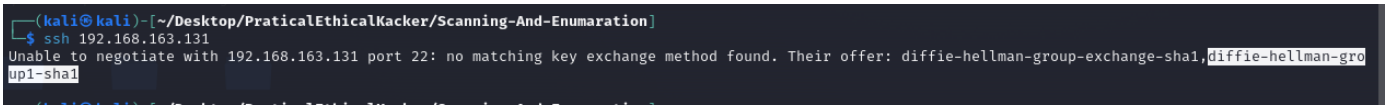
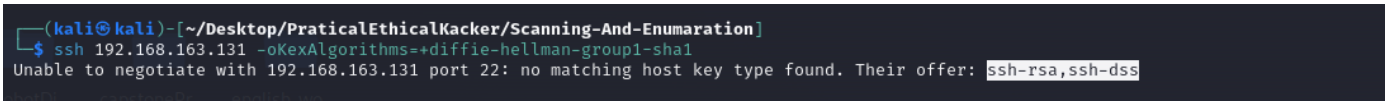
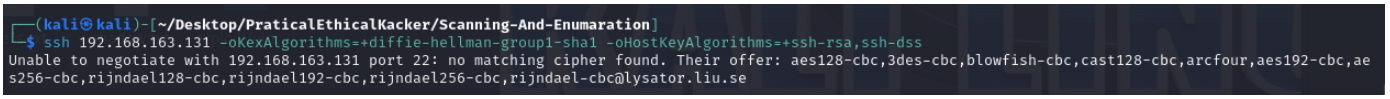
SSH

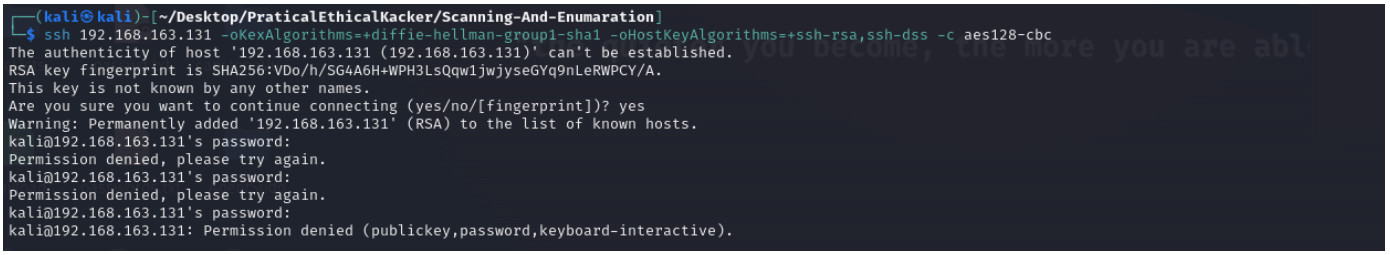
The first and pretty much all we can do is to try a login attempt to see if we can find service version.

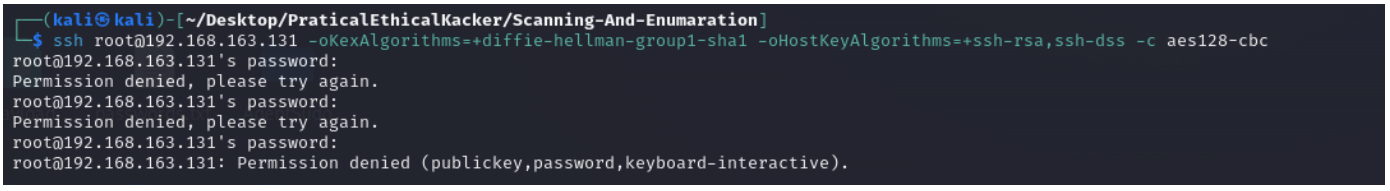
In this case, the machine is very old, and we will find all kind of connection issues with it. The following ssh command should bypass this connection issues, and allow us to attempt to login to the service.











#ssh root@192.168.163.131 -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa,ssh-dss -c aes128-cbc

Unfortunately there is nothing here for us. There might be a user root running, but that is not for sure. At this point, we have the version from the nmap scan, and we can brute force some logins. We can attempt to find some potential users so we could limit our brute force attack to something feasible.

And the service does not seem to allow us to enumerate user names on itself.