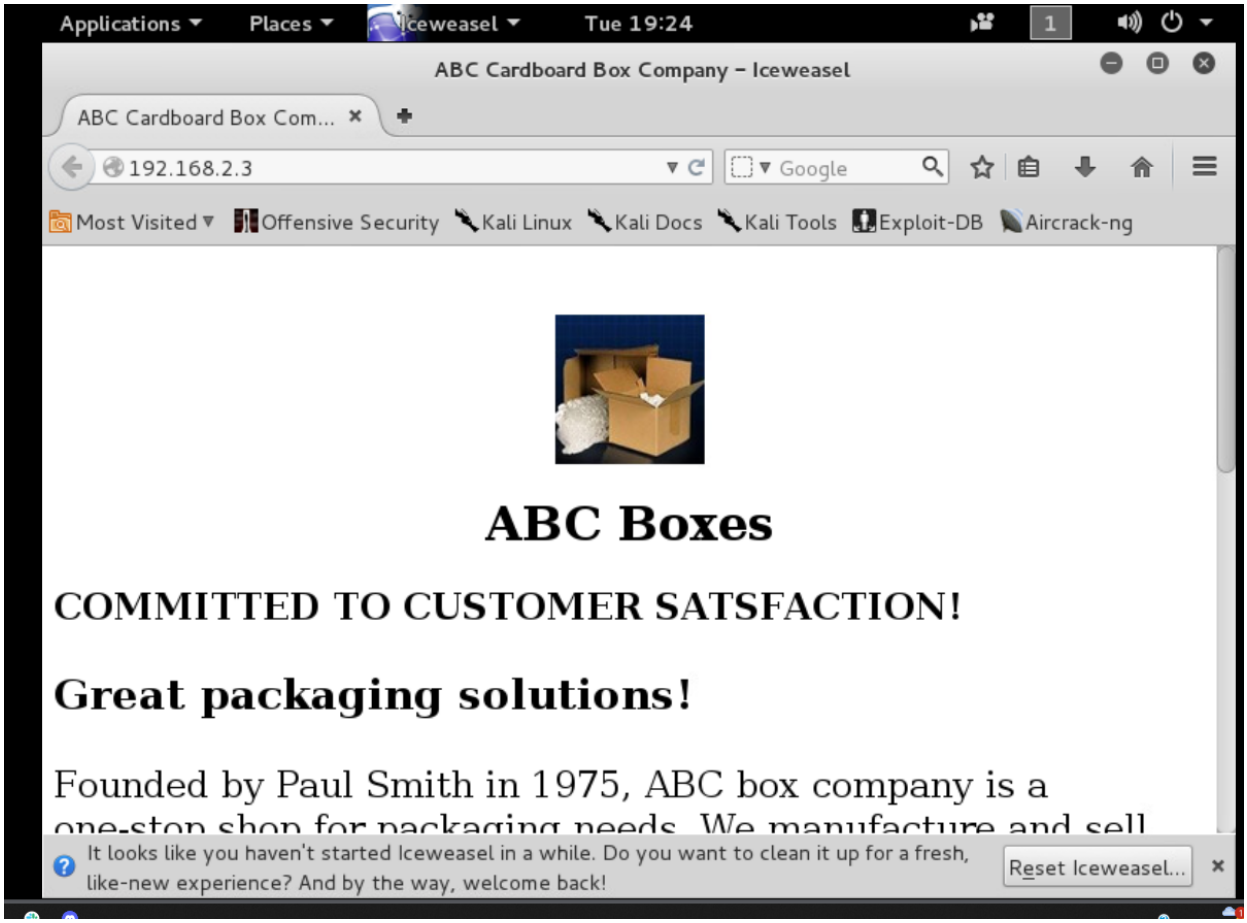
1. I started this mini pentest with an nmap scan using the command: *sudo nmap -oN nmap_scan_priv_net 192.168.2.0/24*

```
root@kali2:~# cat nmap_scan_priv_net
# Nmap 6.49BETA4 scan initiated Tue Oct 17 19:05:48 2023 as: nmap -oN nmap_scan_priv_ne
t 192.168.2.0/24
Nmap scan report for 192.168.2.3
Host is up (0.00024s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:B0:75:AD (VMware)

Nmap scan report for 192.168.2.2
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.2.2 are closed

# Nmap done at Tue Oct 17 19:06:23 2023 -- 256 IP addresses (2 hosts up) scanned in 34.
95 seconds
root@kali2:~#
```

