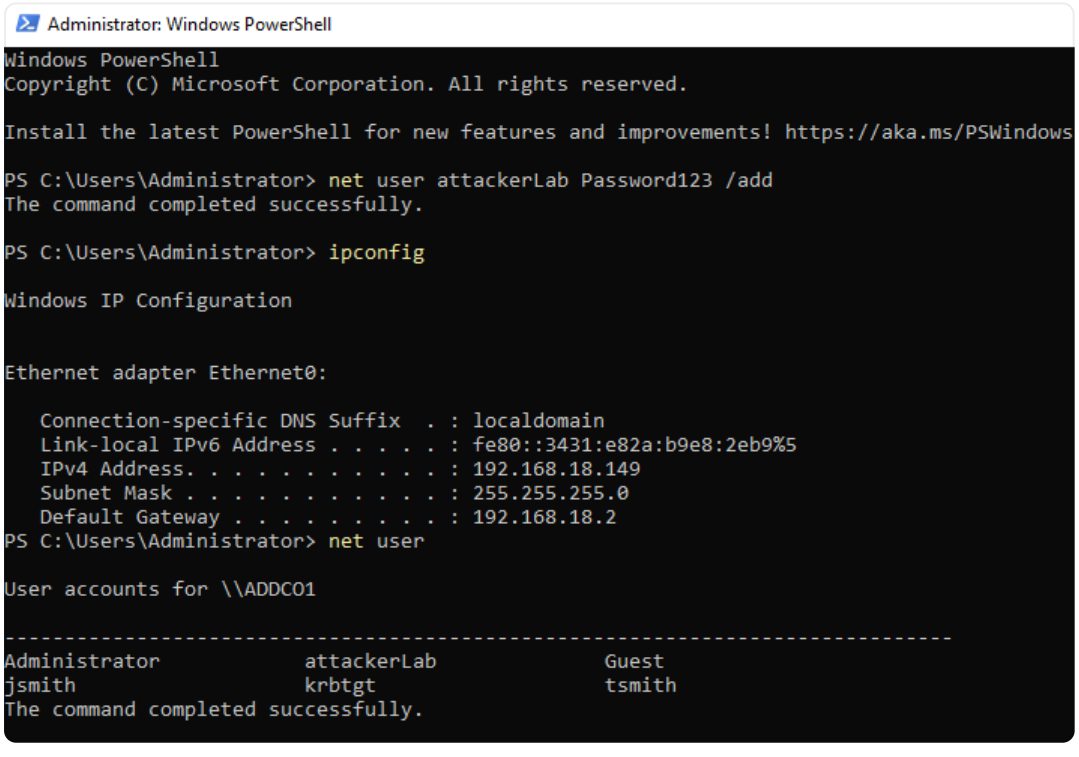
Objective
The objective of this project is to explore the core concepts of incident response, gain familiarity with the incident response lifecycle, and understand how basic threats on Windows systems can be detected, analyzed, and responded to using standard security monitoring tools and techniques.

