**Overpass2 - Hacked**

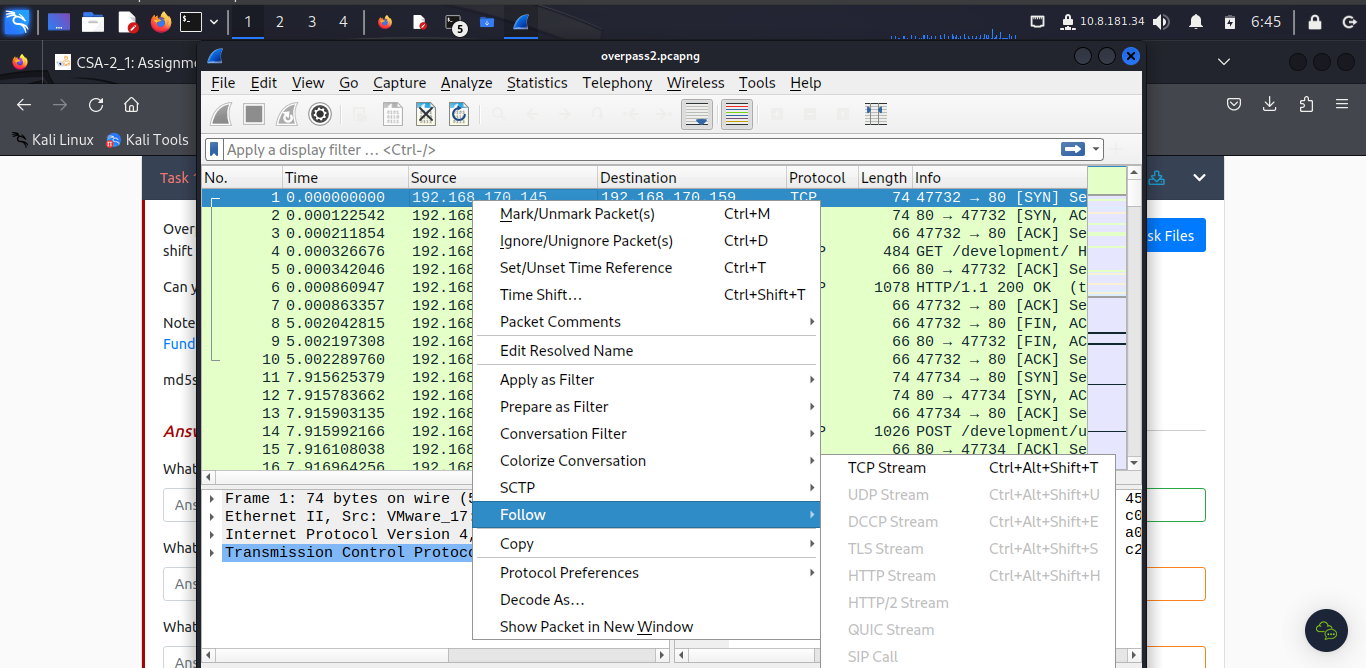
**Introduction**

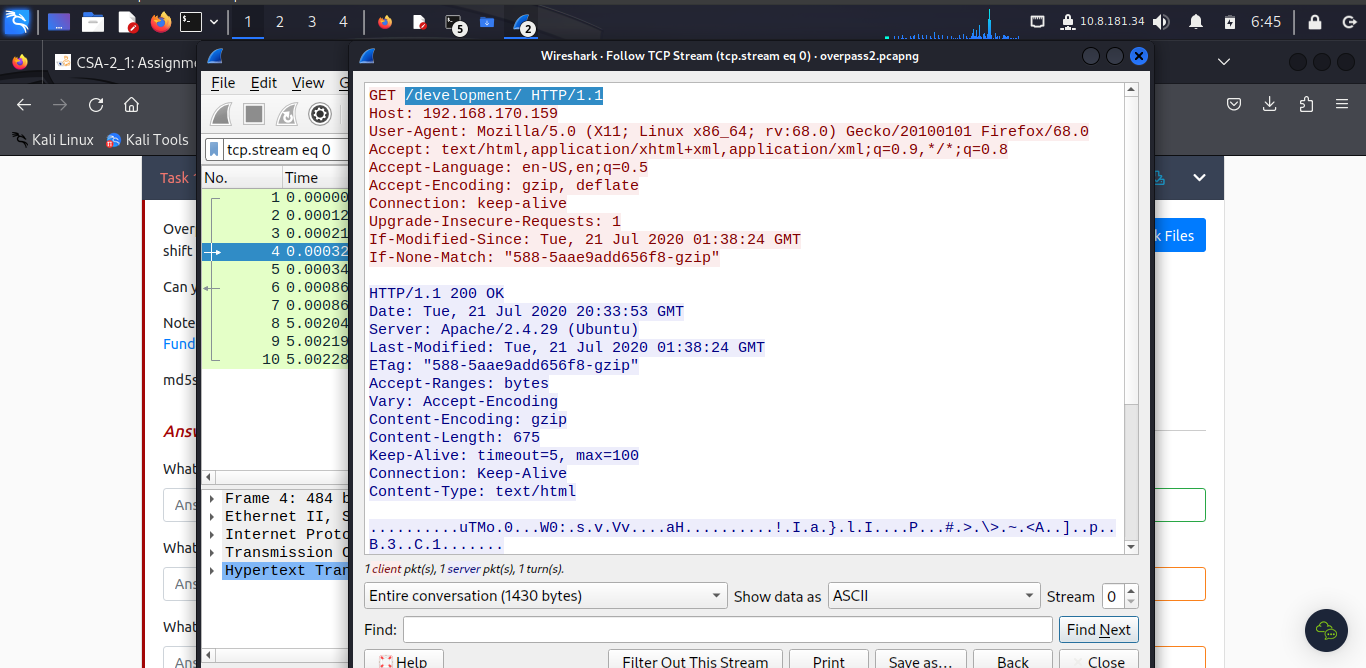
This room’s task introduces the attack concept where by an analysist is expected to analyse the attacker's actions and hack back in.