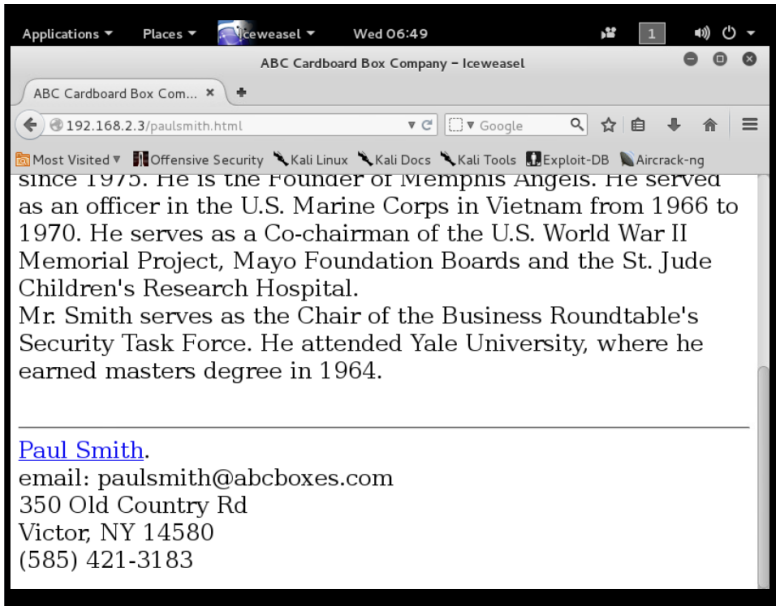
2. Once I got the machine with the IP 192.168.2.3 and its service, I chose to edit the /etc/hosts file to have the IP address point to the word target to make it easy for myself and not type the IP address over and over again.

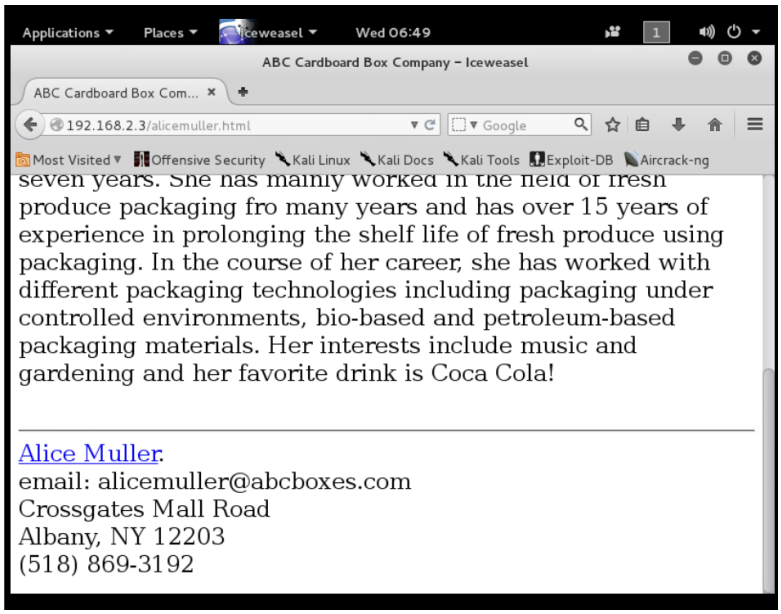
```
Applications  Places  Terminal  Wed 07:01
                                root@kali2: ~
File  Edit  View  Search  Terminal  Help
root@kali2:~# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali2

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.2.3   target
root@kali2:~#
```

