**FOWSNIFF REPORT**

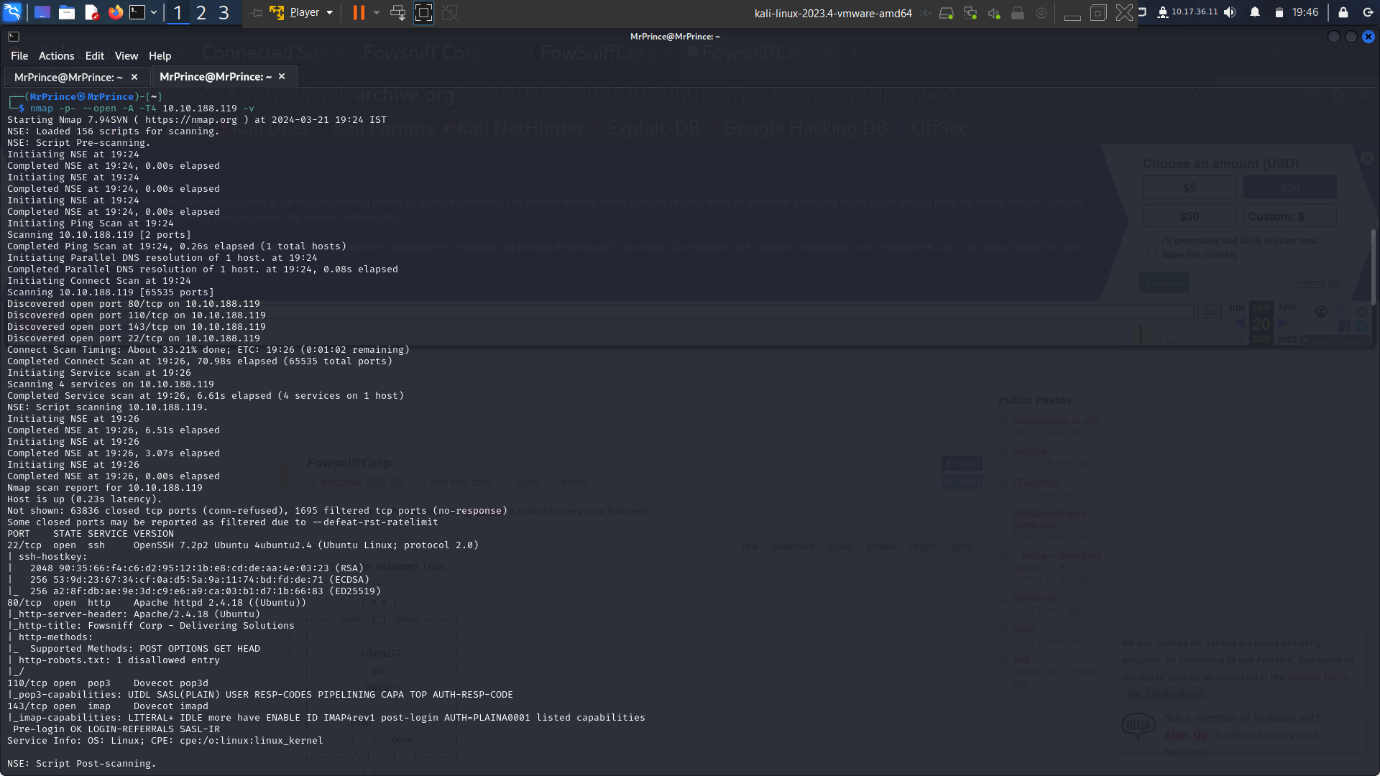
**By: Arun Kumar K (**[**arunkumark.ece2021@citchennai.net**](mailto:arunkumark.ece2021@citchennai.net)**)**

**Summary:**

This report contains the detailed steps involved in pawning a machine called “FOWSNIFF” from try hack me online platform. The main objective of this report is to record all the process done during the CTF challenge.

**Reconnaissance:**

The first thing we should do is to get started with collecting information about the target. So we used a “nmap” to find the open ports and the service running in the target machine



**Scanning:**

TARGET:

