# Detect and Respond: Windows Server RDP Brute Force Attack

## Overview

This lab exercise focuses on simulating a Remote Desktop Protocol (RDP) brute-force attack using Hydra from a Kali Linux machine targeting a Windows Server 2022. The exercise includes monitoring for failed login attempts using the Event Viewer, identifying suspicious behavior through Event ID 4625 logs, and applying basic incident response strategies to secure the system.

## Objective

- Simulate an RDP brute-force attack
- Detect suspicious login attempts using Event Viewer
- Respond with IP blocking and account disabling
- Understand Event ID 4625 and RDP logon type 10

## Tasks

- Configure Windows Server 2019 with RDP and test user
- Launch brute-force attack using Kali Linux and Hydra
- Monitor security logs and identify attack signatures
- Respond by blocking IP and disabling the compromised user
- Document findings and provide screenshots for submission

## Detailed Report

**Lab Setup**

**Environment setup:**

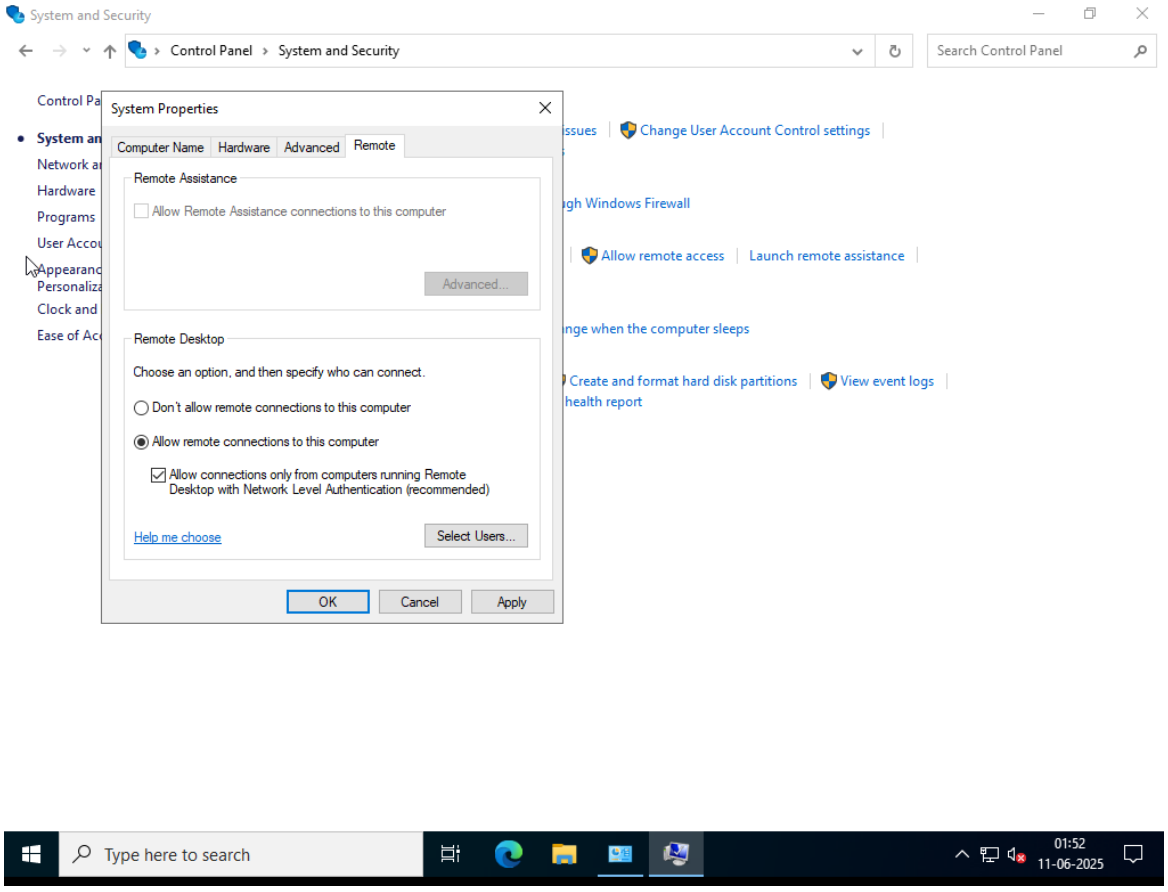
- Windows Server 2022
- Kali Linux
- Both on same NAT/Host-Only

