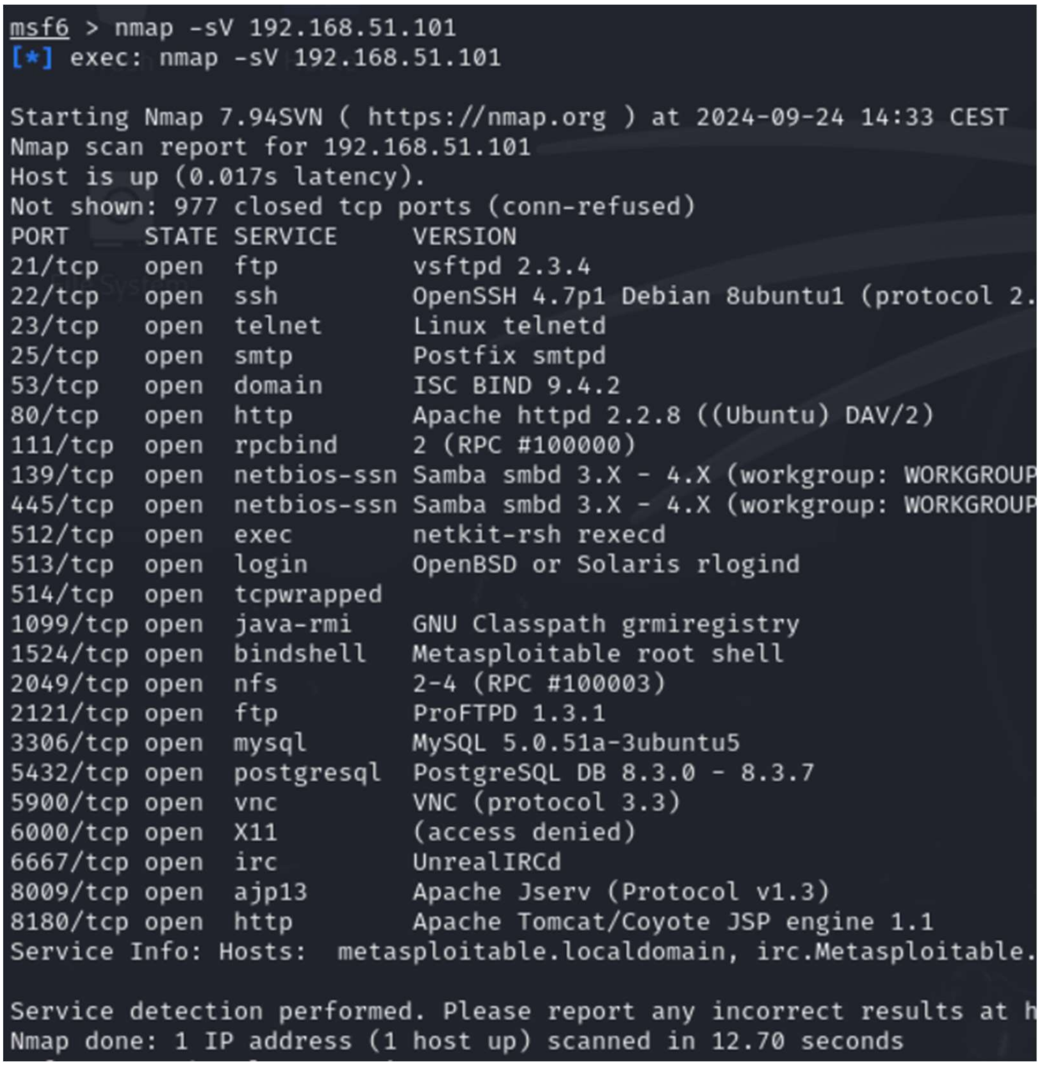
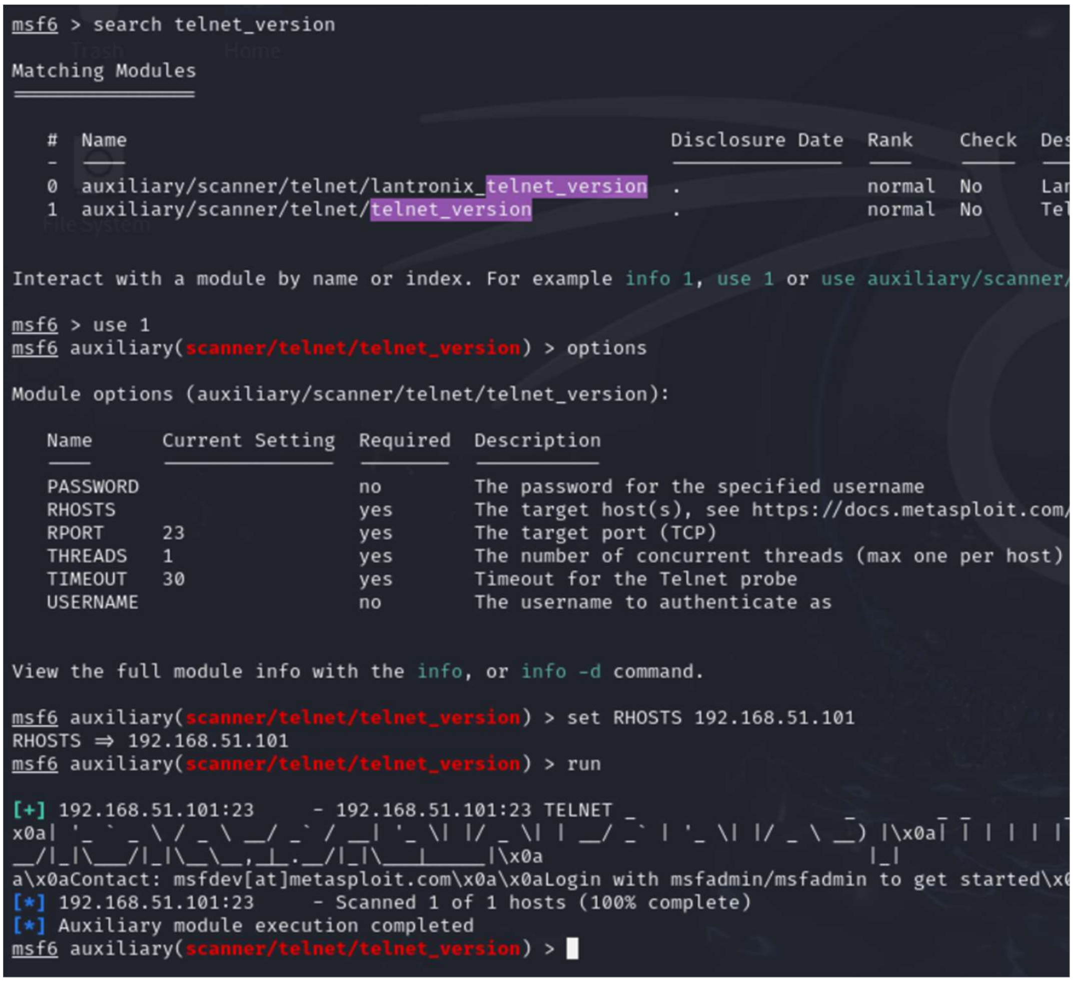


```
msf6 > nmap -sV 192.168.51.101
[*] exec: nmap -sV 192.168.51.101

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 14:33 CEST
Nmap scan report for 192.168.51.101
Host is up (0.017s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.

Service detection performed. Please report any incorrect results at h
Nmap done: 1 IP address (1 host up) scanned in 12.70 seconds
```



```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                            Disclosure Date  Rank    Check  Des
   -  ----                                            ---------------  ----    -----  ---
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .               normal  No     Lan
   1  auxiliary/scanner/telnet/telnet_version            .               normal  No     Tel

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.51.101
RHOSTS ⇒ 192.168.51.101
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.51.101:23     - 192.168.51.101:23 TELNET _                  _              _ _
x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |
__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                       |_|
a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0
[*] 192.168.51.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```