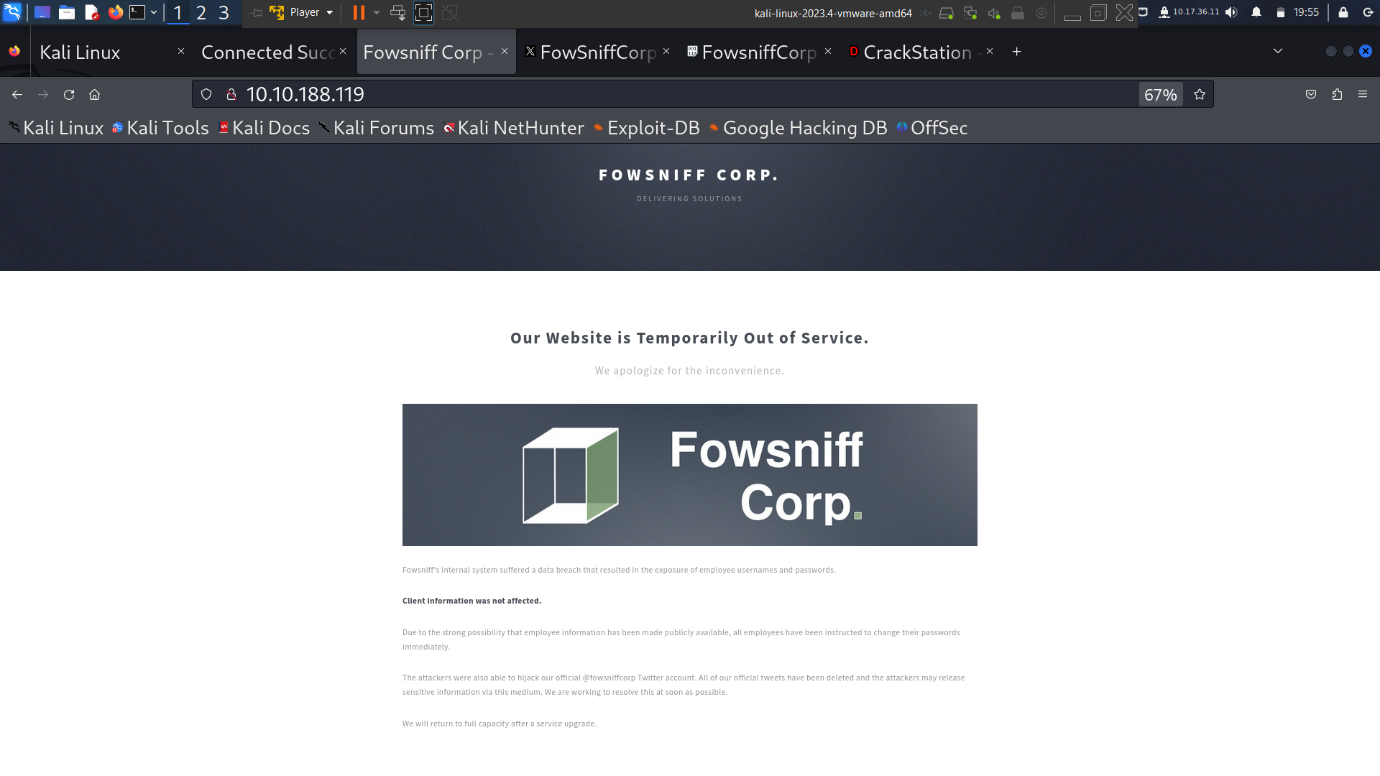
IP: 10.10.188.119

OS: LINUX

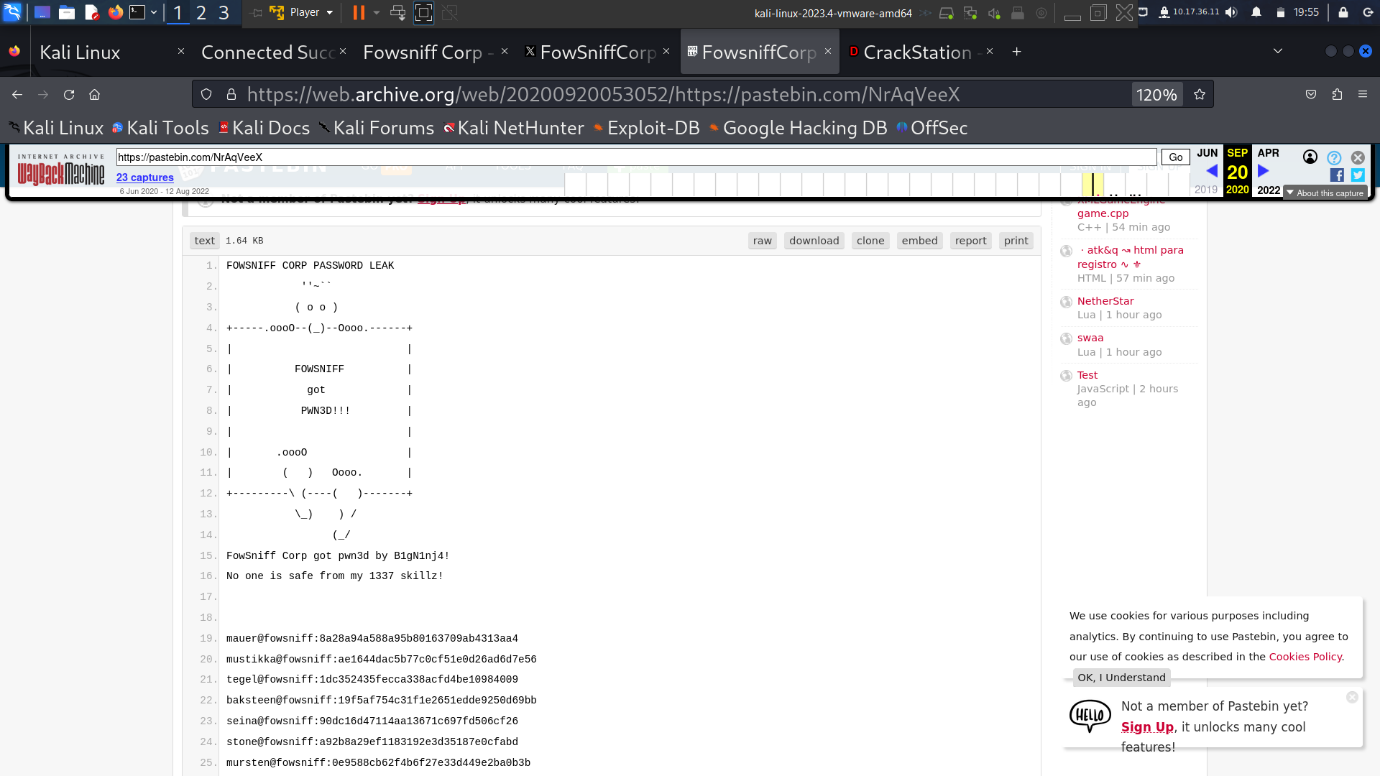
Open Ports: 22,80,110,143

From the initial nmap scan we found that the ports 22,80,110,143 are open and services like pop3, imap and a apache2 service is also running in the target machine. IMAP and POP3 areemail protocols used to retrieve emails from a remote server to a local email client. As we have found that the target machine runs an apache2 sever we can visit the website form the the browser