Tools

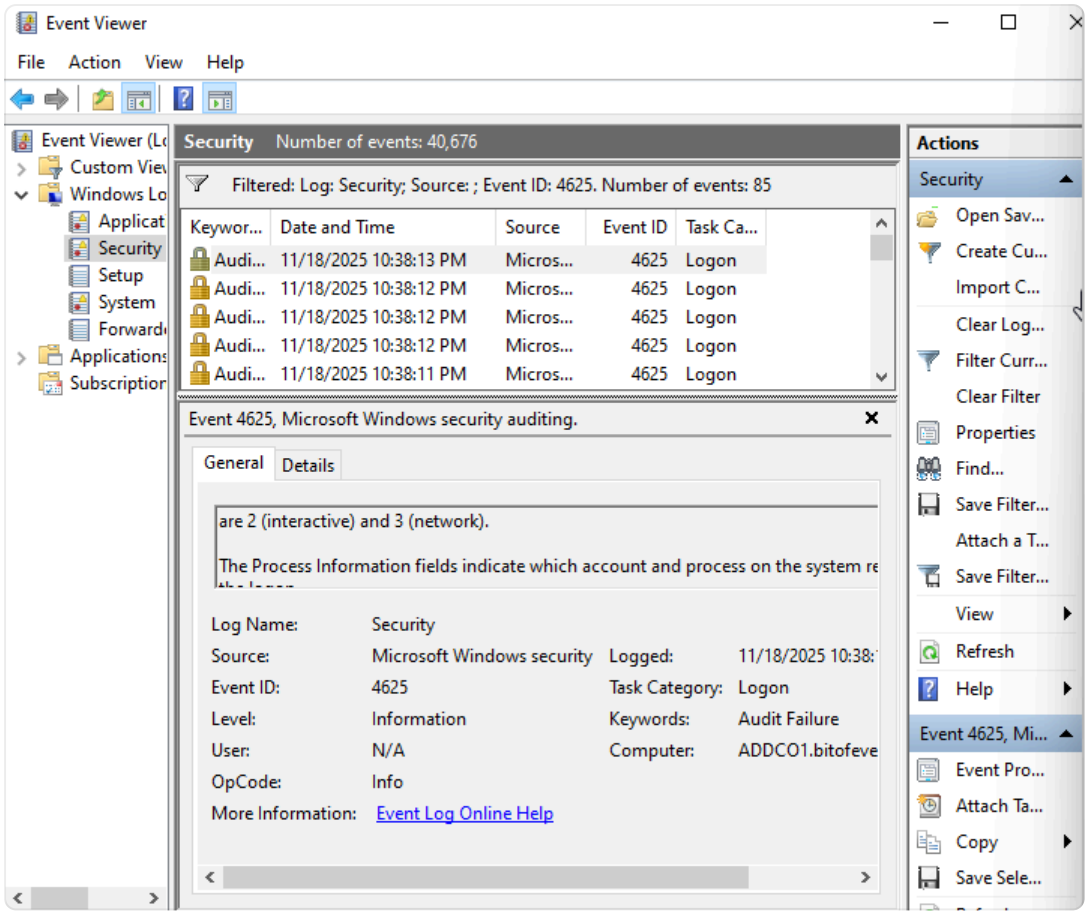
Here are the tools used:

- **Kali Linux**
- **Hydra** (for brute-force attack)
- **Windows Server**
- **Remote Desktop Protocol (RDP)**
- **Windows Event Viewer** (for log analysis)
- **Windows Defender Firewall** (for blocking the attack)

