ATTACK DEFENSE

by PentesterAcademy

Name	Interaction : SSH Service
URL	https://attackdefense.com/challengedetails?cid=1811
Type	Beginner Skills : Linux For Pentesters

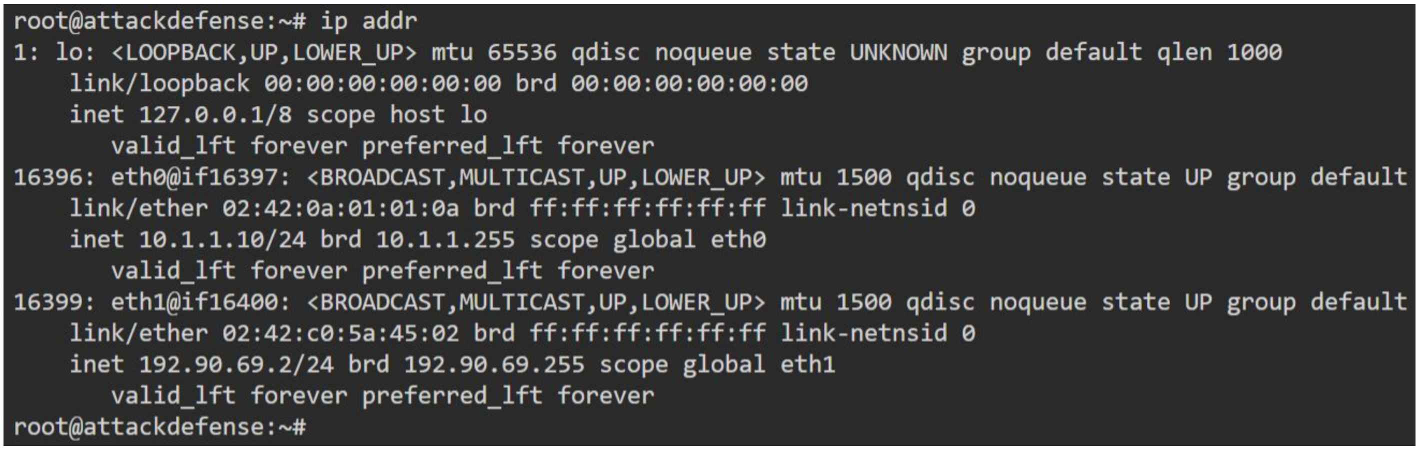
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Use expect to interact with SSH service and retrieve the flag!

Solution:

Step 1: Check the IP address of the machine.

Command: ip addr

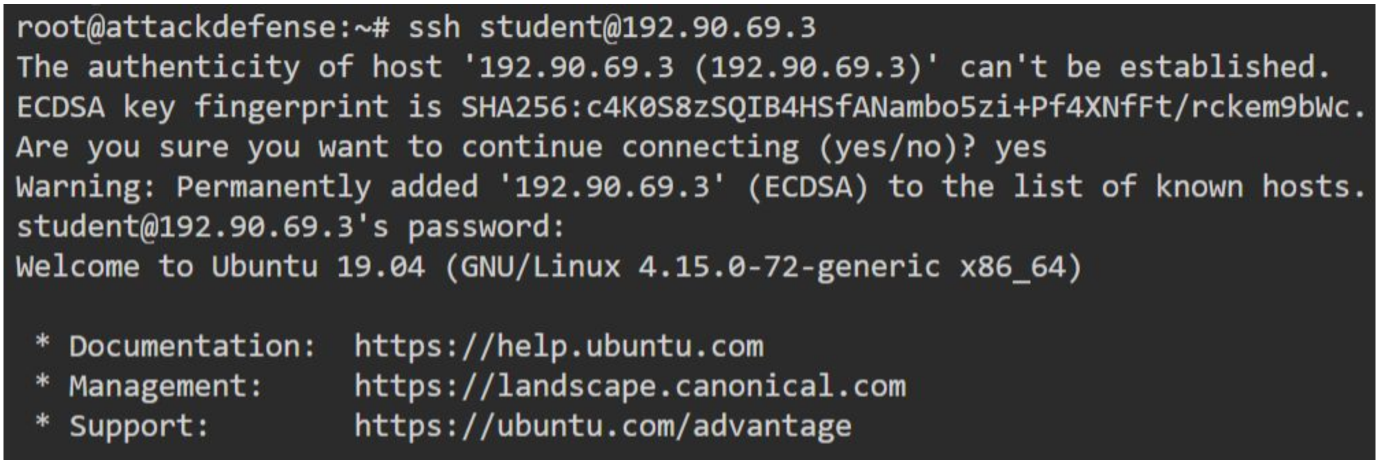


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16396: eth0@if16397: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:0a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.10/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
16399: eth1@if16400: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:5a:45:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.90.69.2/24 brd 192.90.69.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP of user's machine is 192.90.69.2, so as per the guidelines the IP of remote Linux machine should be 192.90.69.3

