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?

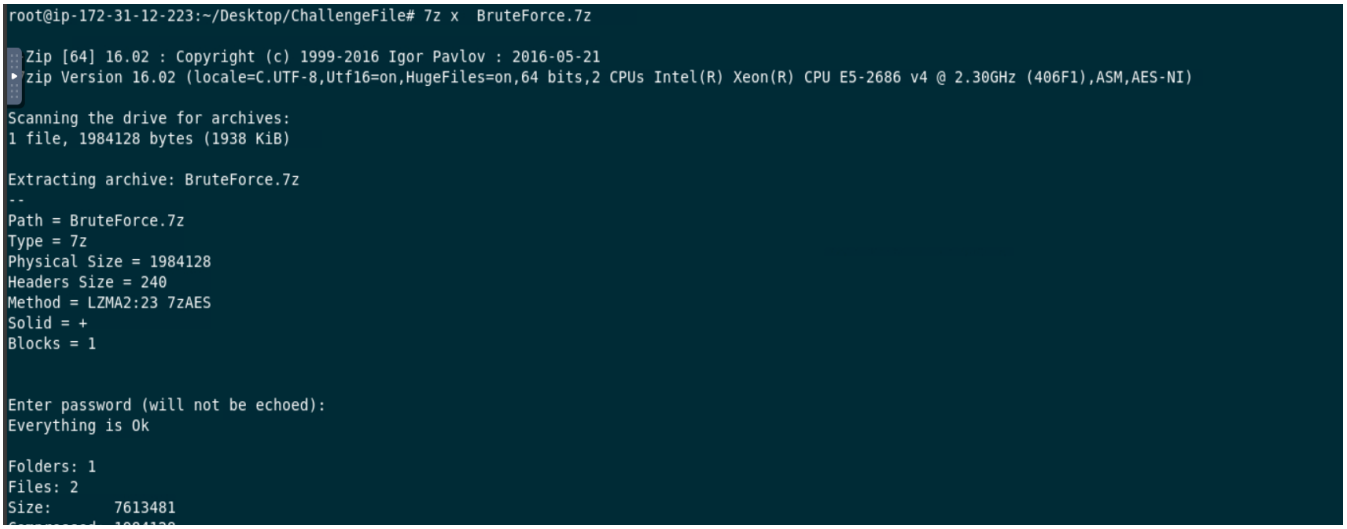
File Location: /root/Desktop/ChallengeFile/BruteForce.7z

File Password: infected

Start Investigation

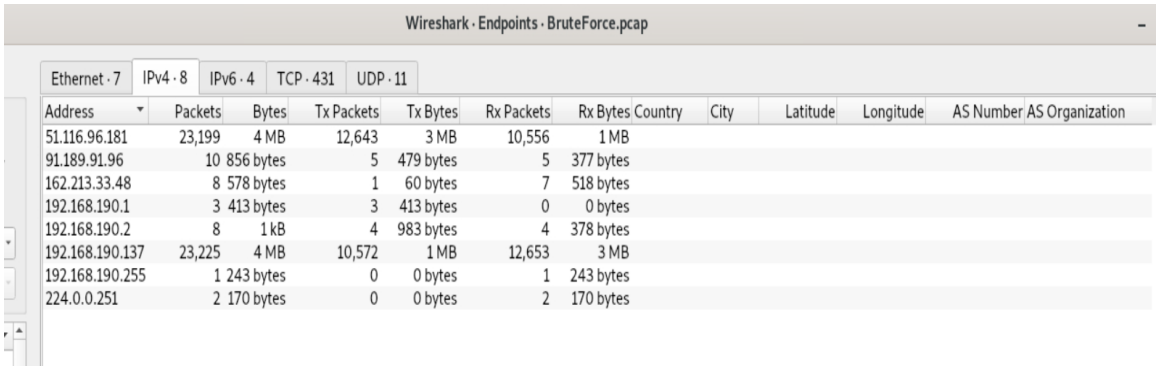
Q1: What is the IP address of the server targeted by the attacker's brute-force attack?

The BruteForce.7z file was successfully extracted using the 7z tool. After extraction, the contents were found to include two main files:



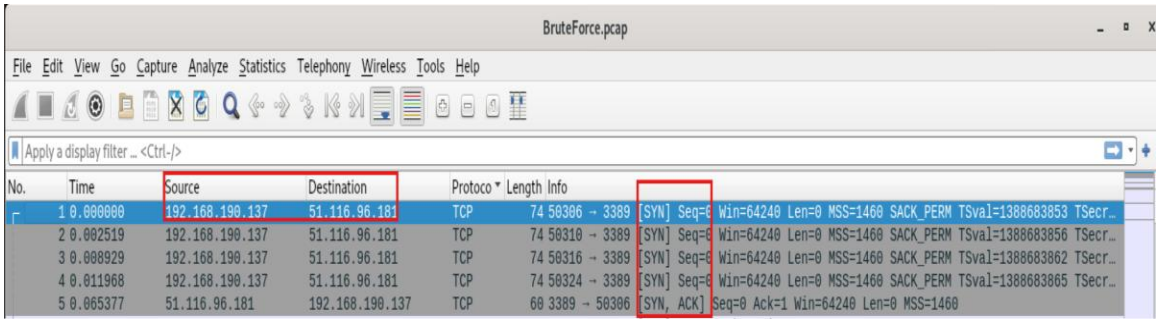
- BruteForce.pcap
- Auth.log

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.