- RDP port 3389 open and accessible

## Configuration Steps on Windows Server

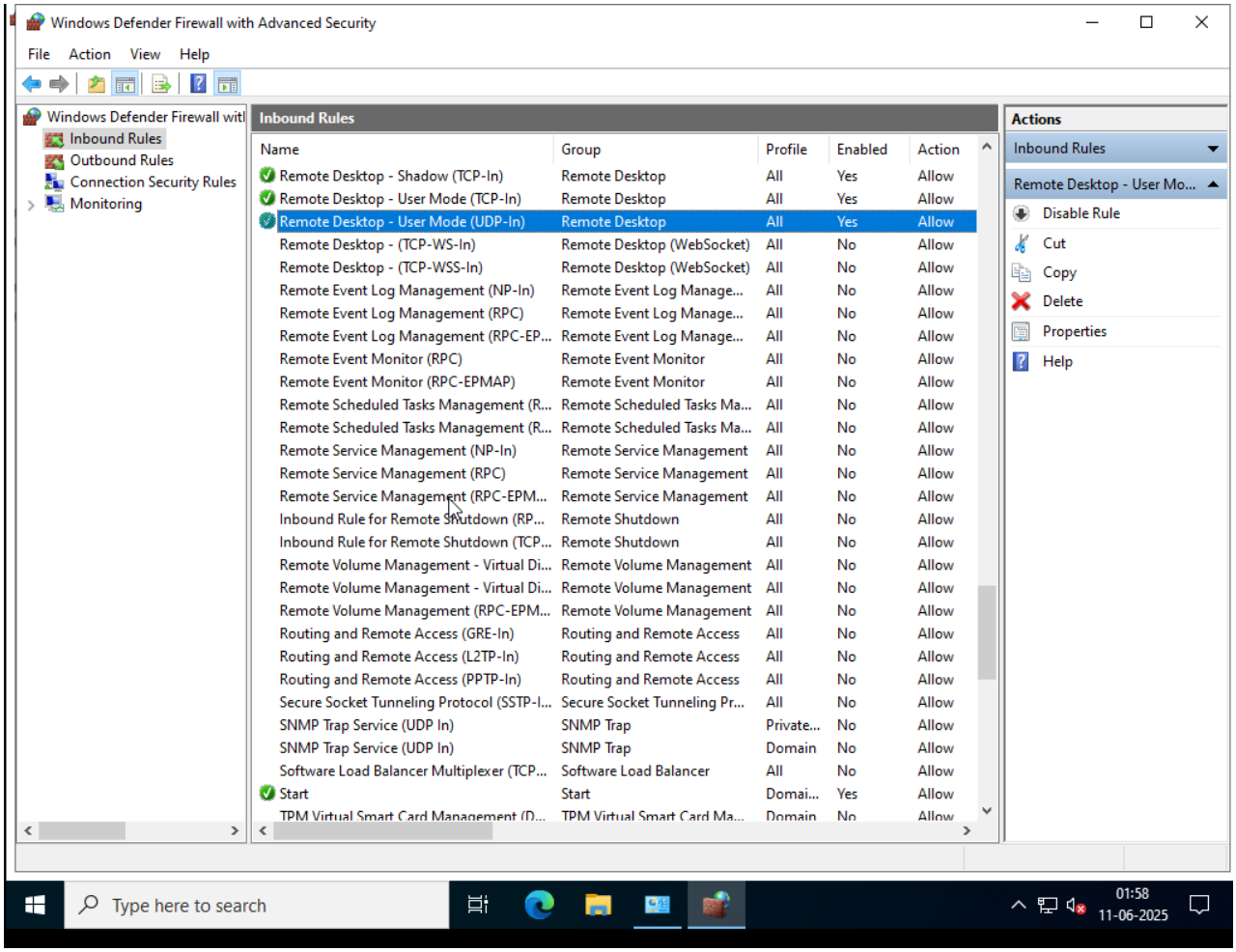
1. Enable Remote Desktop

Control Panel → System → Remote Settings → Enable Remote Desktop



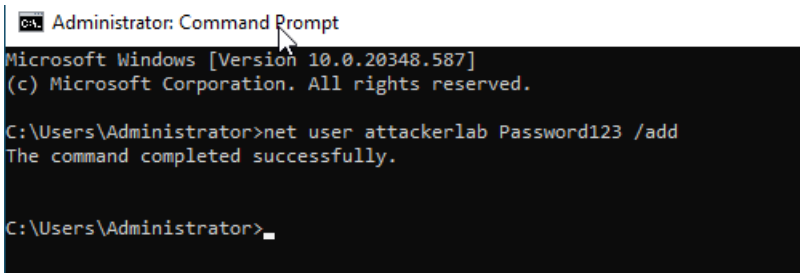

2. Allow RDP in Windows Firewall

Windows Defender Firewall → Advanced Settings → Enable “Remote Desktop (TCP-In)”




