**Brute Force Attacks Write-up [LetsDefend]**

**Brute Force Attacks**

Our web server has been compromised, and it's up to you to investigate the breach. Dive into the system, analyze logs, dissect network traffic, and uncover clues to identify the attacker and determine the extent of the damage. Are you up for the challenge?

**File Location**: /root/Desktop/ChallengeFile/BruteForce.7z

**File Password**: infected

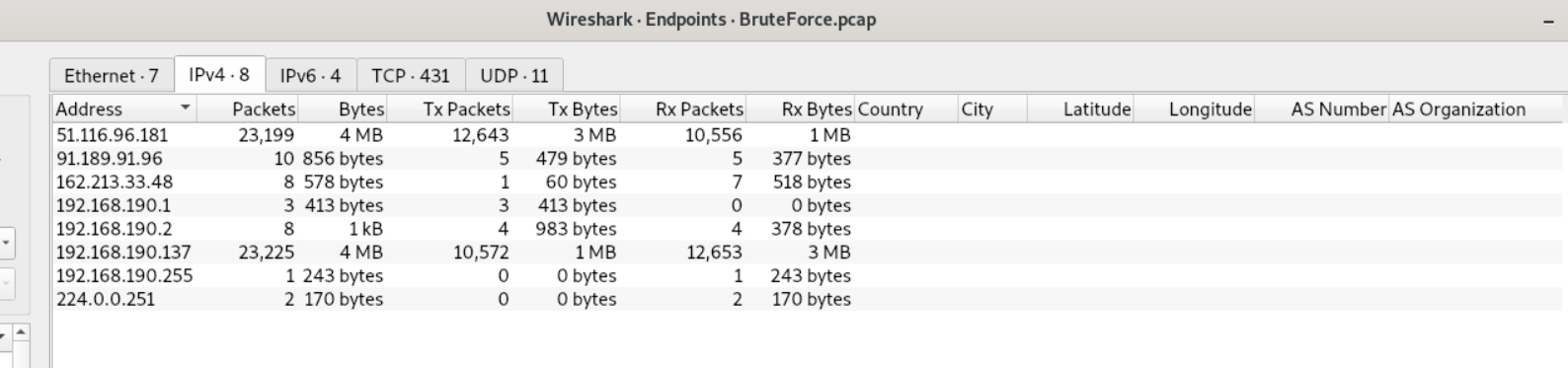
**Start Investigation**

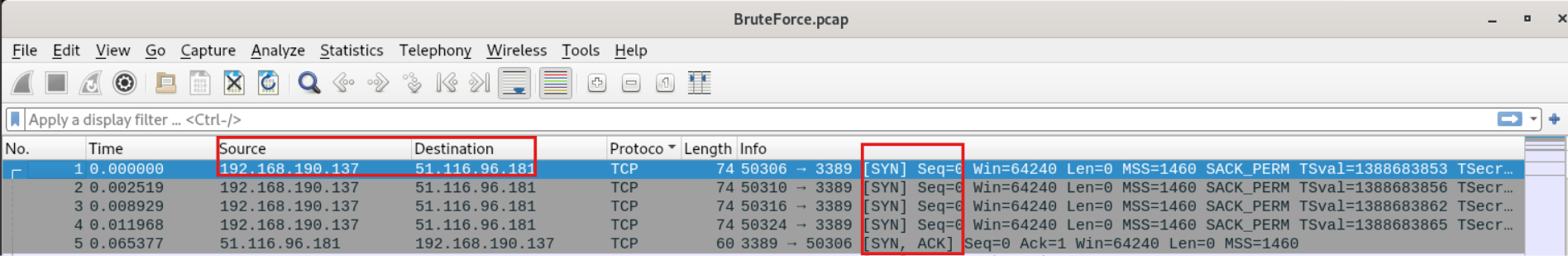
**Q1: What is the IP address of the server targeted by the attacker’s brute-force attack?**

صورة تحتوي على نص, لقطة شاشة, الخط

قد يكون المحتوى الذي تم إنشاؤه بواسطة الذكاء الاصطناعي غير صحيح.The BruteForce.7z file was successfully extracted using the 7z tool. After extraction, the contents were found to include two main files:

