

Day 6: Incident Respond

Objective

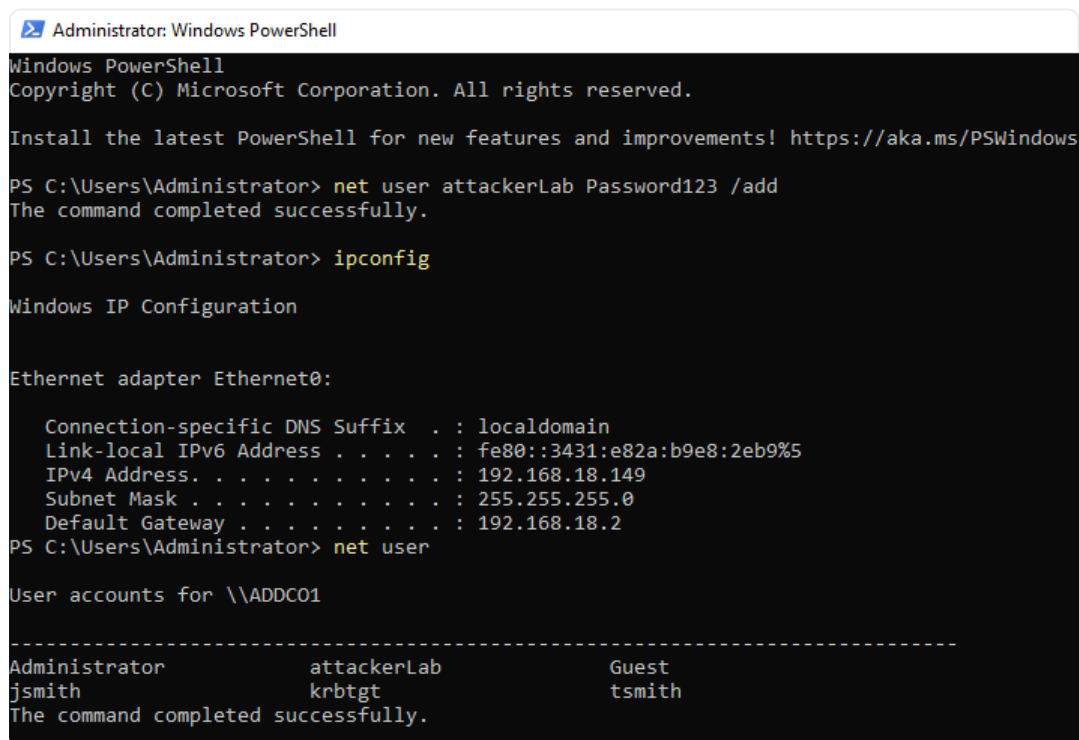
The objective of this project is to explore the core concepts of incident response, gain familiarity with the incident response lifecycle, and understand how basic threats on Windows systems can be detected, analyzed, and responded to using standard security monitoring tools and techniques.