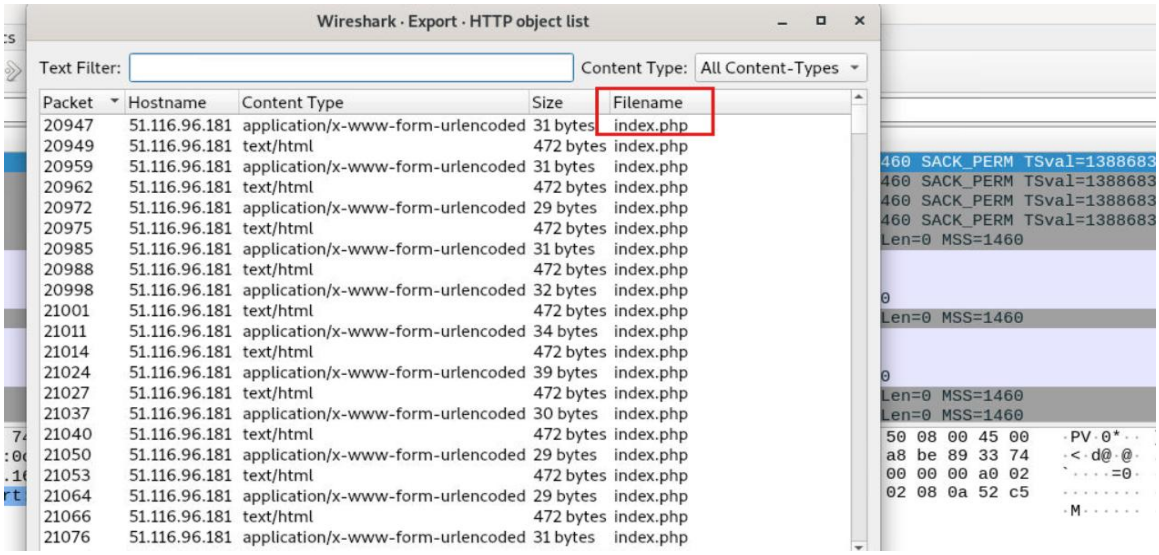
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
51.116.96.181	23,199	4 MB	12,643	3 MB	10,556	1 MB						
91.189.91.96	10	856 bytes	5	479 bytes	5	377 bytes						
162.213.33.48	8	578 bytes	1	60 bytes	7	518 bytes						
192.168.190.1	3	413 bytes	3	413 bytes	0	0 bytes						
192.168.190.2	8	1 kB	4	983 bytes	4	378 bytes						
192.168.190.137	23,225	4 MB	10,572	1 MB	12,653	3 MB						
192.168.190.255	1	243 bytes	0	0 bytes	1	243 bytes						
224.0.0.251	2	170 bytes	0	0 bytes	2	170 bytes						

- 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.

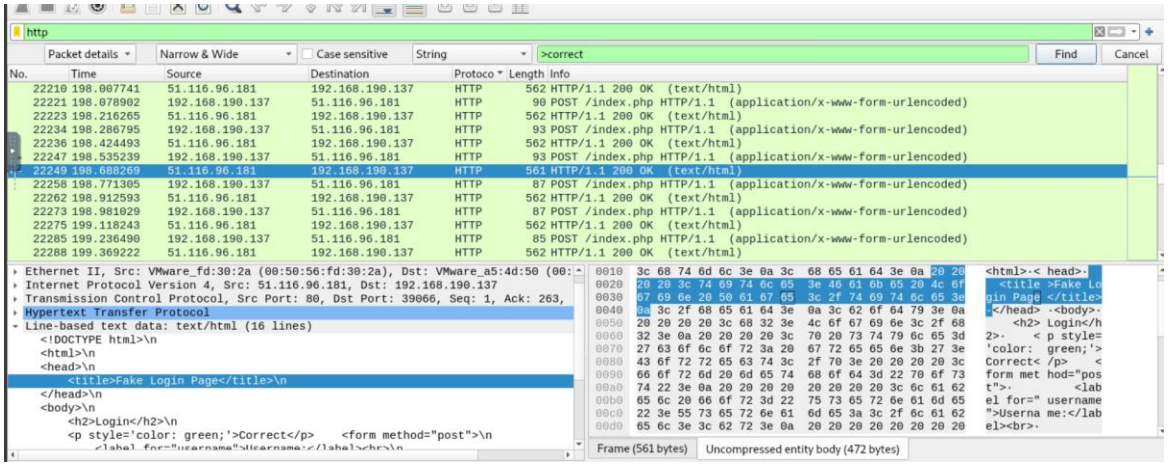
Q2: Which directory was targeted by the attacker's brute-force attempt?



