

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.

```
(kali@kali)-[~/Desktop/PracticalEthicalKacker/Scanning-And-Enumeration]
$ ssh 192.168.163.131
Unable to negotiate with 192.168.163.131 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
```

```
(kali@kali)-[~/Desktop/PracticalEthicalKacker/Scanning-And-Enumeration]
$ ssh 192.168.163.131 -oKexAlgorithms=+diffie-hellman-group1-sha1
Unable to negotiate with 192.168.163.131 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

```
(kali@kali)-[~/Desktop/PracticalEthicalKacker/Scanning-And-Enumeration]
$ ssh 192.168.163.131 -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa,ssh-dss
Unable to negotiate with 192.168.163.131 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
```

```
(kali@kali)-[~/Desktop/PracticalEthicalKacker/Scanning-And-Enumeration]
$ ssh 192.168.163.131 -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa,ssh-dss -c aes128-cbc
The authenticity of host '192.168.163.131 (192.168.163.131)' can't be established.
RSA key fingerprint is SHA256:VDo/h/SG4A6H+WPH3LsQqwIjwjySeGYq9nLeRWPCY/A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.163.131' (RSA) to the list of known hosts.
kali@192.168.163.131's password:
Permission denied, please try again.
kali@192.168.163.131's password:
Permission denied, please try again.
kali@192.168.163.131's password:
kali@192.168.163.131: Permission denied (publickey,password,keyboard-interactive).
```

```
(kali@kali)-[~/Desktop/PracticalEthicalKacker/Scanning-And-Enumeration]
$ ssh root@192.168.163.131 -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa,ssh-dss -c aes128-cbc
root@192.168.163.131's password:
Permission denied, please try again.
root@192.168.163.131's password:
Permission denied, please try again.
root@192.168.163.131's password:
root@192.168.163.131: Permission denied (publickey,password,keyboard-interactive).
```

```
#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.