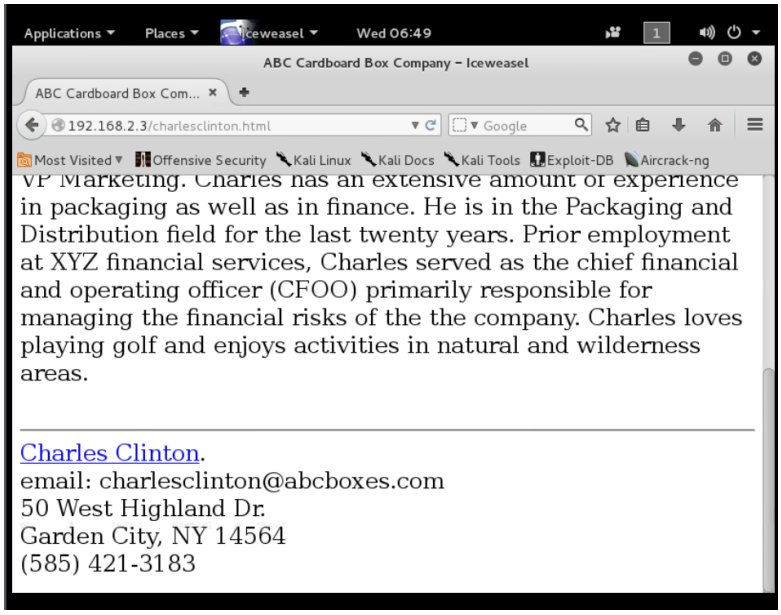
3. This is the website on the machine in port 80

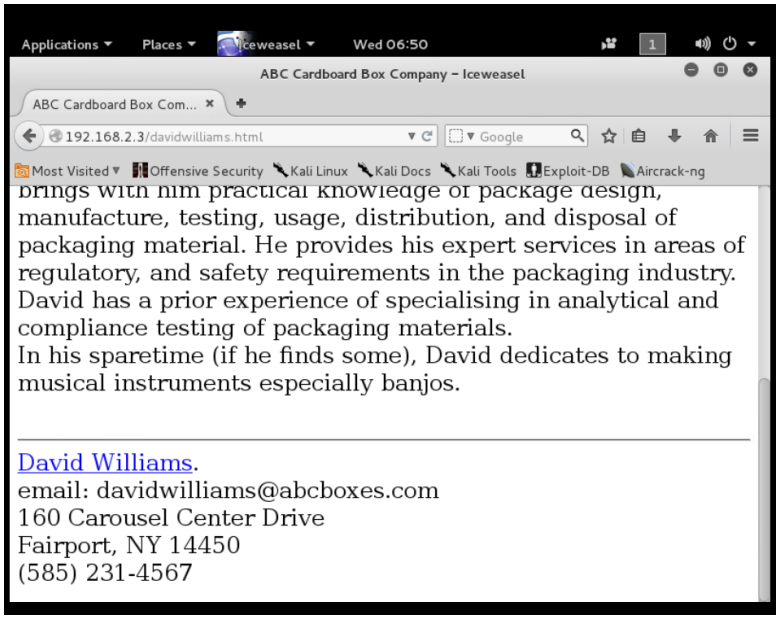


4. I got the username by doing a little OSINT in the people section of the website. I went through each of their bio and got the username from their email address and put them in users.txt file.