3. Create a Test User

net user attackerlab Password123 /add




4. Open Event Viewer

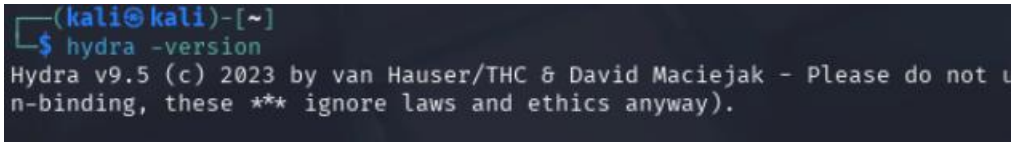
- Windows Logs → Security → Filter Event ID: 4625

## Simulating the Attack

**On Kali Linux (Hydra Command)**

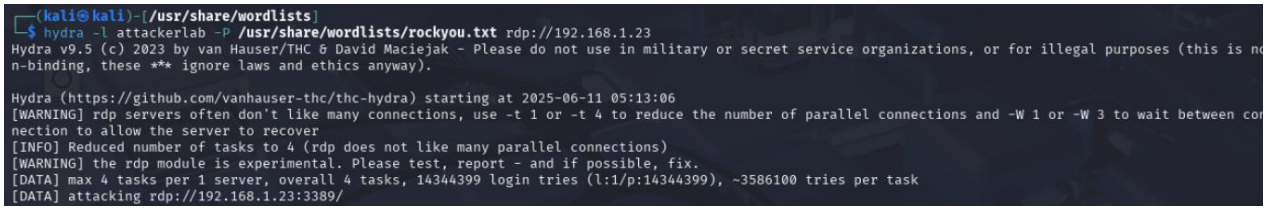
1. Install Hydra (if not already installed):

   sudo apt update && sudo apt install hydra




2. Run RDP brute-force attack:

hydra -l attackerlab -P /usr/share/wordlists/rockyou.txt rdp://192.168.1.23

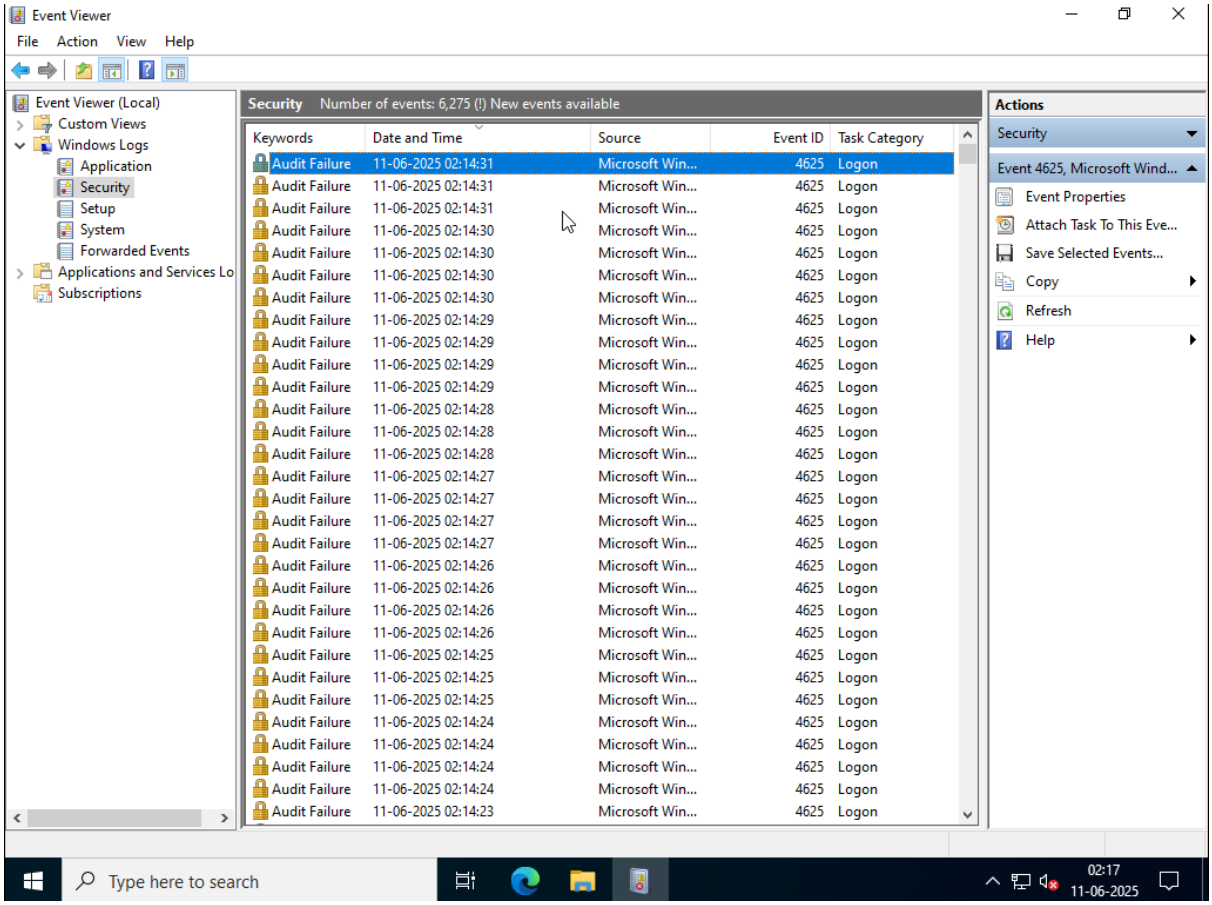



## Detection and Visualization

🔍 On Windows Server

Open Event Viewer > Windows Logs > Security

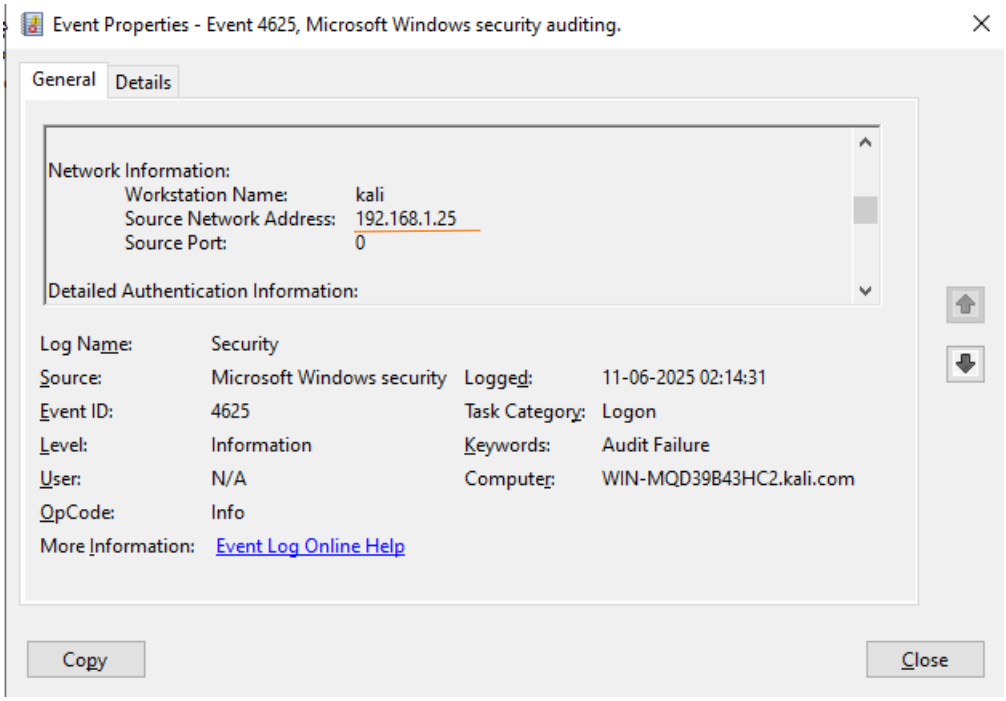
Look for Event ID: 4625




- Logon Type: 10 (RemoteInteractive)

- Failure Reason: "Unknown user name or bad password"

- Source IP: Kali Linux IP Address



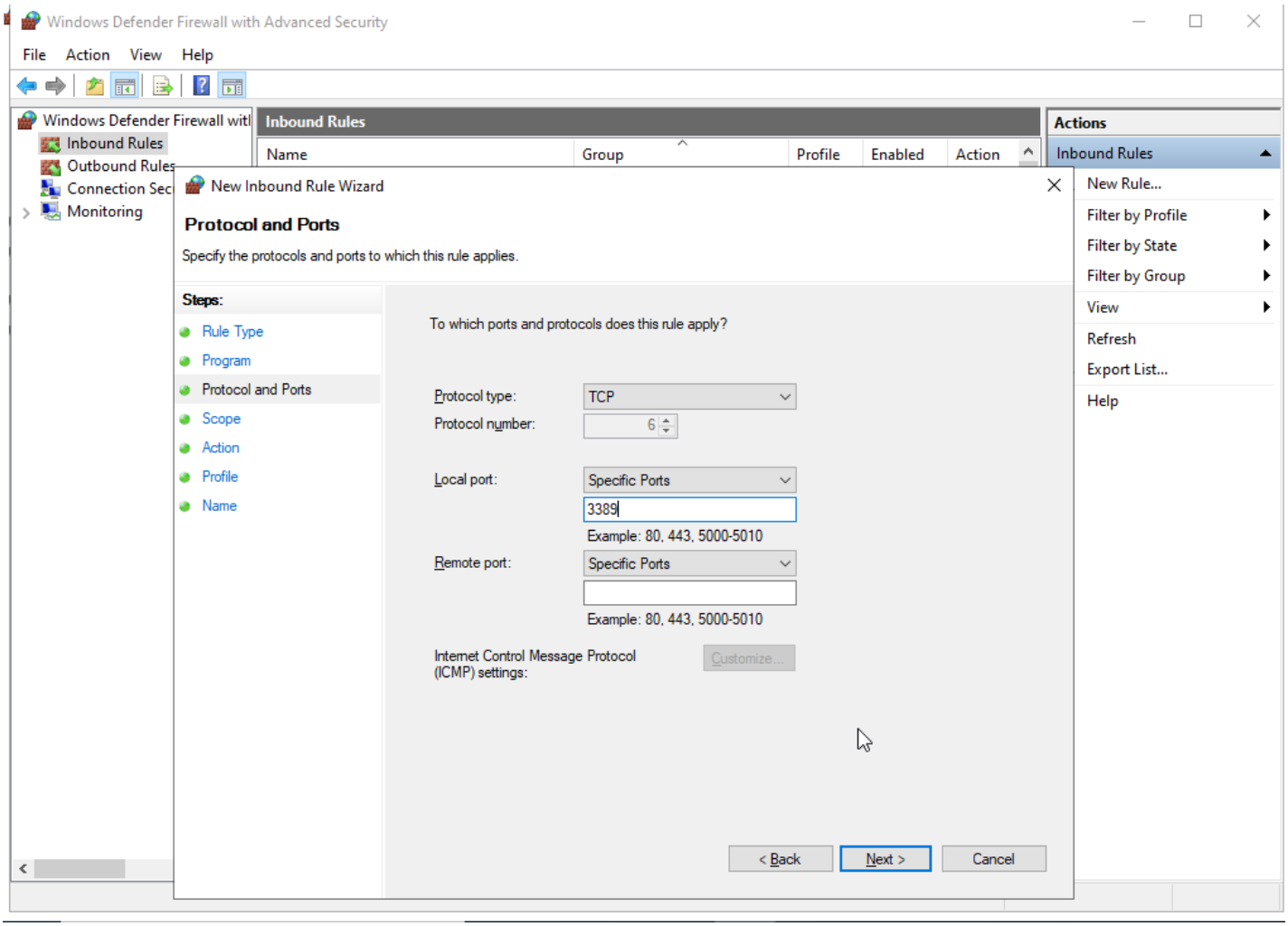