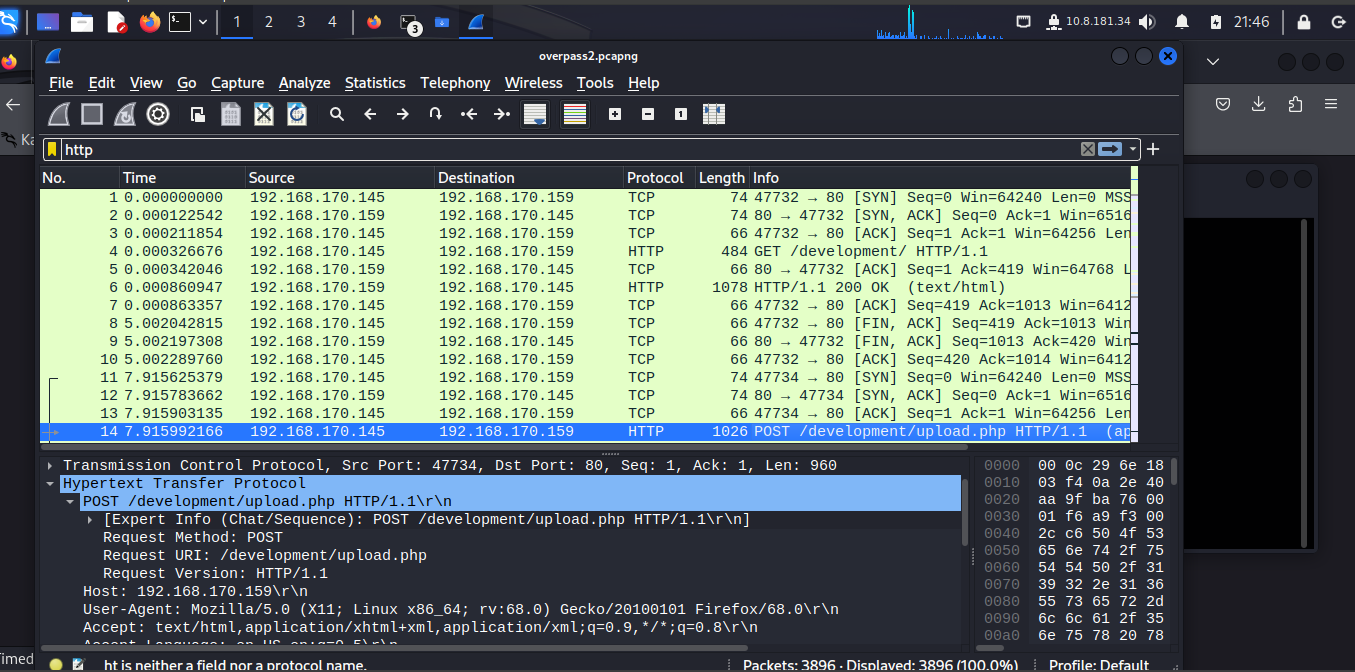
***Activities***

***Task 1: Forensics – Analyse the PCAP***

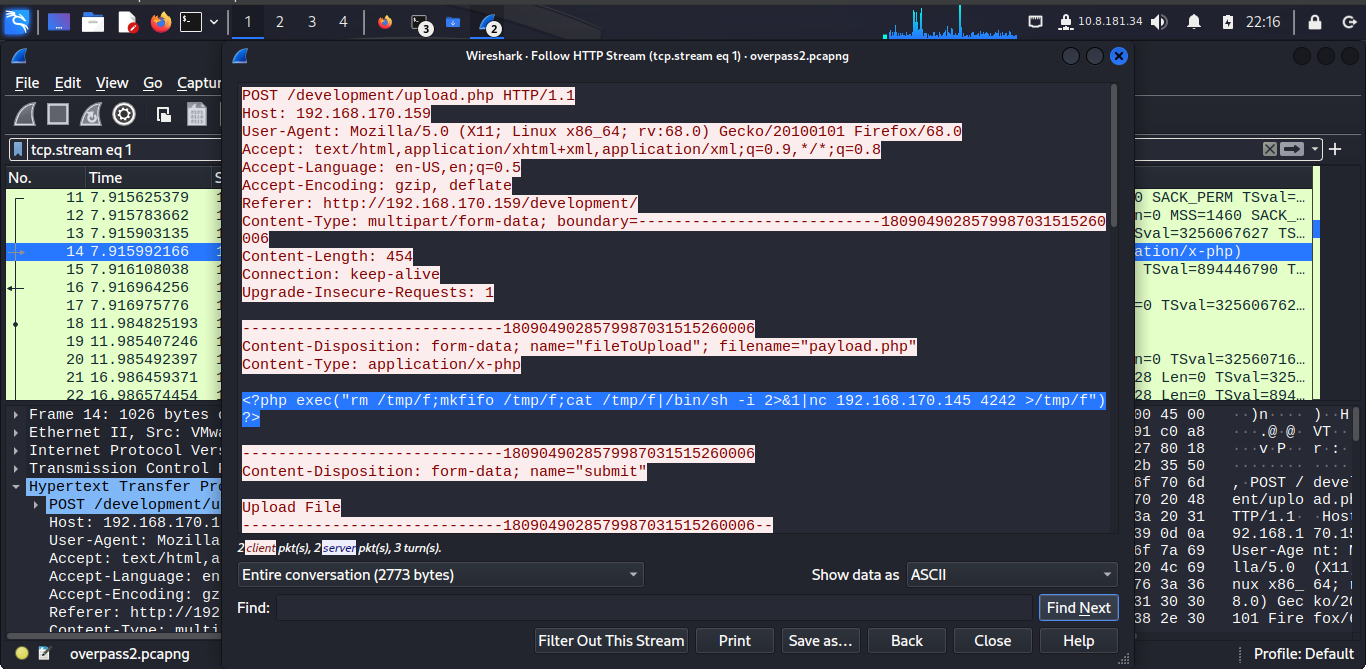
The room starts by providing a PCAP file that contains the packets captured during the attack. There are five questions that need to be answered by forensically analyzing the captured network packets. Using **Wireshark**, I opened the PCAP file to analyze the network packets and start answering the questions.

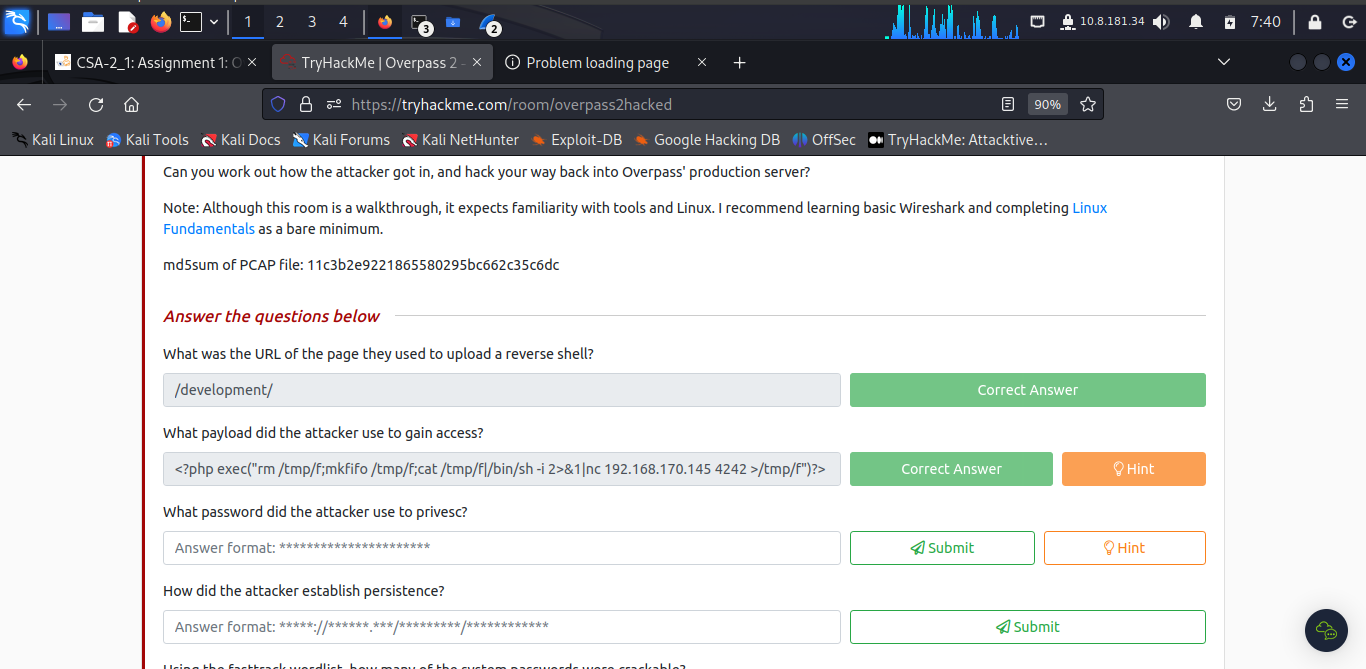






To access the full access to tags, navigate follow > HTTP stream.