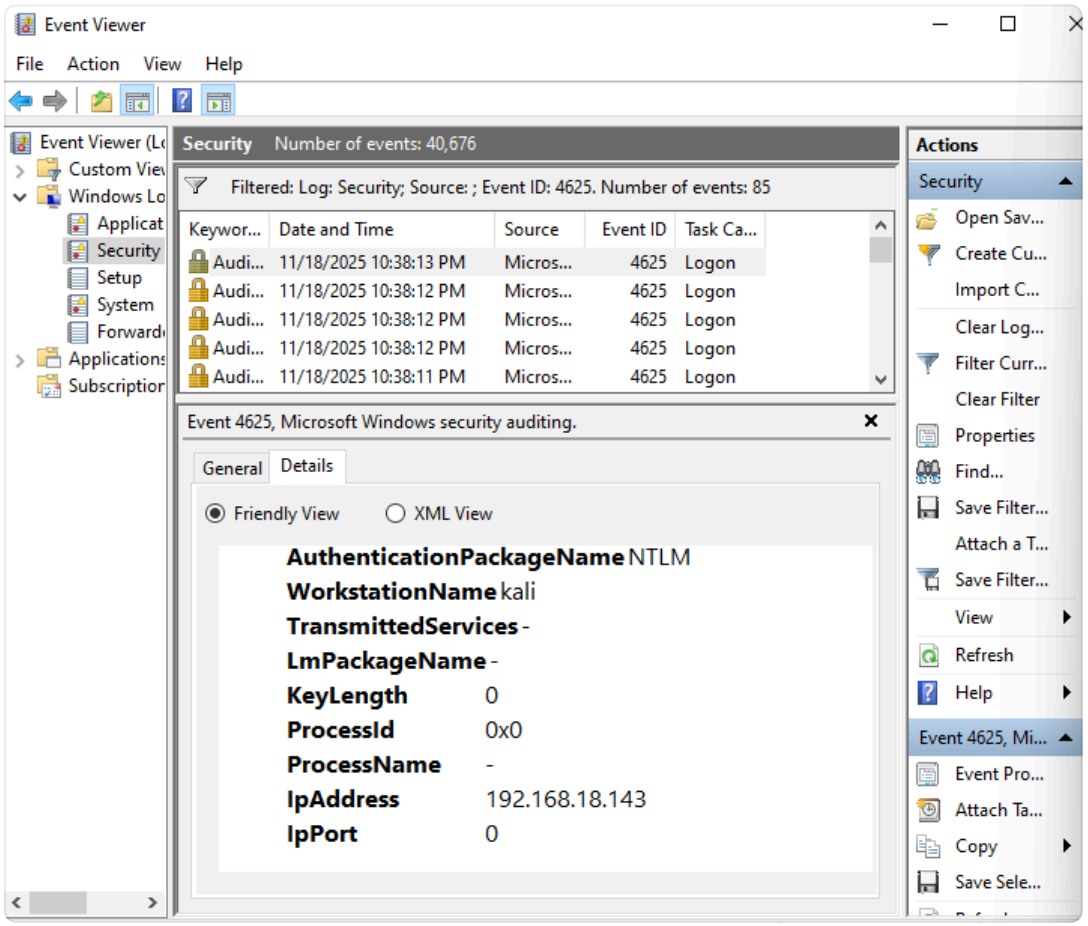
A controlled brute-force attack was initiated from a Kali Linux system targeting a Windows Server machine where Remote Desktop Protocol (RDP) was enabled. The attack was executed using Hydra, simulating an unauthorized attempt to gain access by trying multiple credential combinations.



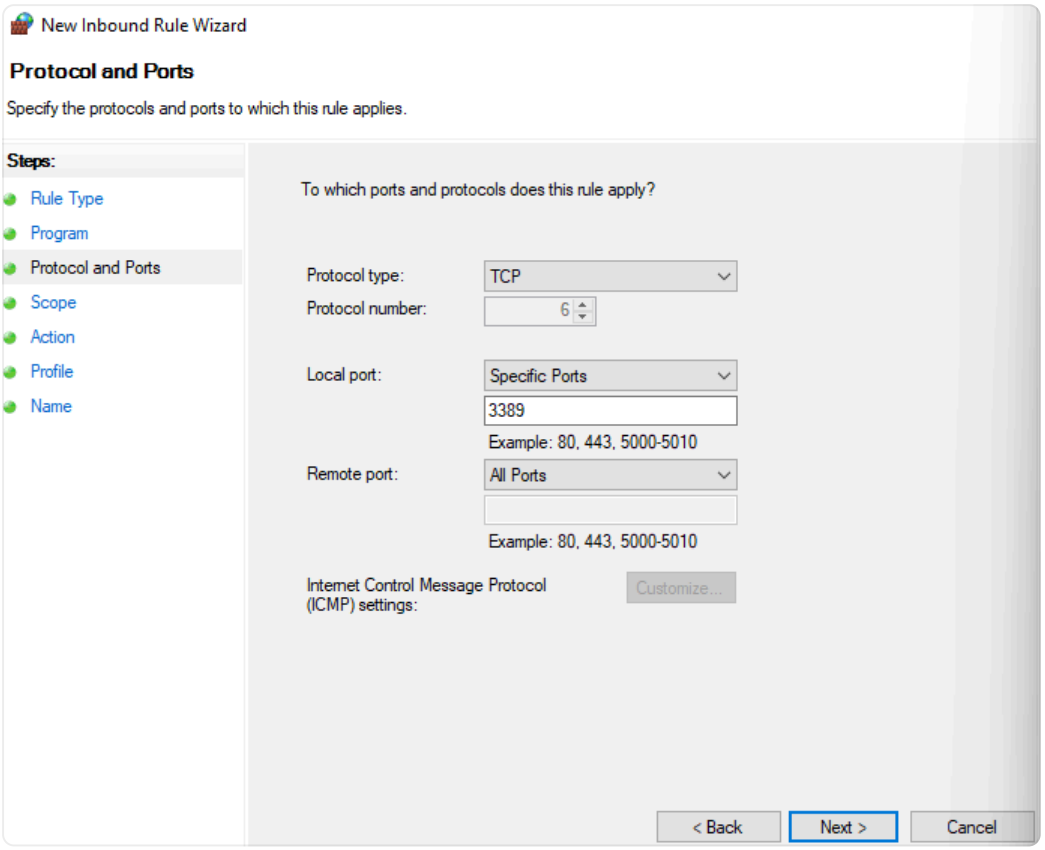
The attack did not succeed. To validate the outcome, the Windows Event Viewer was examined by navigating to Windows Logs → Security and filtering for Event ID 4625, which records failed logon attempts. The security log revealed multiple entries corresponding to Event ID 4625, each indicating failed authentication attempts originating from the same source IP address associated with the Kali Linux machine.

