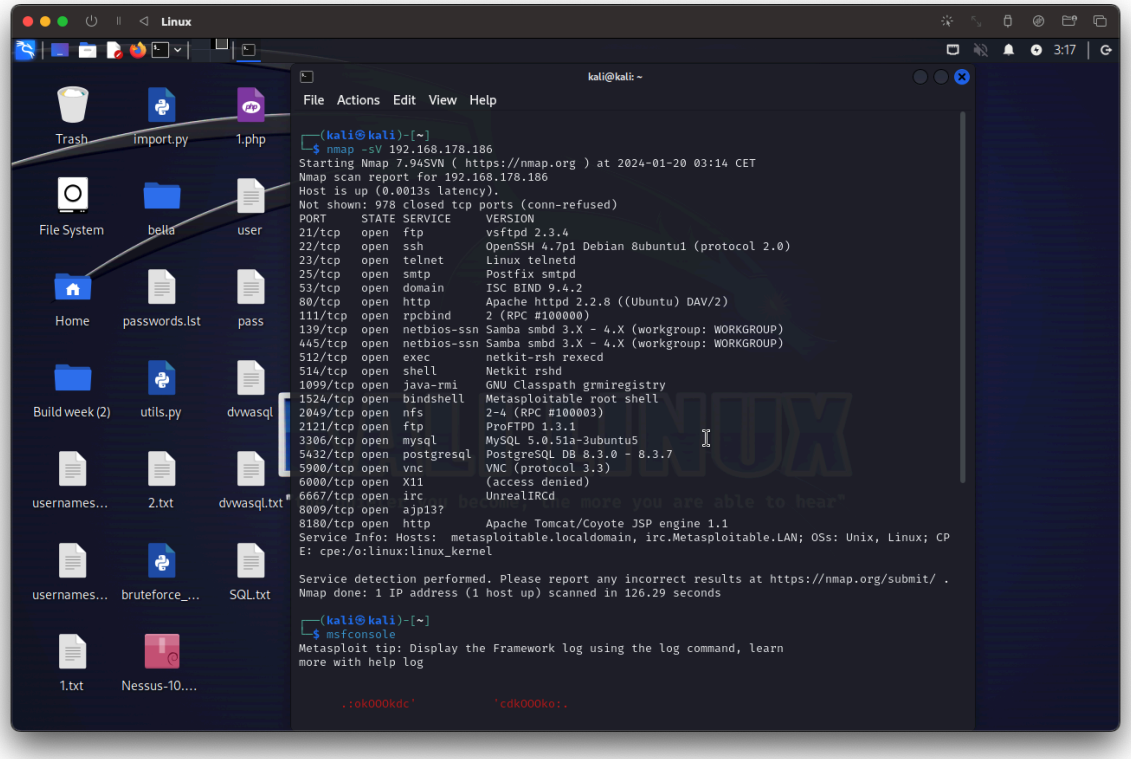
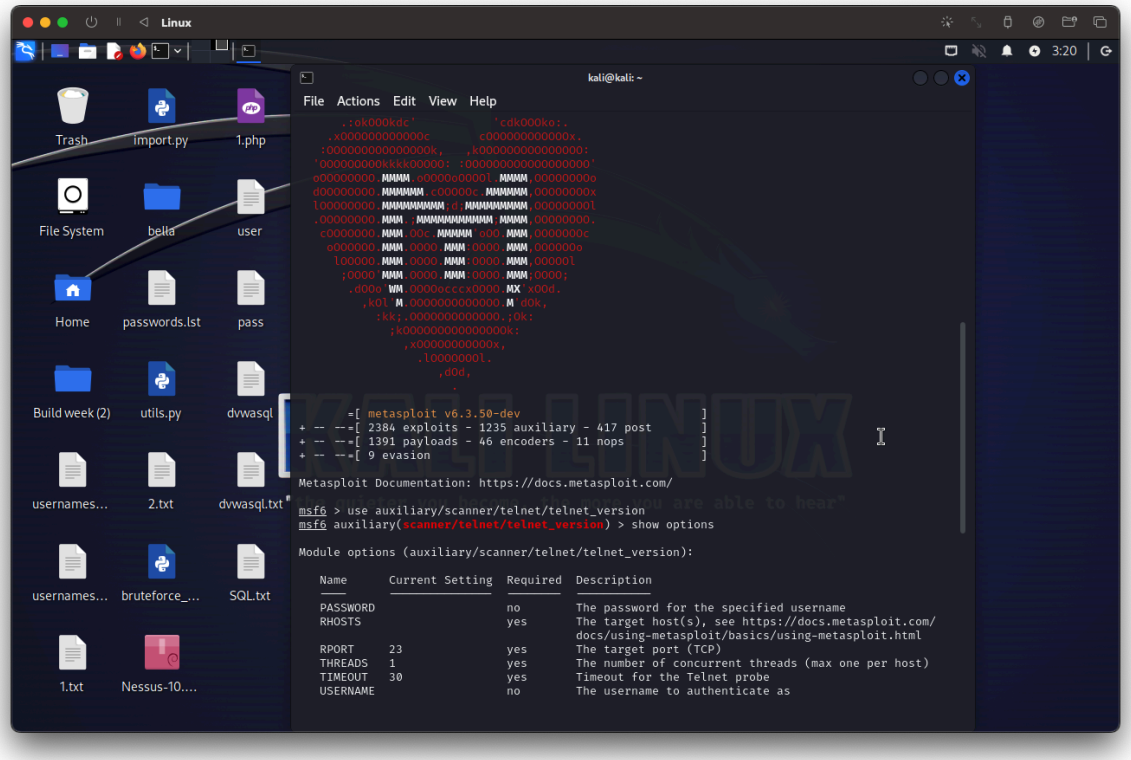
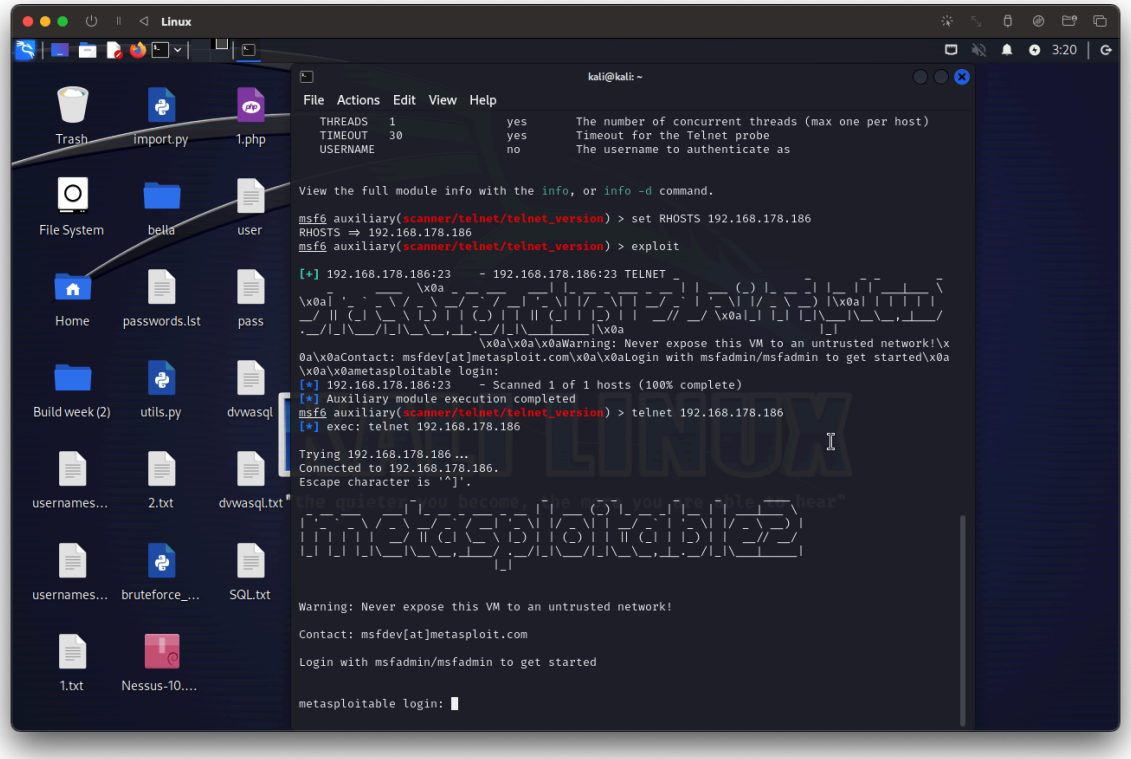

Linux
3:17
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV 192.168.178.186
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-20 03:14 CET
Nmap scan report for 192.168.178.186
Host is up (0.0013s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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
514/tcp open shell Netkit rshd
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?
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.29 seconds
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log


Linux
3:20
kali@kali: ~
File Actions Edit View Help
=[metasploit v6.3.50-dev]
+ -- --=[2384 exploits - 1235 auxiliary - 417 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show 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/
docs/using-metasploit/basics/using-metasploit.html
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


Linux
3:20
Trash
import.py
1.php
File System
bella
user
Home
passwords.lst
pass
Build week (2)
utils.py
dvwasql
usernames...
2.txt
dvwasql.txt
usernames...
bruteforce_...
SQL.txt
1.txt
Nessus-10....
kali@kali: ~
File Actions Edit View Help
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 192.168.178.186
RHOSTS => 192.168.178.186
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.178.186:23 - 192.168.178.186:23 TELNET
\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.178.186:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.178.186
[*] exec: telnet 192.168.178.186
Trying 192.168.178.186 ...
Connected to 192.168.178.186.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: