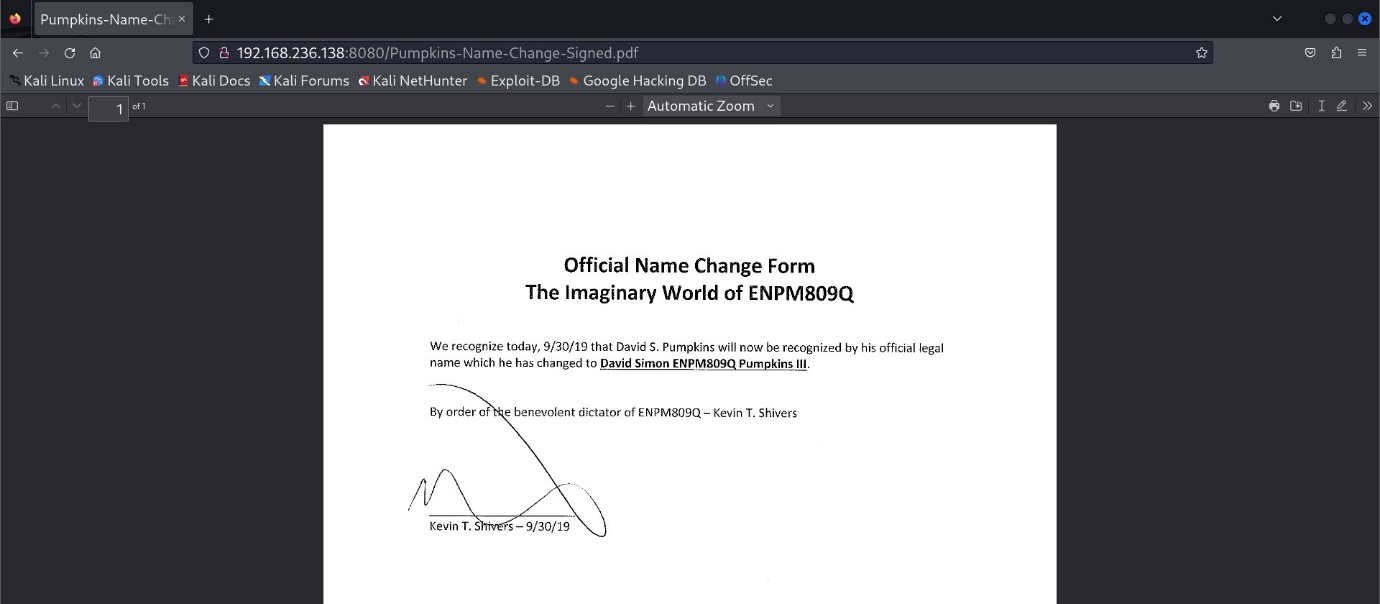
Name: Rithik Sarvesh Bharathiraja

UID: 120395246

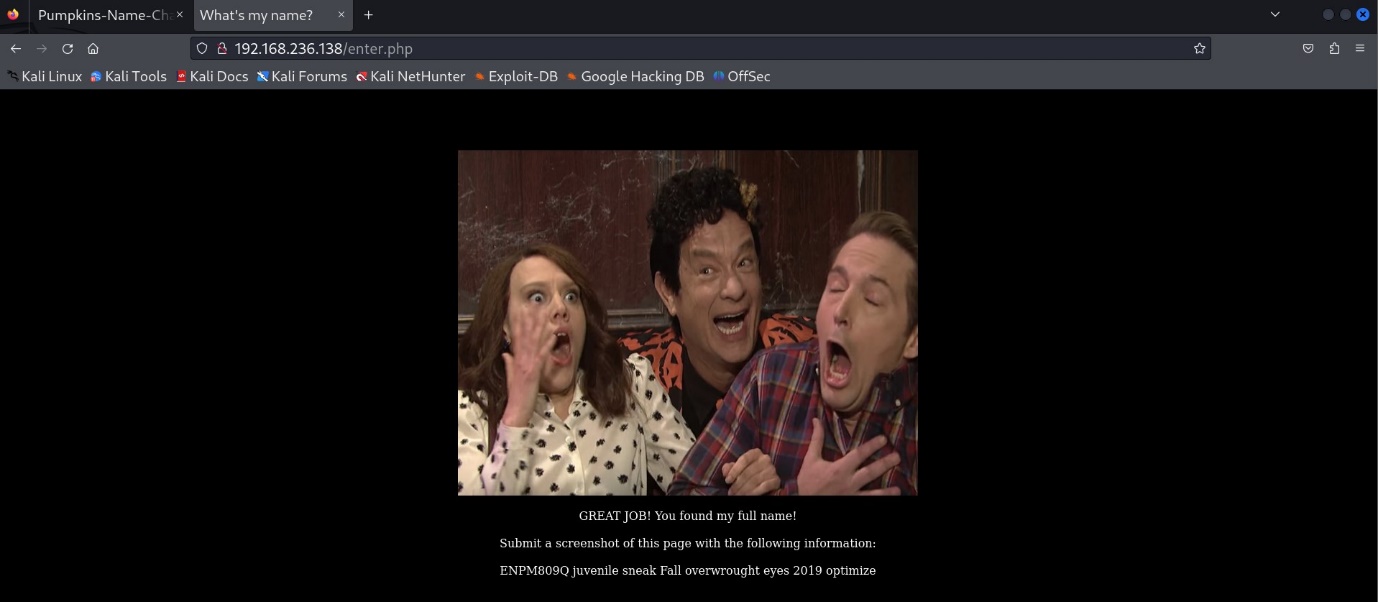
Course: ENPM634

Task: Midterm

The Final Result

To find the full name of the creator of the web app that is running on the VM. His name was “David Simon ENPM809Q Pumpkins III”  