* BruteForce.pcap
* Auth.log

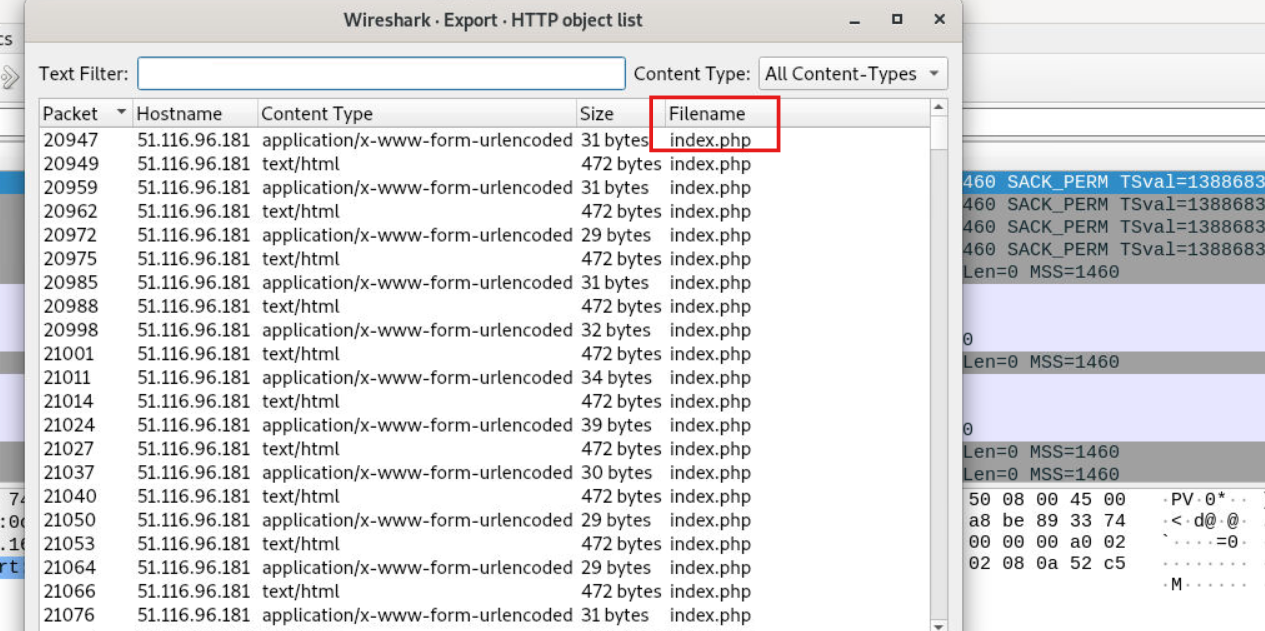
To identify the target IP address, I navigated to the **Endpoints** statistics in Wireshark. I noticed several IP addresses listed; however, two specific IPs caught my attention due to their unusually high packet counts, indicating significant network activity.

* Ip addres: 51.116.96.181
* Ip addres: 192.168.190.137

By analyzing the TCP 3-way handshake, I identified the server IP **51.116.96.181** as it responds with [SYN, ACK] to the repeated [SYN] requests initiated by the attacker.