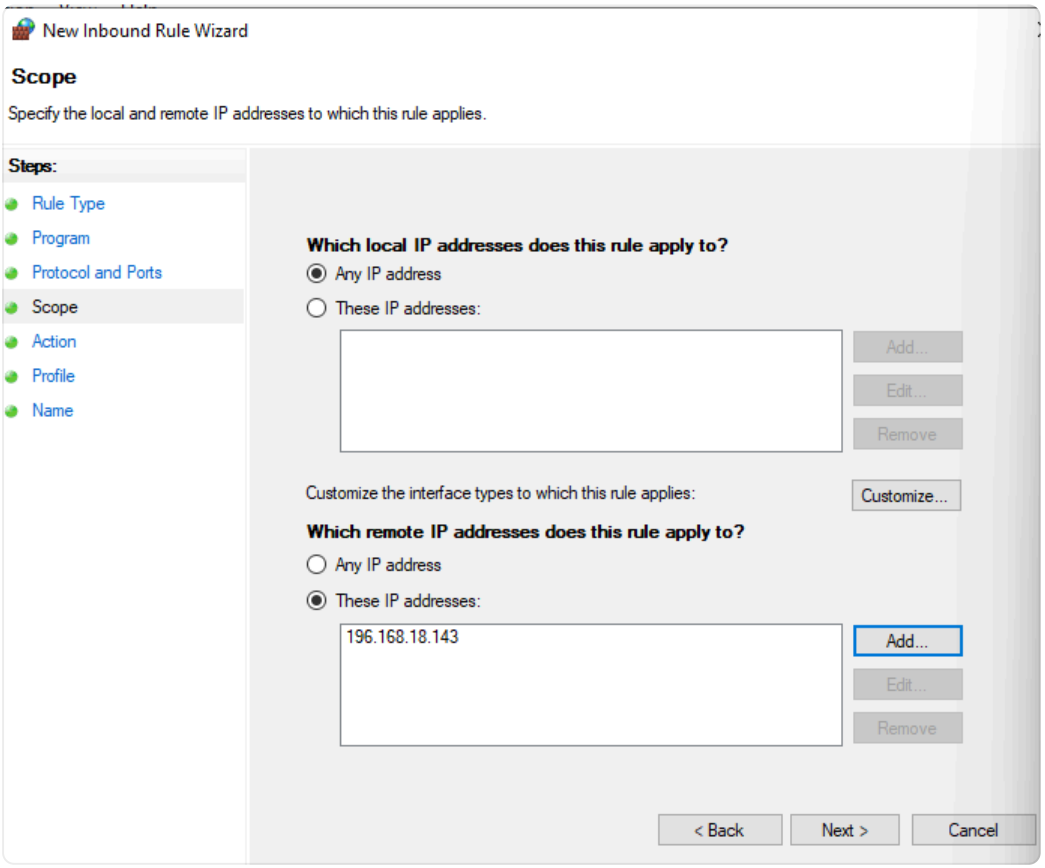


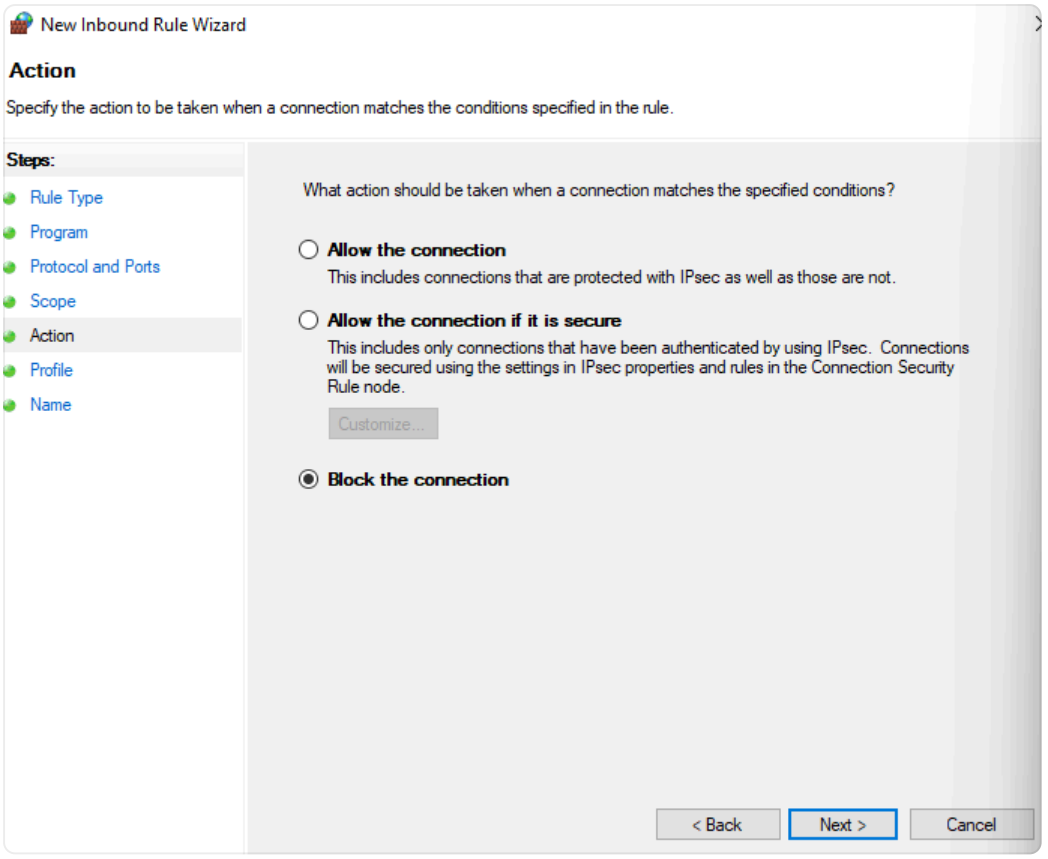
This confirmed that the Windows Server correctly detected and logged the brute-force activity, showing clear evidence of repeated failed login attempts and the source system responsible. The correlation of timestamps, Event ID 4625 entries, and the originating IP address demonstrated the system's ability to provide reliable audit trails during a security incident.