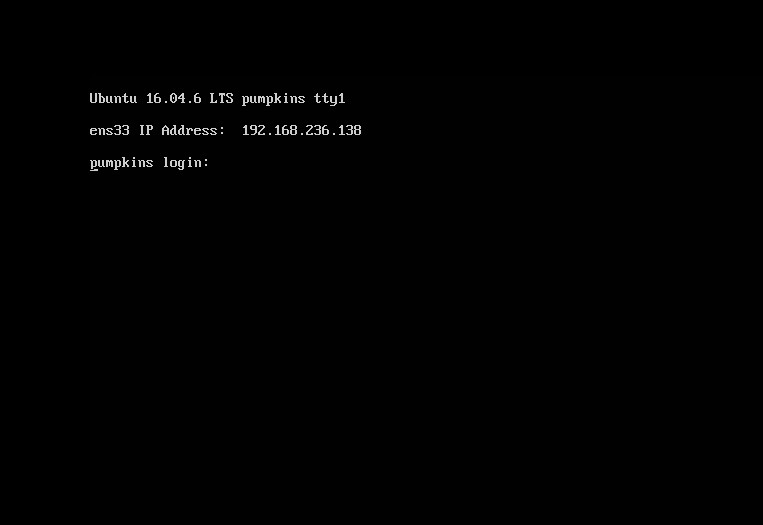
And the flag after giving the full name as the input.



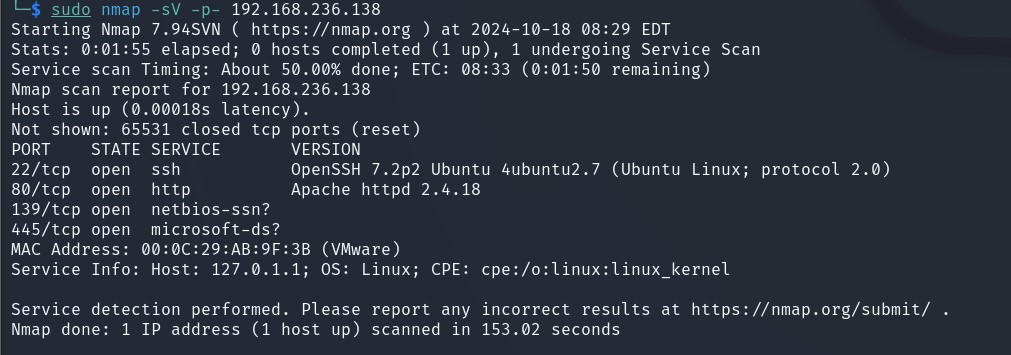
Walkthrough

1. Recon

Once the VM – Pumpkins was turned on, its IP address was displayed in the terminal.