## Incident Response Steps

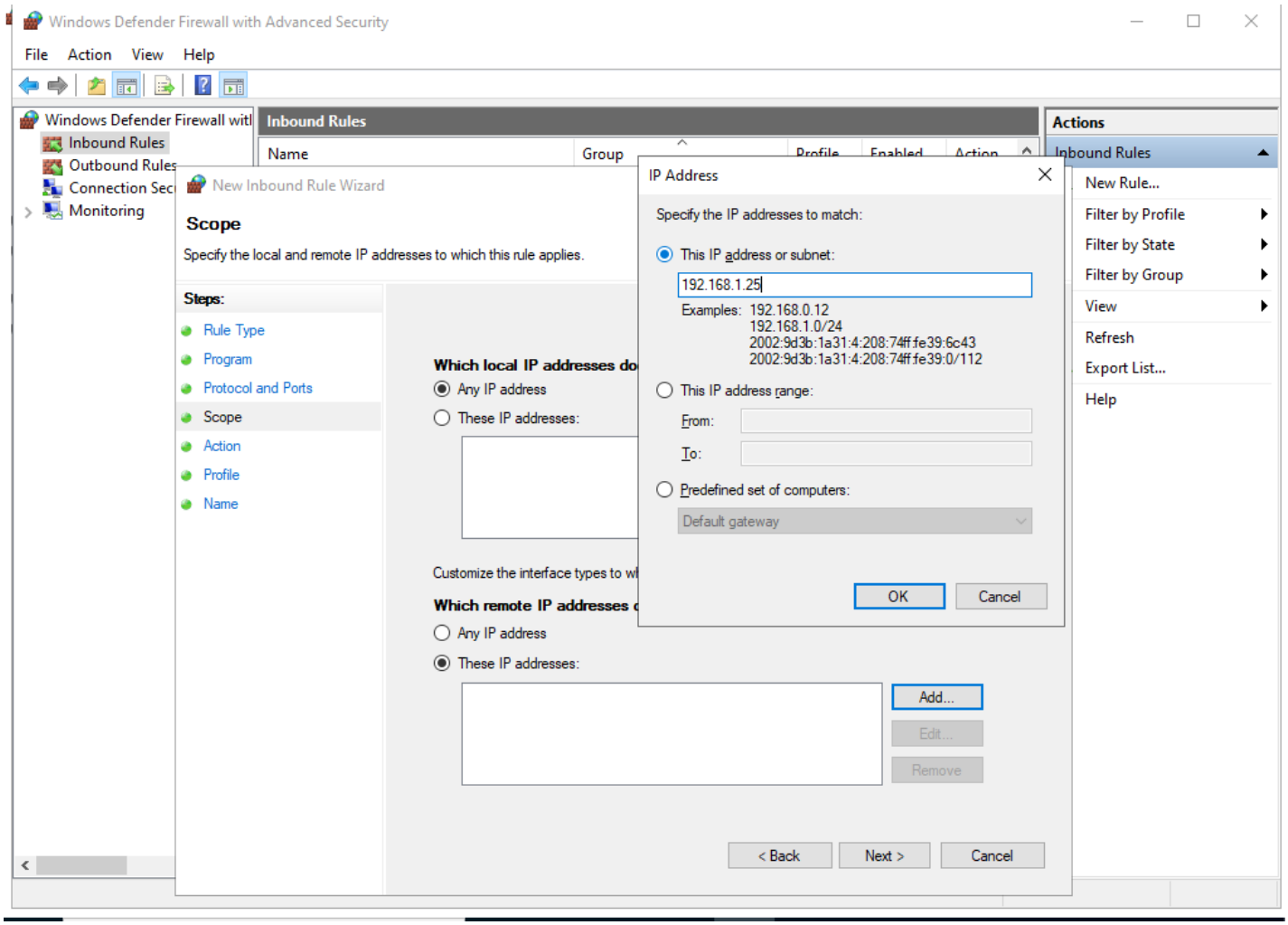
1. Identify Repeated Failures - Event ID 4625 with same source IP and logon type 3