أعلى النموذج

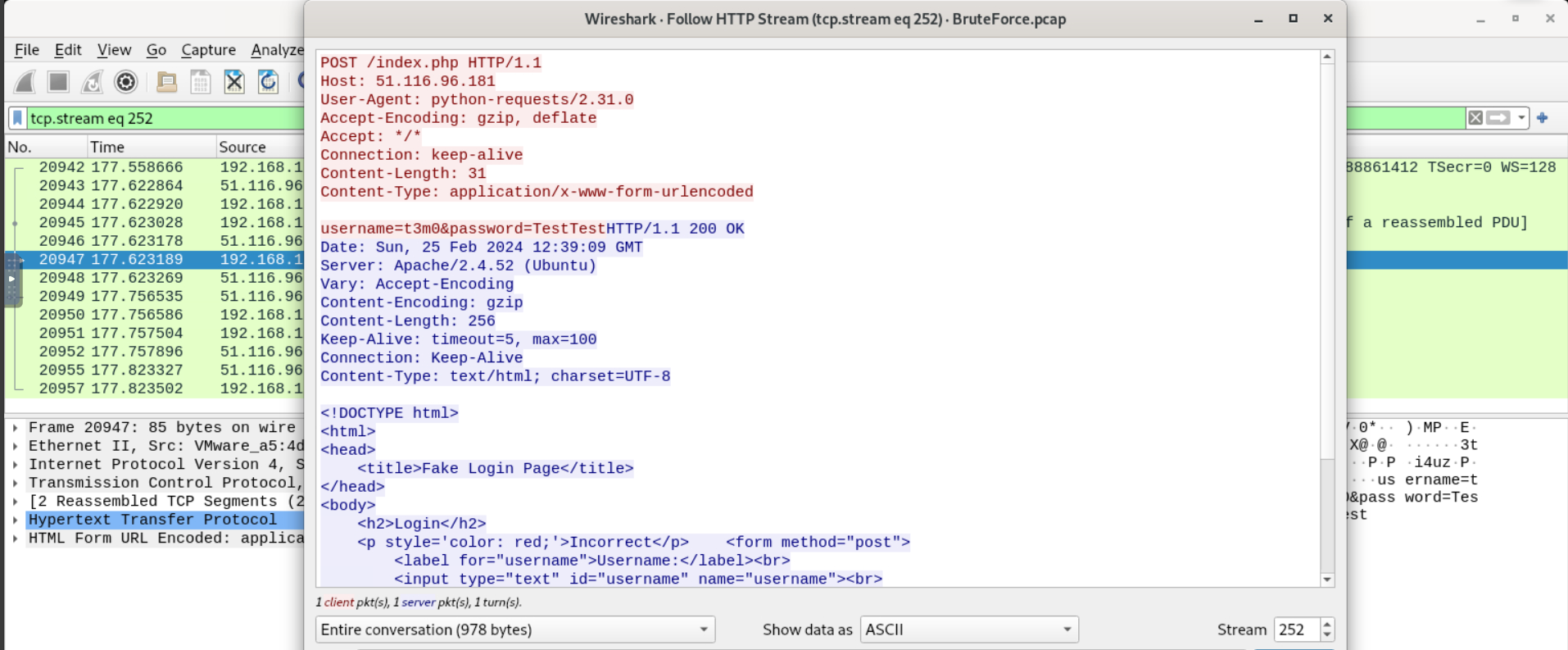
**Q2: Which directory was targeted by the attacker's brute-force attempt?**

****

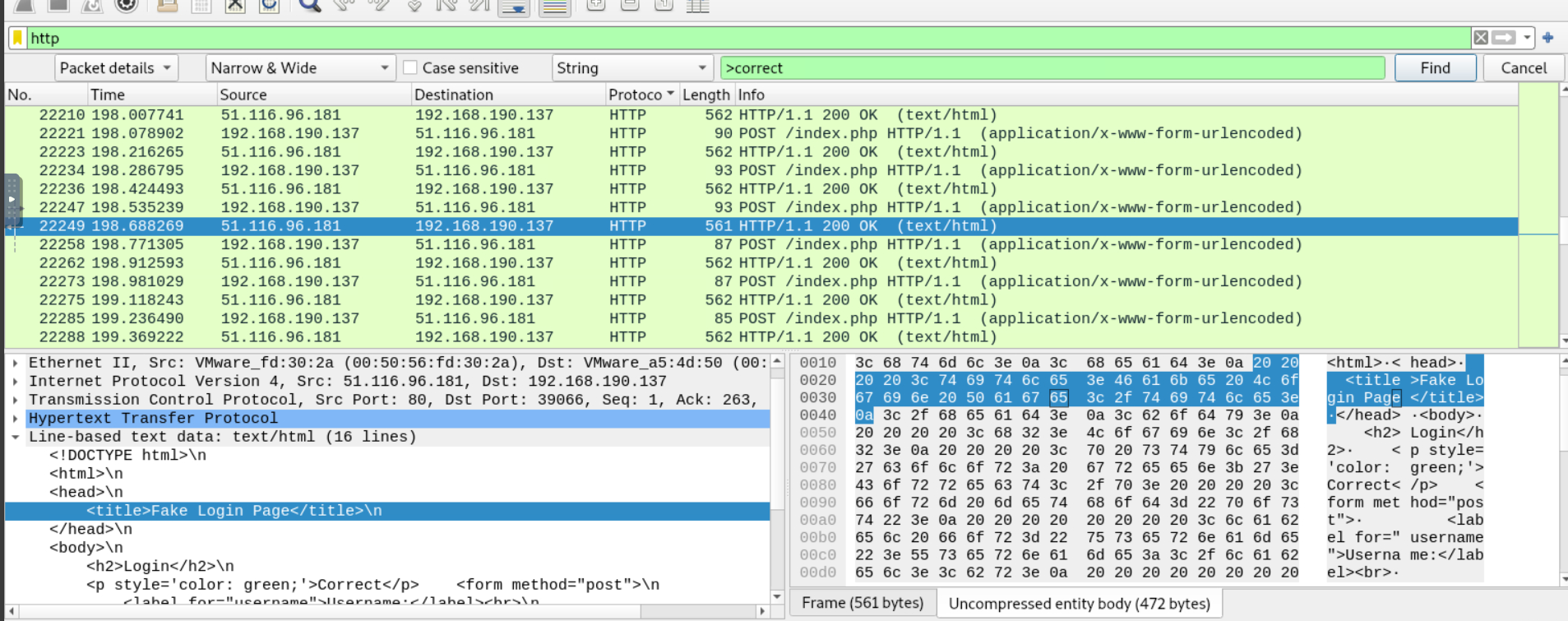
By exporting HTTP objects, I identified that the attacker targeted the **index.php** directory for the brute-force attempt.