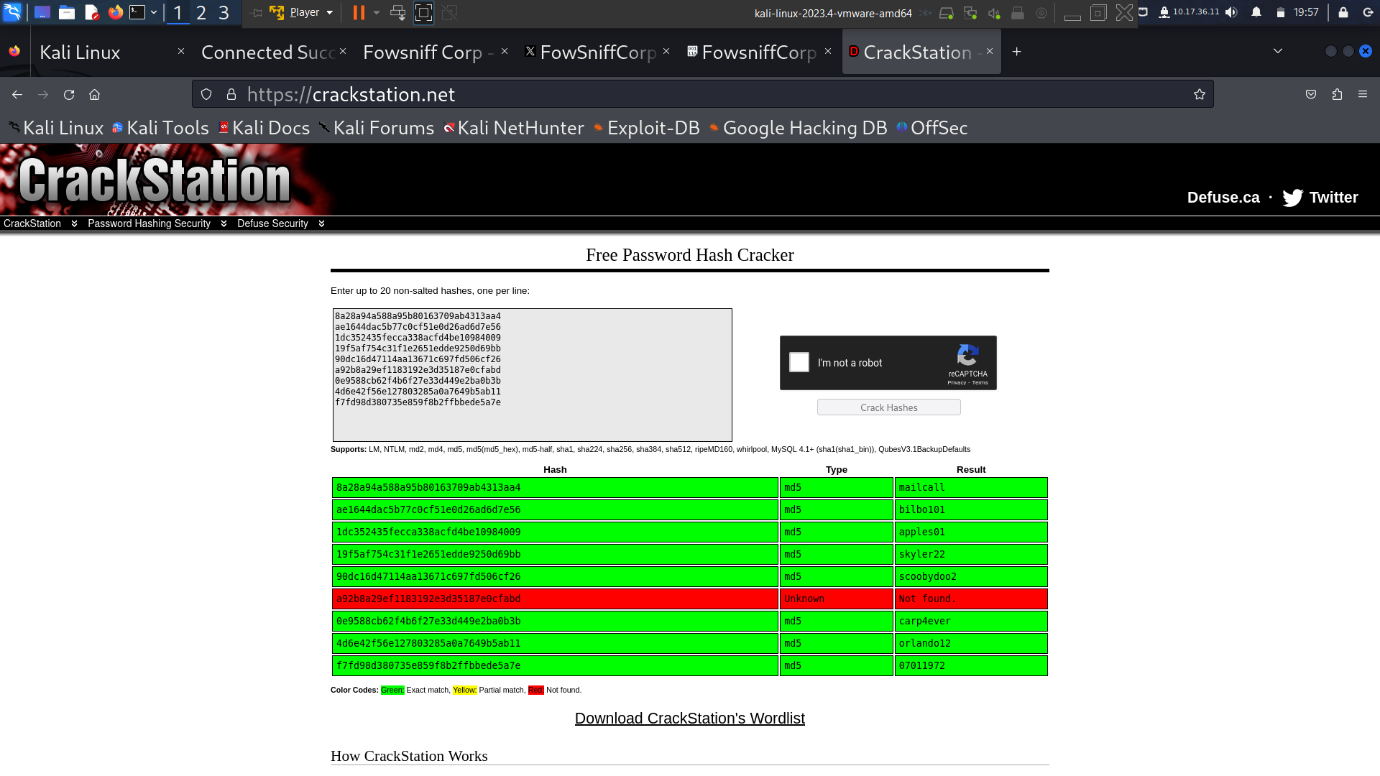
After Visiting the website it seems like the website is currently down due to an cyber attack happened some time ago. And it was also mentioned that the previous hacker has already gained the usernames and password of all the employees and their twitter account is also got hacked

Upon visiting the said twitter account we found that the hacker had already posted the usernames along with the their password hash in a Pastebin. It is mentioned that that the hashes are md5 encrypted

So we used the “Crack Station” website to decrypt the hashes and stored it in a separate files and usernames in separate files

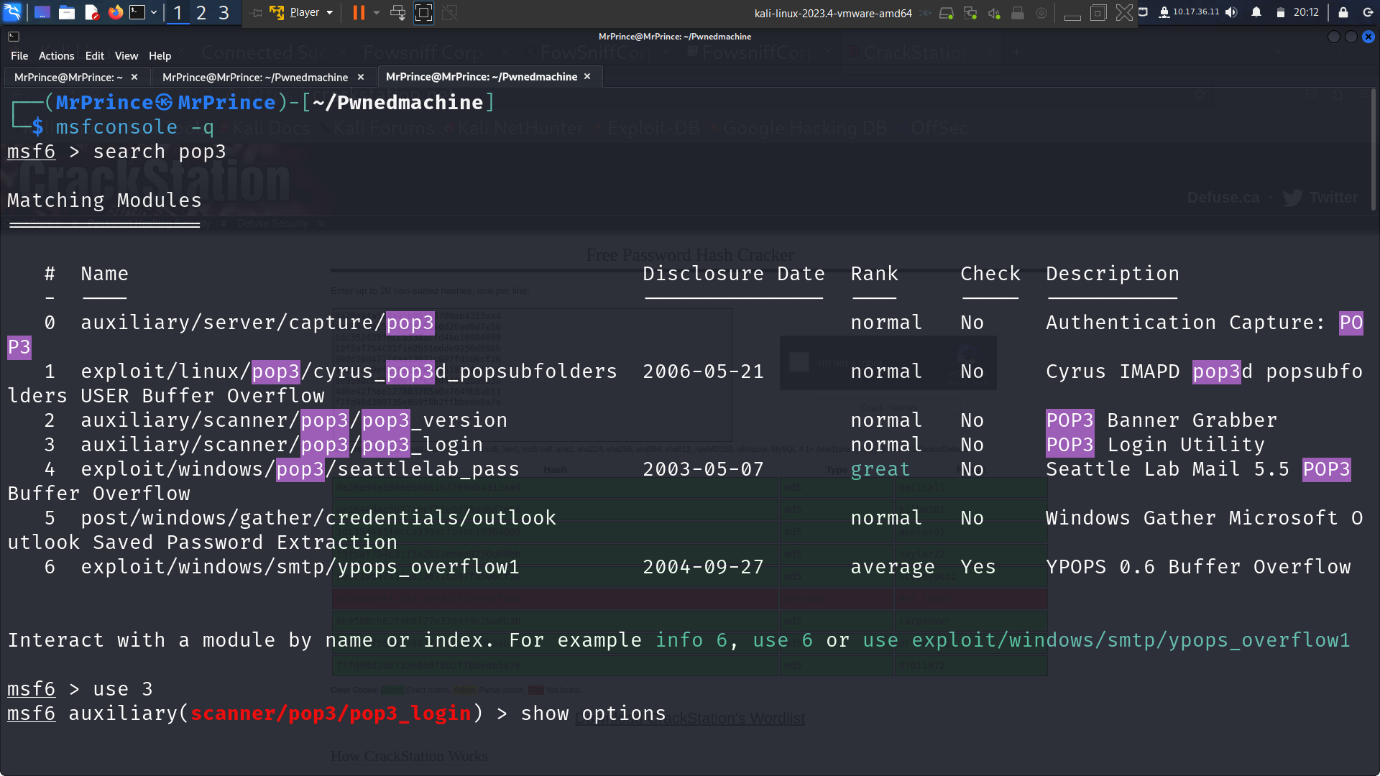


Since an attack is already happened it is also possible that the employees have already changed their passwords or the admin may already blocked the login from the leaked usernames and password to their server so we need to exploit this login credintials in a short span of time



