

# 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.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> net user attackerLab Password123 /add
The command completed successfully.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::3431:e82a:b9e8:2eb9%5
IPv4 Address . . . . . : 192.168.18.149
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.18.2
PS C:\Users\Administrator> net user

User accounts for \\ADDC01

-----
Administrator          attackerLab           Guest
jsmith                krbtgt                 tsmith
The command completed successfully.
```

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.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom View, Windows Logs (selected), Applications, and Subscriptions. Under Windows Logs, Application, Security, Setup, System, Forwarder, and Forwarded are listed. The main pane shows the Security log with 40,676 events. A filter is applied: Log: Security; Source: ; Event ID: 4625. Number of events: 85. The results show multiple failed logon attempts from the same source IP (192.168.18.143) at different times on November 18, 2025. The right pane is the Actions menu, and the bottom pane shows the details of a selected event (Event ID 4625).

| Keyword | Date and Time          | Source    | Event ID | Task Category |
|---------|------------------------|-----------|----------|---------------|
| Audi... | 11/18/2025 10:38:13 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:11 PM | Micros... | 4625     | Logon         |

Event 4625, Microsoft Windows security auditing.

General Details

are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system re

Log Name: Security  
 Source: Microsoft Windows security  
 Event ID: 4625  
 Level: Information  
 User: N/A  
 OpCode: Info  
 More Information: [Event Log Online Help](#)

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.

The screenshot shows the Windows Event Viewer interface, identical to the first one but with a different view. The left pane shows the same log structure. The main pane shows the Security log with 40,676 events. A filter is applied: Log: Security; Source: ; Event ID: 4625. Number of events: 85. The results show multiple failed logon attempts from the same source IP (192.168.18.143) at different times on November 18, 2025. The right pane is the Actions menu. The bottom pane shows the details of a selected event (Event ID 4625) in XML View.

| Keyword | Date and Time          | Source    | Event ID | Task Category |
|---------|------------------------|-----------|----------|---------------|
| Audi... | 11/18/2025 10:38:13 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:12 PM | Micros... | 4625     | Logon         |
| Audi... | 11/18/2025 10:38:11 PM | Micros... | 4625     | Logon         |

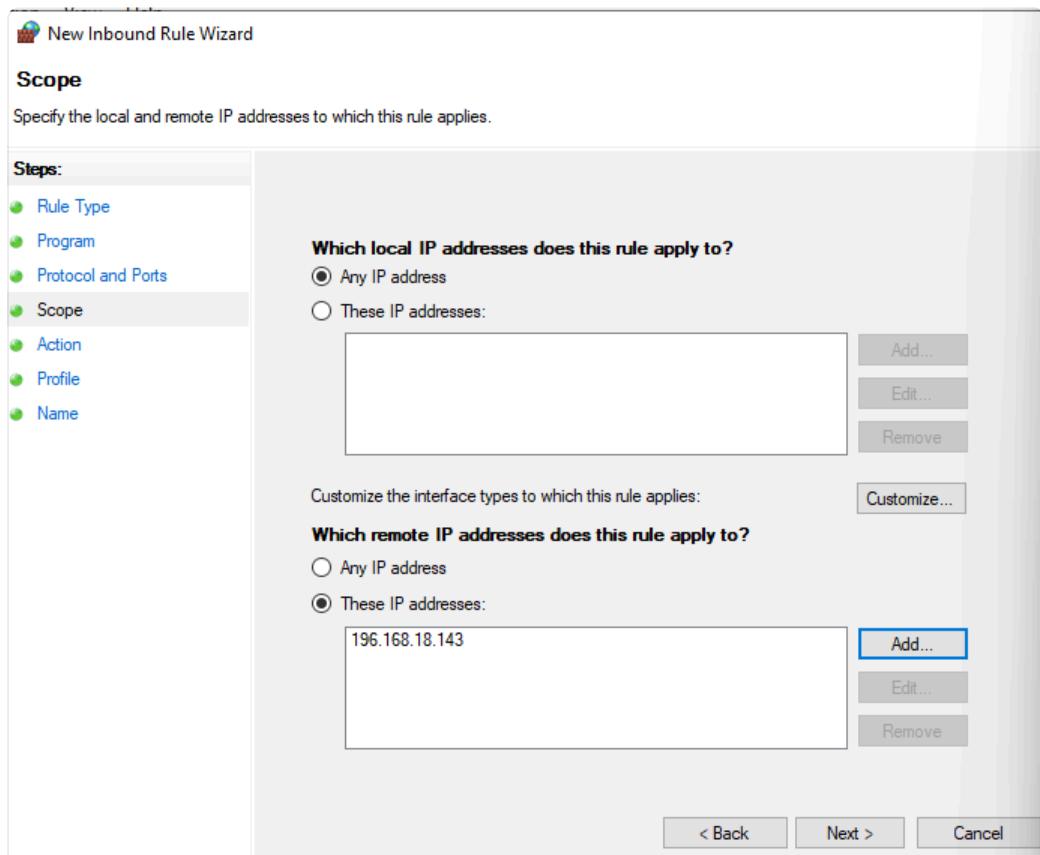
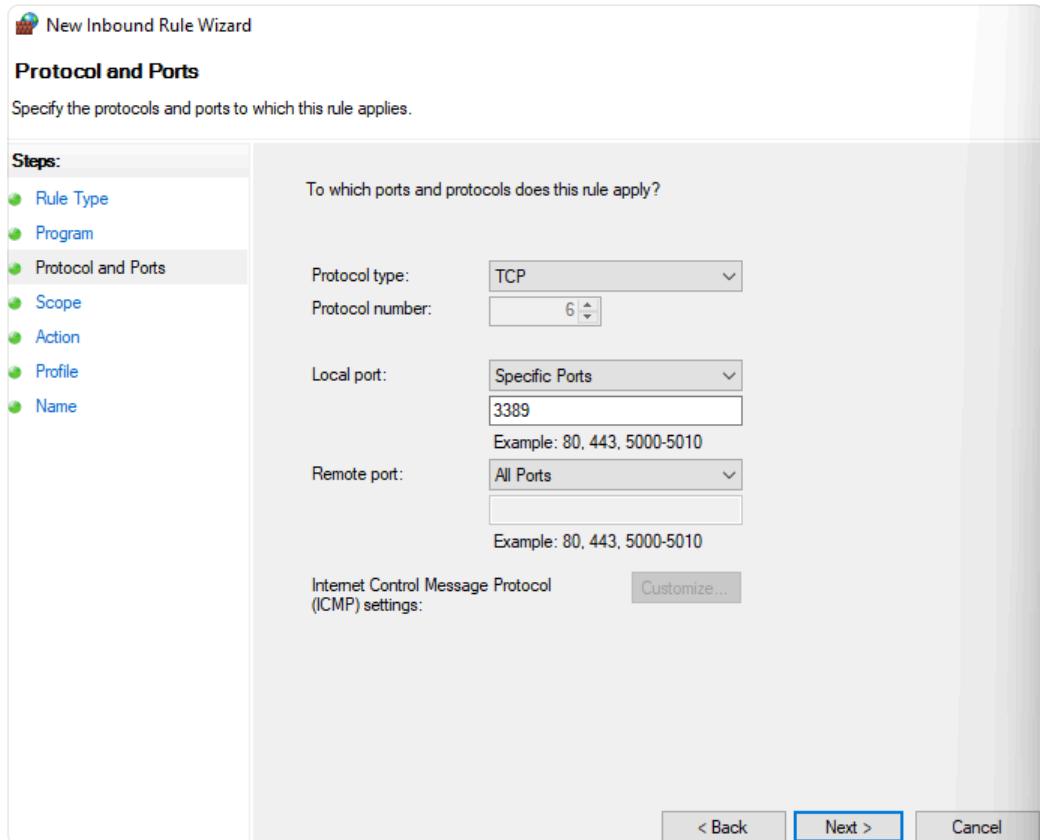
Event 4625, Microsoft Windows security auditing.