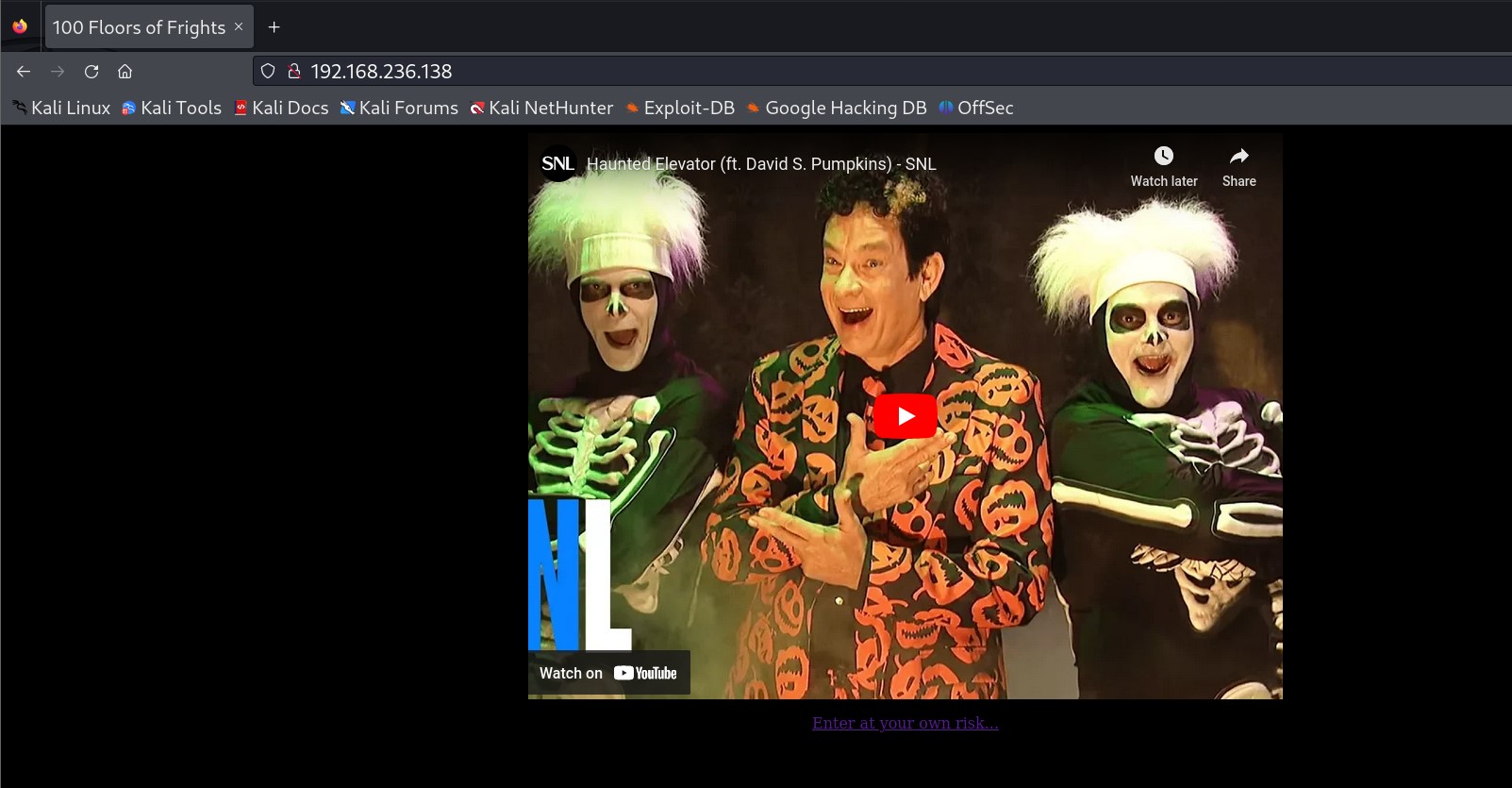


With that Nmap scan was conducted to find out the open ports.