Step 2: Connect to SSH service as "student" user

Command: ssh student@192.90.69.3



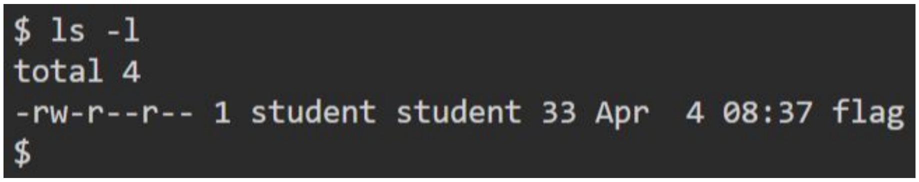
```
root@attackdefense:~# ssh student@192.90.69.3
The authenticity of host '192.90.69.3 (192.90.69.3)' can't be established.
ECDSA key fingerprint is SHA256:c4K0S8zSQIB4HSfANambo5zi+Pf4XNfFt/rckem9bWc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.90.69.3' (ECDSA) to the list of known hosts.
student@192.90.69.3's password:
Welcome to Ubuntu 19.04 (GNU/Linux 4.15.0-72-generic x86_64)

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

Provide password “student” on prompt.

Step 3: List the files present in the SSH directory.

Command: ls -l

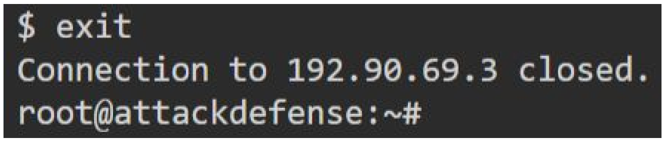


```
$ ls -l
total 4
-rw-r--r-- 1 student student 33 Apr  4 08:37 flag
$
```

Flag file “flag” is present on the server.

Step 4: Exit from the server.

Command: exit

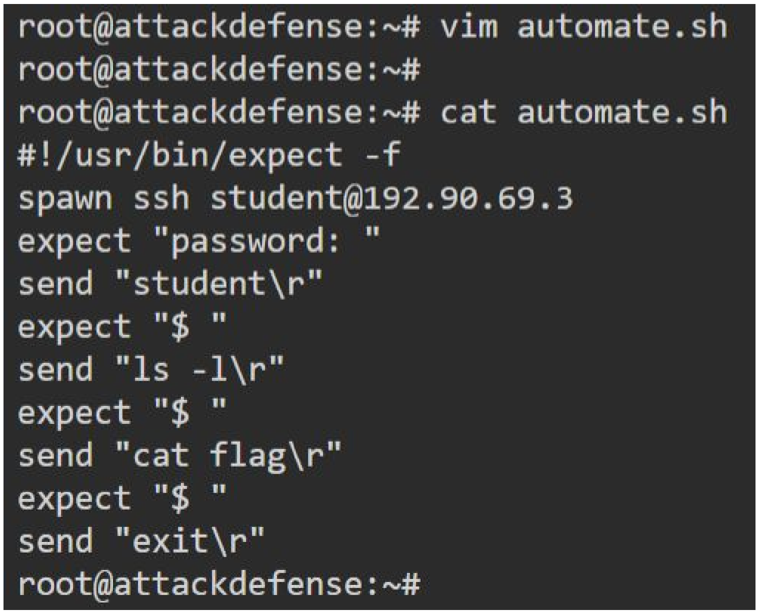


```
$ exit
Connection to 192.90.69.3 closed.
root@attackdefense:~#
```

Step 5: Whole manual process is clear now, automate this with expect now. Write expect script and save it as automate.sh

Bash script

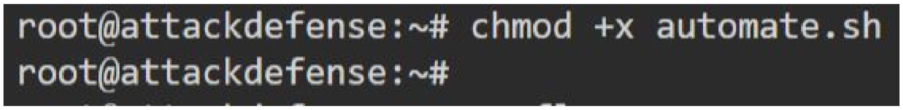
```
#!/usr/bin/expect -f
spawn ssh student@192.90.69.3
expect "password: "
send "student\r"
expect "$ "
send "ls -l\r"
expect "$ "
send "cat flag\r"
expect "$ "
send "exit\r"
```