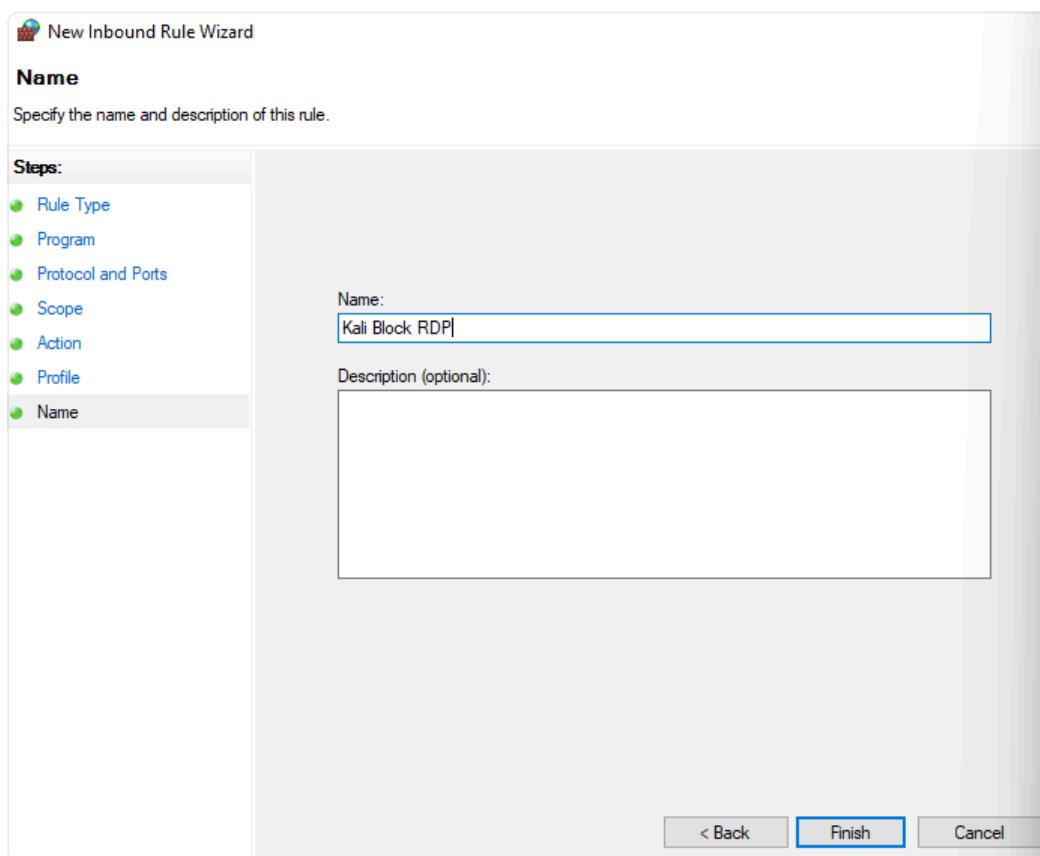
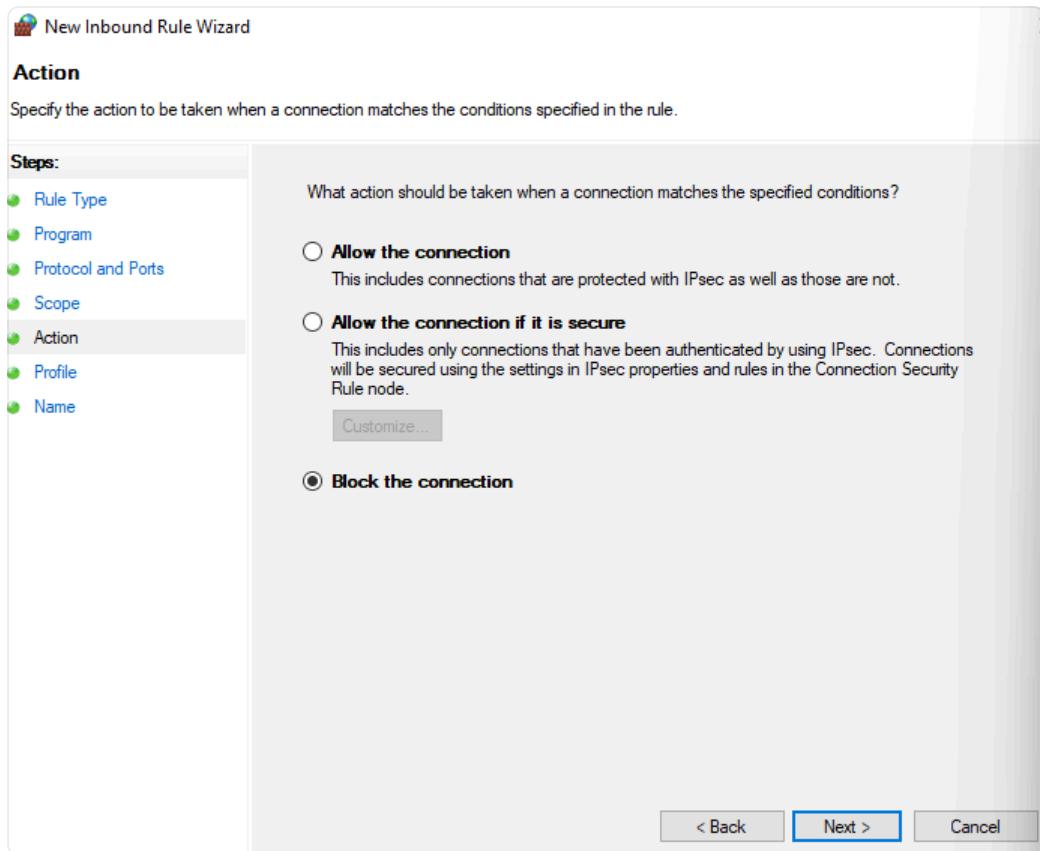
General Details

Friendly View  XML View

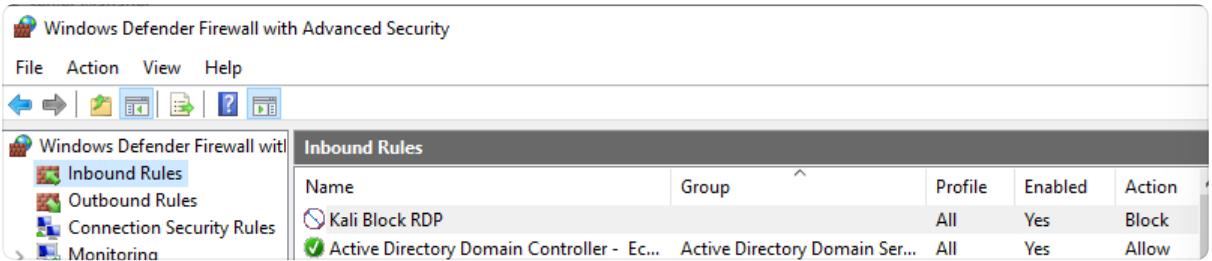
**AuthenticationPackageName** NTLM  
**WorkstationName** kali  
**TransmittedServices** -  
**LmPackageName** -  
**KeyLength** 0  
**ProcessId** 0x0  
**ProcessName** -  
**IpAddress** 192.168.18.143  
**IpPort** 0

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.

```
kali@kali: ~
File Actions Edit View Help

[(kali㉿kali)-[~]]$ nmap -p3389 192.168.18.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-19 13:41 EST
Nmap scan report for 192.168.18.149
Host is up (0.0012s latency).

PORT      STATE      SERVICE
3389/tcp  filtered  ms-wbt-server
MAC Address: 00:0C:29:C1:AC:56 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```