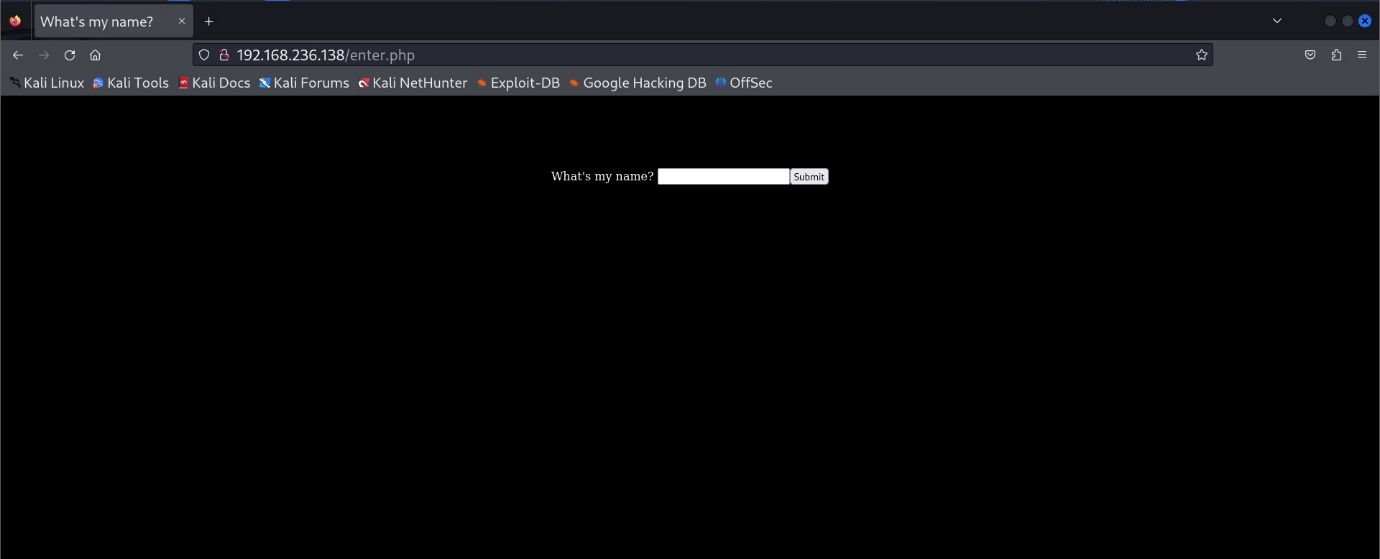


SSH service was available and it was hosting a web app in port 80 (HTTP) and SMB server too.

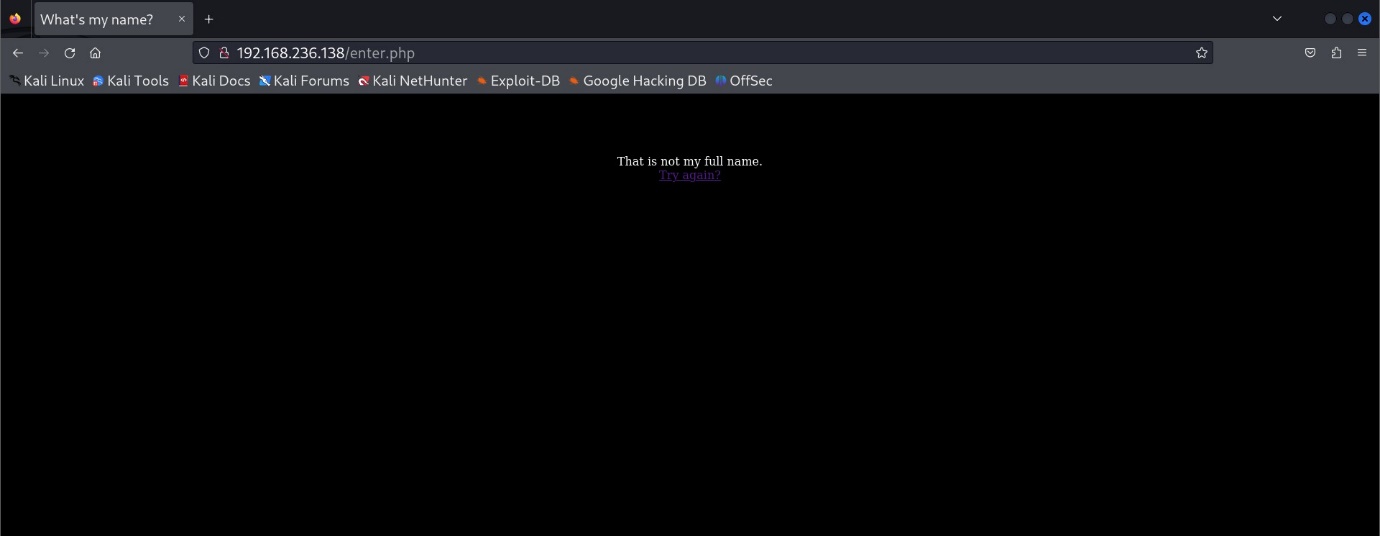
In the web app, a YouTube video was there with a link below for redirection to another page.