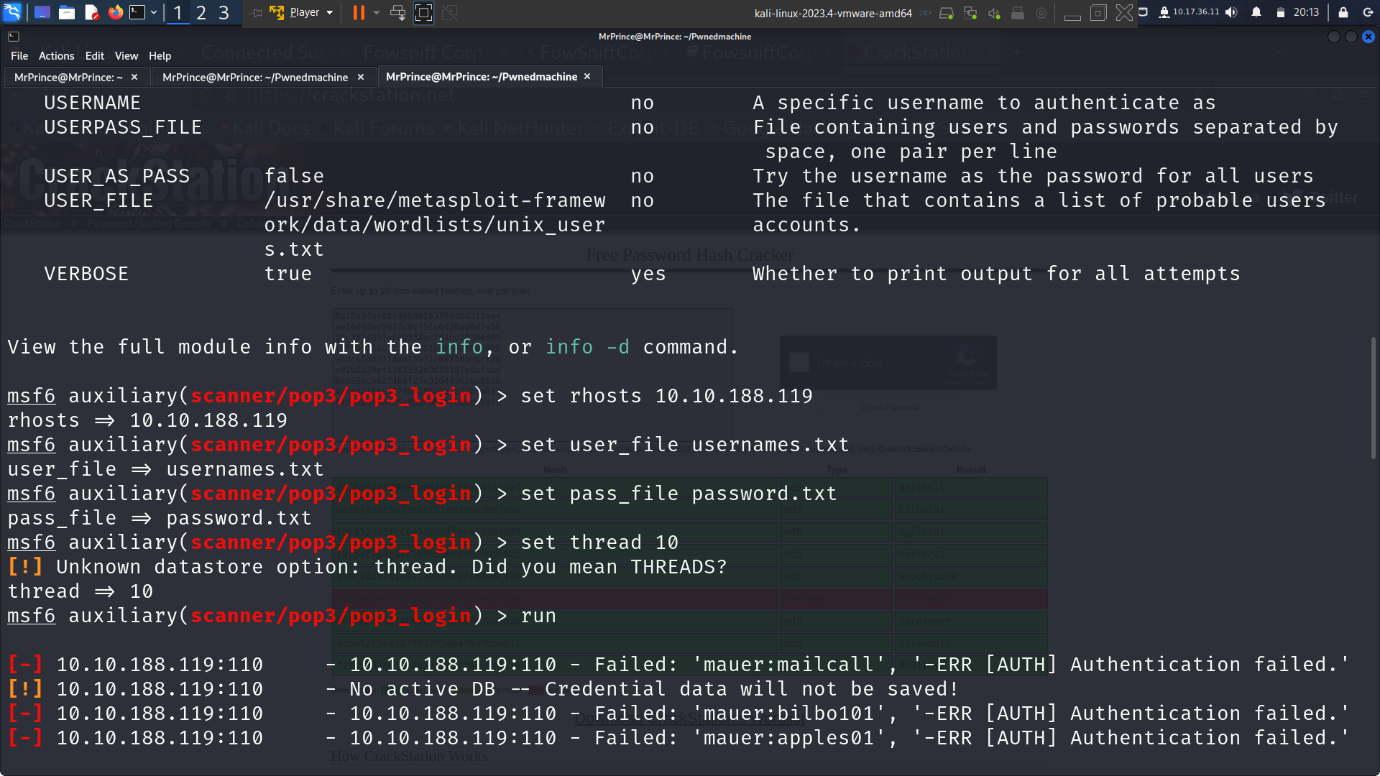
**GAINING ACCESS:**

So we decided to the metsploit to see if there are any existing vulnerabilities available for the services running in the target machine