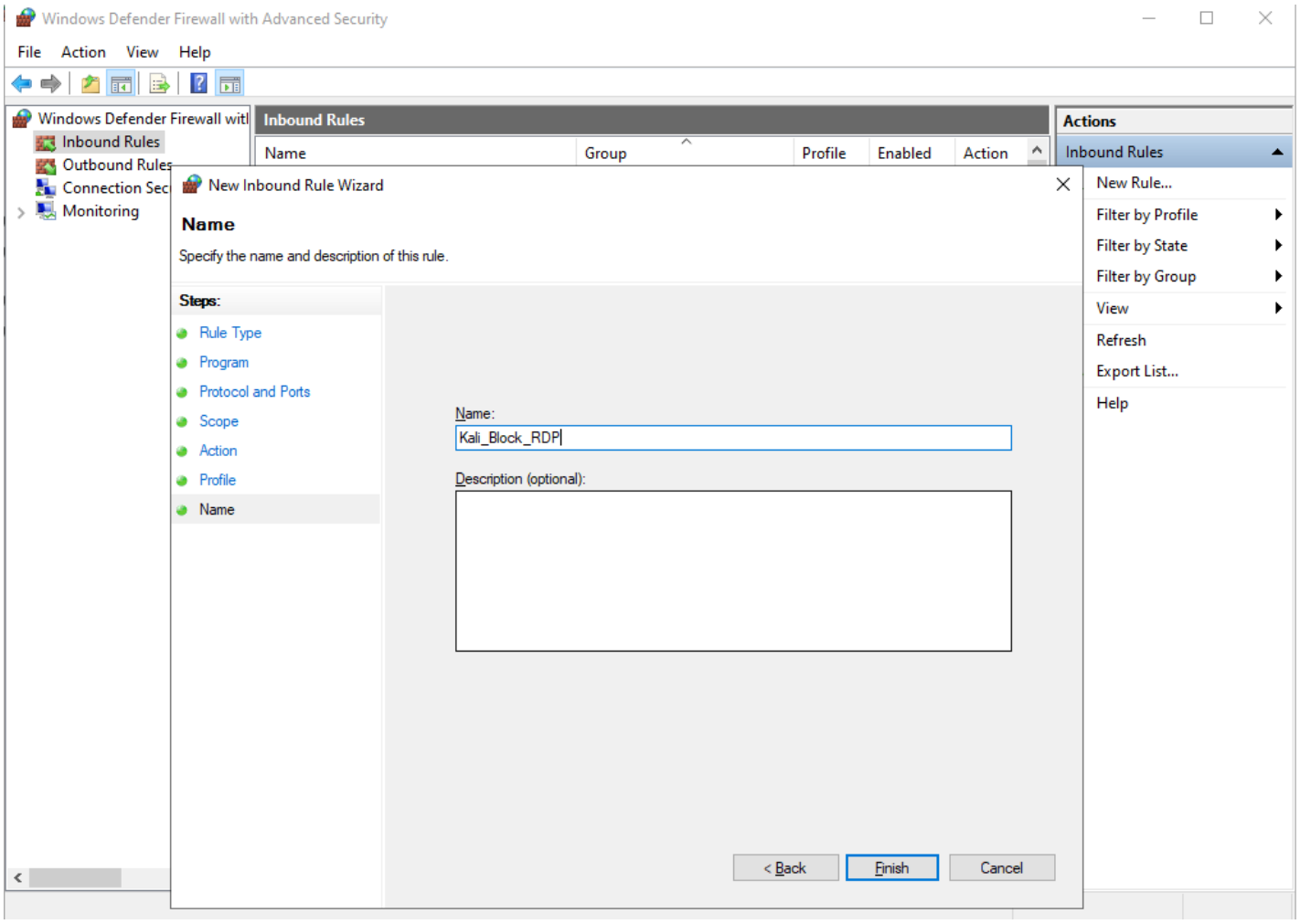
2. Disable the User Account: net user attackerlab /active:no