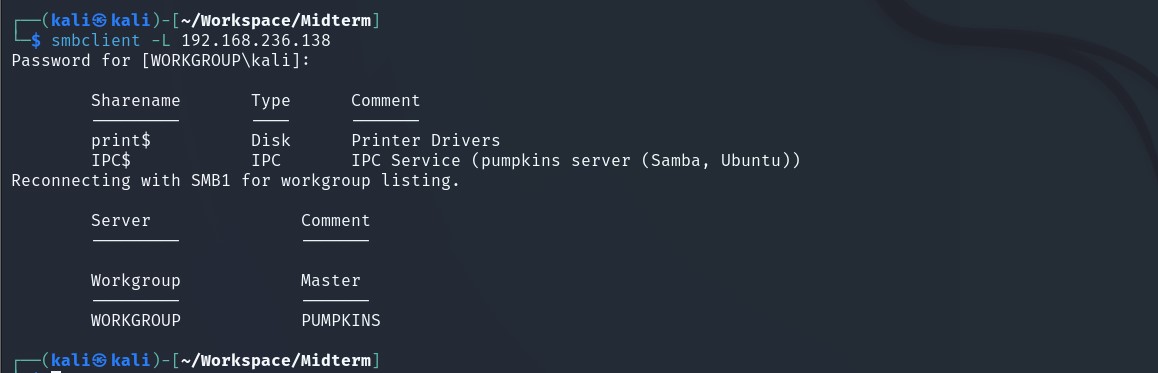
When the link was clicked, it took us to a page with an input field asking for a full name, we didn’t know.



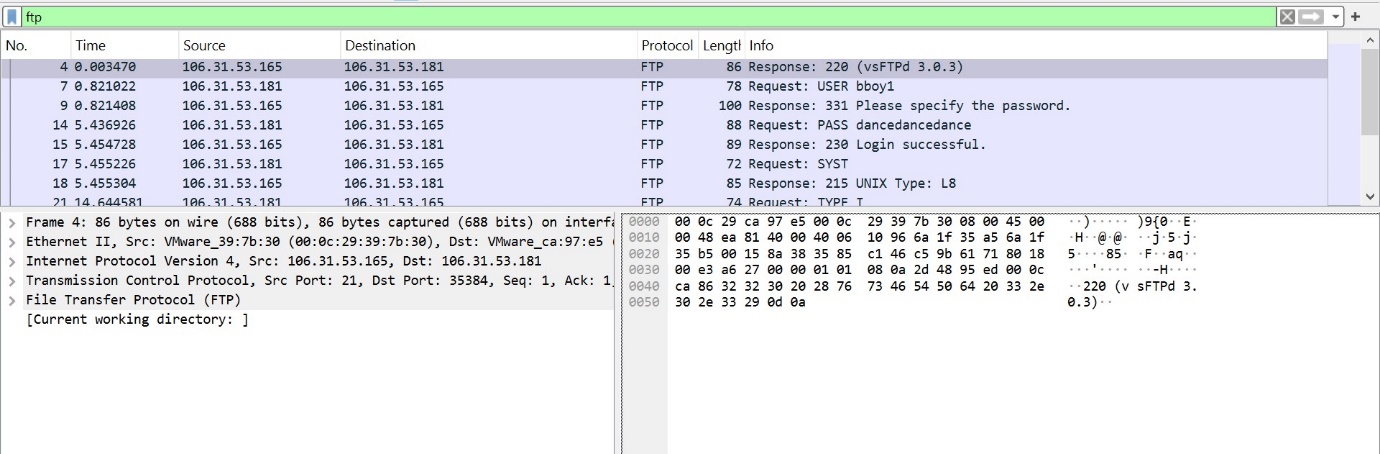
After several rounds of different SQL injection, we came to know that the web app was immune to everything. Burpsuite didn’t give us much useful information either.



So, Tried to find anything useful in SMB. But, we were left with nothing again.