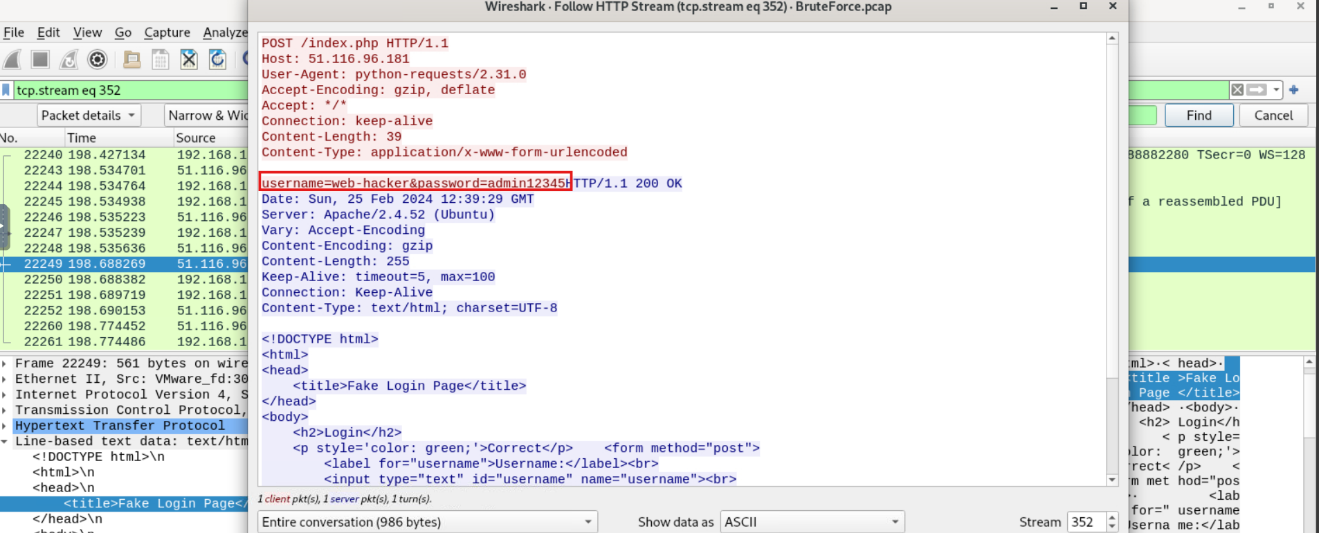
**Q3: Identify the correct username and password combination used for login.**

After analyzing the index.php packets and seeing multiple 'incorrect' login responses, I filtered for the successful attempt to identify the correct credentials.