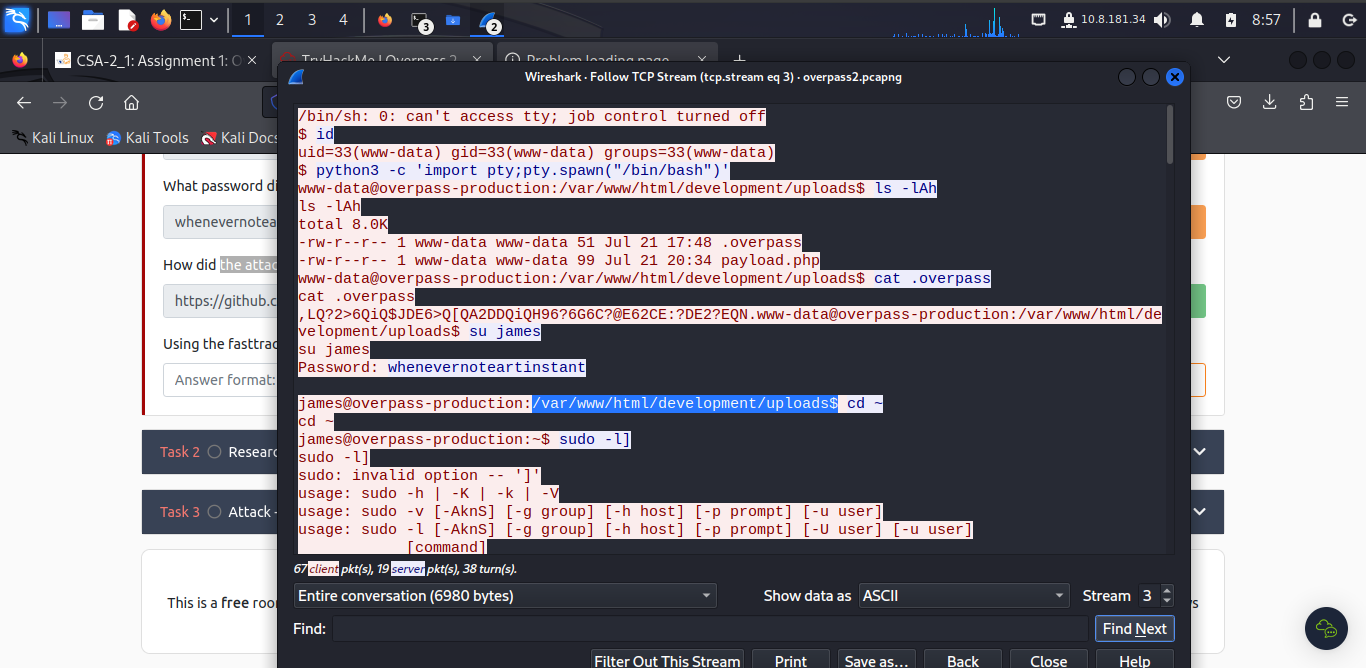


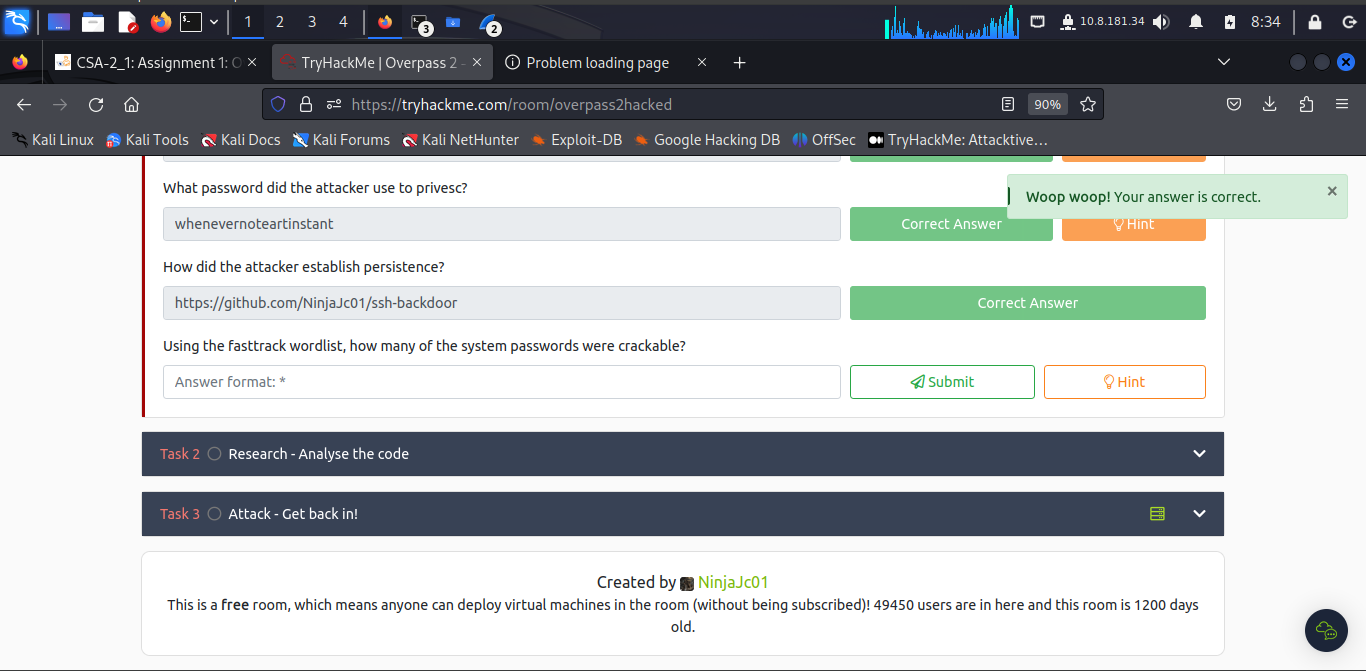


To get the password, first locate tcp with complete handshake. Then **follow > http stream**

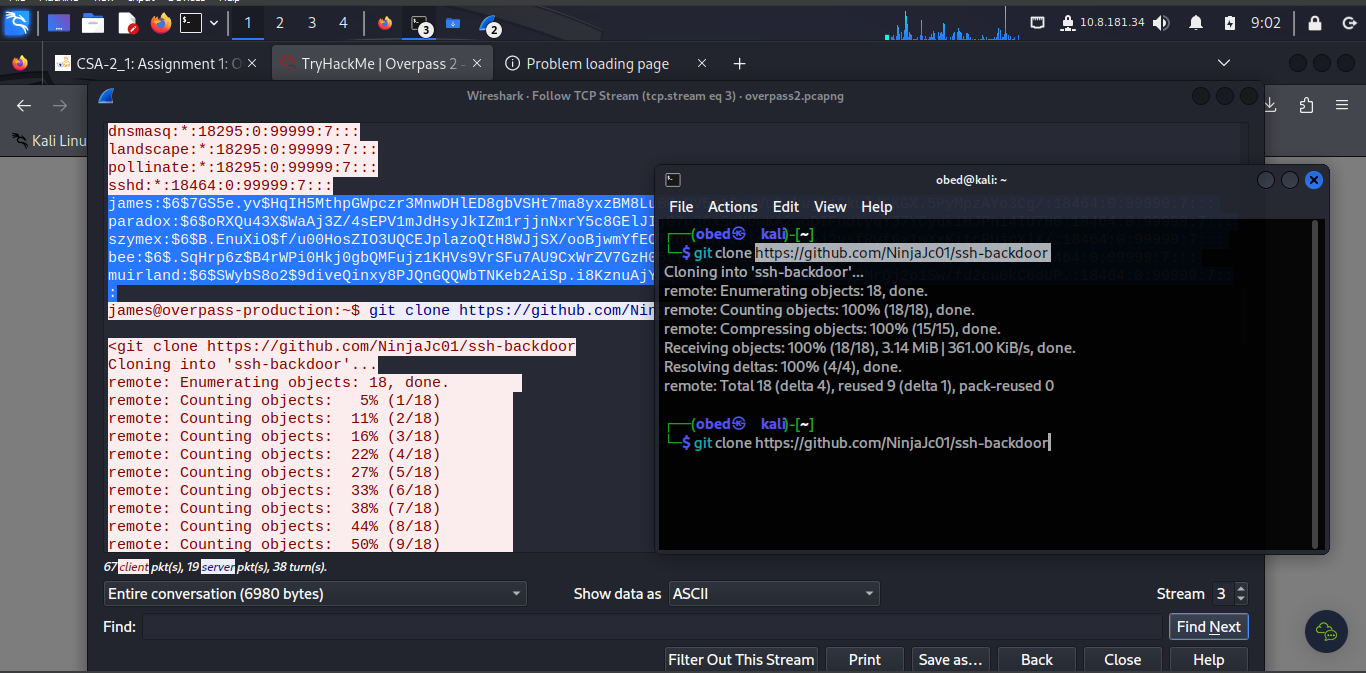


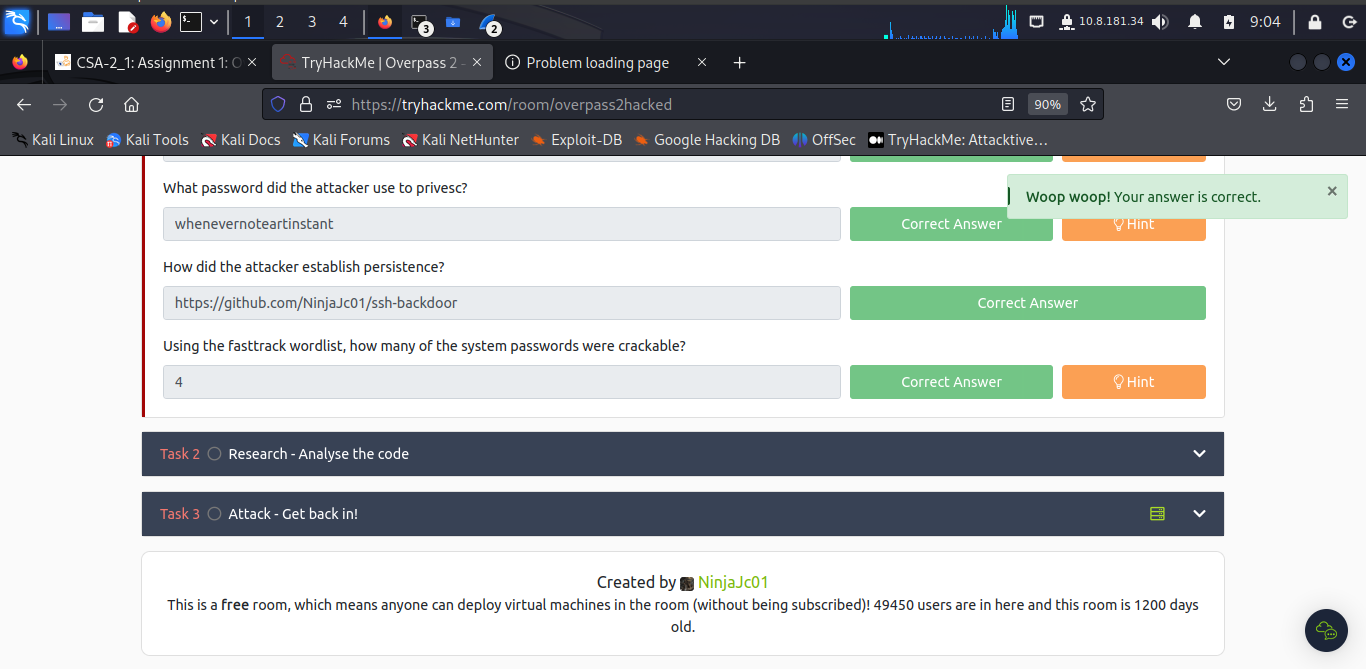
The attacker established persistence by **cloning** a github repository to a local machine (**https://github.com/NinjaJc01/ssh-backdoor**)