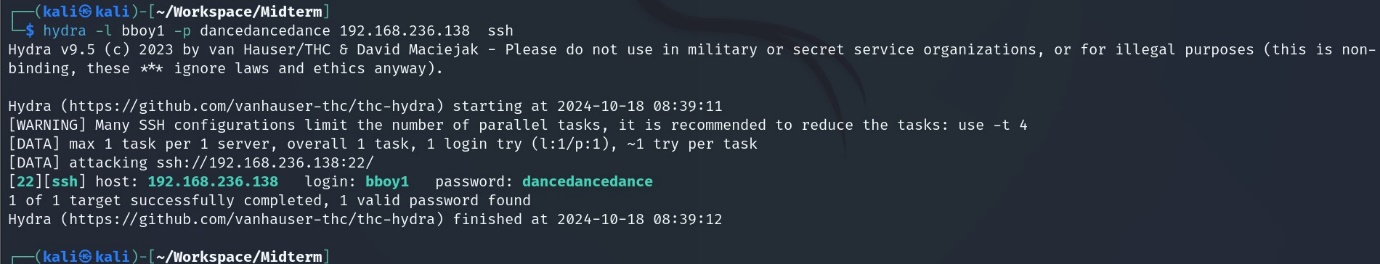


As we were looking helpless, then came our best friend, Wireshark. It was made to capture the traffic of the adapter the VM using. Bingo! It looked like our VM was trying to login in a FTP server in a different system maybe(As the IP of the source and destination were different !?). But, we got a username and a password to try on the SSH service.

