Document Name	Brute-Force Protection (Windows Server 2022)	Version	1.3
Author	Anusha Ramu Chakravarthi	Date Created	24/04/2025
Protection Type	Brute-Force Defense (RDP and SMB Services)	Last Modified	27/042025

Document Description

This playbook outlines the steps to implement brute-force protection on Windows Server 2022 using **RDP Guard** for RDP, and **Windows Firewall + Account Lockout Policies** for SMB. These controls protect the server against automated login attempts via Remote Desktop Protocol (RDP) and Server Message Block (SMB). It aligns with the **Protect** function of the NIST Cybersecurity Framework.

Step 1

Task: Download and Install RDP Guard

Download and install RDP Guard on the Windows Server 2022 system.

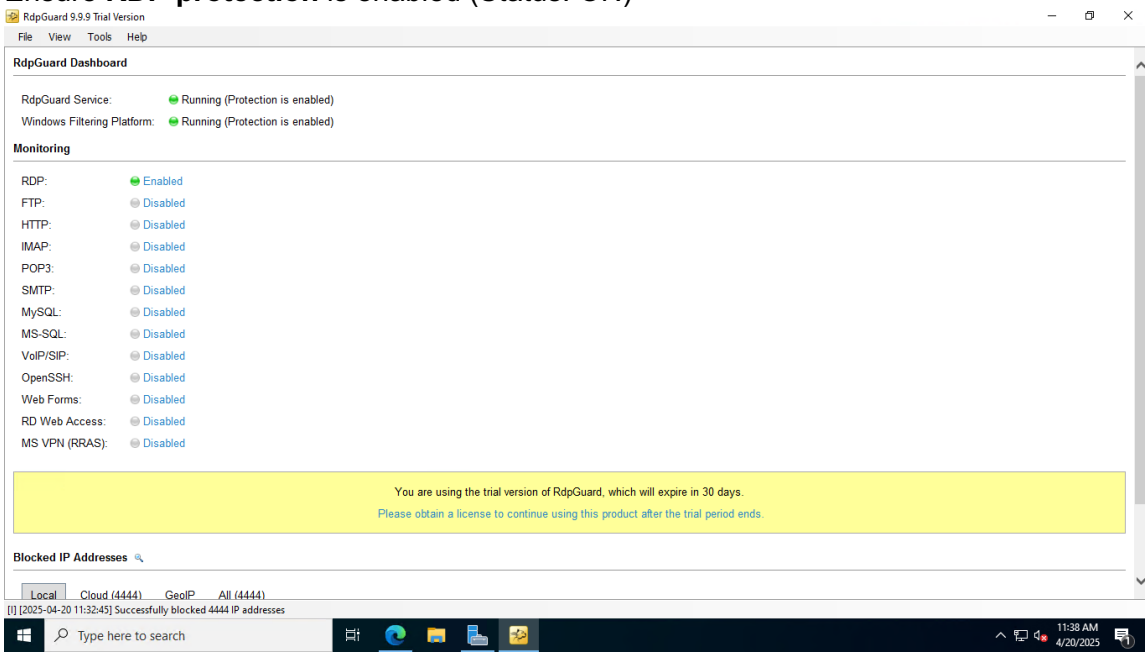
- Visit https://rdpguard.com/download.aspx
- Download and run the installer as Administrator
- Complete installation using default options unless customization is required

Step 2

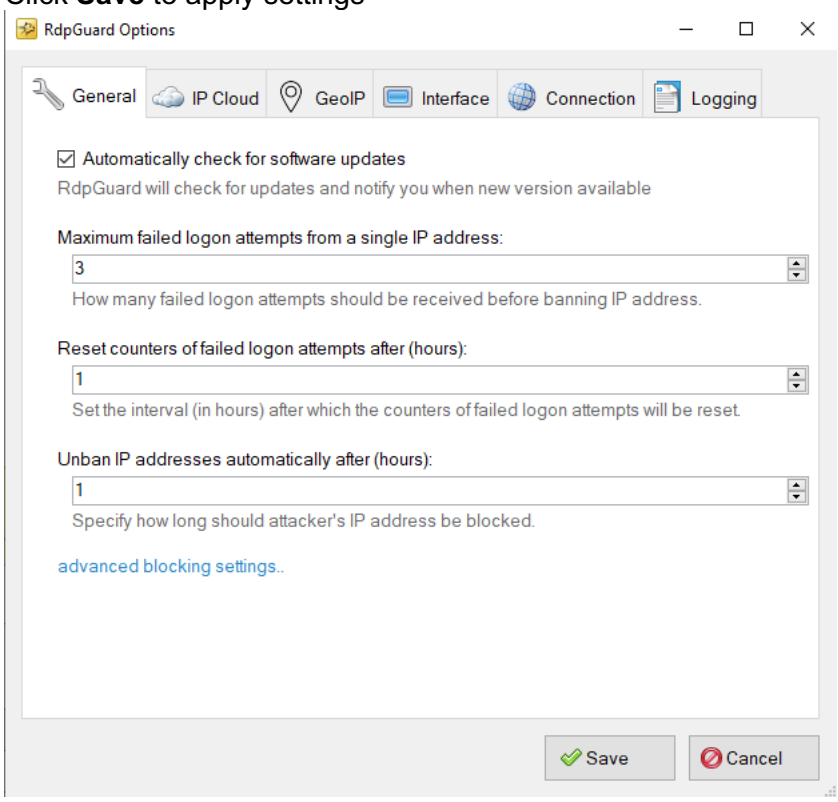
Task: Activate RDP Guard and Configure Protection Rules

Start the service and configure brute-force protection settings for RDP.

- Launch RDP Guard GUI
- Ensure **RDP protection** is enabled (Status: ON)



- In version 9.9.9, note that specific threshold configuration (e.g., 3 attempts in 5 minutes) is no longer editable via the GUI
- Use default behavior or edit rules via configuration files if advanced customization is required
- RDP Guard 9.9.9 minimum ban duration is 1 hour. This setting was applied to ensure attacker IPs remain blocked after repeated failed RDP login attempts, mitigating brute-force attacks on the OzCazual server.
- Click **Save** to apply settings

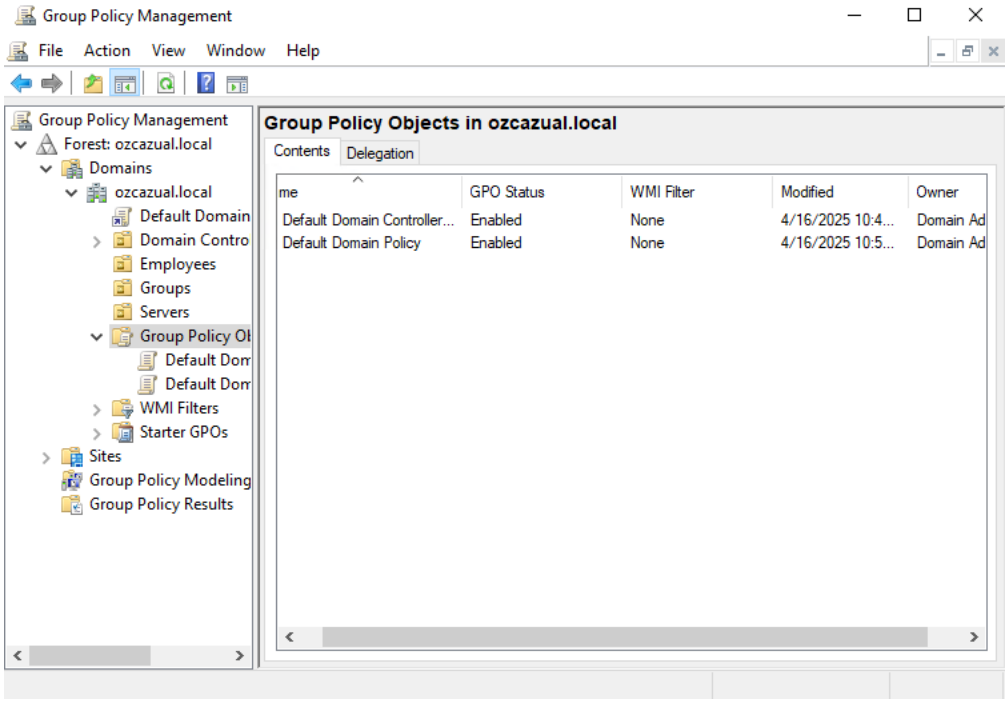


Step 3

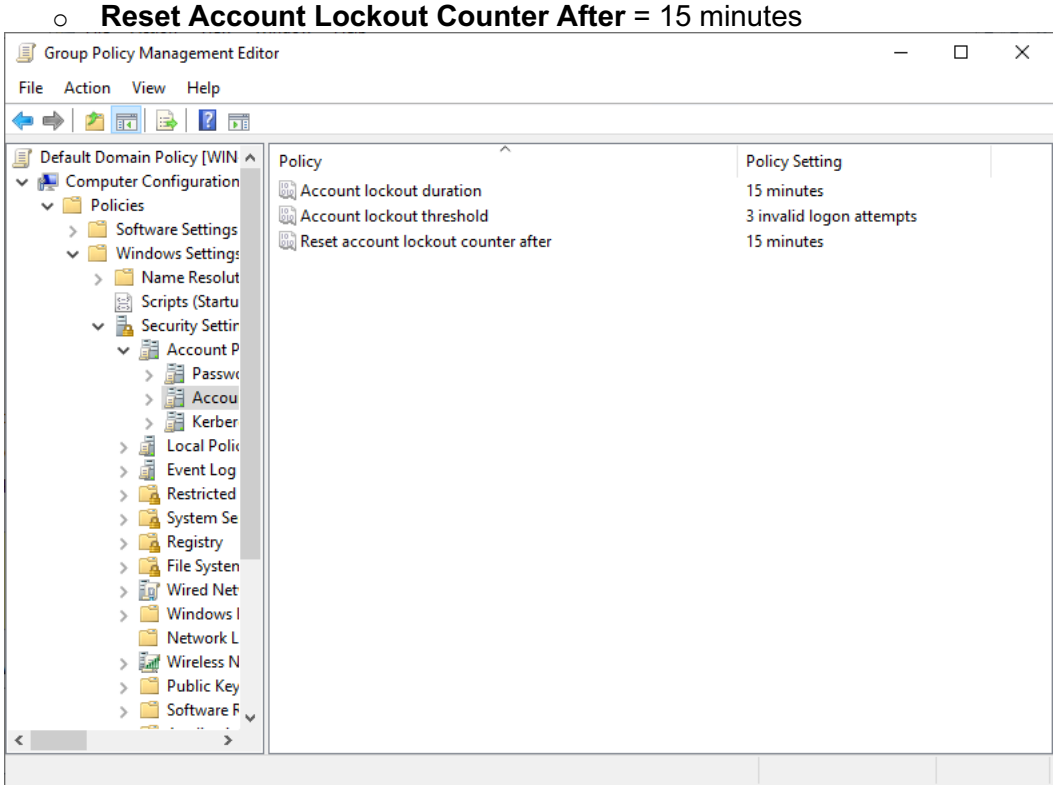
Task: Implement SMB Protection Using Native Windows Features

Protect against brute-force attacks on SMB (CME/Metasploit) using Windows built-in controls.

- Open **Group Policy Management Console** (gpmc.msc)



- Navigate to: Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy
  Set:
  - **Account Lockout Threshold** = 3 or 5 invalid attempts
  - **Account Lockout Duration** = 15 minutes
  - **Reset Account Lockout Counter After** = 15 minutes



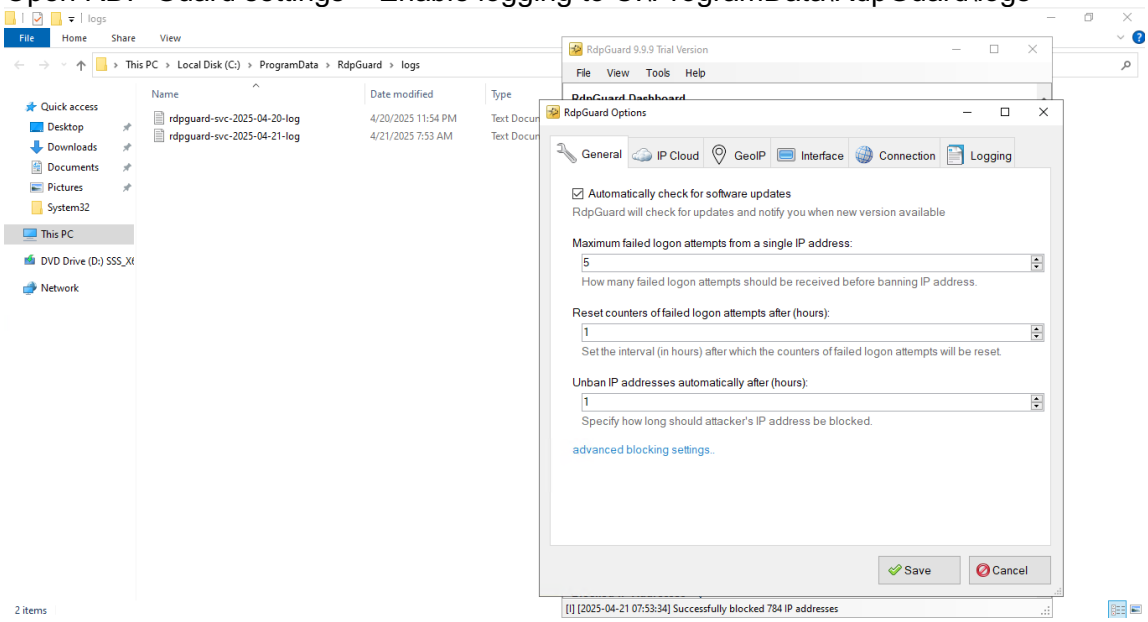
- Apply changes and update Group Policy with gpupdate /force

Step 4

Task: Enable Logging and Alerting

Ensure logging is enabled for incident tracking.

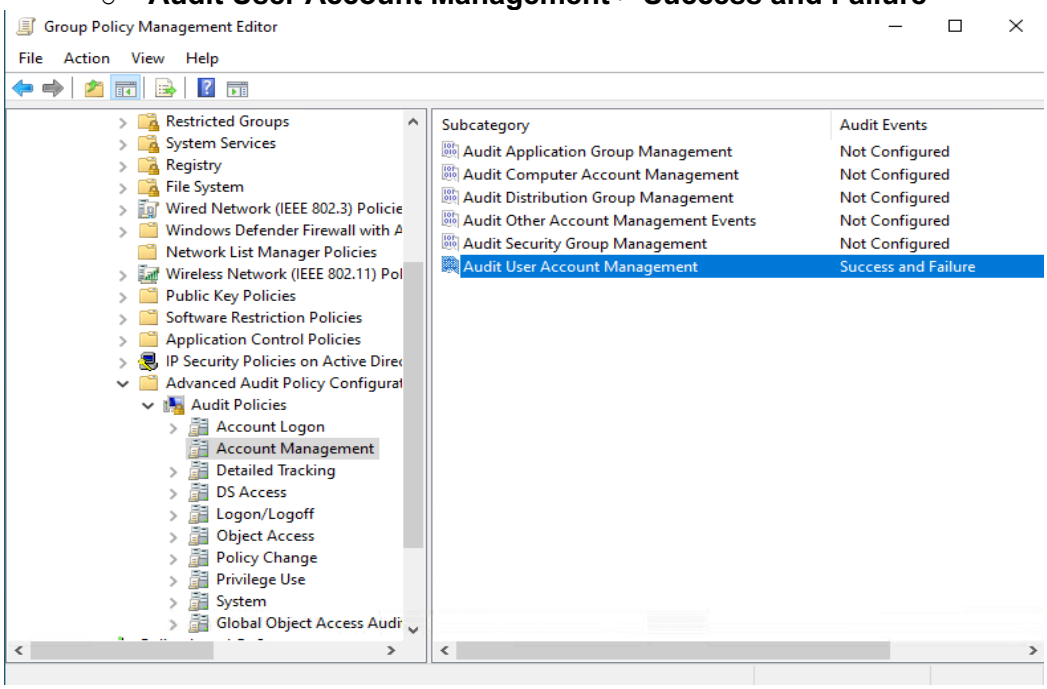
- For RDP:
  Open RDP Guard settings > Enable logging to C:\ProgramData\RdpGuard\logs



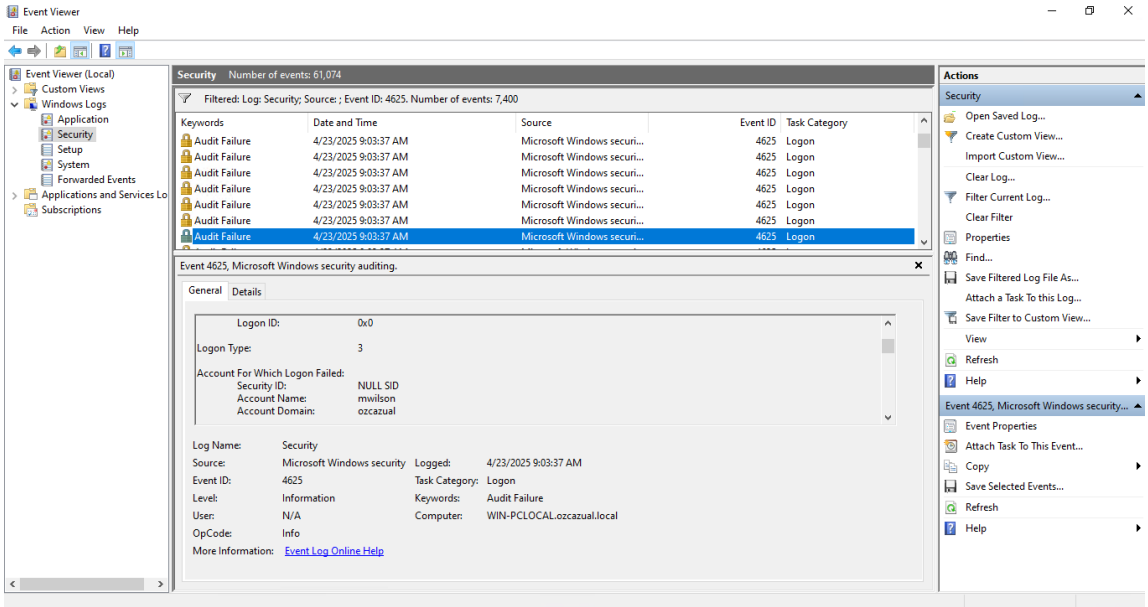
- For SMB:
  Enable Windows Event Log for **Security** category
  Enable "Audit Account Management" in Group Policy (For getting 4740 event logs)
  1. **Open Group Policy Editor**:
     - On the DC > Run gpmc.msc (Group Policy Management Console)
  2. **Edit Default Domain Controllers Policy**:
     - Navigate to:

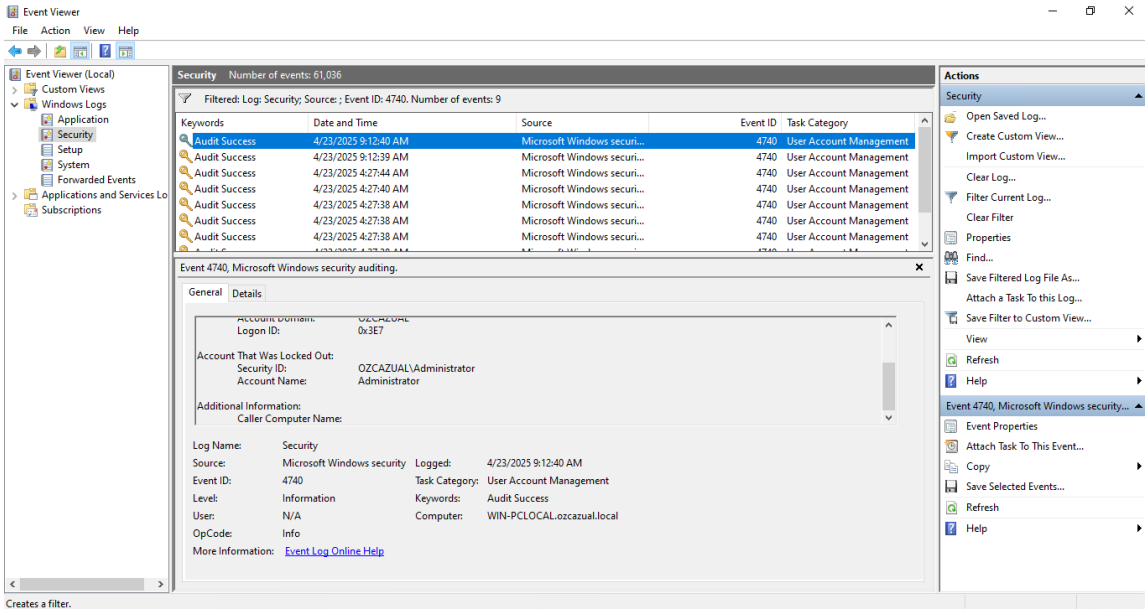
  Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management

  3. **Enable the following**:
     - **Audit User Account Management** > **Success and Failure**



- Use Event Viewer to monitor Event IDs:
  - **4625** – Failed Logon Attempts
  - **4740** – Account Lockout





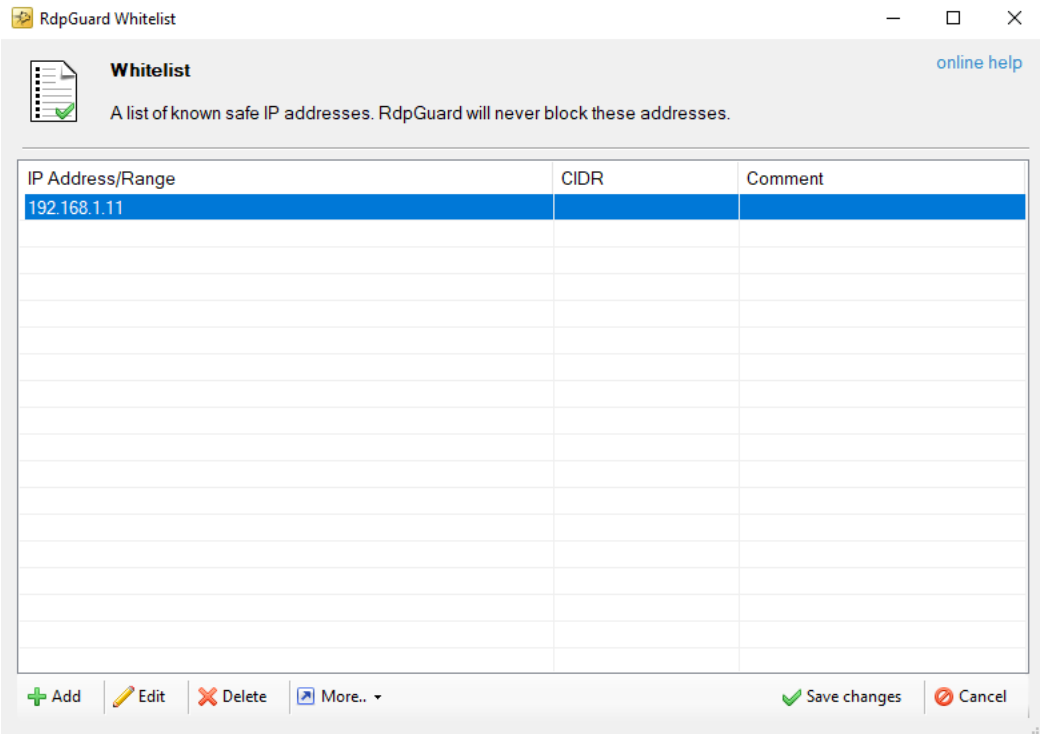
- Optionally configure email alerts using Task Scheduler

Step 5

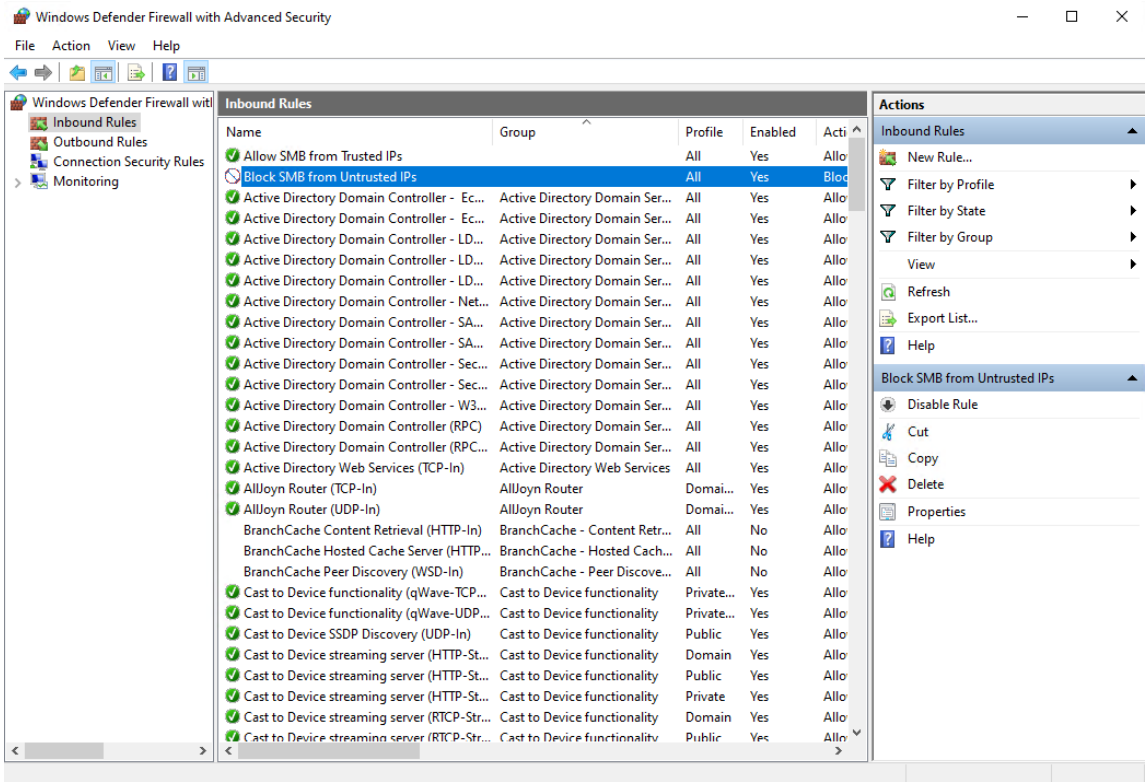
Task: Whitelist Internal IPs and Safe Hosts

Prevent false positives from legitimate internal users.

- In RDP Guard: Add trusted IPs to **Whitelist**



- For SMB: Create Windows Firewall rule to allow trusted IPs only for SMB (Port 445)



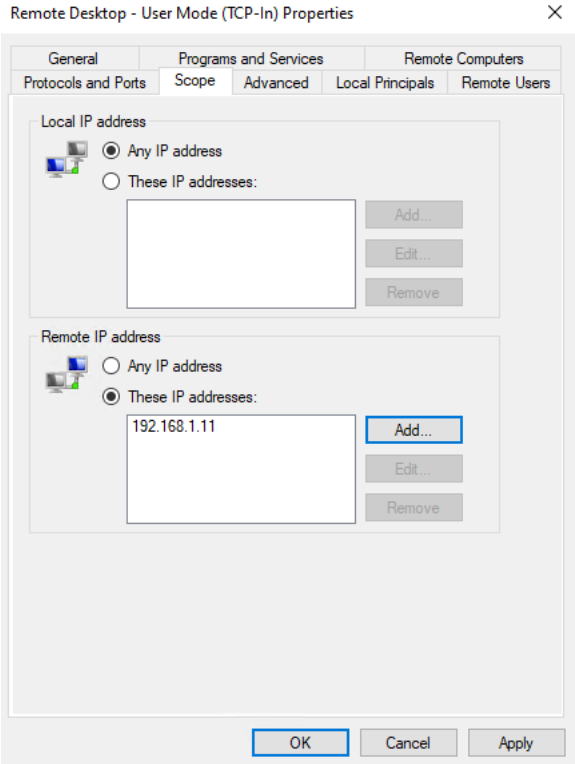
- Save and verify exclusion from monitoring

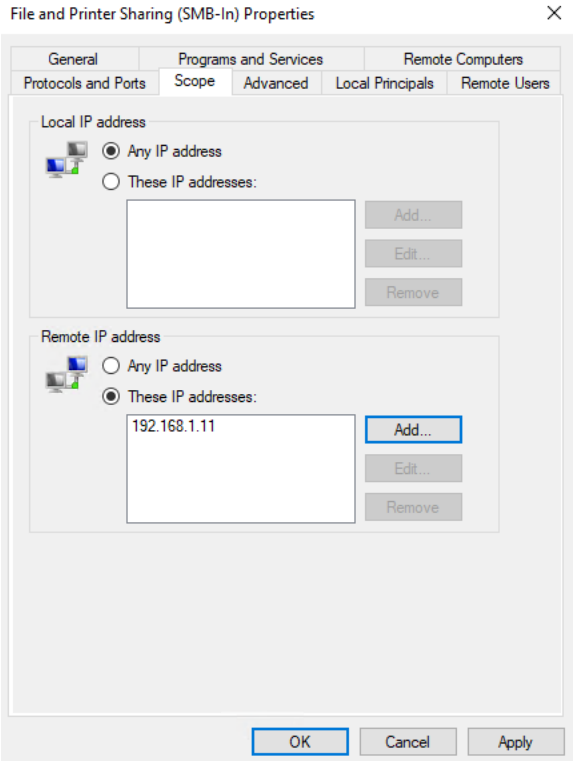
Step 6

Task: Harden RDP/SMB Access and Firewall Rules

Reduce attack surface and ensure services are locked down.

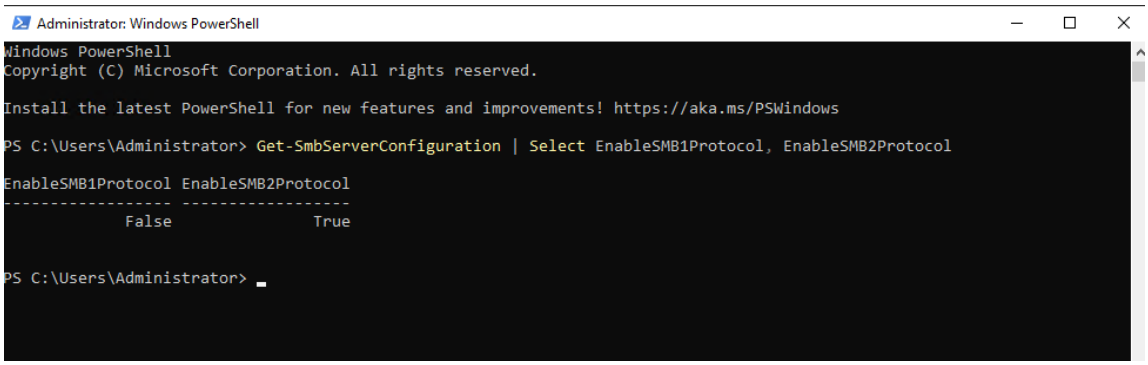
- Use **Windows Defender Firewall** to restrict RDP (3389) and SMB (445) to known Ips



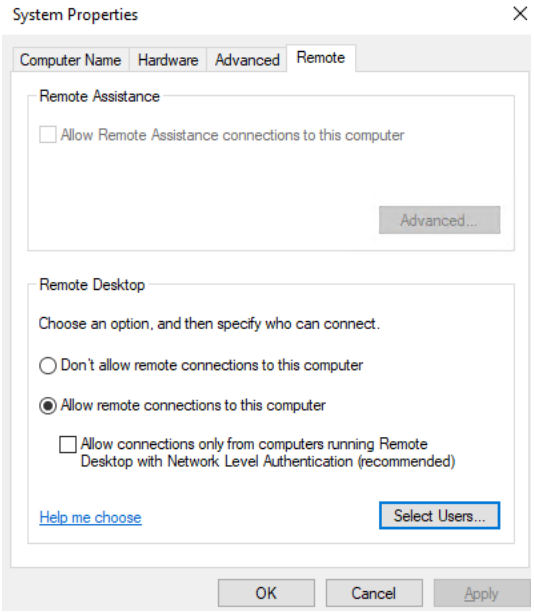


- Disable SMBv1 protocol using PowerShell:

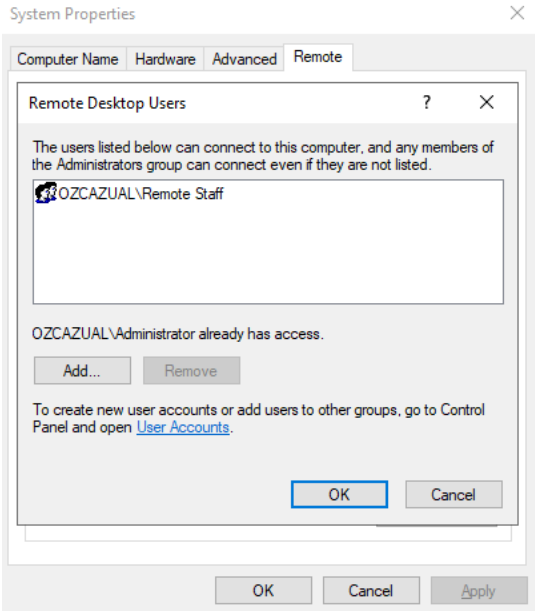
```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```



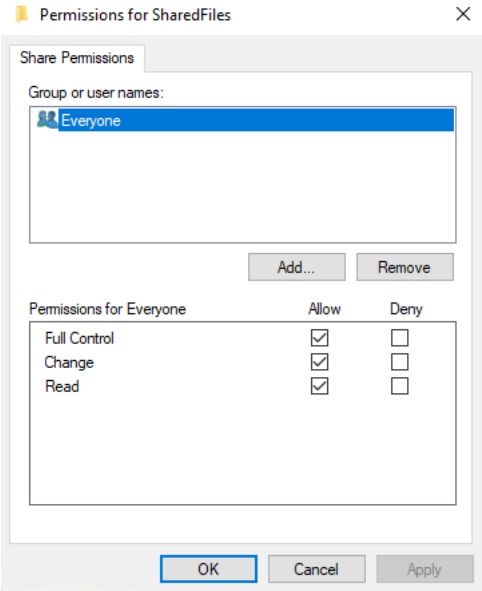
- Disable RDP/SMB access for accounts that don't require it
  Disable RDP access via System Properties (**sysdm.cpl**):



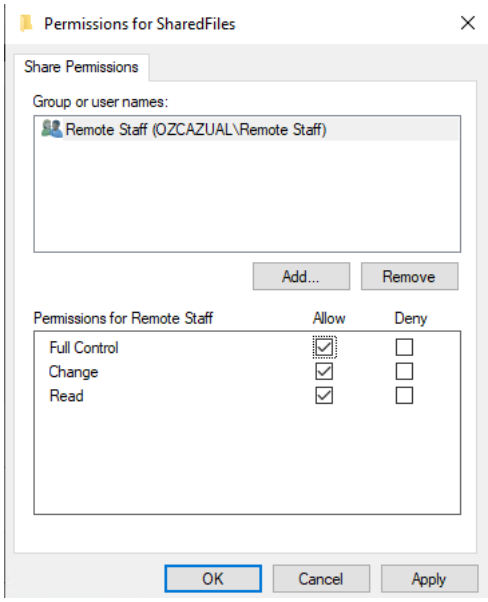
Remove access for "Everyone" and select the group that needs RDP/SMB access:



Disable SMB on shared folder for others:



Allow access to only Domain users:
Remove the group Everyone and add just the group that can access SMB shared folder



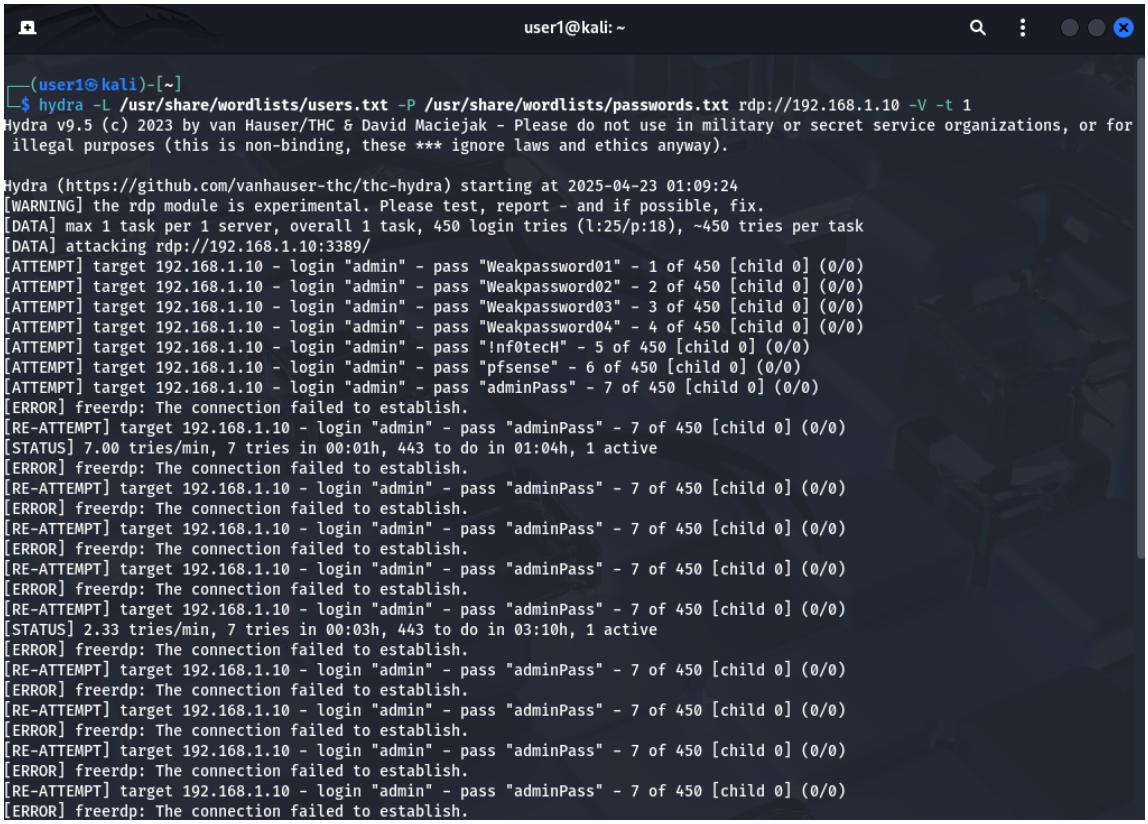
Step 7

Task: Test Brute-Force Attempt and Validate Protection

Simulate brute-force attempts to verify protection for both RDP and SMB.

- Use Hydra to simulate RDP brute-force attempts