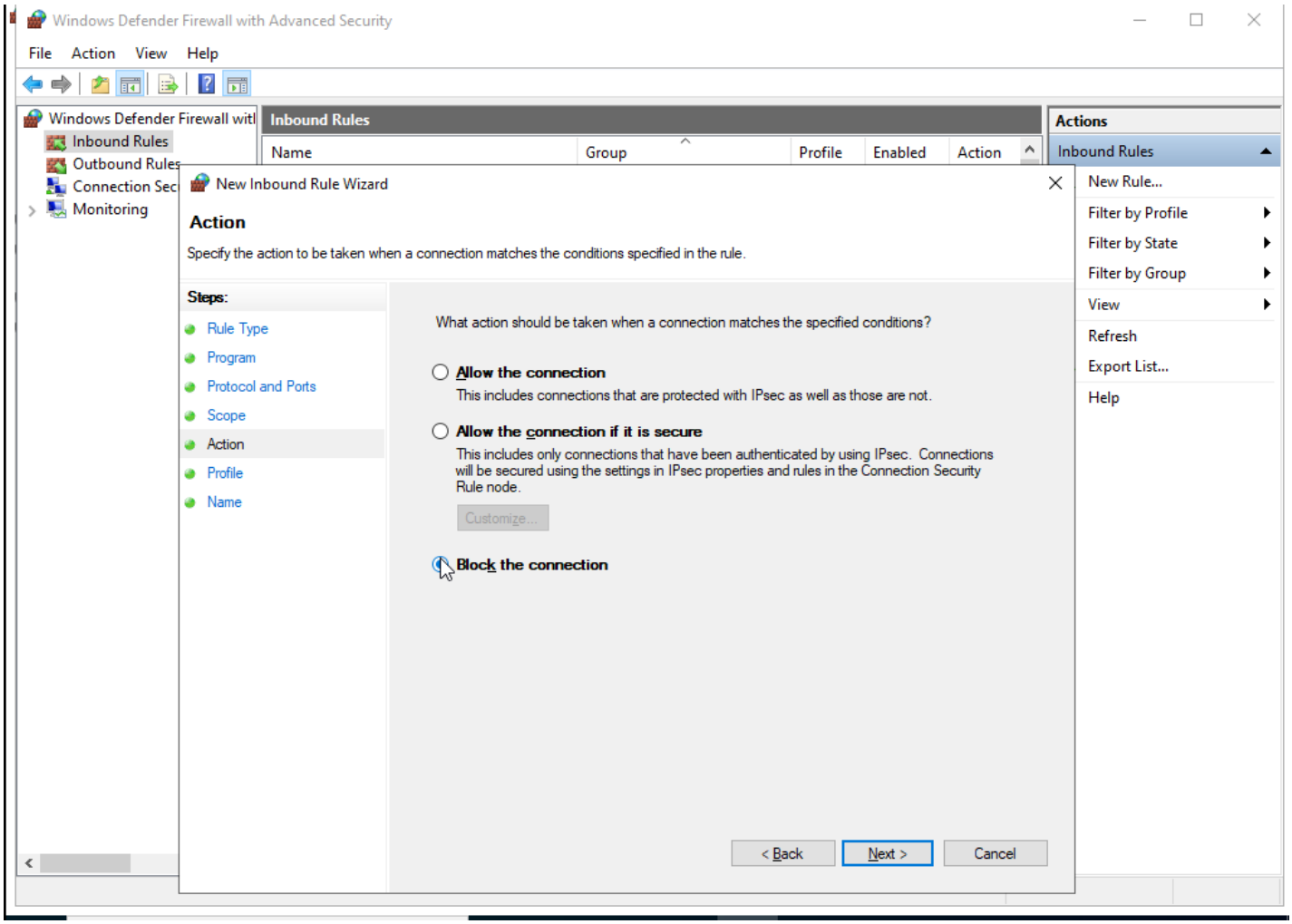
3. Block Attacker's IP:

New-NetFirewallRule -DisplayName "Block Attacker" -Direction Inbound -RemoteAddress 192.168.1.25 -Action Block


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Sec
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
To which ports and protocols does this rule apply?
Protocol type:
TCP
Protocol number:
6
Local port:
Specific Ports
3389
Example: 80, 443, 5000-5010
Remote port:
Specific Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:
Customize...
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Sec
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses do
Any IP address
These IP addresses:
Customize the interface types to wl
Which remote IP addresses c
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel
IP Address
Specify the IP addresses to match:
This IP address or subnet:
192.168.1.25
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
Predefined set of computers:
Default gateway
OK
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Sec
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
Kali_Block_RDP
Description (optional):
< Back
Finish
Cancel




## Progress

- Environment setup - Completed
- RDP attack simulation - Completed
- Detection via Event Viewer - Completed
- IP blocking & account disable - Completed

## Challenges and Solutions

- Firewall blocking RDP: Enabled TCP-In rule manually
- Too many log entries: Filtered using Event ID and IP
- Delay in attack: Adjusted Hydra thread setting (-t 4)

## Next Steps

- Automate detection with PowerShell or SIEM integration
- Extend monitoring using Sysmon or ELK stack
- Implement account lockout policies

## Conclusion

This task successfully demonstrated a simulated brute-force attack and its detection using Windows security features. By identifying Event ID 4625 log entries and analyzing attack behavior, the lab reinforced key cybersecurity response skills relevant for enterprise environments.