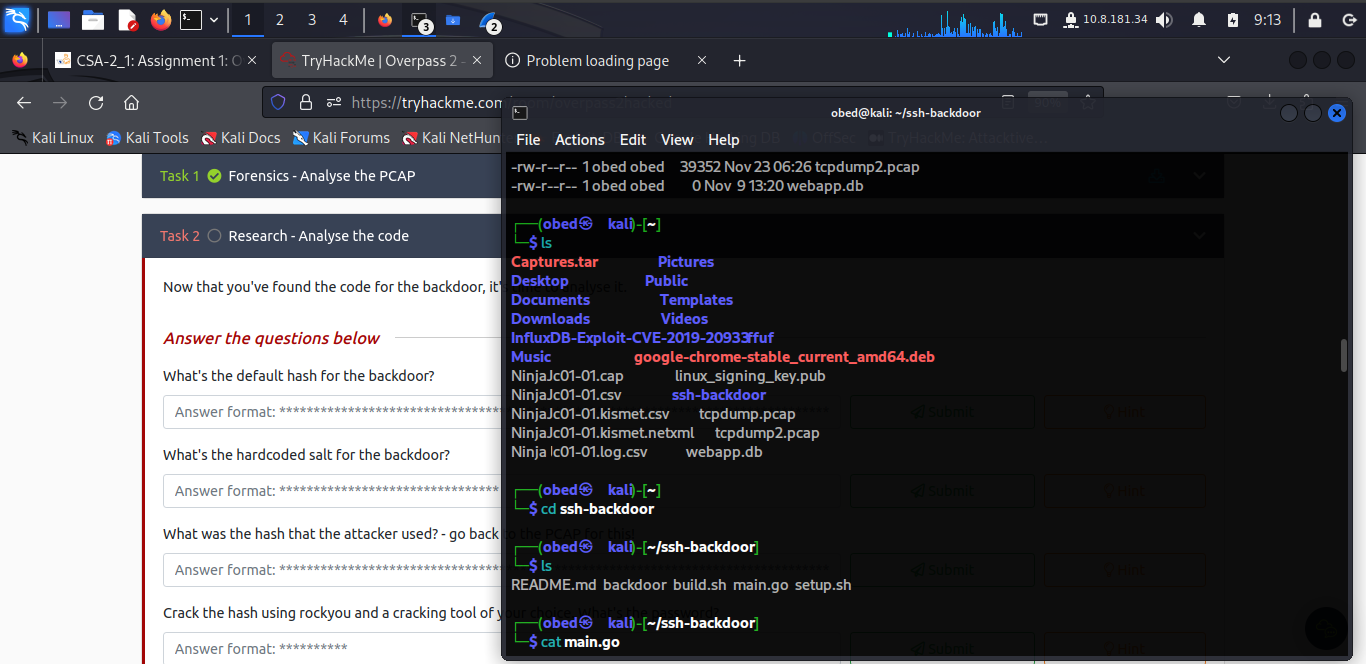
It can be that there are **4** system passwords cracked.

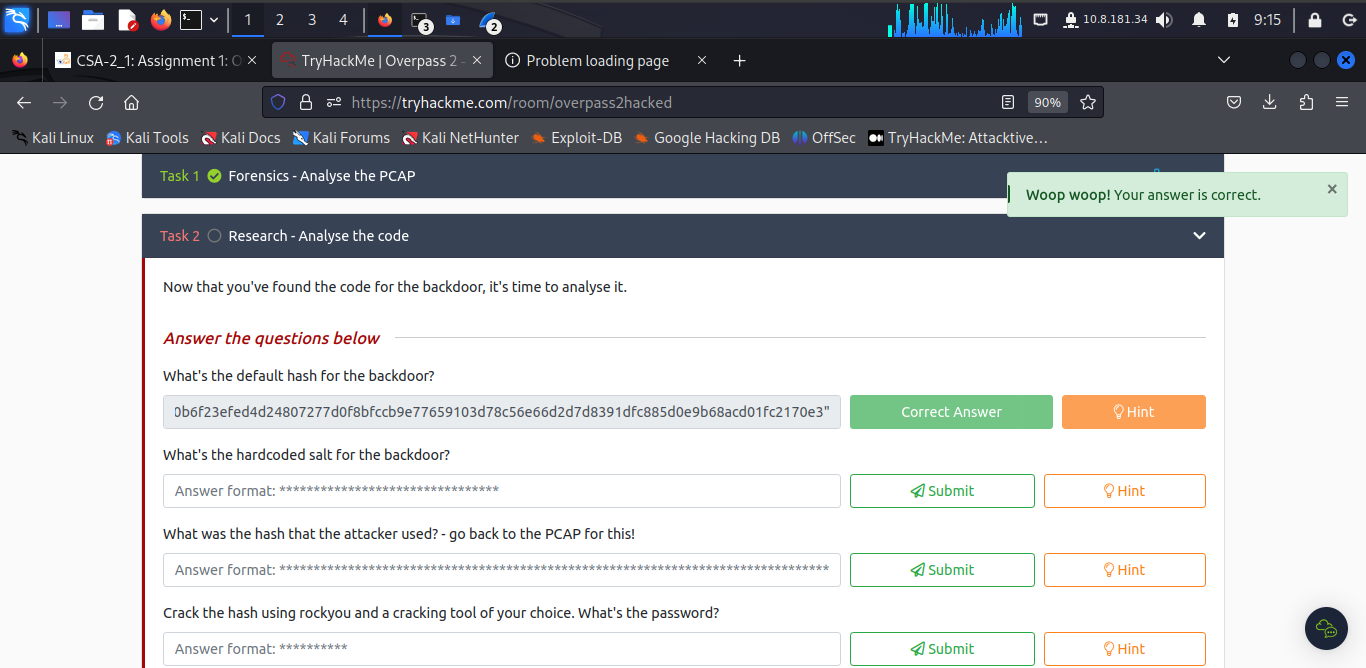




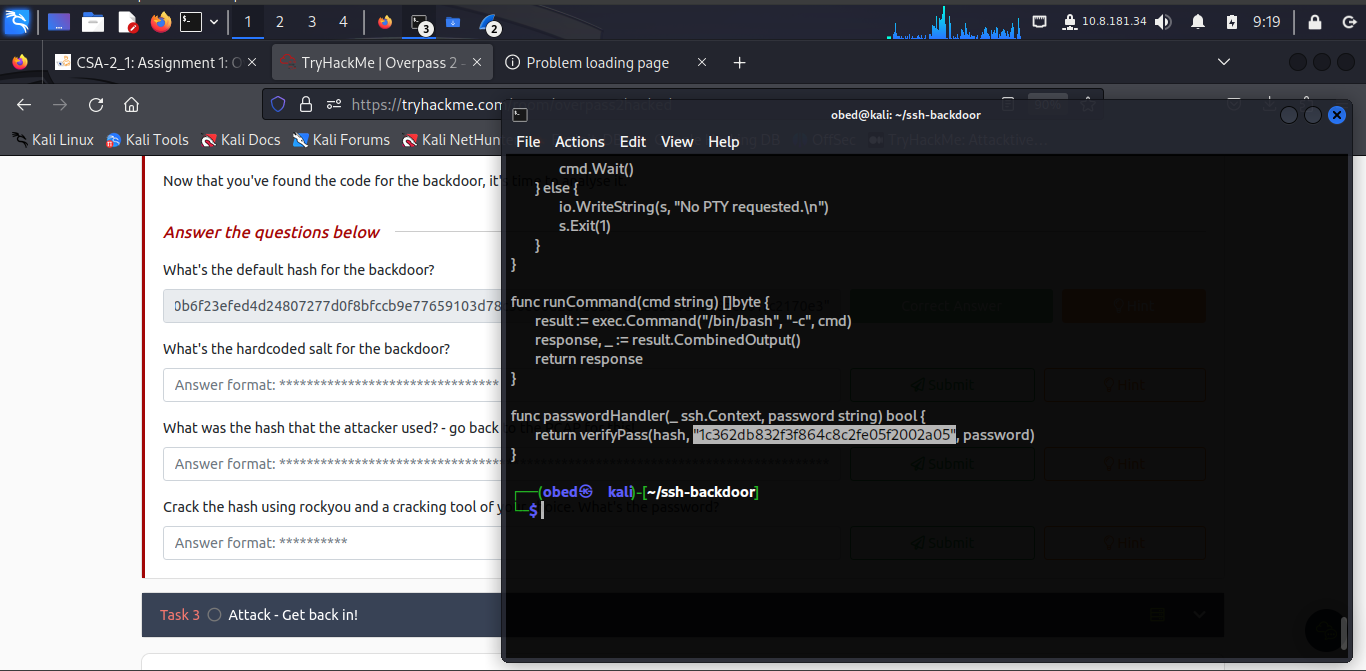
***Task 2: Research – Analyse the code***