```
hydra -L users.txt -P passwords.txt rdp://<server_IP> -V -t
1
```

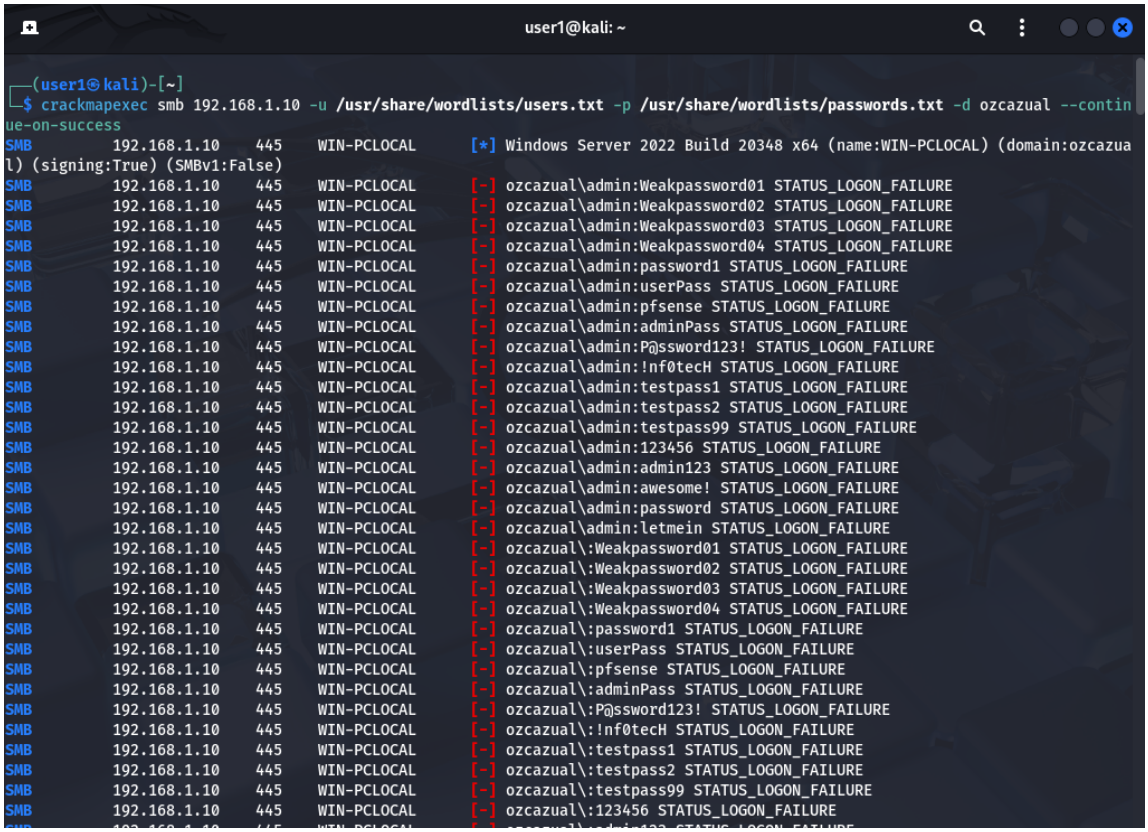


