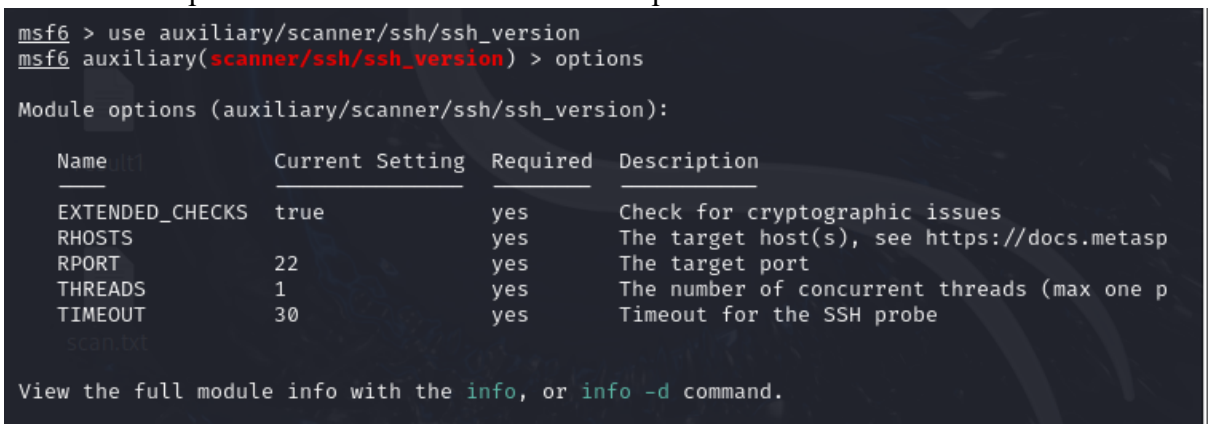
Learning Metaslpoit

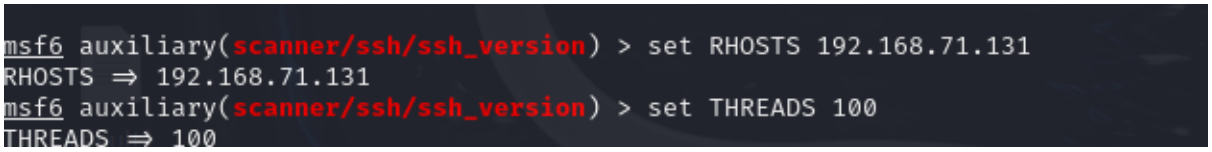
In Metasploit, auxiliary scanners are modules designed to perform a variety of tasks such as scanning for vulnerabilities, discovering services, or gathering information about target systems. These scanners are not used for exploitation but for information gathering and reconnaissance.

- Command : ***search ssh_version***
  This command searches for the ssh versions available in Metasploit