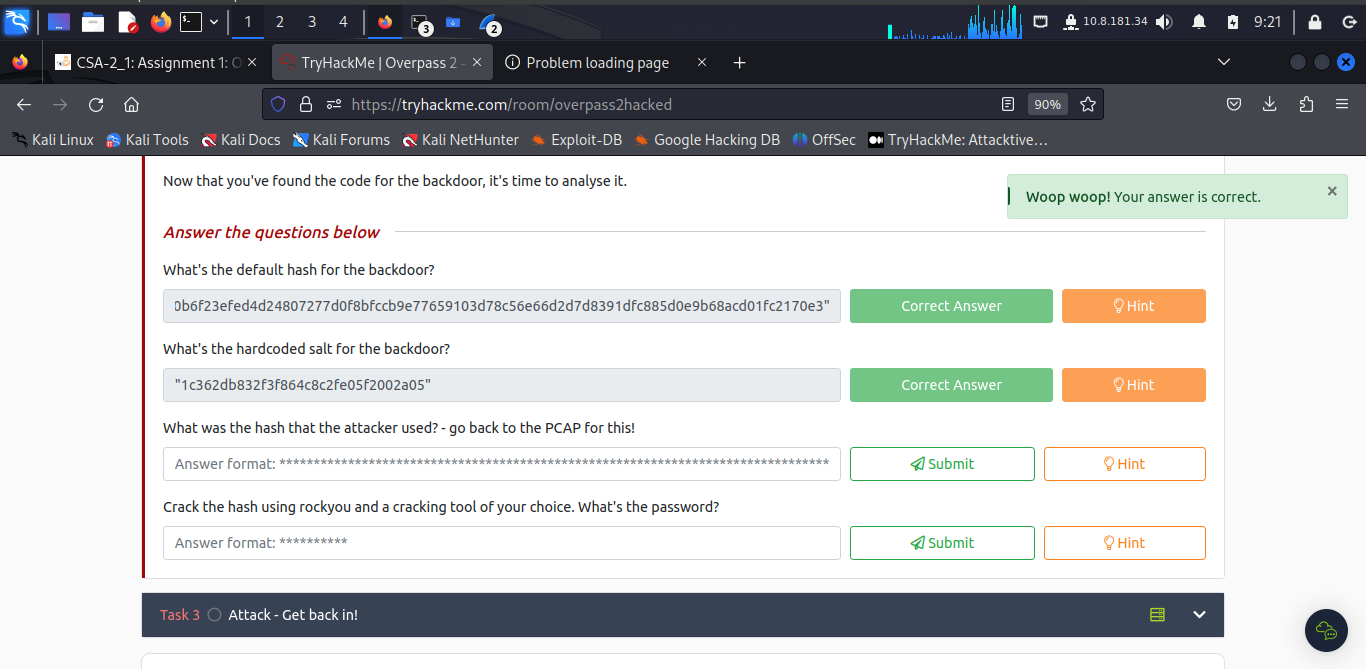
In this task, we require the cloned repository which I have already done in the previous task.



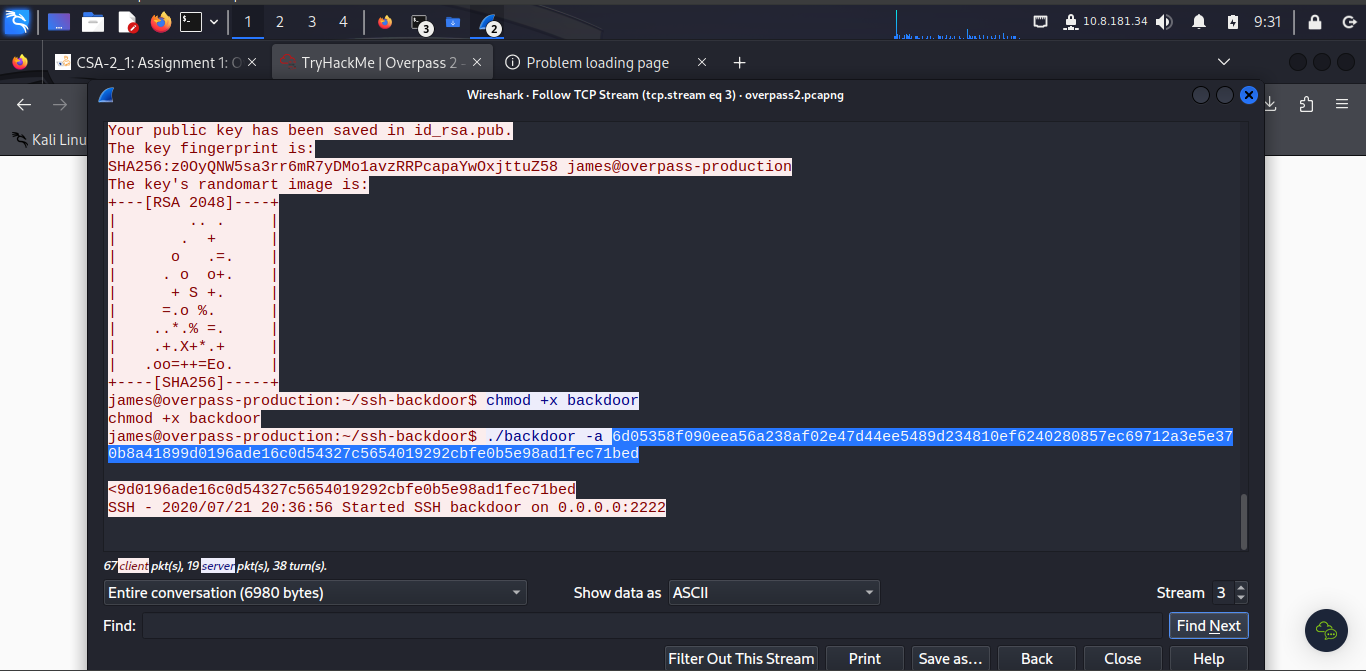


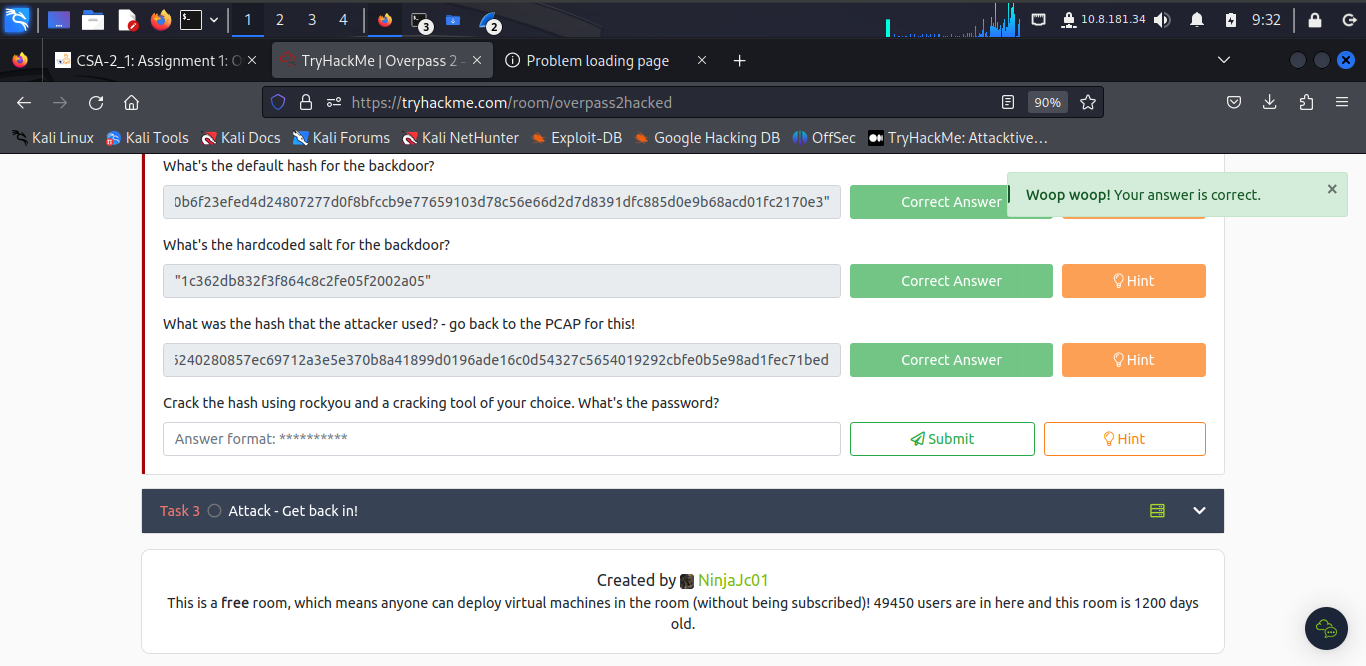
To find the salt, locate the salt in file, near the end part of the file.