```
root@attackdefense:~# vim automate.sh
root@attackdefense:~#
root@attackdefense:~# cat automate.sh
#!/usr/bin/expect -f
spawn ssh student@192.90.69.3
expect "password: "
send "student\r"
expect "$ "
send "ls -l\r"
expect "$ "
send "cat flag\r"
expect "$ "
send "exit\r"
root@attackdefense:~#
```

Step 6: Make this script executable.

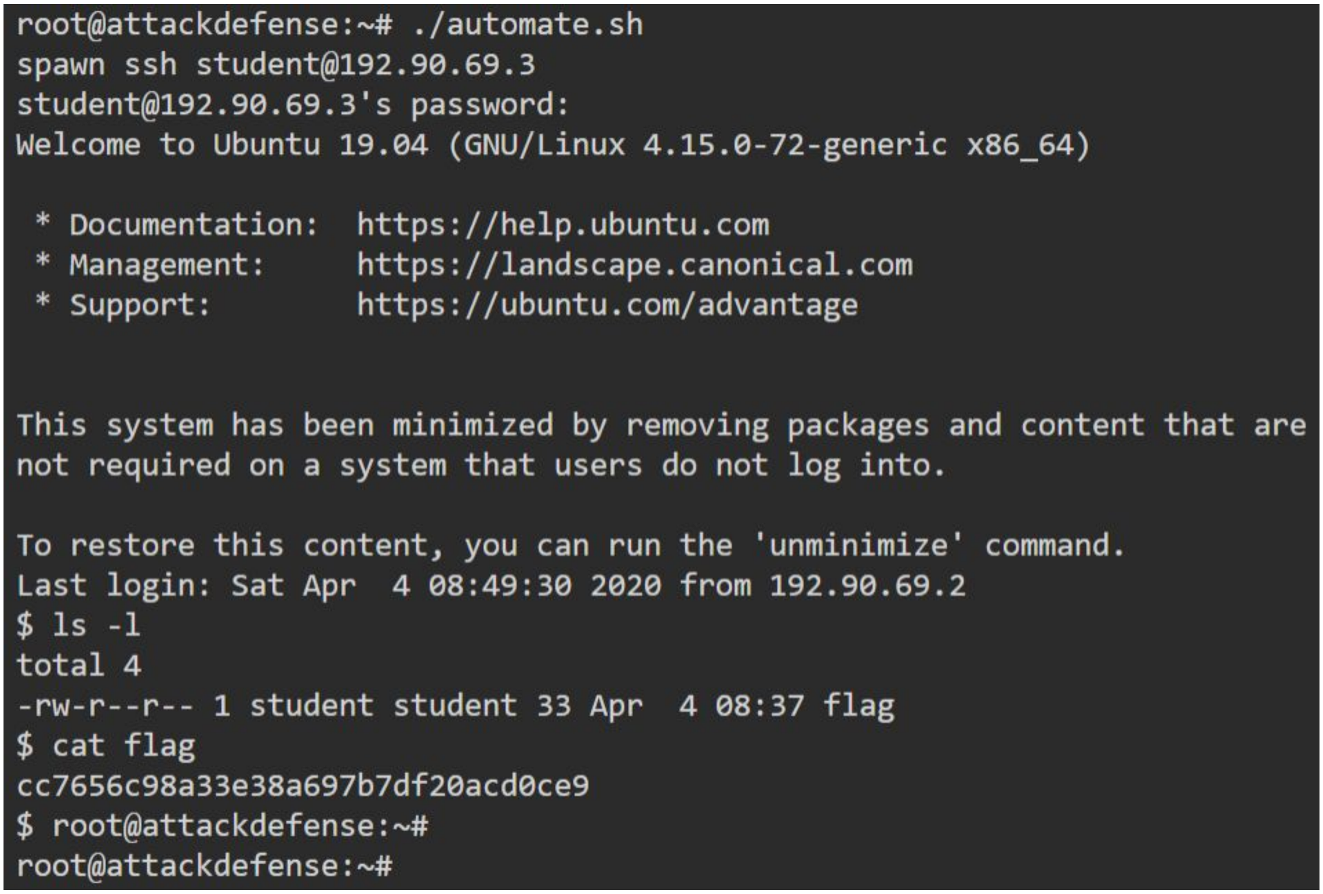
Command: chmod +x automate.sh



```
root@attackdefense:~# chmod +x automate.sh
root@attackdefense:~#
```

Step 7: Run this script.

Command: ./automate.sh



```
root@attackdefense:~# ./automate.sh
spawn ssh student@192.90.69.3
student@192.90.69.3's password:
Welcome to Ubuntu 19.04 (GNU/Linux 4.15.0-72-generic x86_64)

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


This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Apr  4 08:49:30 2020 from 192.90.69.2
$ ls -l
total 4
-rw-r--r-- 1 student student 33 Apr  4 08:37 flag
$ cat flag
cc7656c98a33e38a697b7df20acd0ce9
$ root@attackdefense:~#
root@attackdefense:~#
```

Flag: cc7656c98a33e38a697b7df20acd0ce9