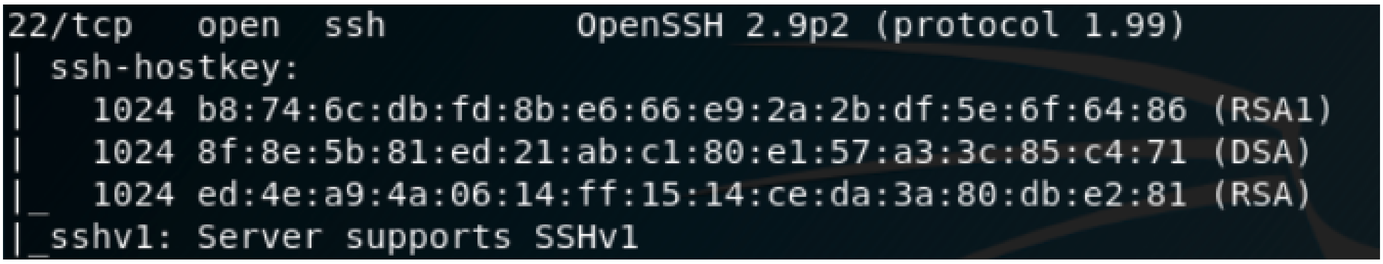
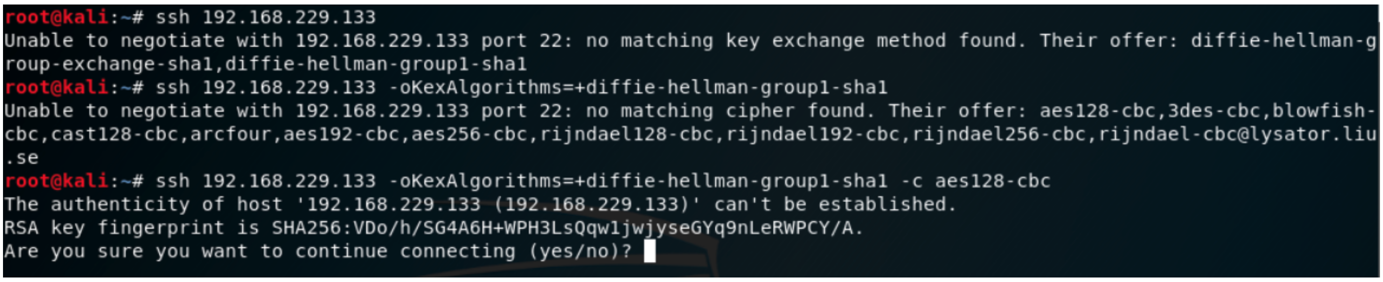
Enumerating SSH

In our nmap scan, we can see that our Kioptrix machine is running on OpenSSH version 2.9p2 as shown below:



```
22/tcp   open  ssh        OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
```

We can try connecting to the SSH port by using the `ssh <IP_address>` command. However, we get an error regarding the failed key exchange because the Kioptrix machine is really old and outdated. So we can try using a slightly different command `ssh <IP_address> -oKexAlgorithms=+diffie-hellman-group1-sha1`. However, it gives a different error regarding a cipher. So we will use this command `ssh <IP_address> -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc` as shown below:



```
root@kali:~# ssh 192.168.229.133
Unable to negotiate with 192.168.229.133 port 22: no matching key exchange method found. Their offer: diffie-hellman-g
roup-exchange-sha1,diffie-hellman-group1-sha1
root@kali:~# ssh 192.168.229.133 -oKexAlgorithms=+diffie-hellman-group1-sha1
Unable to negotiate with 192.168.229.133 port 22: no matching cipher found. Their offer: aes128-cbc,3des-cbc,blowfish-
cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael128-cbc,rijndael192-cbc,rijndael256-cbc,rijndael-cbc@lysator.liu
.se
root@kali:~# ssh 192.168.229.133 -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes128-cbc
The authenticity of host '192.168.229.133 (192.168.229.133)' can't be established.
RSA key fingerprint is SHA256:VDo/h/SG4A6H+WPH3LsQqw1jwjyseGYq9nLeRWPCY/A.
Are you sure you want to continue connecting (yes/no)?
```

When asked to connect, type in `yes`. No we are asked for a password (dead end) and we don't know the password so we will `Ctrl+C` to exit.