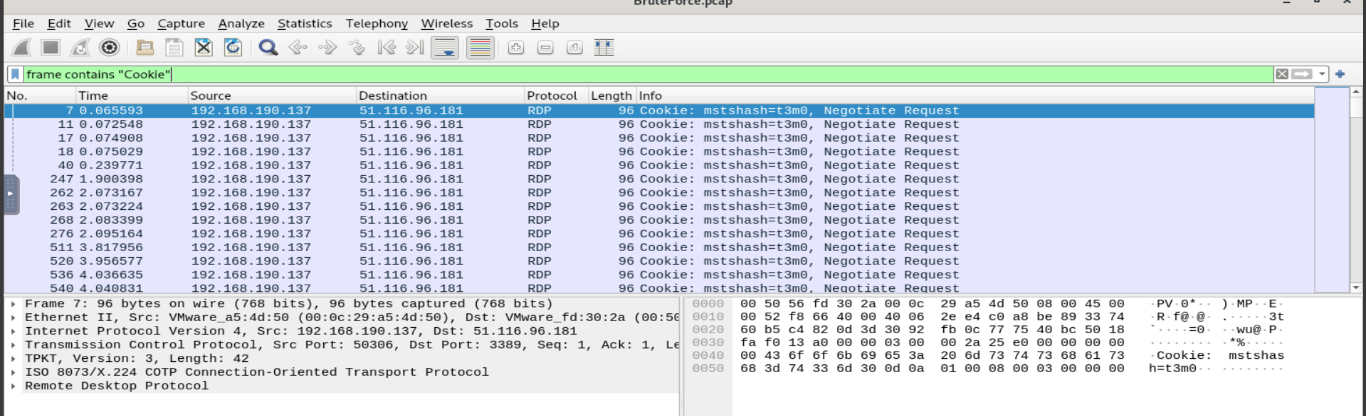


أعلى النموذج



After identifying the packet containing the 'correct' login response, I analyzed the HTTP stream to extract the valid username and password.

* **Username: web-hacker**
* **Password: admin12345**

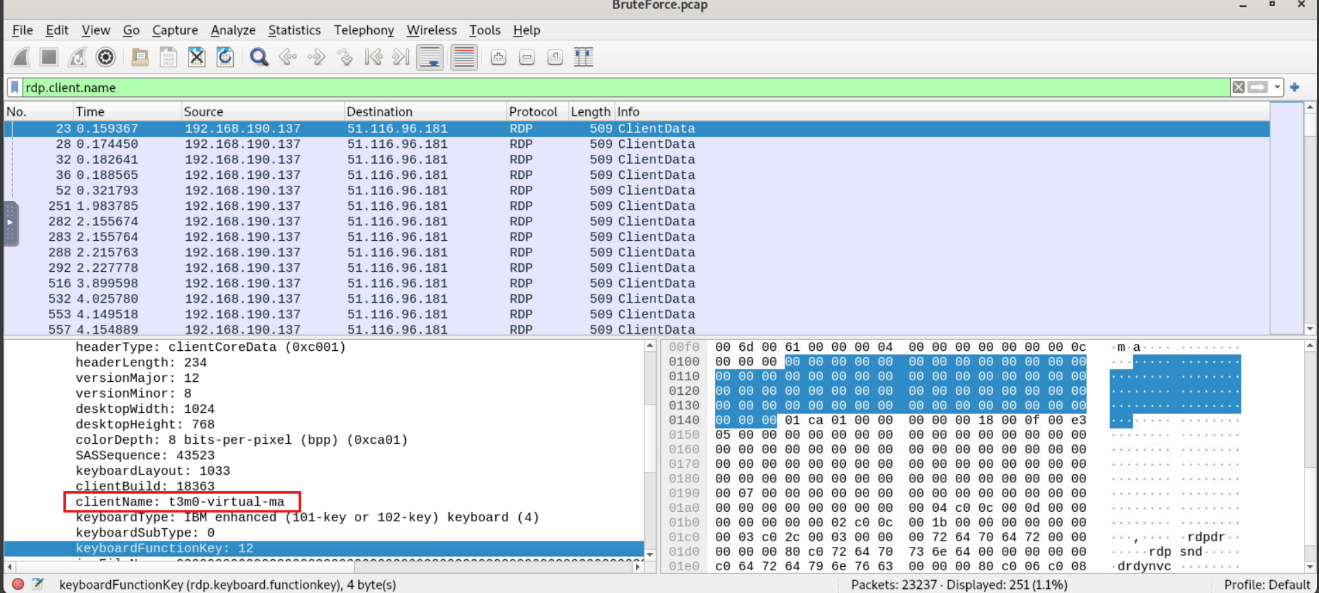
**Q4: How many user accounts did the attacker attempt to compromise via RDP brute-force?**