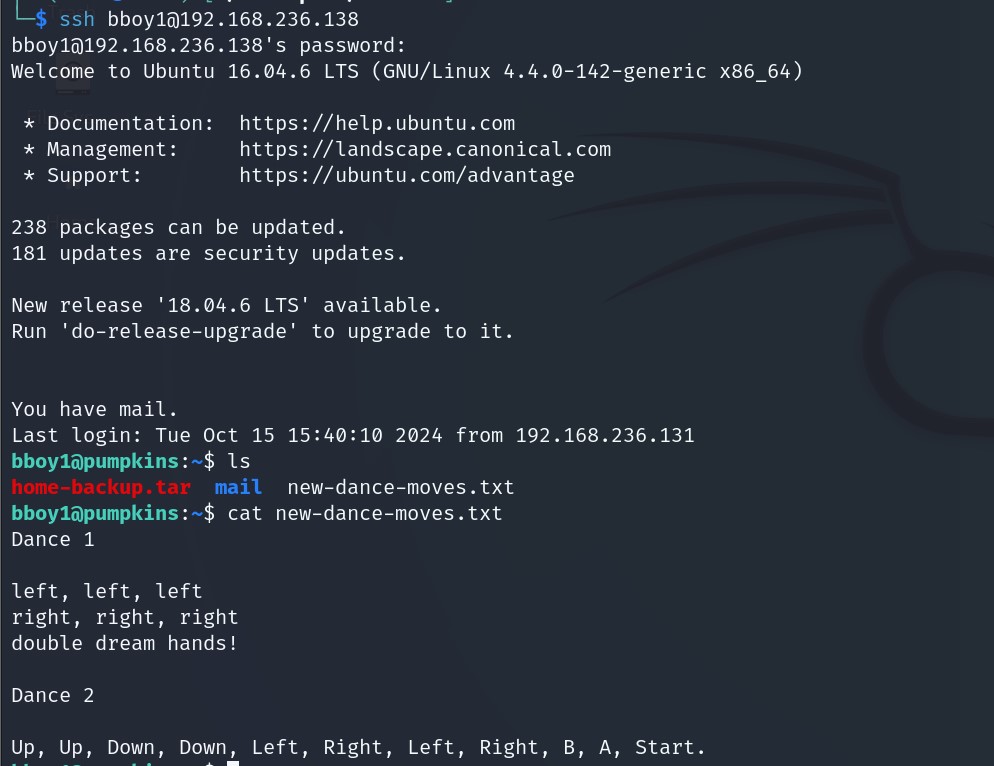


1. Enumeration

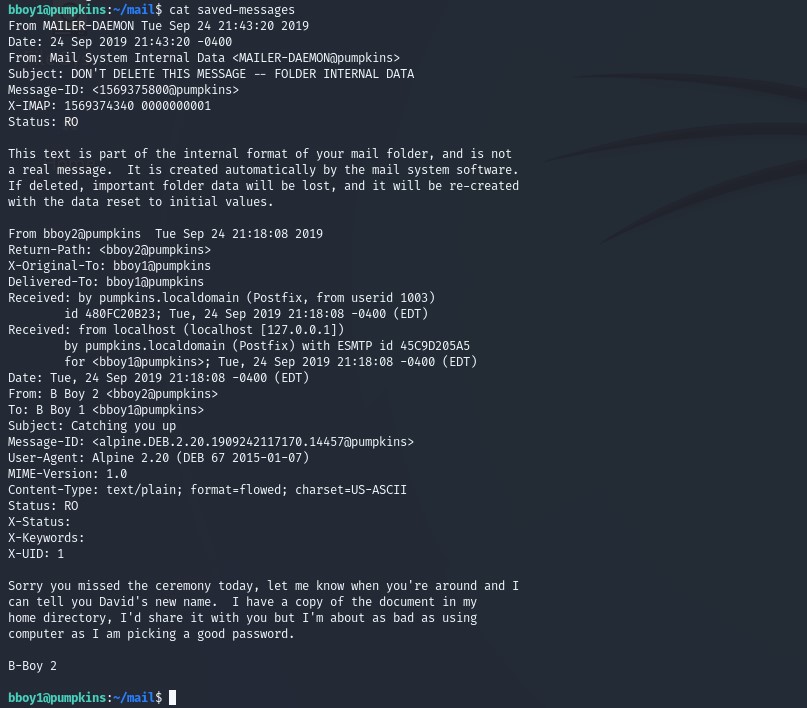
We used hydra to verify whether it was a valid credential for the SSH service. (We could have tried directly, but I love using hydra )



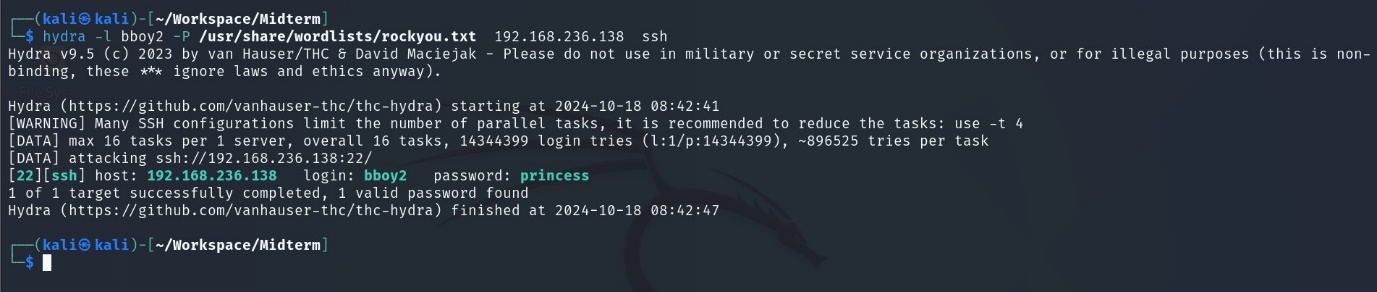
And, it was a valid credential. So, we tried to connect to the VM-pumpkins through SSH and we gained access.



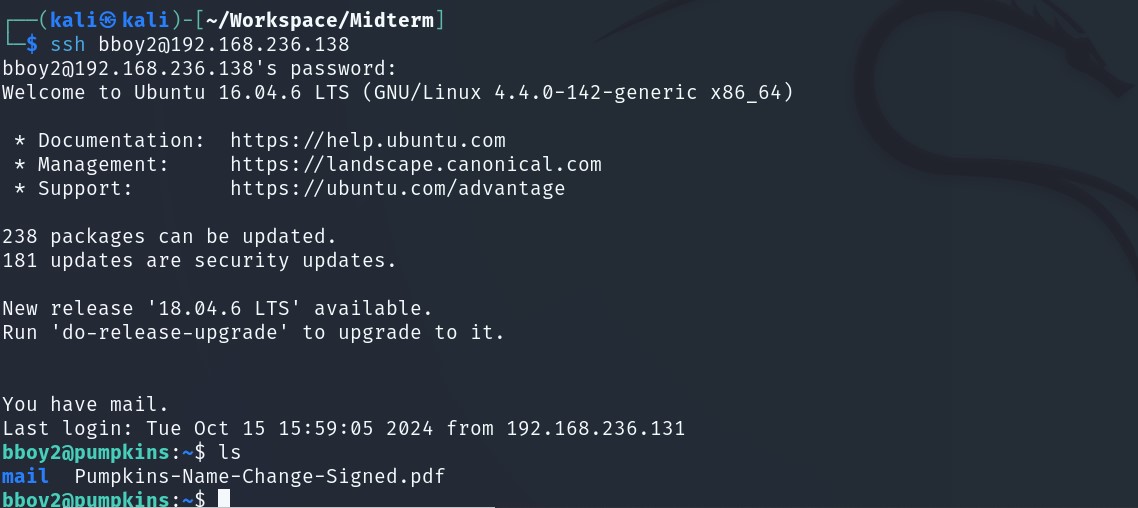
While going through the files and directories in the home directory, there was a saved mail in the ‘~/mail’ directory which turned to be helpful. It was a communication between two users – bboy1 and bboy2 (Another user? Sounds like a good day to enumerate ) and bboy2 saying that he/she had a document revealing the full name of David (David Copperfield, is that you? ) in his home directory and also mentioning that bboy2 had a password not so good. (I feel for you, bboy2)