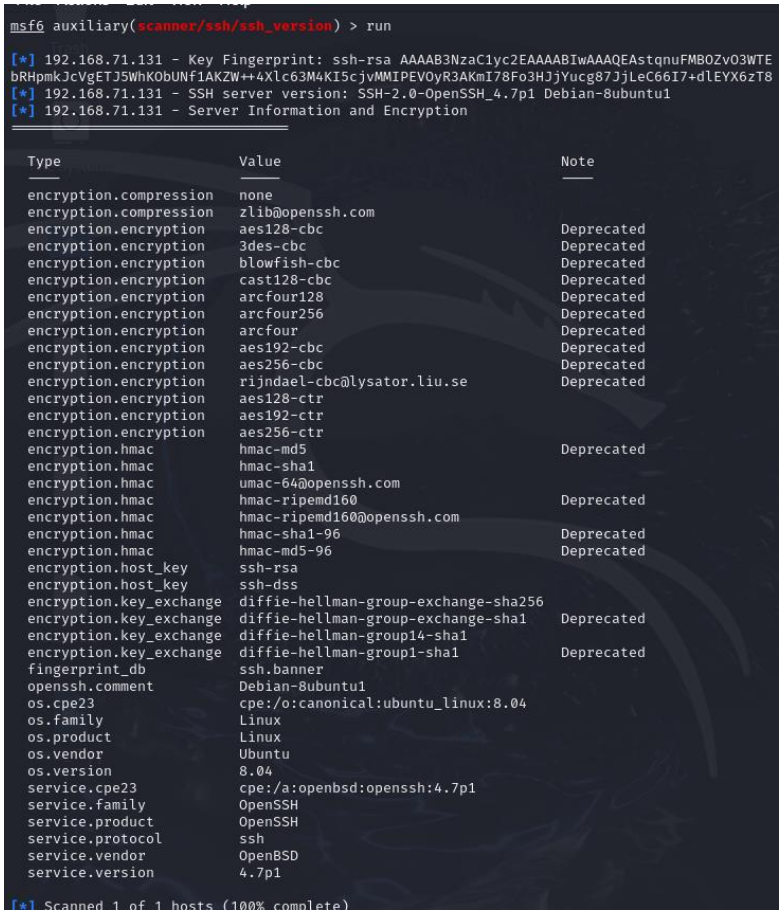
use auxiliary/scanner/ssh/ssh_version
if we look at options then we can see the module options.



Here we can see that the RHOST is not set so we set the Ip of the target machine



Now if we ***run*** it we will get the OS that it is running the version of the OS etc.



```
msf6 auxiliary(scanner/ssh/ssh_version) > run

[*] 192.168.71.131 - Key Fingerprint: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTE
bRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8
[*] 192.168.71.131 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
[*] 192.168.71.131 - Server Information and Encryption
═══════════════════════════════

  Type                    Value                                  Note
  ────                    ─────                                  ────
  encryption.compression  none
  encryption.compression  zlib@openssh.com
  encryption.encryption   aes128-cbc                             Deprecated
  encryption.encryption   3des-cbc                               Deprecated
  encryption.encryption   blowfish-cbc                           Deprecated
  encryption.encryption   cast128-cbc                            Deprecated
  encryption.encryption   arcfour128                             Deprecated
  encryption.encryption   arcfour256                             Deprecated
  encryption.encryption   arcfour                                Deprecated
  encryption.encryption   aes192-cbc                             Deprecated
  encryption.encryption   aes256-cbc                             Deprecated
  encryption.encryption   rijndael-cbc@lysator.liu.se            Deprecated
  encryption.encryption   aes128-ctr
  encryption.encryption   aes192-ctr
  encryption.encryption   aes256-ctr
  encryption.hmac         hmac-md5                               Deprecated
  encryption.hmac         hmac-sha1
  encryption.hmac         umac-64@openssh.com
  encryption.hmac         hmac-ripemd160                         Deprecated
  encryption.hmac         hmac-ripemd160@openssh.com
  encryption.hmac         hmac-sha1-96                           Deprecated
  encryption.hmac         hmac-md5-96                            Deprecated
  encryption.host_key     ssh-rsa
  encryption.host_key     ssh-dss
  encryption.key_exchange diffie-hellman-group-exchange-sha256
  encryption.key_exchange diffie-hellman-group-exchange-sha1     Deprecated
  encryption.key_exchange diffie-hellman-group14-sha1
  encryption.key_exchange diffie-hellman-group1-sha1             Deprecated
  fingerprint_db          ssh.banner
  openssh.comment         Debian-8ubuntu1
  os.cpe23                cpe:/o:canonical:ubuntu_linux:8.04
  os.family               Linux
  os.product              Linux
  os.vendor               Ubuntu
  os.version              8.04
  service.cpe23           cpe:/a:openbsd:openssh:4.7p1
  service.family          OpenSSH
  service.product         OpenSSH
  service.protocol        ssh
  service.vendor          OpenBSD
  service.version         4.7p1

[*] Scanned 1 of 1 hosts (100% complete)
```

This is a nice way of gathering the information about the target device.