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

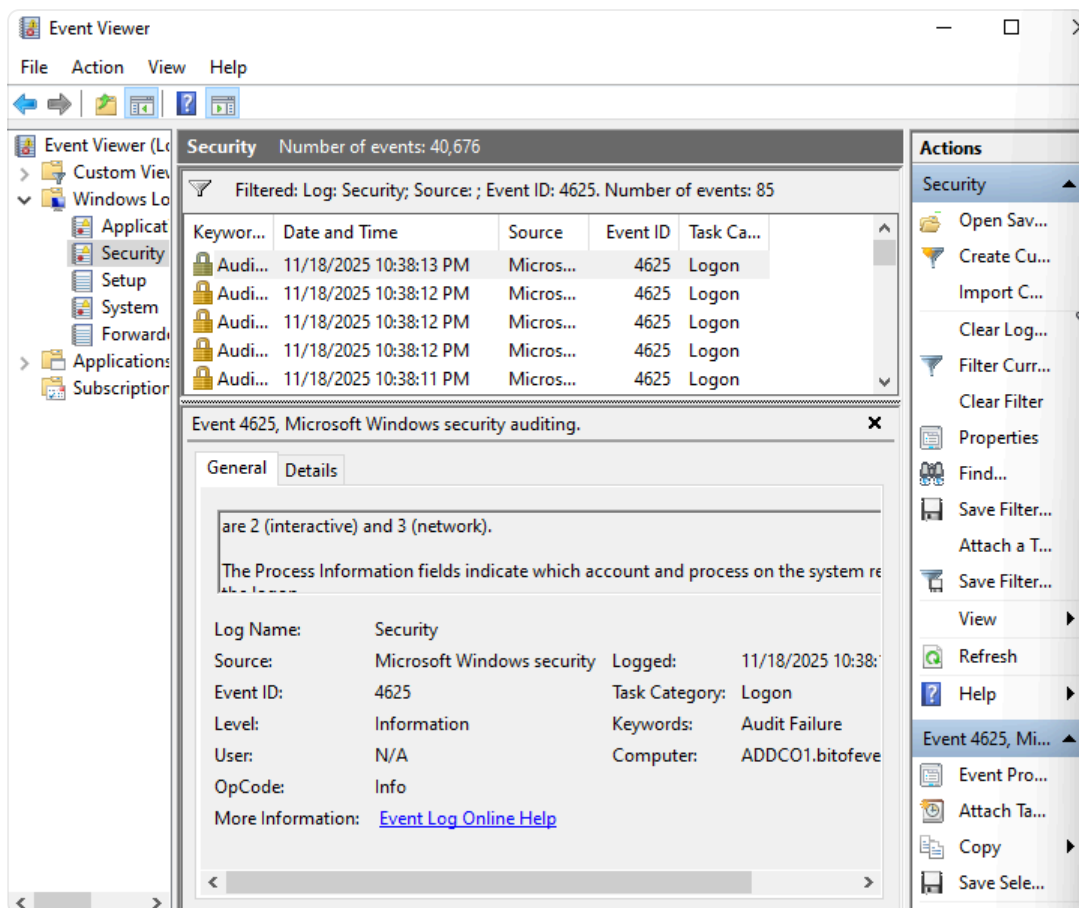
Ethernet adapter Ethernet0:

    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

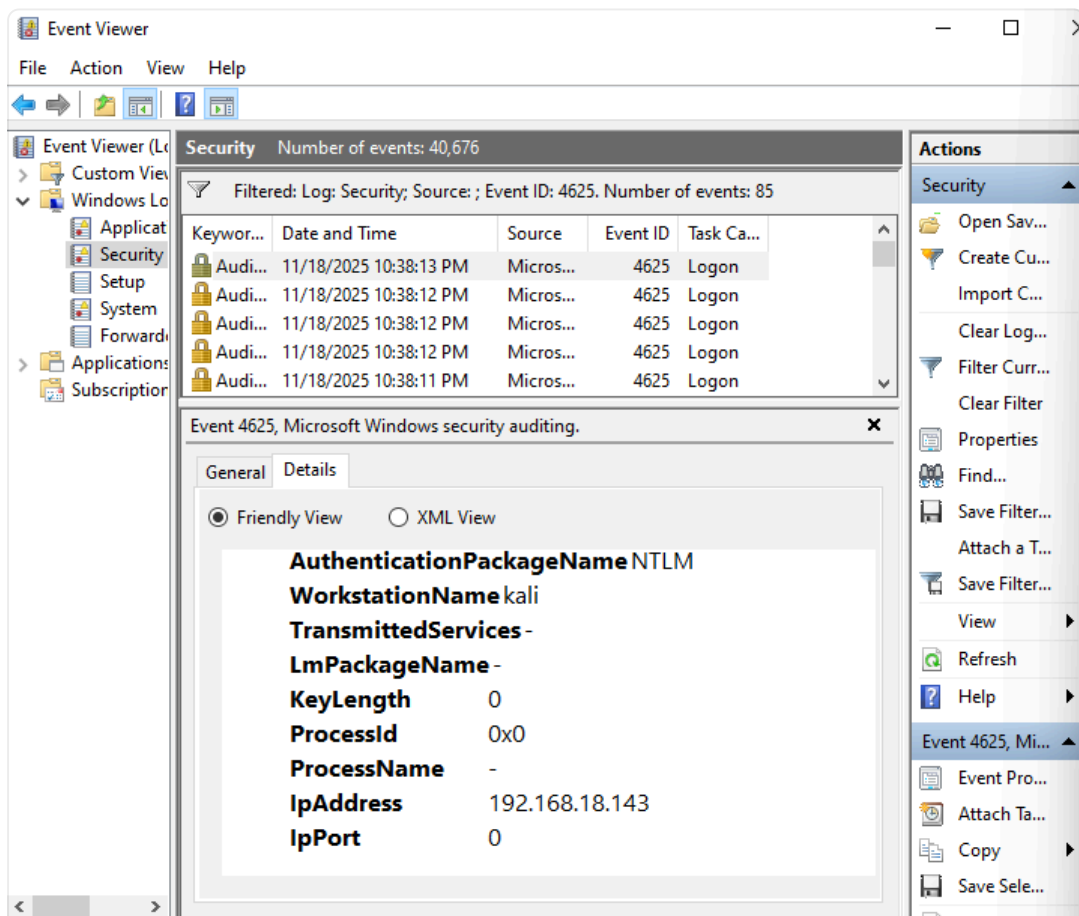
User accounts for \ADDC01

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

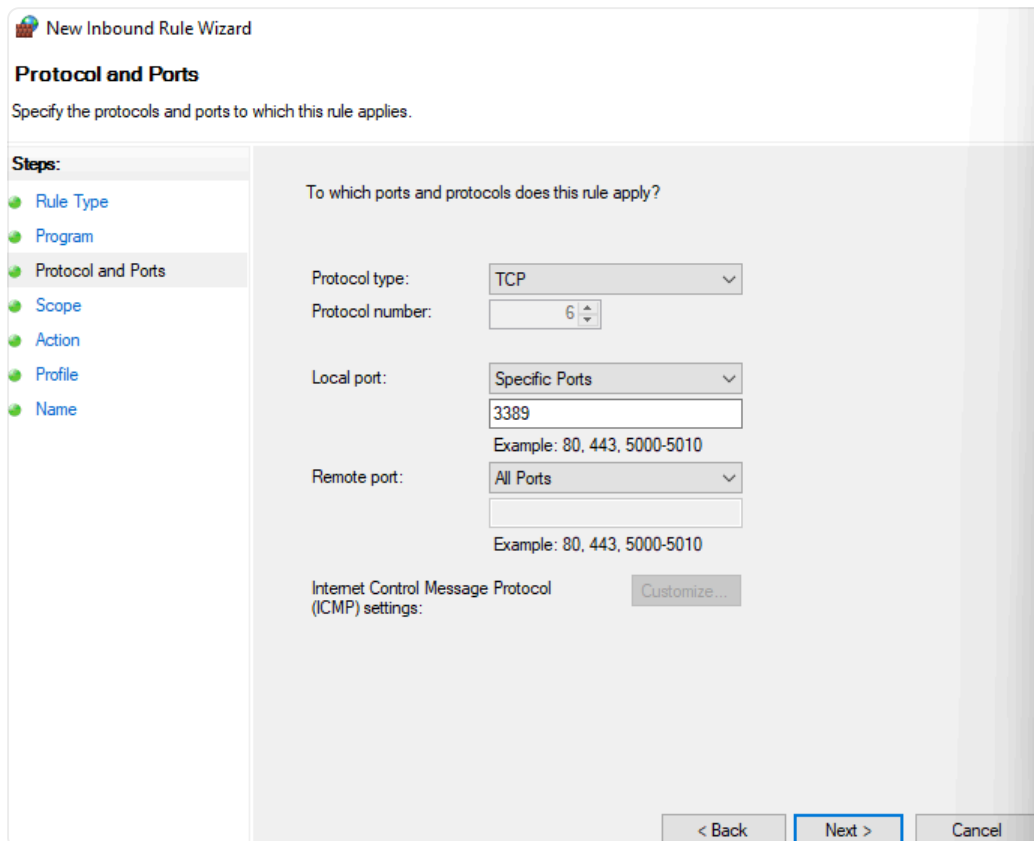
The attack did not succeed. To validate the outcome, the Windows Event Viewer was examined by navigating to Windows Logs → Security and filtering for Event ID 4625, which records failed logon attempts. The security log revealed multiple entries corresponding to Event ID 4625, each indicating failed authentication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



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.