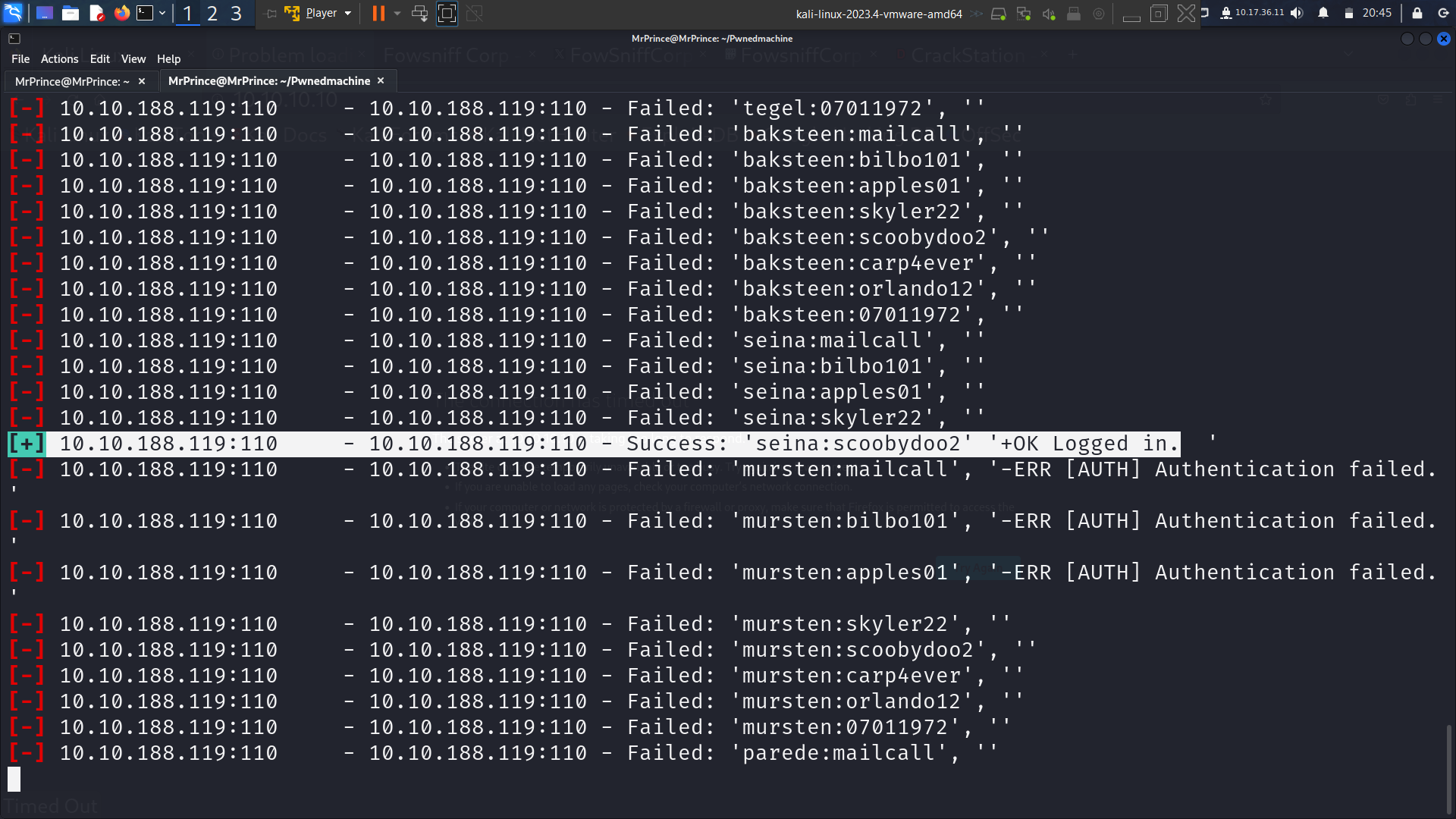


The id of the exploit we are going to use is 3. We are going to use the login credentials we have in our hand to try to verify if it is possible to login to the mail service with the username and password we have in our hands

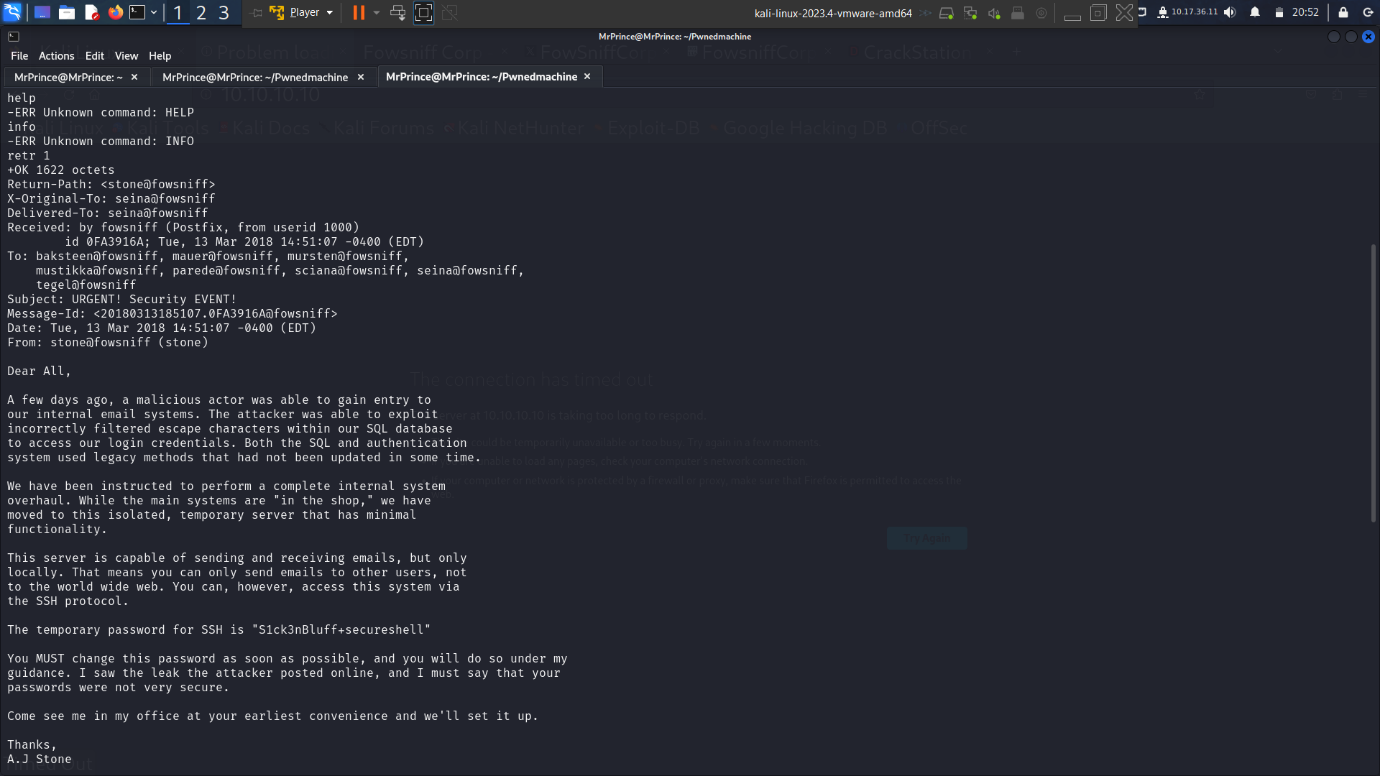
We set the “Rhosts” i.e the remote host as the target machine ip and used the respective files names for the usernames and password we had previously saved

We found that the pop3 service running in the target machine has a vulnerability for login so we can try to exploit this vulnerability with the login credintials we have from twitter

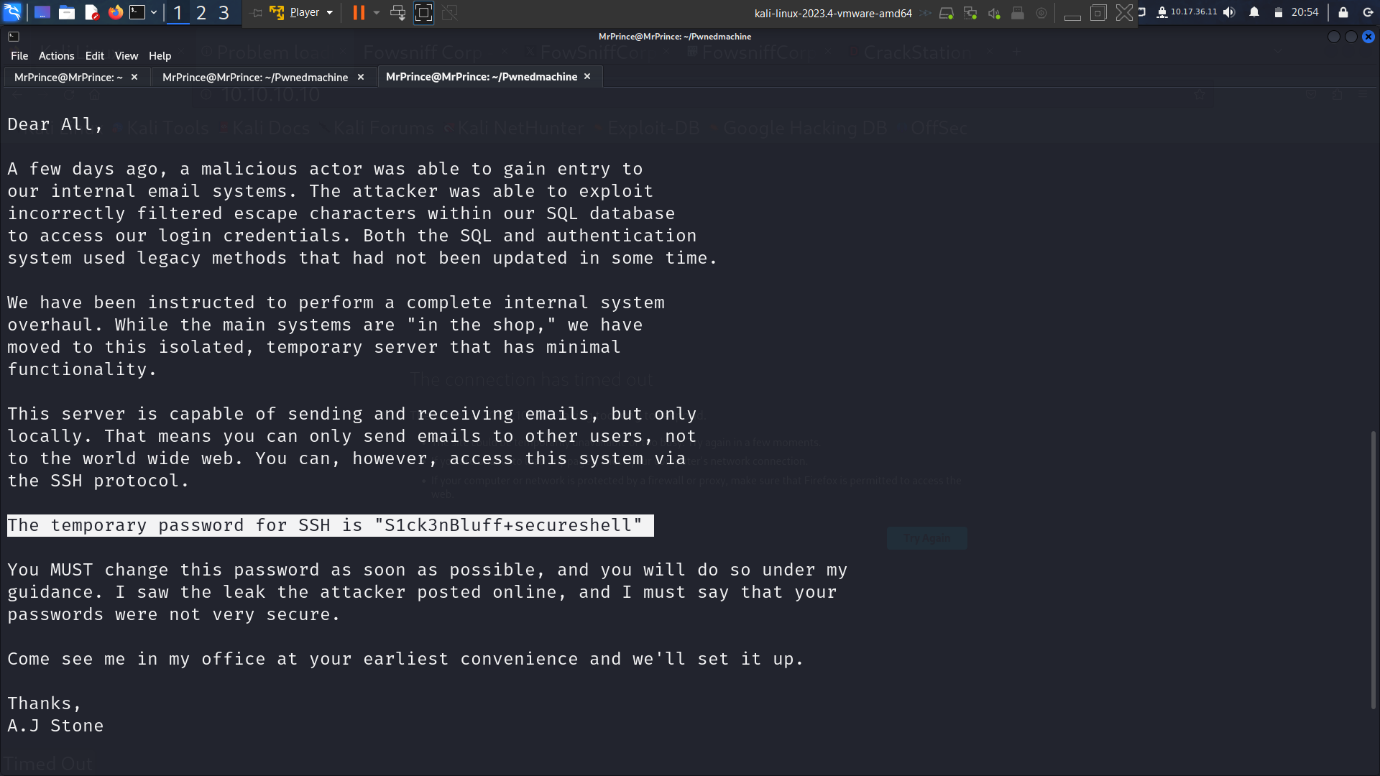
After multiple attempts we have a successful login message



With the correct username and password we successfully login to the mail service and found that there is a temperory ssh login to send mails to other users and we obtaind the username and password from the two mails available in the server



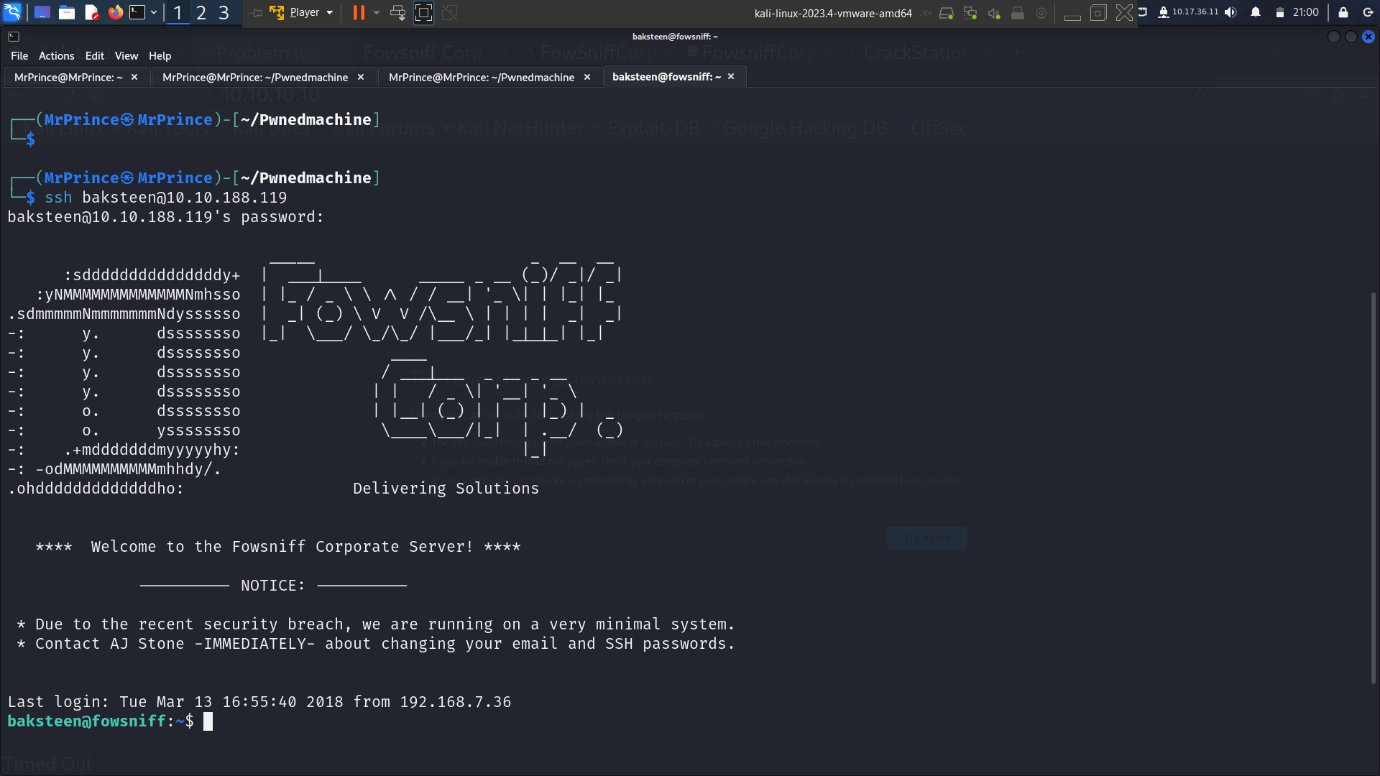
And try to connect to the ssh with the username and password we just obtained