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

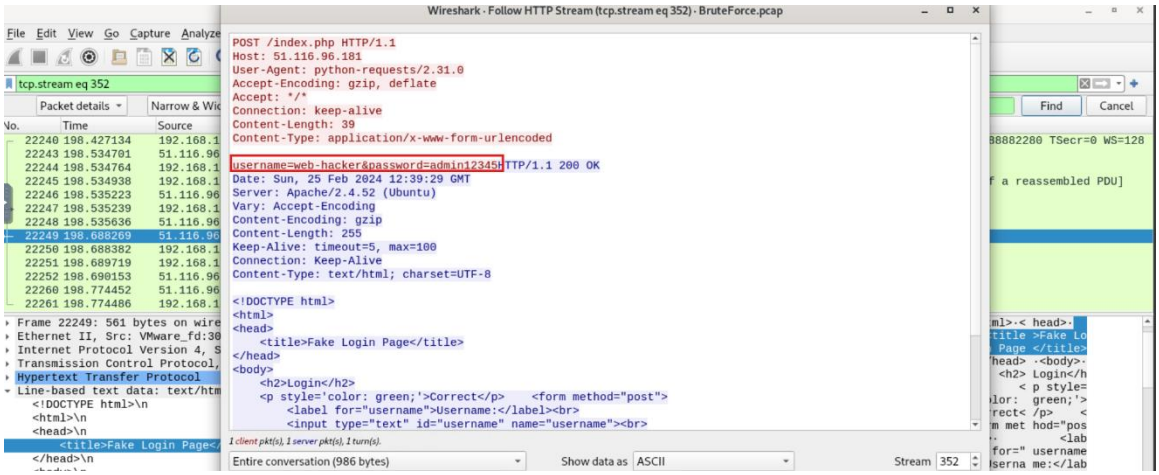
Q3: Identify the correct username and password combination used for login.

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



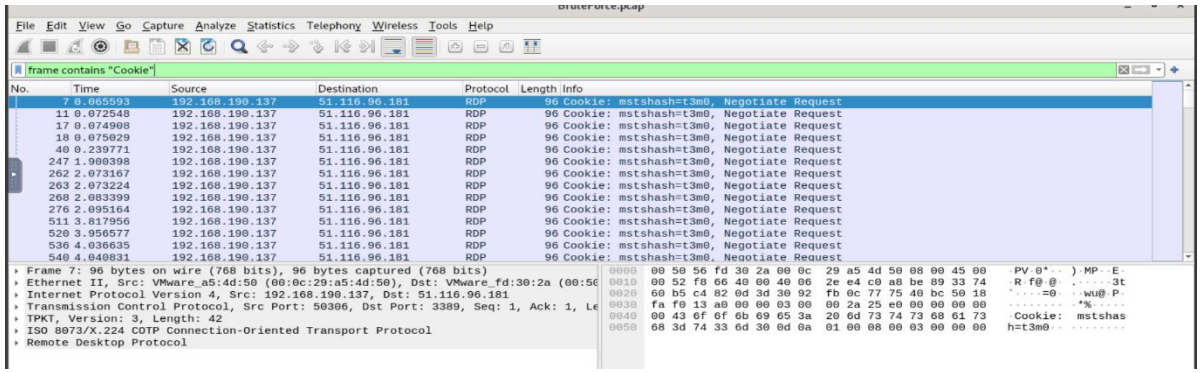
After identifying the packet containing the 'correct' login response, I analyzed the HTTP stream to extract the valid username and password.