```
┌──(user1㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/users.txt -P /usr/share/wordlists/passwords.txt rdp://192.168.1.10 -V -t 1
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 01:09:24
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 450 login tries (l:25/p:18), ~450 tries per task
[DATA] attacking rdp://192.168.1.10:3389/
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "Weakpassword01" - 1 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "Weakpassword02" - 2 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "Weakpassword03" - 3 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "Weakpassword04" - 4 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "!nf0tecH" - 5 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "pfsense" - 6 of 450 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[STATUS] 7.00 tries/min, 7 tries in 00:01h, 443 to do in 01:04h, 1 active
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[STATUS] 2.33 tries/min, 7 tries in 00:03h, 443 to do in 03:10h, 1 active
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[RE-ATTEMPT] target 192.168.1.10 - login "admin" - pass "adminPass" - 7 of 450 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
```

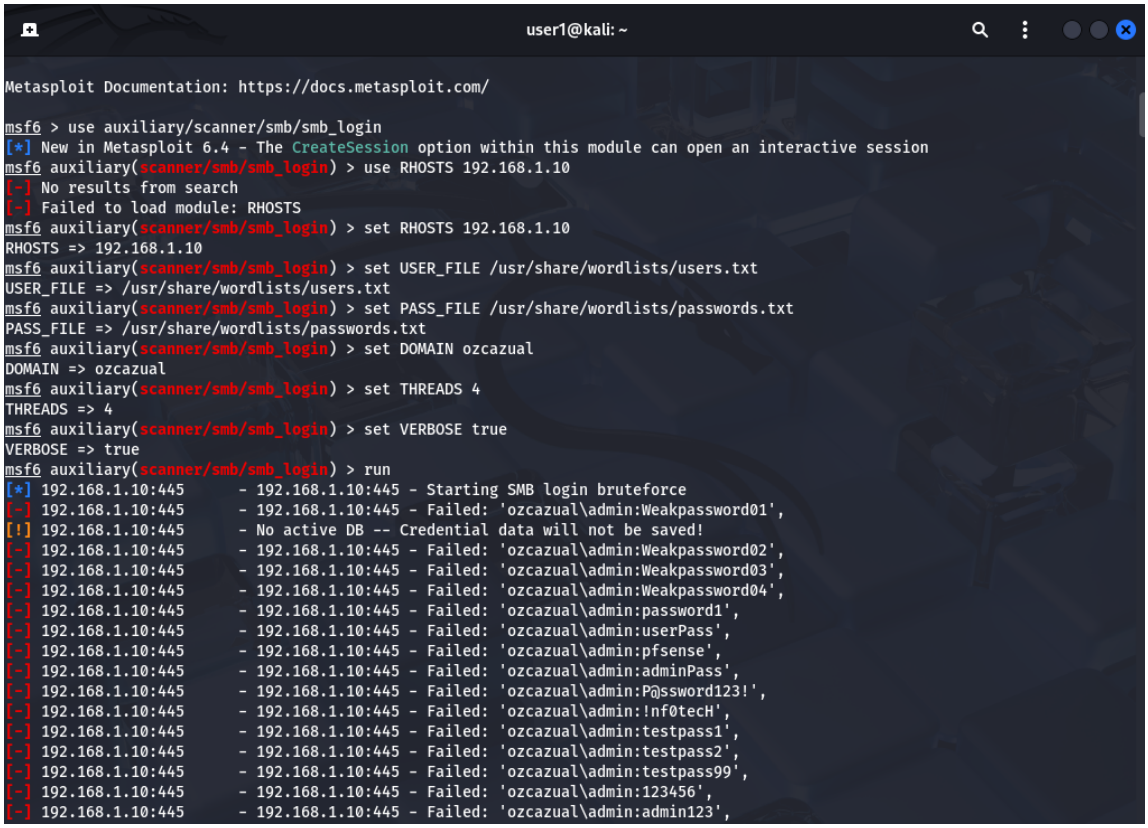
- Use CrackMapExec to simulate SMB brute-force attempts

```
crackmapexec smb <server_IP> -u users.txt -p passwords.txt
-d <domain> --continue-on-success
```



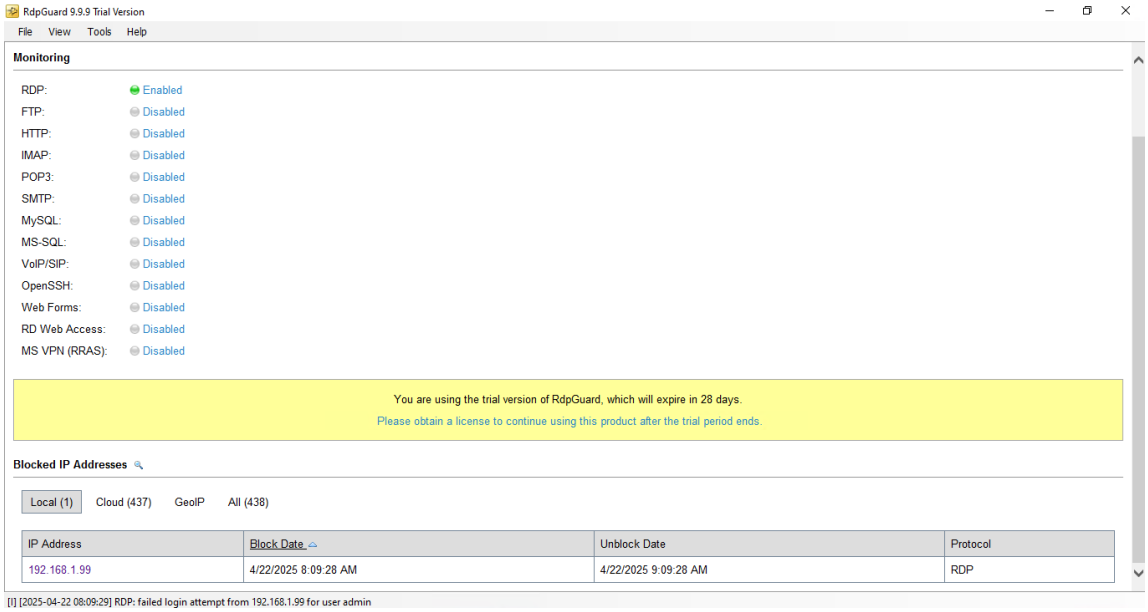
Use Metasploit SMB Module to simulate SMB Brute-Force attempts:

```
msfconsole
use auxiliary/scanner/smb/smb_login
set RHOSTS <server_IP>
set USER_FILE users.txt
set PASS_FILE passwords.txt
set DOMAIN <domain>
set THREADS 4
set VERBOSE true
run
```

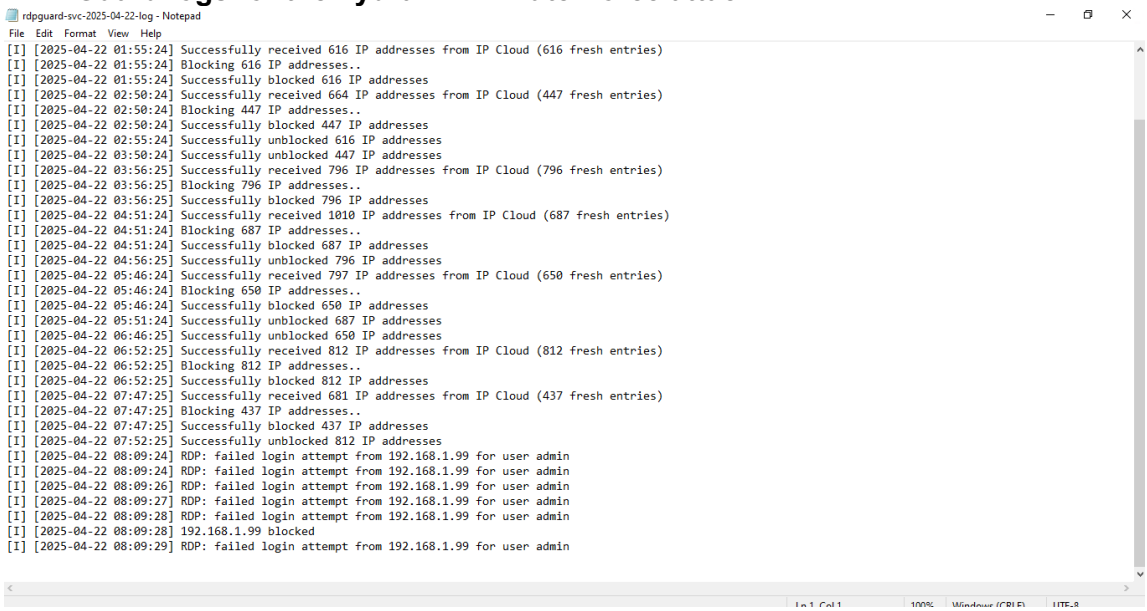


- Monitor RDP Guard and Event Viewer for alerts and blocked attempts
- Confirm account lockout and/or IP block behavior.

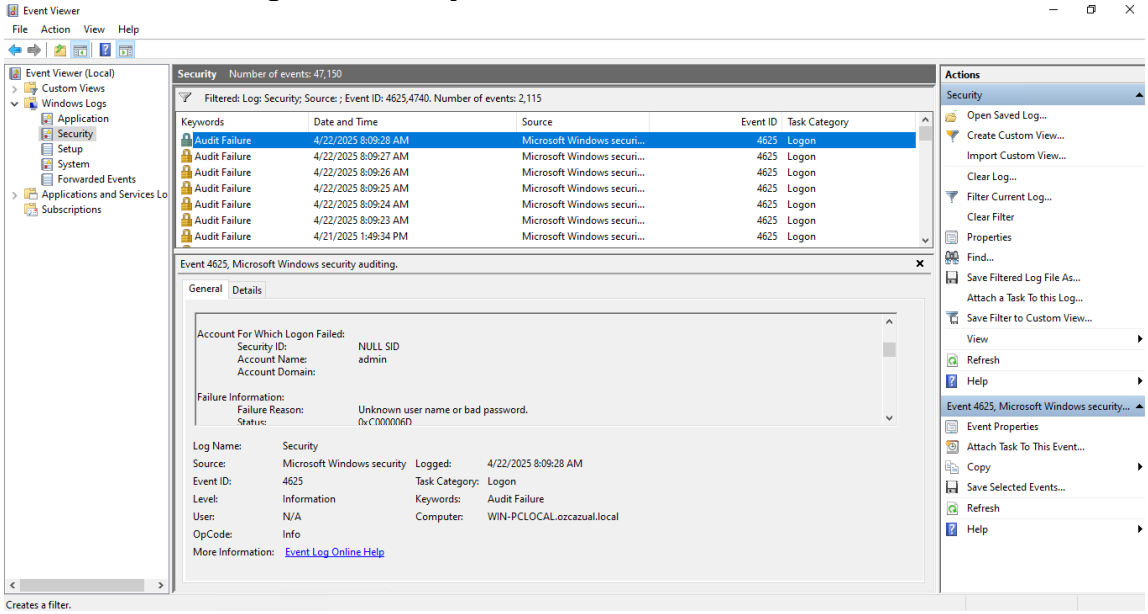
RDP Guard blocks the Attacker IP:



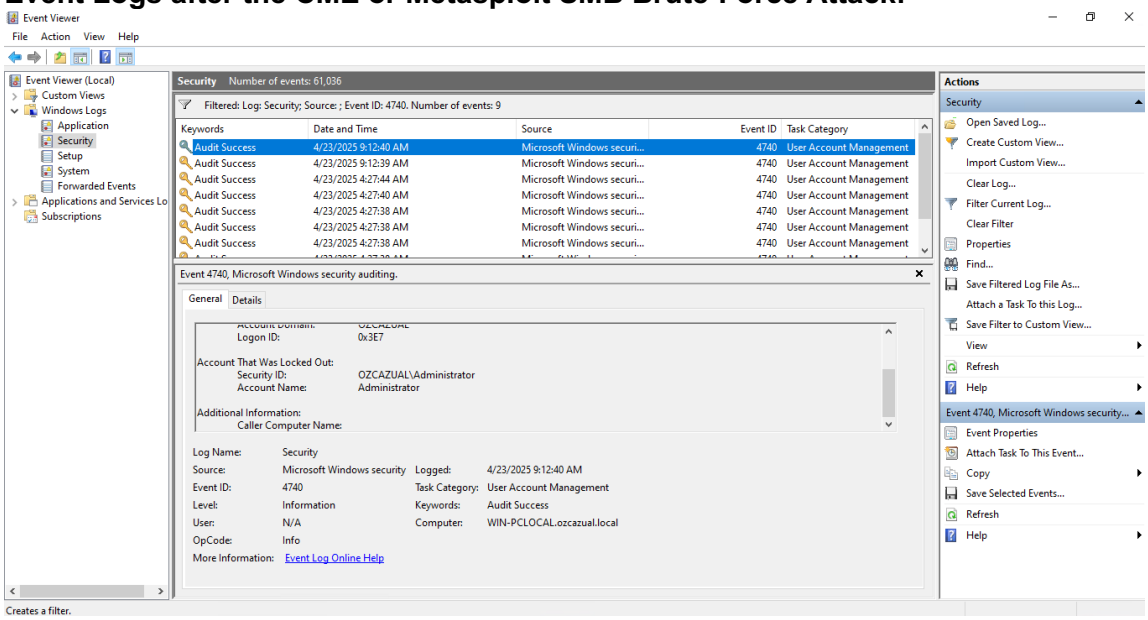
RDP Guard logs for the hydra RDP Brute-Force attack:

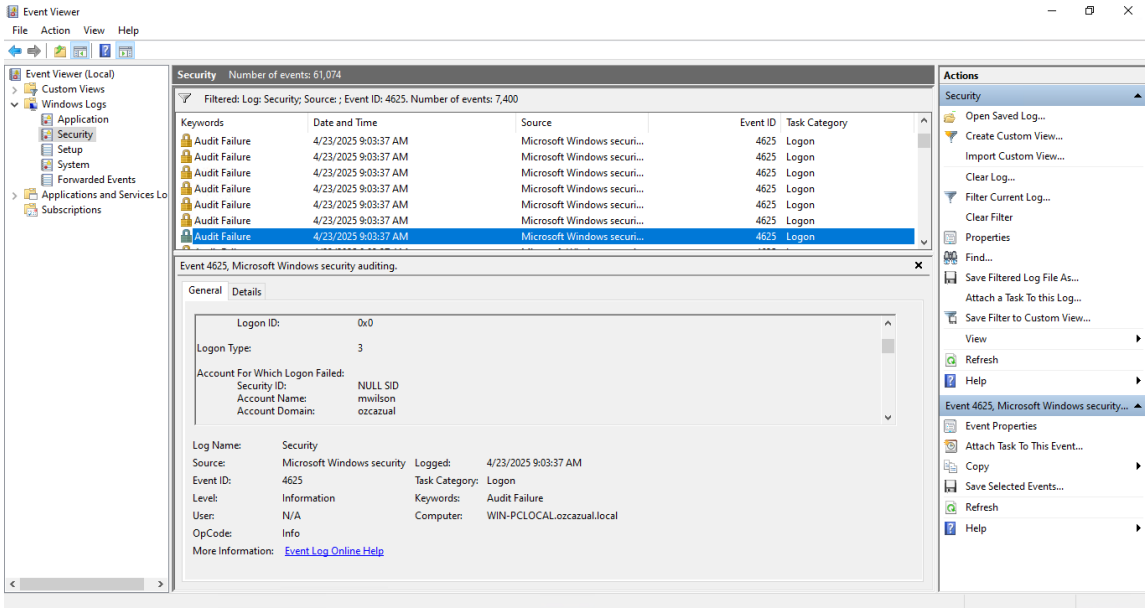


Windows Event Logs after the hydra RDP brute-force attack:



Event Logs after the CME or Metasploit SMB Brute-Force Attack:





Step 8

Task: Document Configuration and Monitor Regularly

Keep records and monitor logs for continuous protection.

- Document RDP Guard settings and GPO lockout configurations
- Save event logs weekly for audit trail
- Include in patch/update cycles
- Conduct monthly brute-force simulations to validate controls