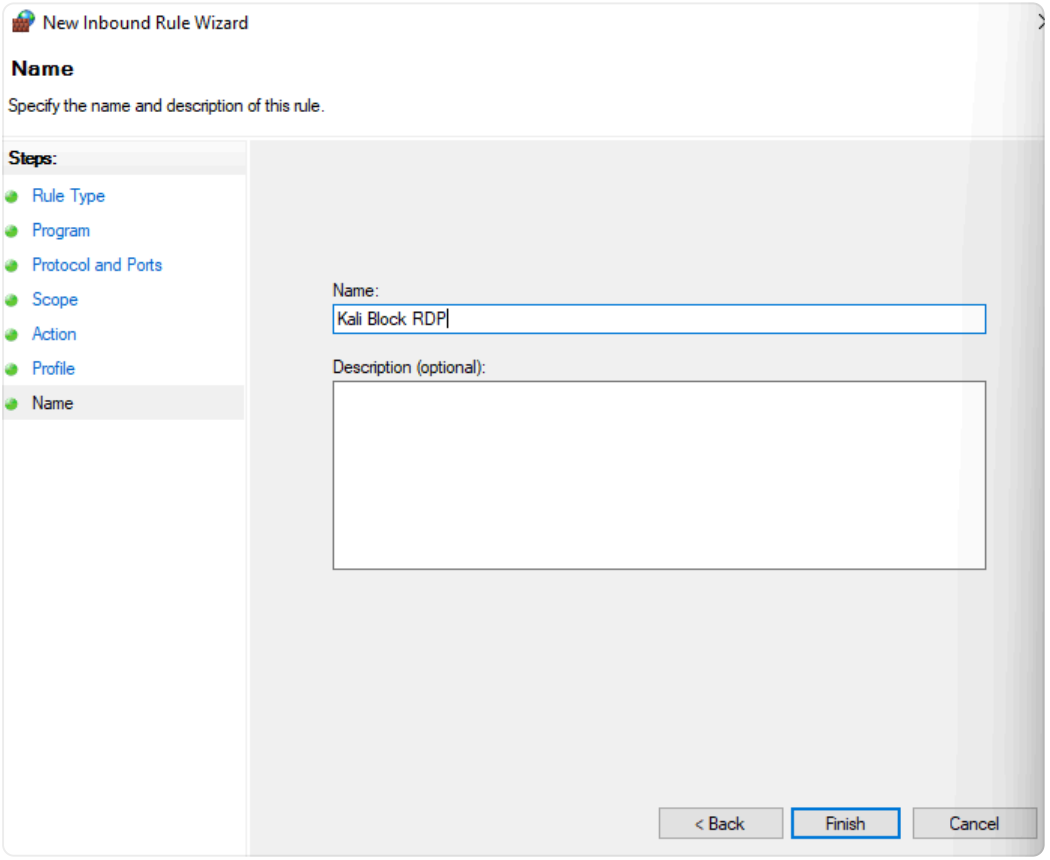


To mitigate the ongoing brute-force attempts, a firewall rule was created on the Windows Server to block incoming traffic from the Kali Linux machine. This was done by navigating to Windows Defender Firewall → Advanced Settings → Inbound Rules and creating a new custom rule. The wizard was followed step by step, specifying the Kali Linux IP address as the source to be denied.

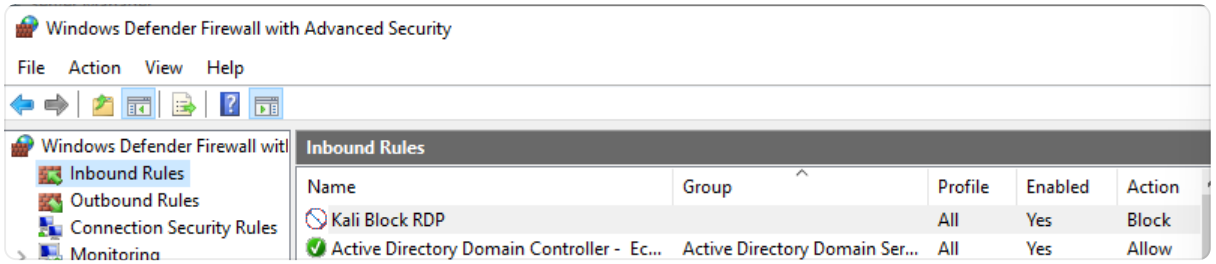








Once the rule was applied, the IP address associated with the attack was successfully blocked, as shown in the corresponding screenshot. With this rule in place, all traffic originating from the Kali Linux system was filtered at the firewall level, preventing further Remote Desktop connection attempts.



This demonstrated the system's ability to enforce network-level controls in response to detected malicious activity, effectively stopping the unauthorized access attempts in real time.