- **Username: web-hacker**



- **Password: admin12345**

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



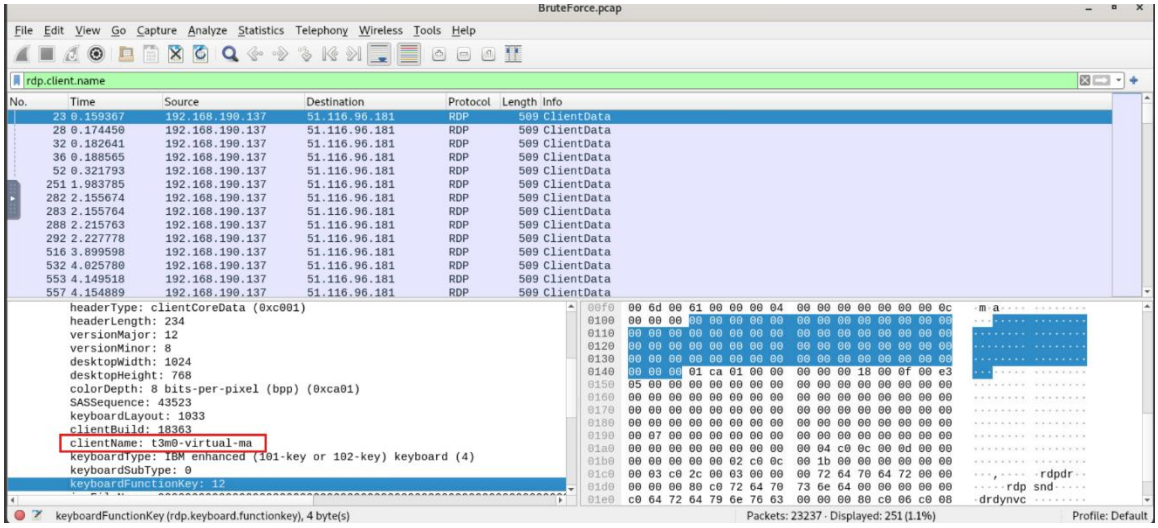
By using frame contains "Cookie", we can determine 10 unique users that sent negotiation request which are

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

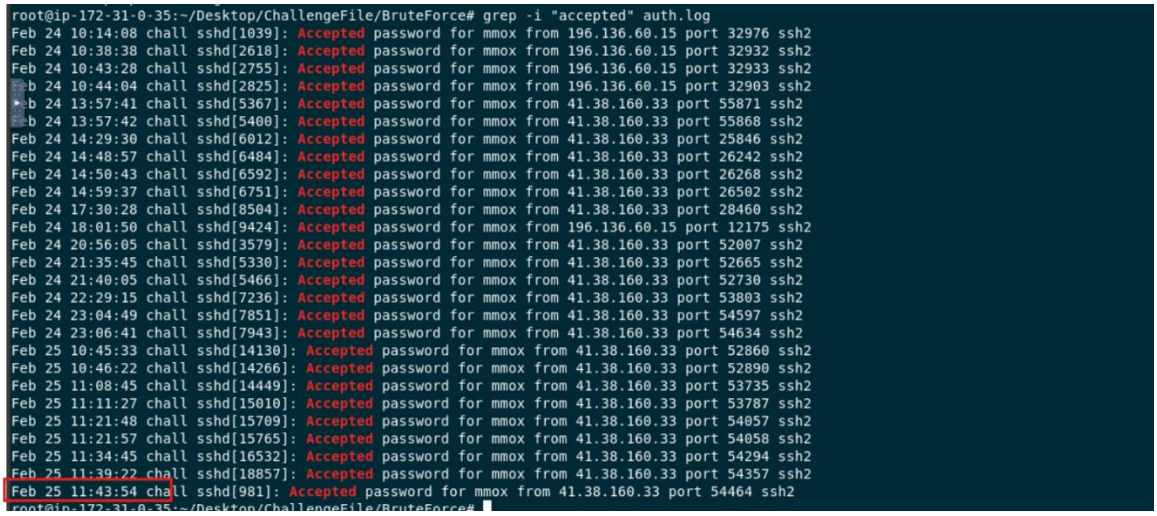
But there are only 7 that got bruteforced

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.



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



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?

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

Home > Techniques > Enterprise > Brute Force

Brute Force

Sub-techniques (4)

Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.[1] Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.[2] Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

Brute forcing credentials may take place at various points during a breach. For example, adversaries may attempt to brute force access to Valid Accounts within a victim environment leveraging knowledge gathered from other post-compromise behaviors such as OS Credential Dumping, Account Discovery, or Password Policy Discovery. Adversaries may also combine brute forcing activity with behaviors such as External Remote Services as part of Initial Access.

ID: T1110

Sub-techniques: T1110.001, T1110.002, T1110.003, T1110.004

Tactic: Credential Access

Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Network, Office 365, SaaS, Windows, macOS

Contributors: Alfredo Oliveira, Trend Micro; David Fiser, @anu4is, Trend Micro; Ed Williams, Trustwave, SpiderLabs; Magno Logan, @magnologan, Trend Micro; Mohamed Kmal; Yossi Weizman, Azure Defender Research Team

Version: 2.5

Created: 31 May 2017

Last Modified: 29 January 2024

Summary

In this challenge, I analyzed network traffic using Wireshark to identify the threat actor's IP address and uncover brute-force attacks targeting the web server and RDP. I also performed a forensic review of the authentication logs to calculate the number of failed login attempts and pinpoint the exact moment the attacker gained a foothold on the server.