Since it is a temprory service it may be closed any time so we need to establish our own connection with a reverse shell if possible

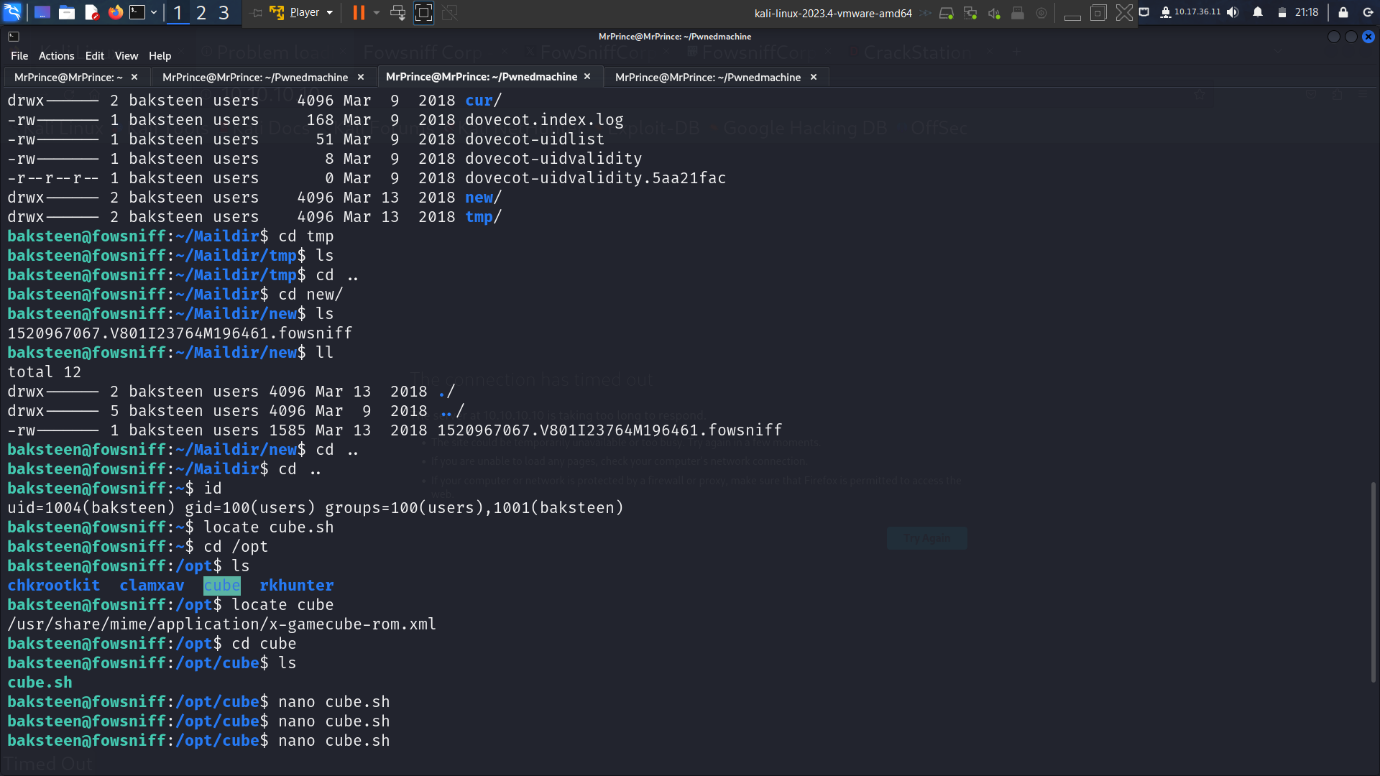
After login to the target system we got a unstable shell so we used a python script to upgrade out shell to stable terminal

Next we need to find a excutable file so that we can add our reverse shell script in it. Since our user does not have any root access privalage we need find a file that is excutable by the root user