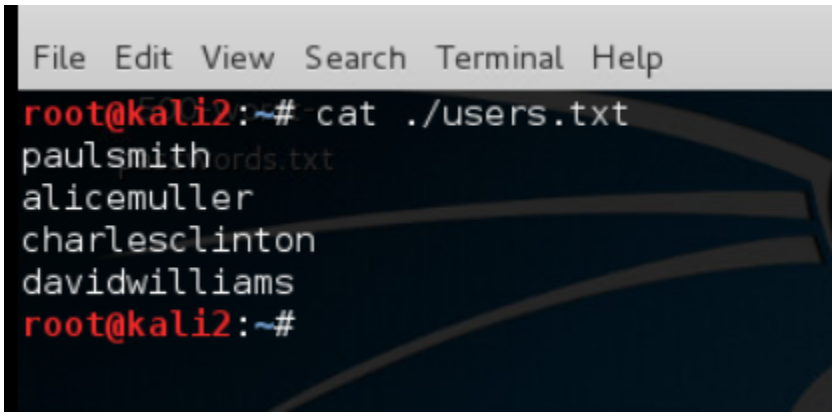

Applications
Places
Iceweasel
Wed 06:49
ABC Cardboard Box Company – Iceweasel
ABC Cardboard Box Com...
192.168.2.3/paulsmith.html
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
since 1975. He is the Founder of Memphis Angels. He served as an officer in the U.S. Marine Corps in Vietnam from 1966 to 1970. He serves as a Co-chairman of the U.S. World War II Memorial Project, Mayo Foundation Boards and the St. Jude Children's Research Hospital.
Mr. Smith serves as the Chair of the Business Roundtable's Security Task Force. He attended Yale University, where he earned masters degree in 1964.
Paul Smith.
email: paulsmith@abcboxes.com
350 Old Country Rd
Victor, NY 14580
(585) 421-3183


Applications
Places
Iceweasel
Wed 06:49
ABC Cardboard Box Company – Iceweasel
ABC Cardboard Box Com...
192.168.2.3/alicemuller.html
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
seven years. She has mainly worked in the field of fresh produce packaging fro many years and has over 15 years of experience in prolonging the shelf life of fresh produce using packaging. In the course of her career, she has worked with different packaging technologies including packaging under controlled environments, bio-based and petroleum-based packaging materials. Her interests include music and gardening and her favorite drink is Coca Cola!
Alice Muller.
email: alicemuller@abcboxes.com
Crossgates Mall Road
Albany, NY 12203
(518) 869-3192