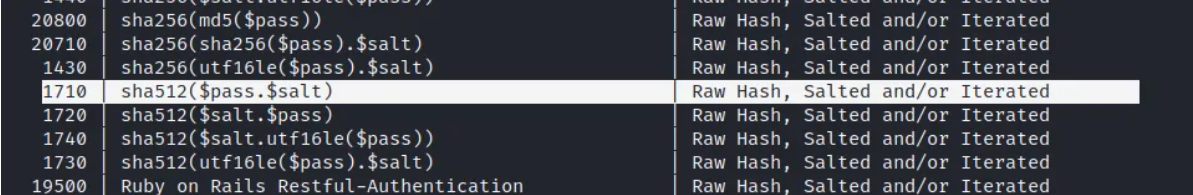
To find the hash that the attacker used, I returned to wireshark platform – now still open and locate the hash as: **6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed**

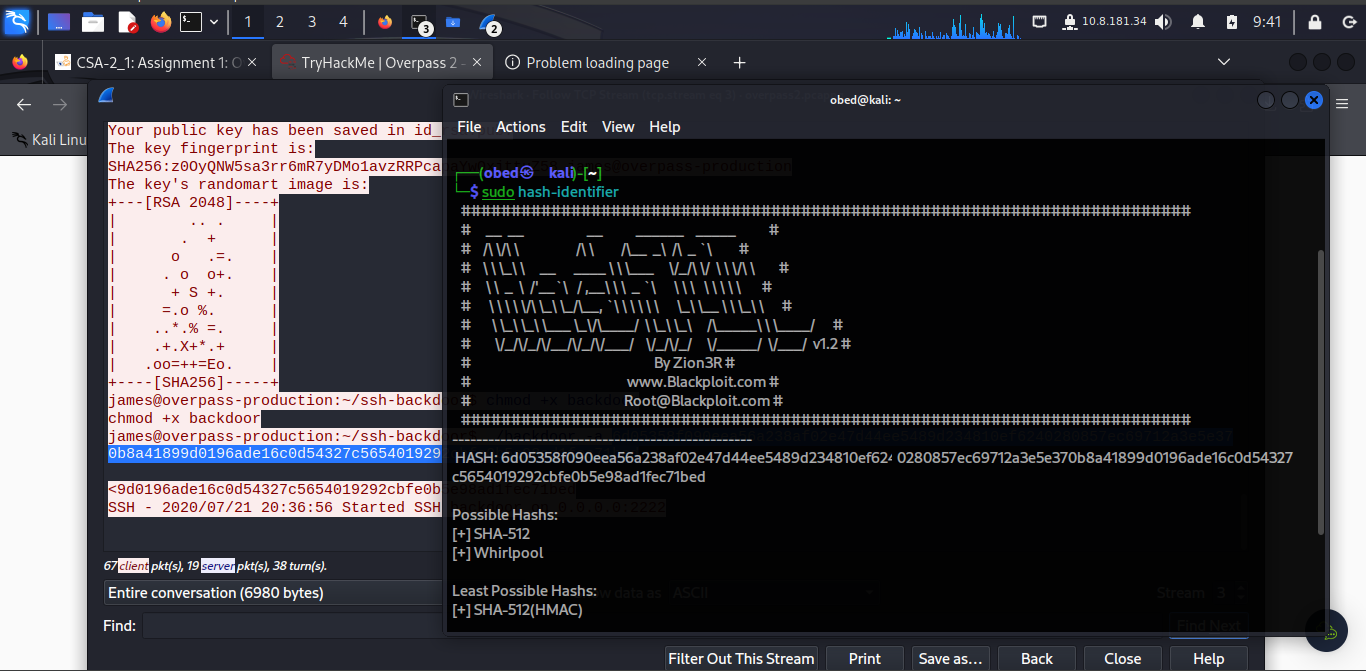
****

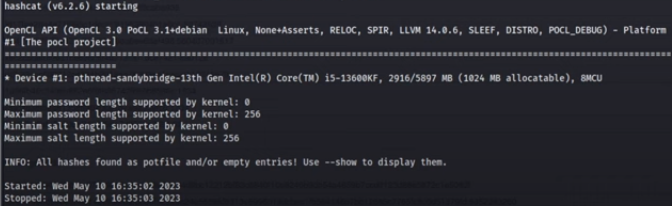
****

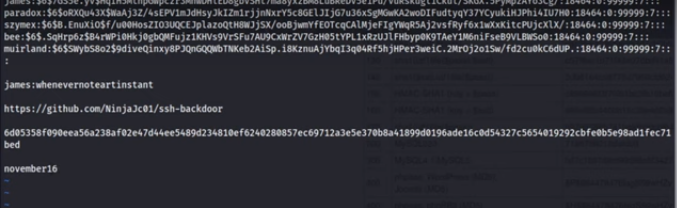
The password, after cracking the hash using **hash-identifier** is:

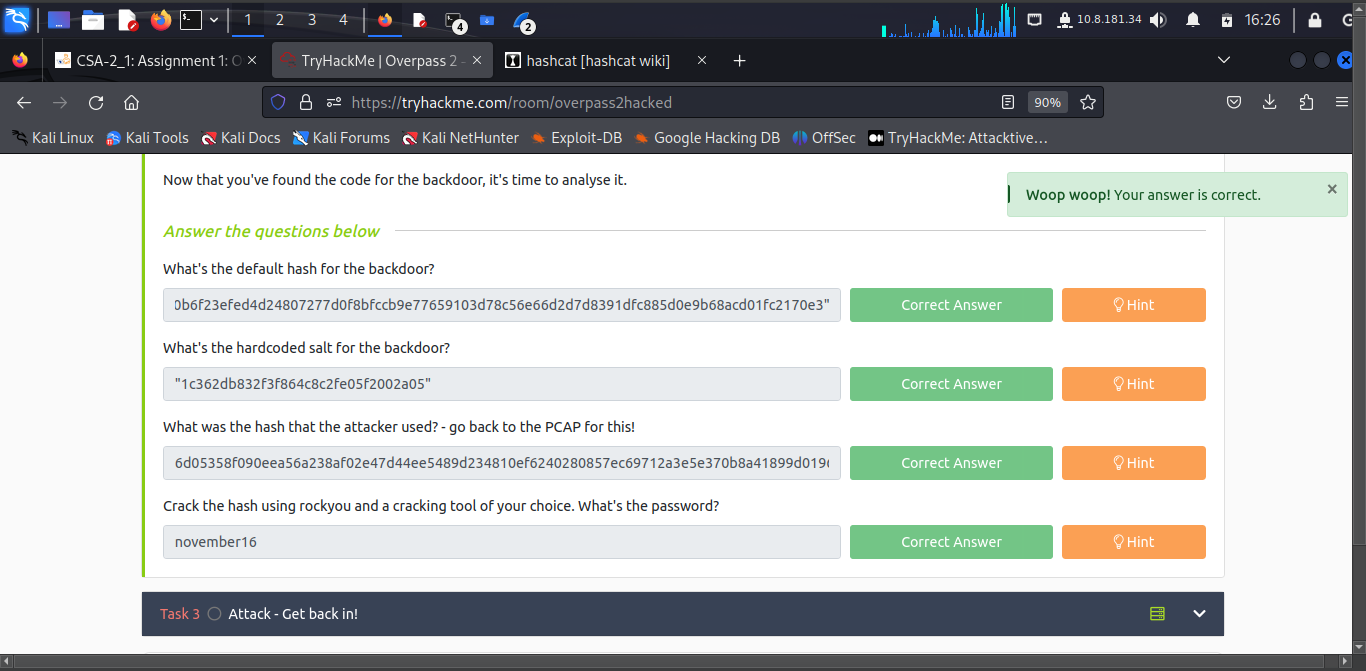
In local machine terminal, I ran ***hash-identifier*** then after in new terminal I run a hashcat method to use for the extracted salt and the hash key code:







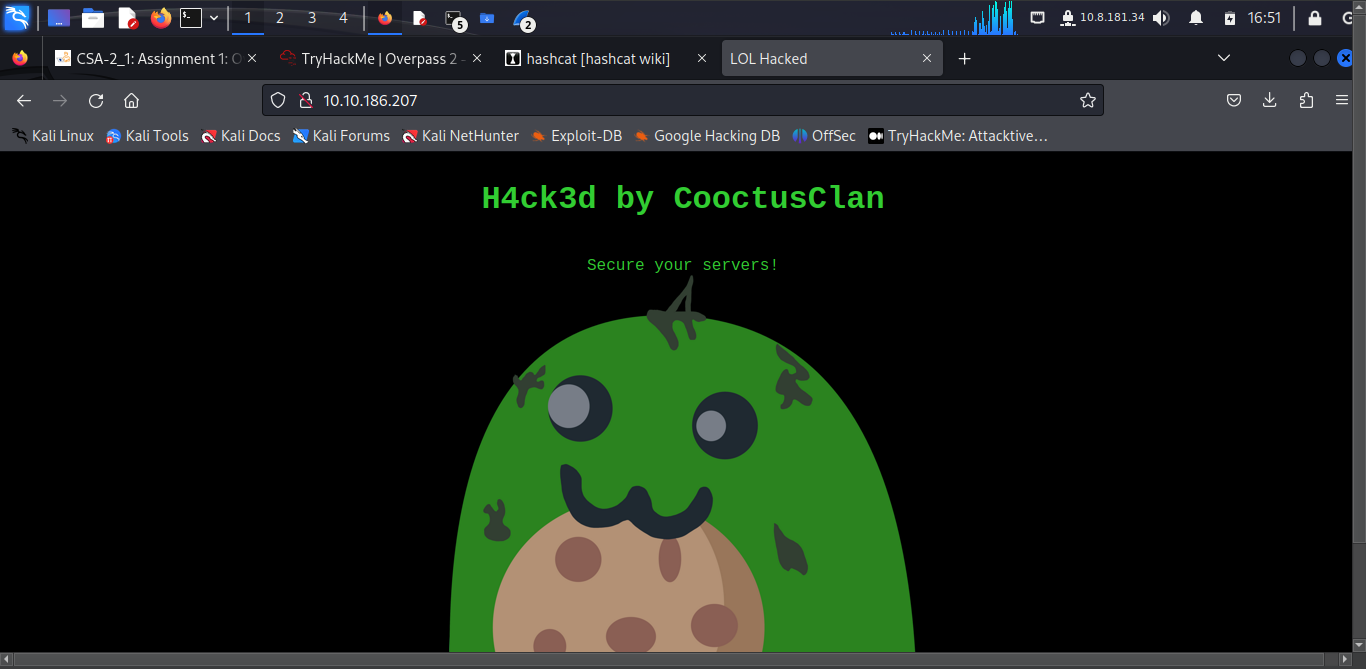




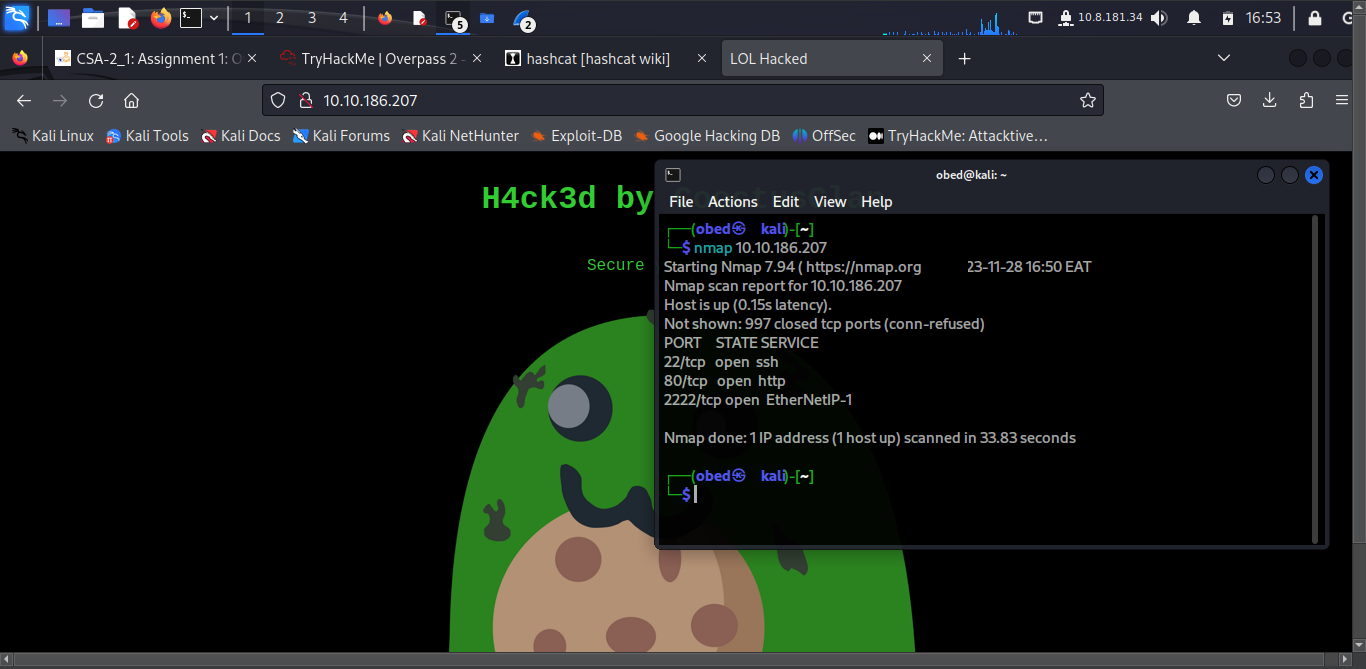
***Task 3: Attack – Get back in!***

The incident needs someone to take control of the Overpass production server again.

Locate the port number **2222**



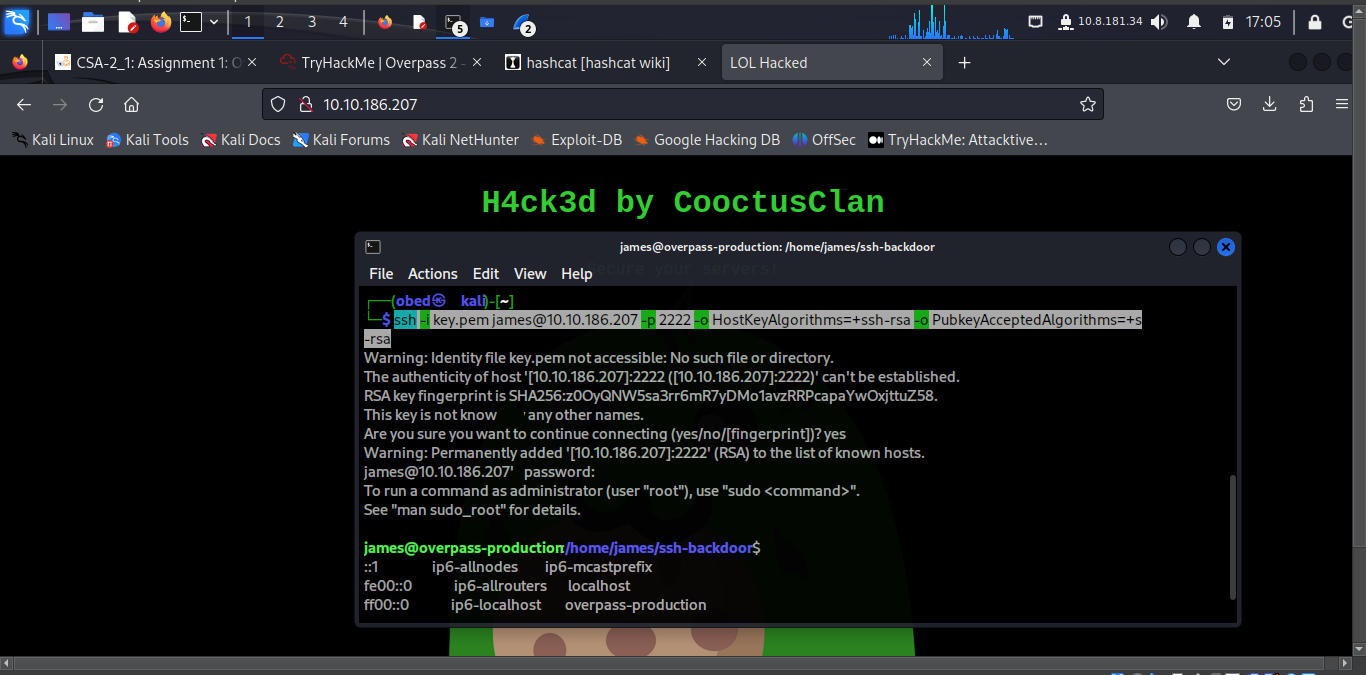
The port we are interested in is **222**



To access the user’s flag, run these piece on local machine:

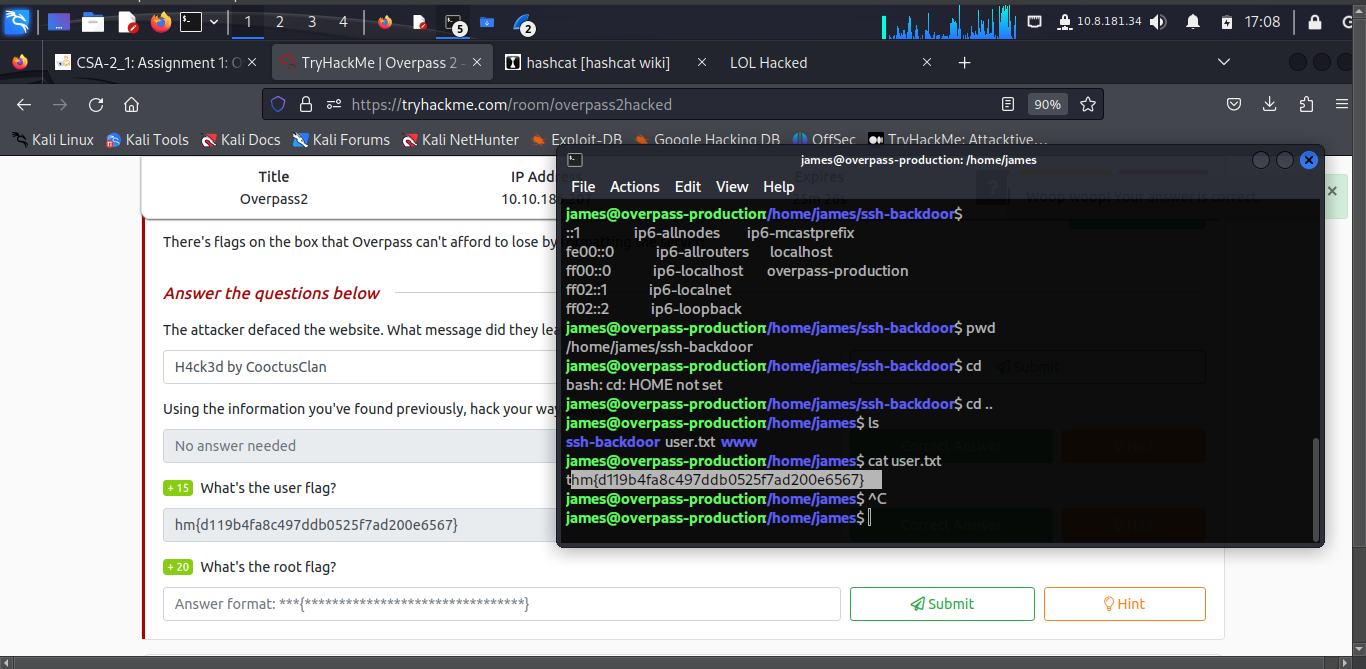
**ssh -i key.pem james@10.10.186.207 -p 2222 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+s-rsa**

This is because when using ssh from OpenSSH >= 8.8 the images use an older ssh server version.

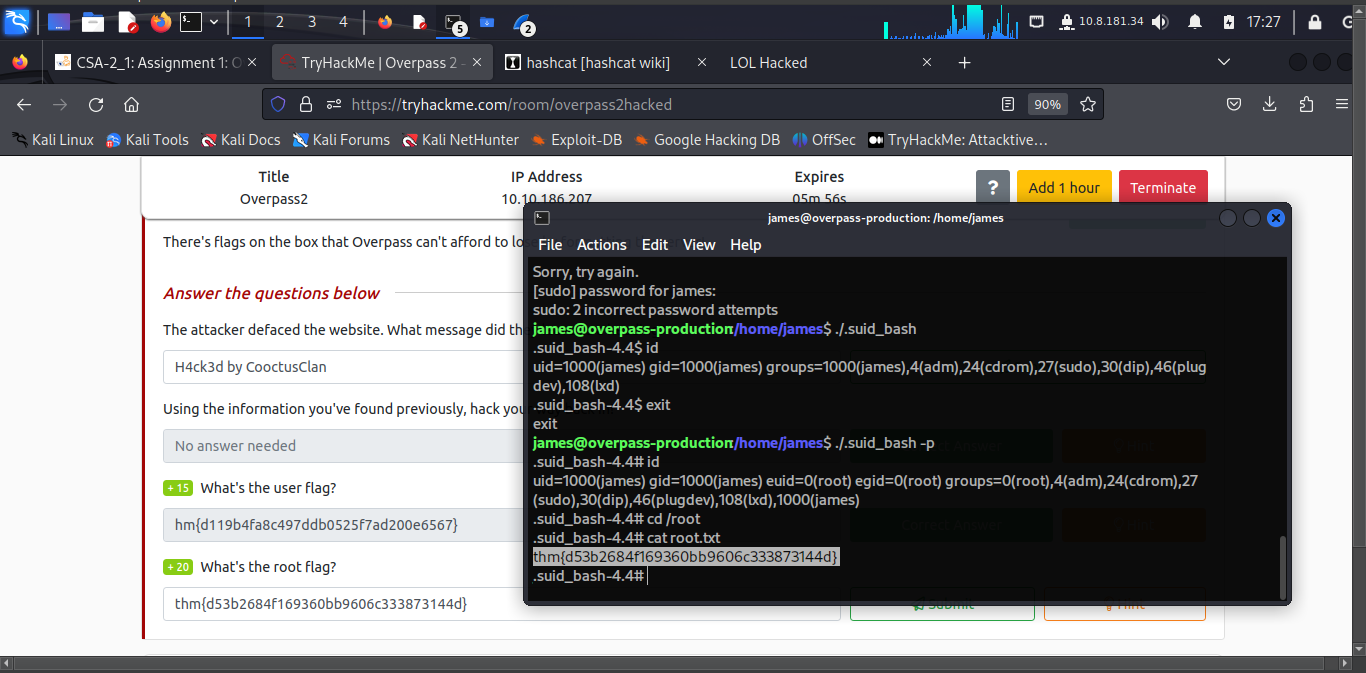


To access the file text containing the flag run: **cd ..** to move the folder step upper or outer.

The **ls** to list and view files available in the directory. Finally run **cat user.txt**

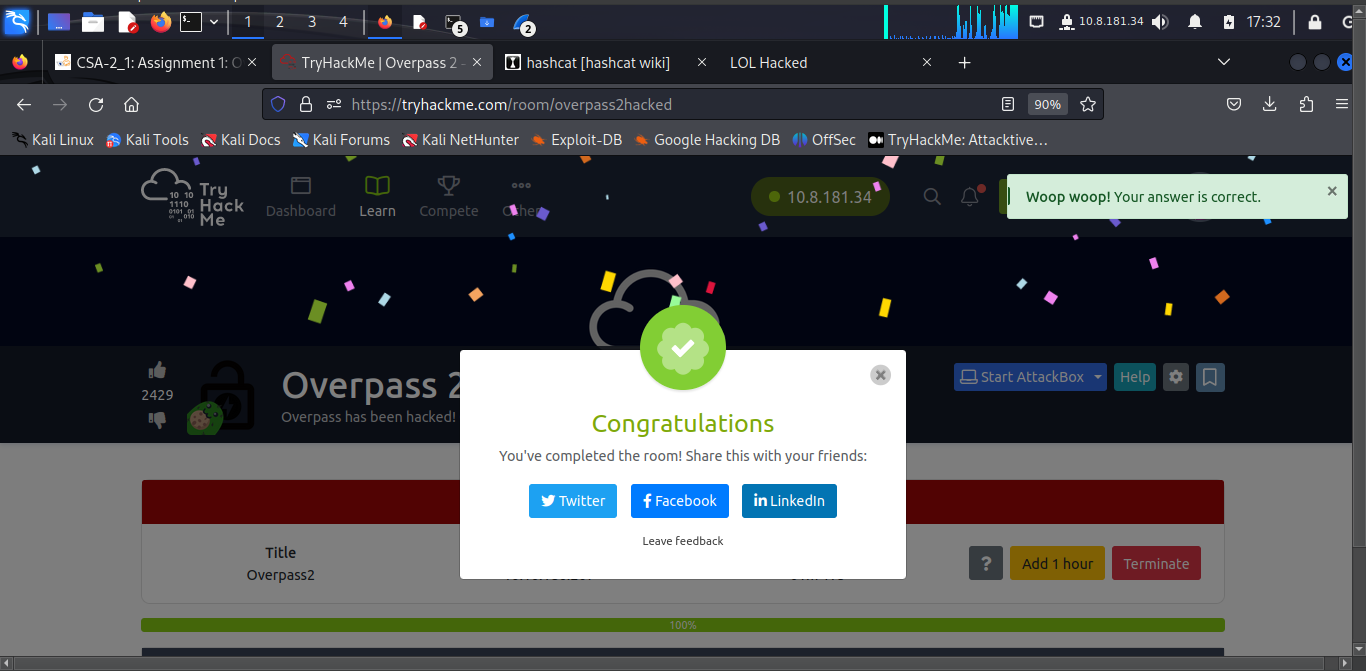


The root file flag is: **thm{d53b2684f169360bb9606c333873144d}**



**Conclusion**

In this activity I have an understanding through the walk through of diffulty in combing Linux command skills, accessing remote desktop – unix based system in this task. By knowing port numbers accessing the remote is possible as long as we have the cracked password initially hashed.



**Completion Link:** <https://tryhackme.com/room/overpass2hacked>