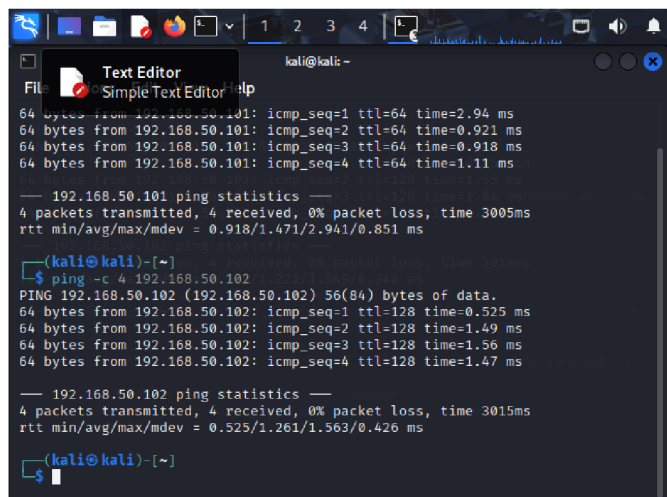


Emy Mangogna - W2D4 – Pratica

Ex1. Creare un laboratorio virtuale con Kali Linux, Metasploitable e Windows10 configurati in internal network, con comunicazione tra le macchine virtuali tramite ping.

Kali Linux(192.168.50.100) Metasploitable(192.168.50.101) Windows10(192.168.50.102)



```
kali@kali:~$ ping -c 4 192.168.50.101
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=2.94 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.921 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.918 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.11 ms

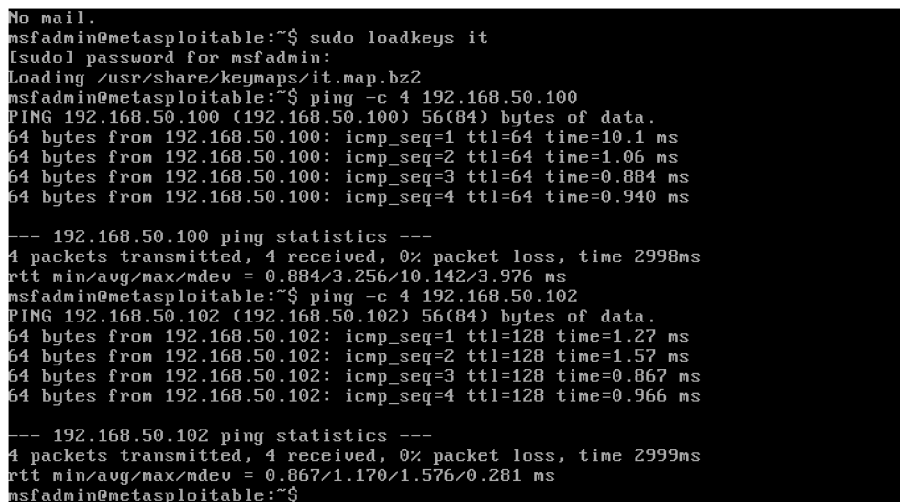
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.918/1.471/2.941/0.851 ms

kali@kali:~$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data:
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.525 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.49 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.56 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.47 ms

--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 0.525/1.261/1.563/0.426 ms

kali@kali:~$
```

Fig.1 Ping eseguito da Kali Linux verso Metasploitable e Windows10, conferma della comunicazione interna

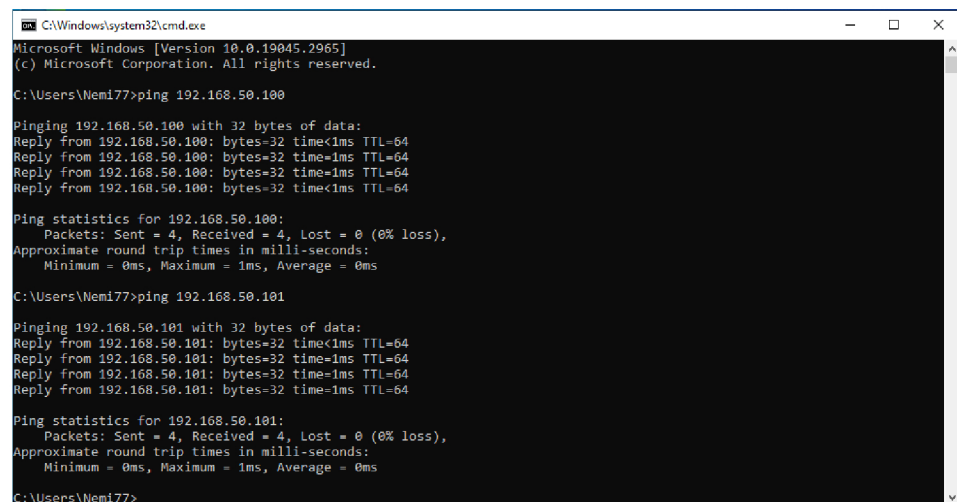


```
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ ping -c 4 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=10.1 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.884 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.940 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.884/3.256/10.142/3.976 ms
msfadmin@metasploitable:~$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data:
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.27 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.57 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.867 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.966 ms

--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.867/1.170/1.576/0.281 ms
msfadmin@metasploitable:~$
```

Fig.2 Ping eseguito da Metasploitable verso Kali Linux e Windows10, conferma della comunicazione interna



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Nemi77>ping 192.168.50.100

Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Nemi77>ping 192.168.50.101

Pinging 192.168.50.101 with 32 bytes of data:
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Nemi77>
```

Fig.2 Ping eseguito da Windows10 verso Kali Linux e Metasploitable, conferma della comunicazione interna

Ex2. creare una versione di recovery di una delle macchine appena create,ad esempio con l'opzione Clona. Clonare dunque una macchina a piacere e verificarne il corretto funzionamento.