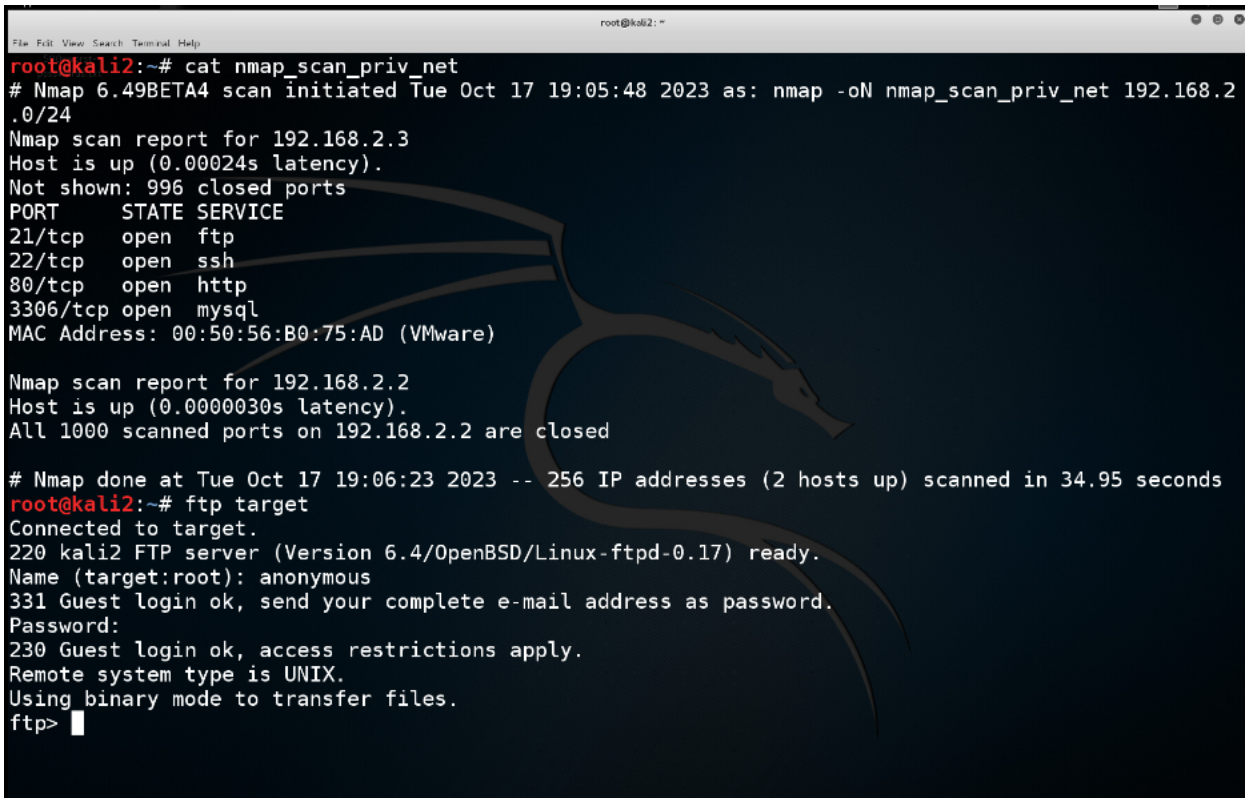




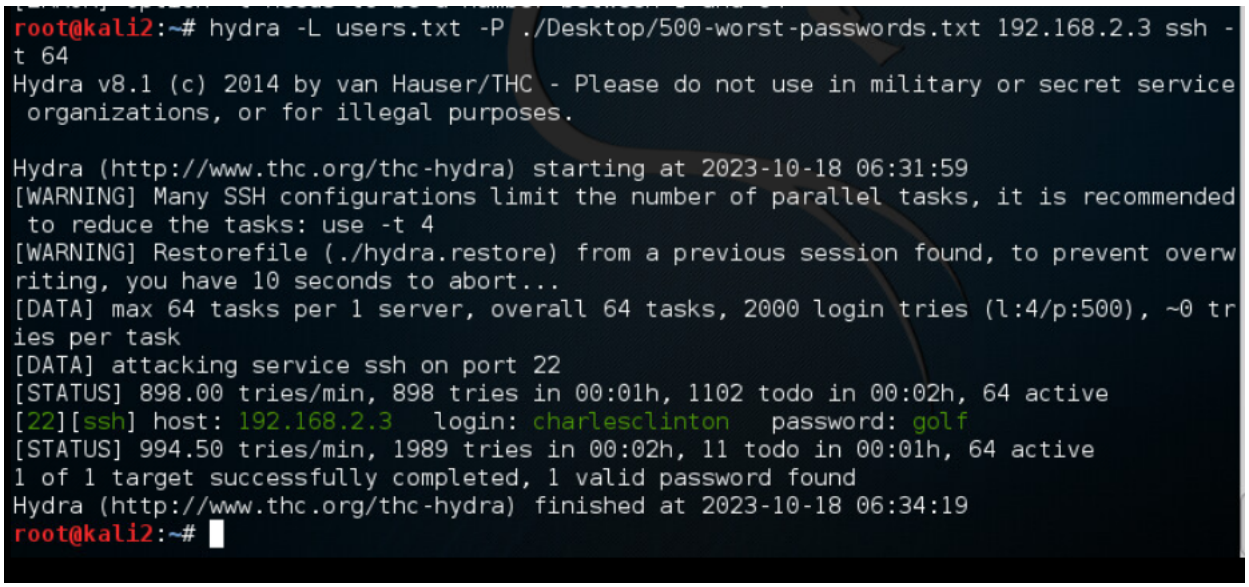
The users are



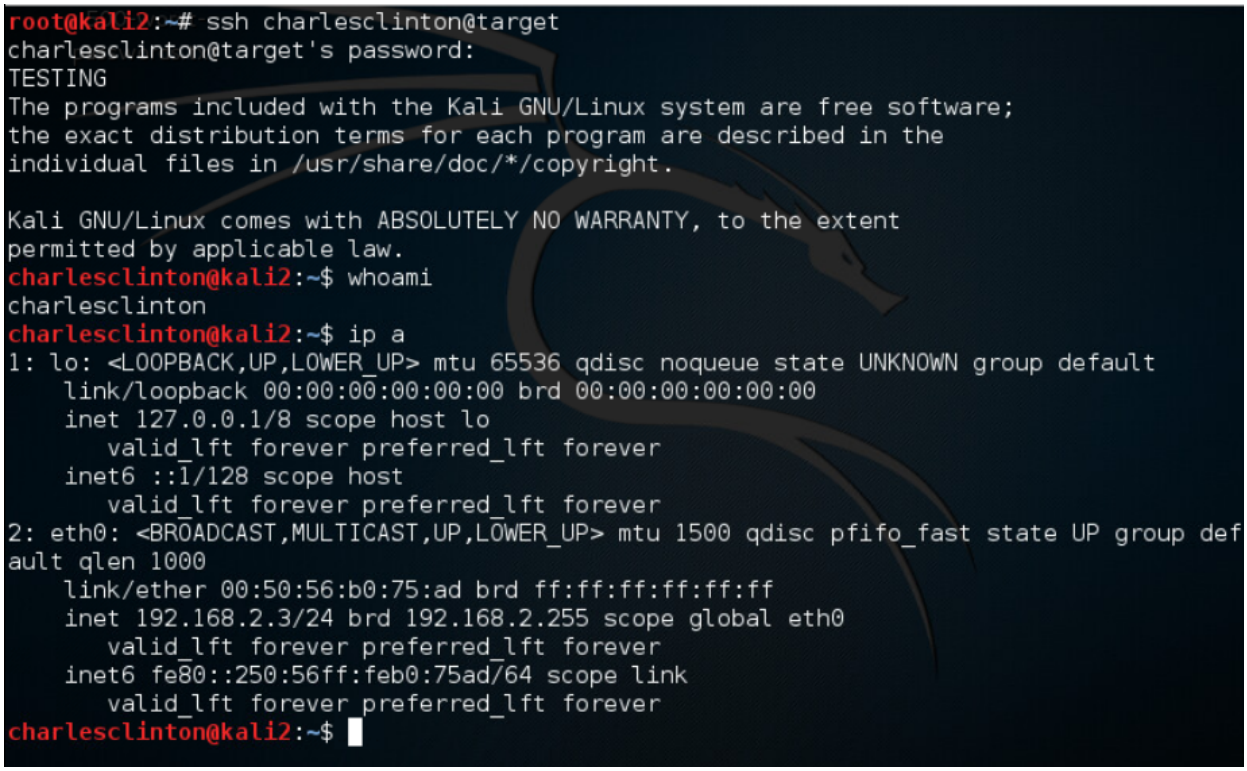
5. From here on, I choose to find vulnerability, and misconfigurations in the services that are running on the machine. I was able to