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

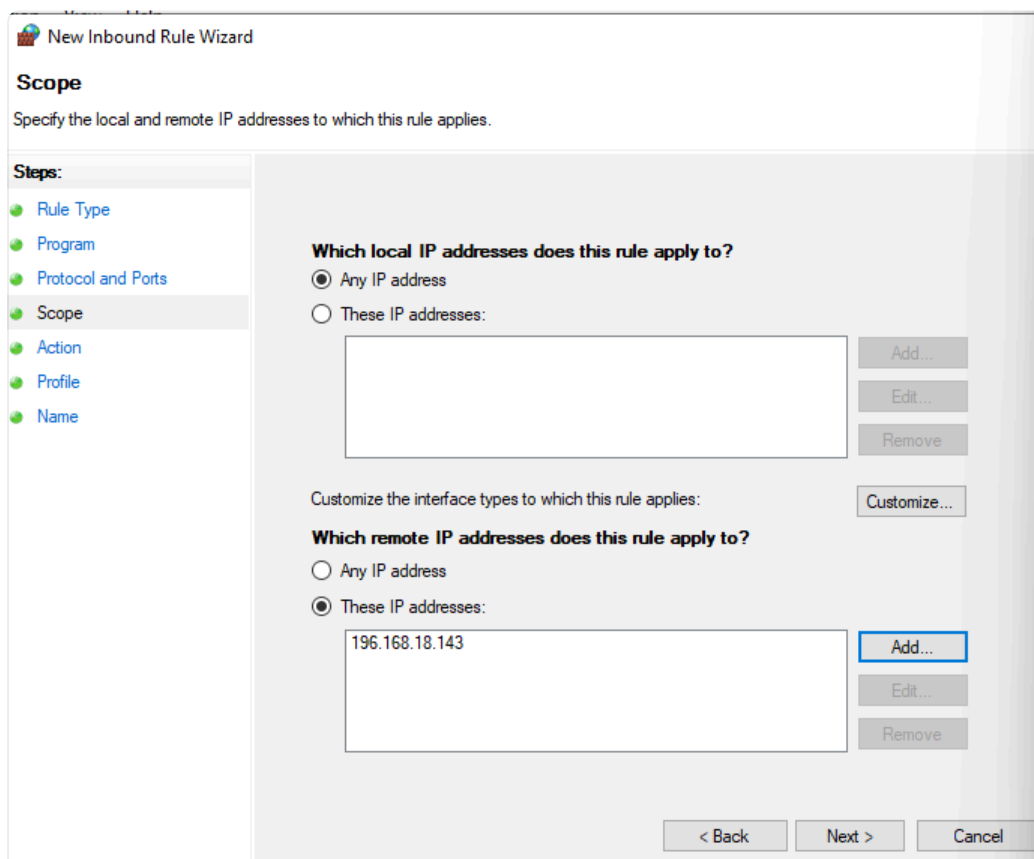
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

< Back Next > Cancel



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 does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

196.168.18.143

Add... Edit... Remove

< Back Next > Cancel

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
[Customize...](#)

☒ **Block the connection**

< Back **Next >** Cancel

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

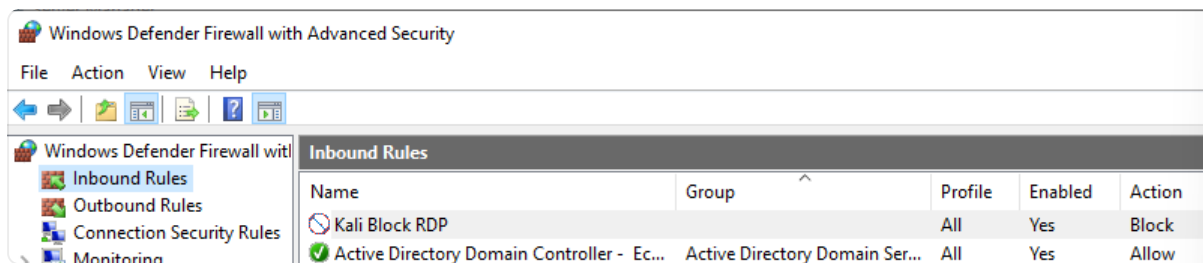
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:

Description (optional):

< Back **Finish** Cancel

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
```