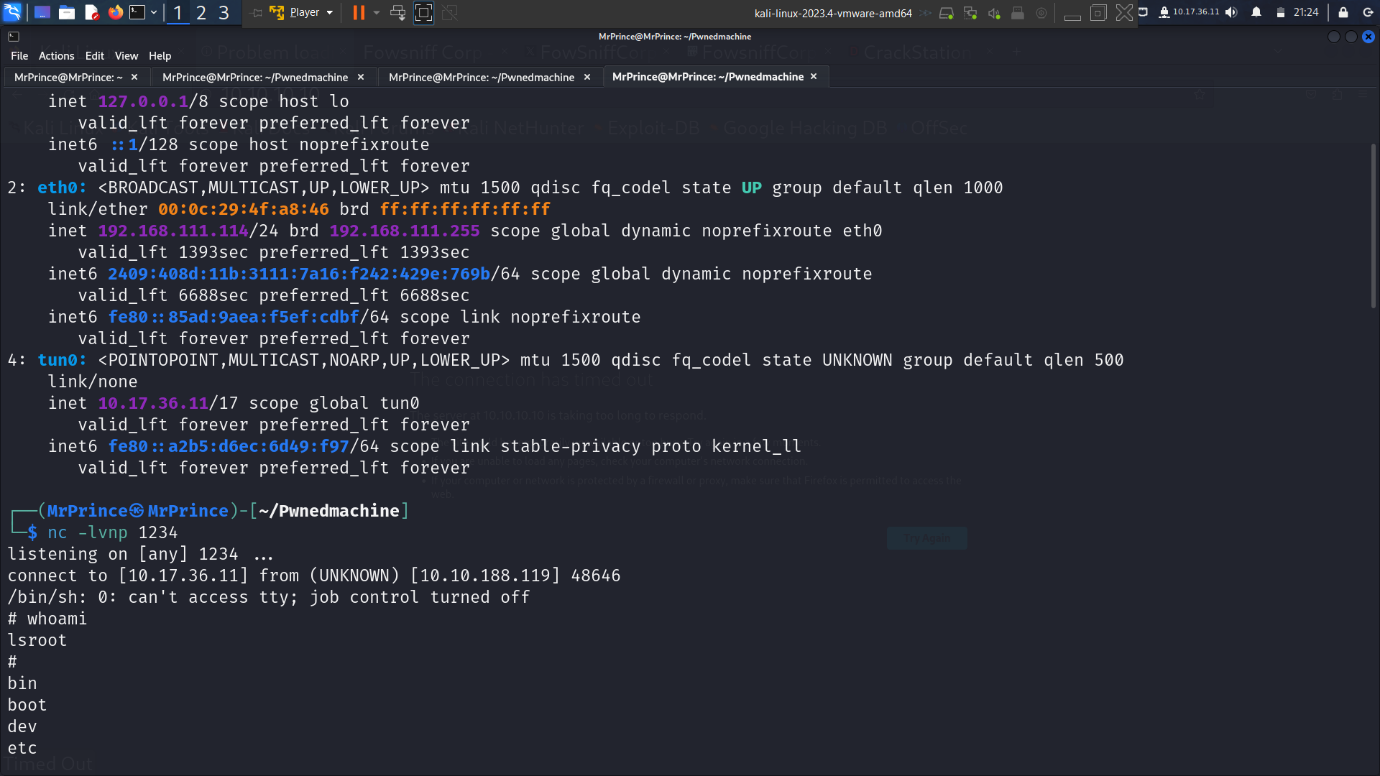


After login we see the company logo displayed automatically. Since it is displayed in the terminal it must by present in the system

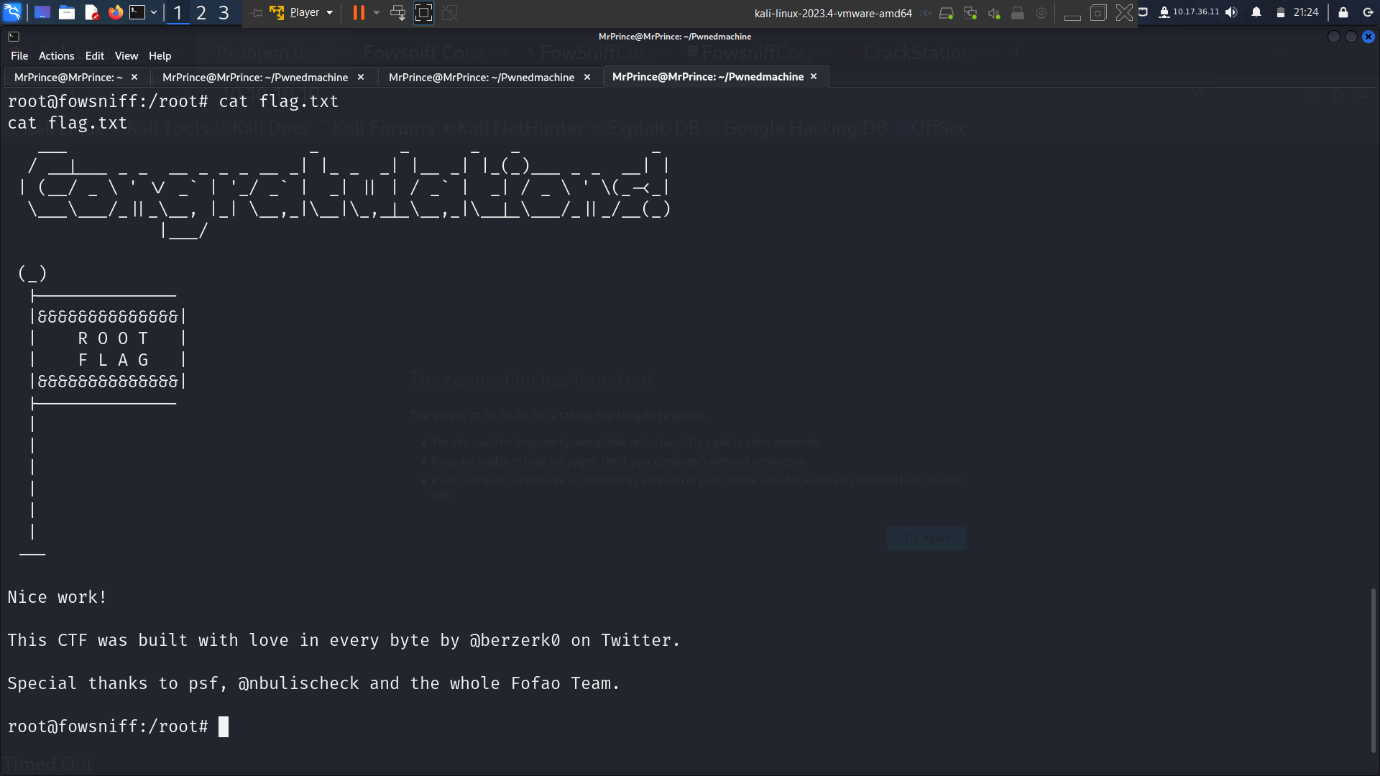
After some searching we found that file called “cube.sh”. we uploaded out reverse shell in it and logout form the server



After logging out we set up a listener in a terminal and try to login to the ssh again to trigger the file to gain the reverse shell



We gained the root access for the target machine and we started searching for the flag



Finally we were able to capture the flag which was located at the root directory

**RESULT:**

This exercise helped me gain hands-on experience in defensive security