log in anonymously for the ftp service. However, nothing useful was found.



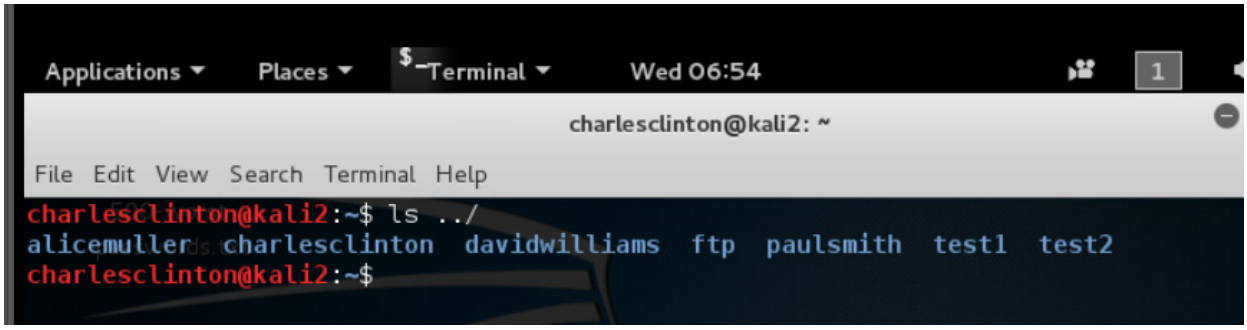
6. Then I used Hydra to bruteforce the next service, which is SSH on port 22. Found a potential login credential with the 500-worst-passwords.txt for SSH.