With the collected intel from the mail, we tried hydra again to get a valid credential for the user ‘bboy2’. rockyou.txt was used to perform the dictionary attack. We came to know that bboy2 password was ‘princess’.

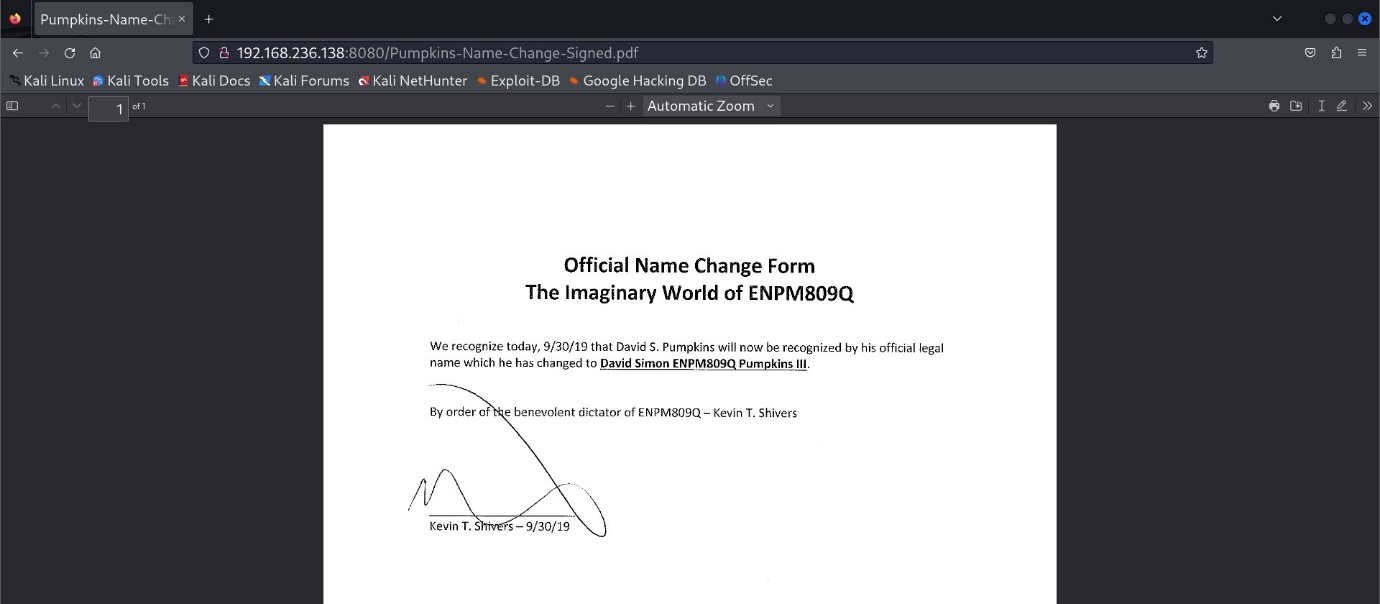


Now using the new credentials, we tried to establish the connection with the VM but as a different user and it was successful too. As a man/woman of his/her words, the file we were looking for was found in the home directory.



1. Exploit

As it was a PDF file, we hosted a python server using Python in the port 8080 (cmd: python3 -m http.server 8080) to get a look at the file. Voila! There was his name. (He might have gone through a lot with such a long name. Same problem.)



1. Profit!

After entering the full name of David, we got a picture of the Tom Hanks as the flag at the end.

