

Connessione abilitata ambo le parti

The image displays four screenshots from a VirtualBox environment, illustrating the setup and connection of a Kali Linux VM to a Metasploit VM.

Top Left Screenshot: Shows the Kali Linux VM interface. The terminal displays the Metasploit logo and a warning: "Warning: Never expose this VM to an untrusted network! Contact: msfdev[at]metasploit.com". The login prompt is "Login with msfadmin/msfadmin to get started".

Top Right Screenshot: Shows the Metasploit VM terminal. The user runs the command `ping 192.168.1.100`, resulting in a successful ping with 4 packets transmitted, 4 received, 0% packet loss, and a time of 2999ms.

Bottom Left Screenshot: Shows the Wireshark network traffic analysis. The interface displays a list of captured packets, including ICMP Echo (ping) requests and responses, and an HTTP GET request. The selected packet is a Transmission Control Protocol (TCP) packet with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
23	18.586577891	192.168.1.100	192.168.32.100	TCP	74	34644 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
24	18.589115944	192.168.32.100	192.168.1.100	TCP	74	80 → 34644 [SYN, ACK] Seq=0 Ack=1 Win=5792
25	18.589193969	192.168.1.100	192.168.32.100	TCP	66	34644 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=
26	18.589344708	192.168.1.100	192.168.32.100	HTTP	404	GET / HTTP/1.1
27	18.591337876	192.168.32.100	192.168.1.100	TCP	66	80 → 34644 [ACK] Seq=1 Ack=339 Win=6912 Len=
28	18.600595814	192.168.32.100	192.168.1.100	TCP	1204	80 → 34644 [PSH, ACK] Seq=1 Ack=339 Win=69
29	18.600648494	192.168.1.100	192.168.32.100	TCP	66	34644 → 80 [ACK] Seq=339 Ack=1139 Win=641
30	18.601524888	192.168.32.100	192.168.1.100	HTTP	71	HTTP/1.1 200 OK (text/html)
31	18.601576841	192.168.1.100	192.168.32.100	TCP	66	34644 → 80 [ACK] Seq=339 Ack=1144 Win=641
32	18.601747595	192.168.1.100	192.168.32.100	TCP	66	[TCP Keep-Alive] 34644 → 80 [ACK] Seq=339
44	28.899675356	192.168.32.100	192.168.1.100	TCP	66	[TCP Keep-Alive ACK] 80 → 34644 [ACK] Seq=
45	33.603153186	192.168.1.100	192.168.32.100	TCP	66	80 → 34644 [FIN, ACK] Seq=339 Ack=1144 Win=
46	33.606695642	192.168.32.100	192.168.1.100	TCP	66	80 → 34644 [FIN, ACK] Seq=1144 Ack=340 Win=
47	33.606195291	192.168.1.100	192.168.32.100	TCP	66	34644 → 80 [ACK] Seq=340 Ack=1145 Win=641
74	111.807578913	192.168.32.100	192.168.1.100	ICMP	98	Echo (ping) request id=0xe912, seq=1/256
75	111.807688218	192.168.1.100	192.168.32.100	ICMP	98	Echo (ping) reply id=0xe912, seq=1/256
76	112.808915759	192.168.32.100	192.168.1.100	ICMP	98	Echo (ping) request id=0xe912, seq=2/512
77	112.808941488	192.168.1.100	192.168.32.100	ICMP	98	Echo (ping) reply id=0xe912, seq=2/512
78	113.809048889	192.168.32.100	192.168.1.100	ICMP	98	Echo (ping) request id=0xe912, seq=3/768

Bottom Right Screenshot: Shows the Metasploit VM terminal. The user runs the command `ping 192.168.1.100`, resulting in a successful ping with 4 packets transmitted, 4 received, 0% packet loss, and a time of 2999ms.

Connessione abilitata solo da meta verso kali

The image displays two screenshots of a Kali Linux virtual machine running in Oracle VM VirtualBox.

Left Screenshot: Network Capture (Wireshark)

The Wireshark interface shows a capture on the `eth0` interface. The filter is `ip.addr == 192.168.32.100`. The packet list shows several TCP and ICMP packets:

No.	Time	Source	Destination	Protocol	Length	Info
35	9.451298315	192.168.1.100	192.168.32.100	TCP	74	33945 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
37	9.456790622	192.168.1.100	192.168.32.100	TCP	74	33952 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
38	10.416663580	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33946 → 80 [SYN] Seq=
39	10.476360116	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33952 → 80 [SYN] Seq=
40	12.435459577	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33946 → 80 [SYN] Seq=
41	12.690928422	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33952 → 80 [SYN] Seq=
42	14.655681702	192.168.1.100	192.168.32.100	TCP	74	33954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
43	15.064532650	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33954 → 80 [SYN] Seq=
44	16.498000974	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33946 → 80 [SYN] Seq=
45	17.692351982	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33964 → 80 [SYN] Seq=
46	21.876191755	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33964 → 80 [SYN] Seq=
51	24.693084400	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33946 → 80 [SYN] Seq=
52	30.864363589	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33964 → 80 [SYN] Seq=
55	49.816471292	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33946 → 80 [SYN] Seq=
66	46.227049956	192.168.1.100	192.168.32.100	TCP	74	[TCP Retransmission] 33964 → 80 [SYN] Seq=
71	55.416501935	192.168.32.100	192.168.1.100	ICMP	98	Echo (ping) request id=0xf112, seq=1/256,
72	55.416541635	192.168.1.100	192.168.32.100	ICMP	98	Echo (ping) reply id=0xf112, seq=1/256,
73	56.419465499	192.168.32.100	192.168.1.100	ICMP	98	Echo (ping) request id=0xf112, seq=2/512,
74	56.419584790	192.168.1.100	192.168.32.100	ICMP	98	Echo (ping) reply id=0xf112, seq=2/512,

The packet details pane shows the selected packet (No. 74) as a Transmission Control Protocol, Src Port: 33946, Dst Port: 80, Seq: 0, Len: 0.

Right Screenshot: Terminal Output

The terminal shows the output of a ping command from the `meta` machine to the `kali` machine:

```
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=63 time=1.30 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=63 time=2.20 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=63 time=1.71 ms

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 1.302/1.677/2.285/0.382 ms
msfadmin@metasploitable:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=63 time=2.36 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=63 time=1.96 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=63 time=3.49 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 1.960/2.605/3.495/0.651 ms
msfadmin@metasploitable:~$
```