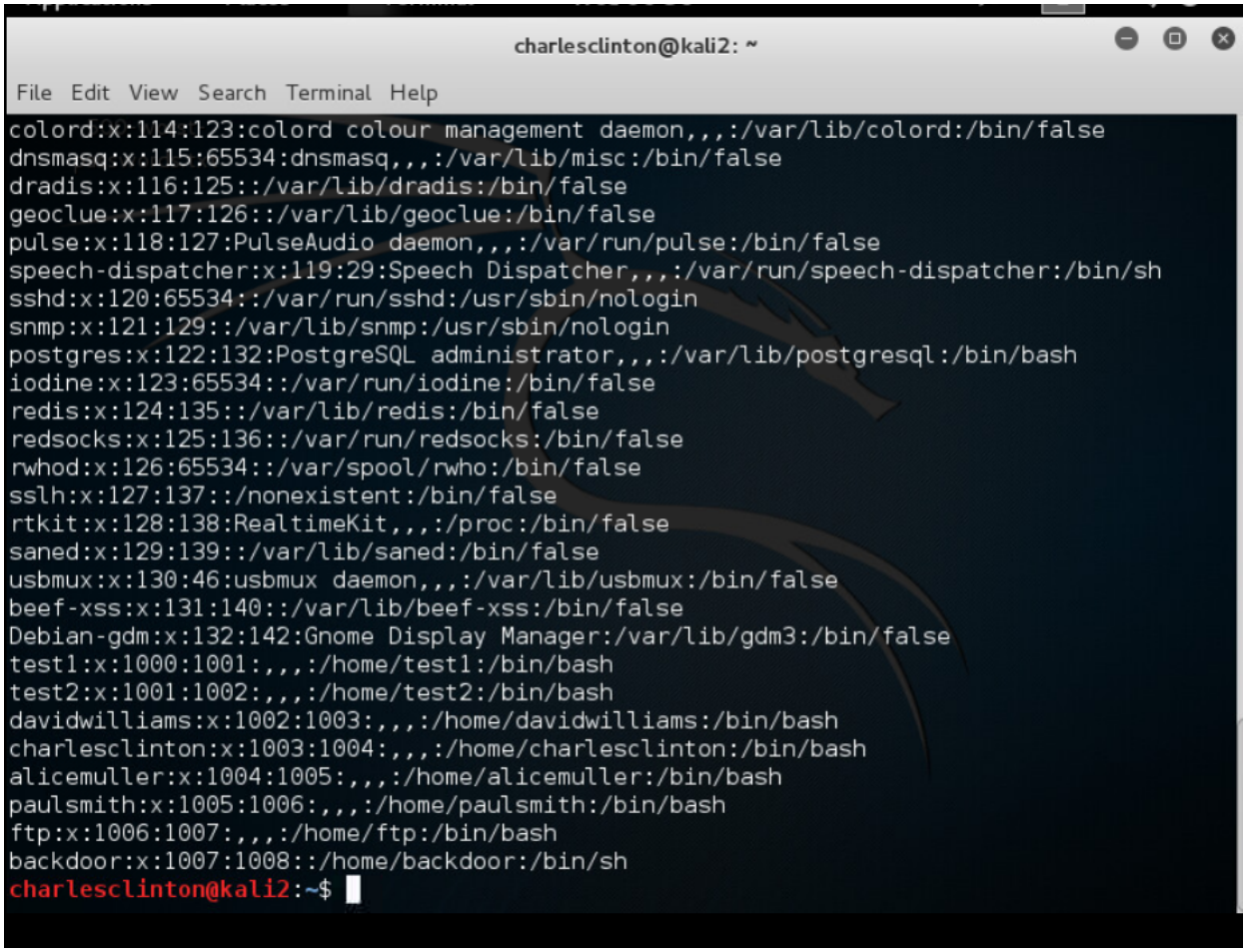
7. Logged in with charlesclinton as the user and golf as the password.



8. Confirming all the users that I found through OSINT actually exists.

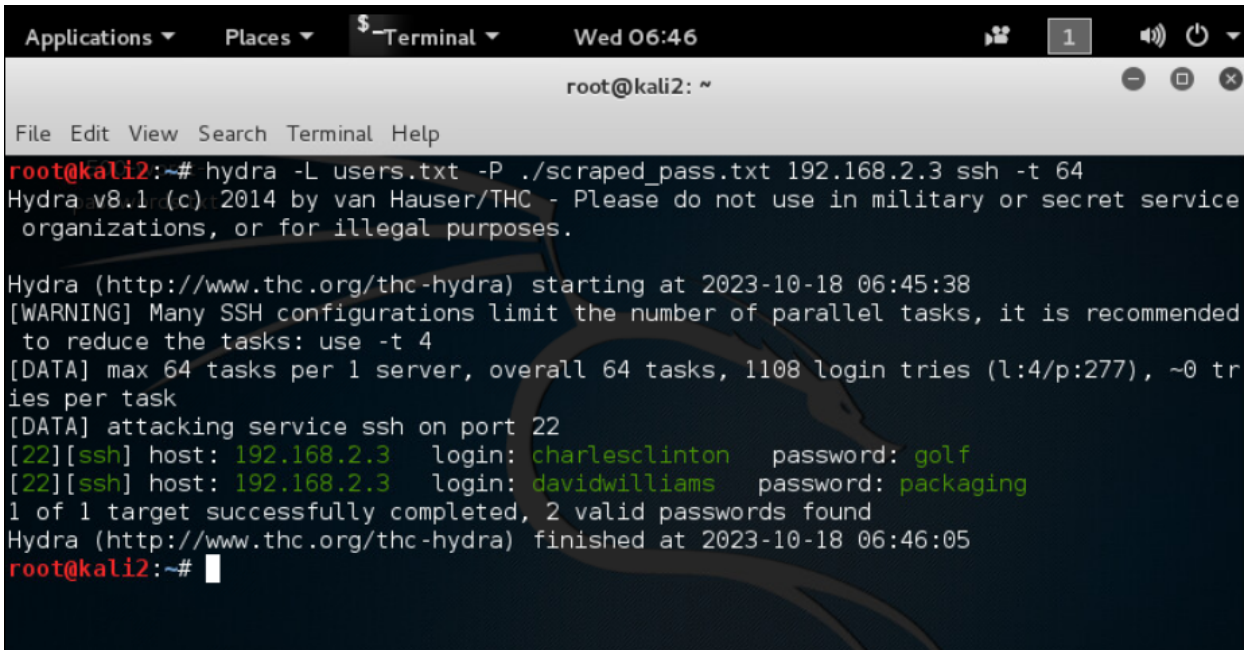


Used *cat /etc/passwd* command to display all the users on the machine.



9. Then I used cewl tool to get the all the words in the website using the command: cewl –min_word_length 1 http://192.168.2.3/ -o -w scraped._pass.txt

10. Then I bruteforced the ssh service using the scraped passwords from the website.



Using Nmap, CeWL, and Hydra, I was able to brute force the password of two users on the machine with the IP address of 192.168.2.3, which is in the local network.

The users are:

1. **User:**charlesclinton, **Password:**golf
2. **User:**davidwilliams, **Password:**packaging