By using frame contains "Cookie", we can determine 10 unique users that sent negotiation request which are

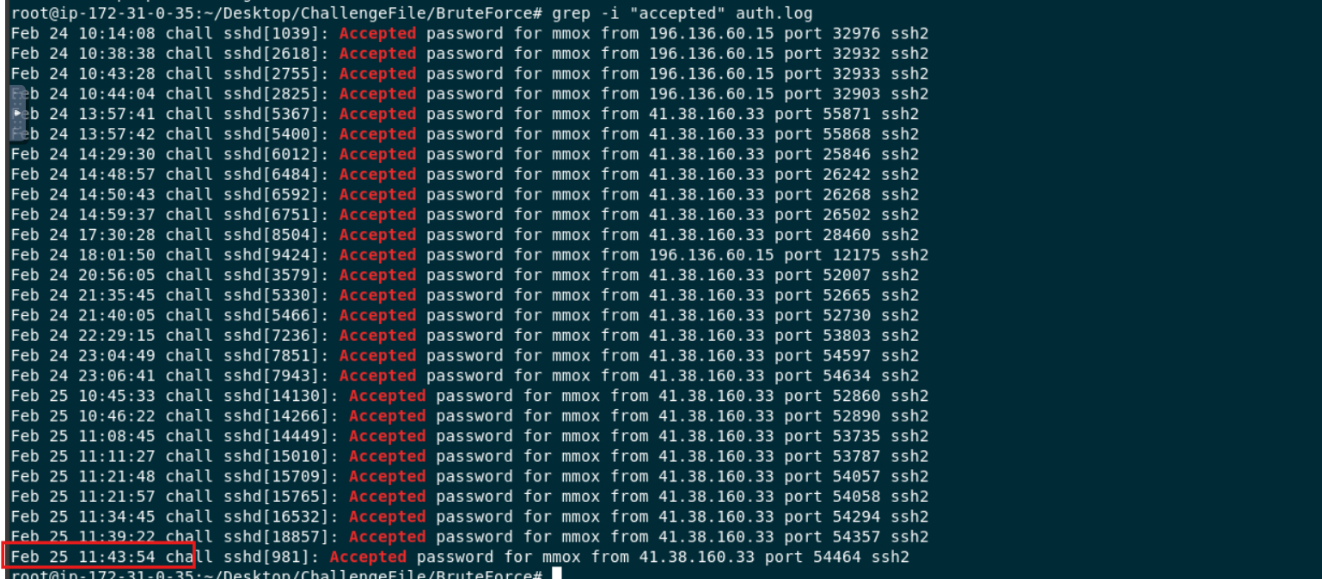
* t3m0
* Mosalah
* Messi
* web-hacker
* Kareem
* Mostafa
* mmox
* Mohamed
* Ali
* Mohsen

**But there are only 7 that got bruteforced**

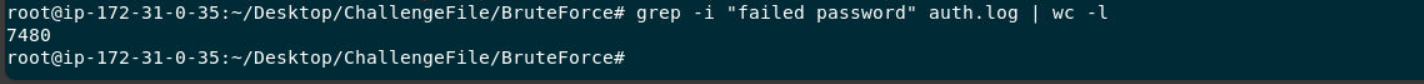
**Q5: What is the “clientName” of the attacker's machine?**

To find the attacker's machine name, I applied the rdp.client.name filter in Wireshark, which revealed the client name as: t3m0-virtual-ma.

**أعلى النموذج**

**Q6: When did the user last successfully log in via SSH, and who was it?أعلى النموذج**

The user 'mmox' last successfully logged in via SSH on Feb 25 at 11:43:54, as indicated by the final 'Accepted password' entry in the log file.

**Q7: How many unsuccessful SSH connection attempts were made by the attacker?**

**أعلى النموذج**

By running the command grep -i "failed password" auth.log | wc -l, I determined that the attacker made 7,480 unsuccessful SSH login attempts.

**Q8: What technique is used to gain access?**

Answer: T1110

