EPICODE W2D4 - Creazione e configurazione laboratorio virtuale

Pasquale Agizza

• RICHIESTA

L'obiettivo dell'esercitazione è quello di creare e configurare un laboratorio dove convivono e sono collegate fra loro tre macchine virtuali. Sulla prima di queste deve essere installato correttamente Kali Linux, sulla seconda Metasploitable 2 e sulla terza Windows 10

Le macchine virtuali devono poter comunicare fra di loro, ma allo stesso tempo devono essere completamente isolate rispetto alla macchina host.

• SOLUZIONE

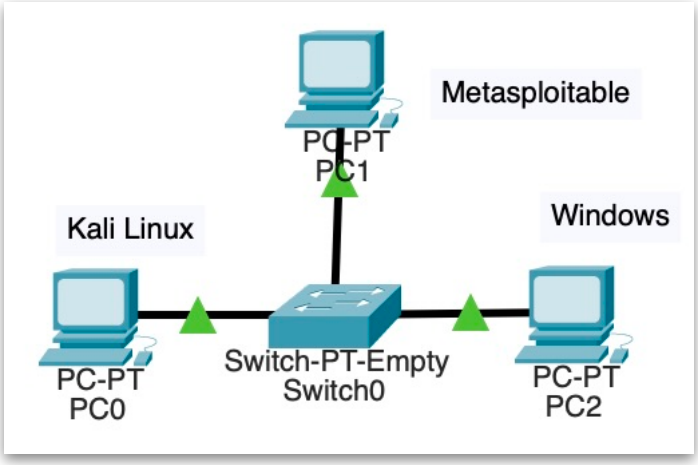
Utilizzando come host un MacBook Air con processore M1 e architettura ARM, ho scelto il virtualizzatore UTM, l'unico utilizzabile per installare Metaspoitable 2 e Windows 10

Ho innanzitutto creato la macchina virtuale denominata Kali Linux - EPICODE, e in questa ho installato e configurato correttamente l'omonima distribuzione Linux. Ho poi creato le macchine virtuali Metaspoitable - EPICODE e Windows 10 - EPICODE, dove ho installato e configurato gli altri due sistemi operativi richiesti.

Dopo le opportune configurazioni di rete, le tre macchine virtuali comunicano fra di loro. Nessuna delle macchine virtuali comunica con la macchina host.

• IMMAGINI

Concettualmente, il nostro laboratorio virtuale può essere sintetizzato con la seguente immagine



• APPROFONDIMENTO TECNICO

Per la creazione della macchina virtuale Kali Linux - EPICODE ho utilizzato le funzionalità di virtualizzazione di UTM, dato che l'architettura ARM della versione 2024.4 è la stessa del MacBook Air che utilizzo e che fa da host.

Per Metaspoitable 2 e Windows 10 ho invece dovuto utilizzare l'emulazione, dato che sono entrambi sistemi operativi in versione x64, non direttamente utilizzabile dal MacBook Air con architettura ARM.

Una volta installati i tre sistemi operativi, ho configurato la rete secondo quanto richiesto. In particolare, ho utilizzato questi parametri:

- Kali Linux IP 192.168.50.100/24 Gateway 192.168.50.1
- Metasploitable IP 192.168.50.101/24 Gateway 192.168.50.1
- Windows 10 IP 192.168.50.102/24 Gateway 192.168.50.1

Per testare l'effettivo collegamento fra le macchine, ho effettuato una richiesta di Ping da Metasploitable verso le altre due macchine. Entrambi i test hanno dato risultato positivo.

```
msfadmin@metasploitable:~$ ping 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=9.89 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.610 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.756 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.483/2.937/9.899/4.020 ms
msfadmin@metasploitable:~$ ping 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=18.0 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=3.07 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=2.12 ms

--- 192.168.50.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 2.125/7.738/18.018/7.279 ms
```

Per ragioni di sicurezza, era necessario però che le tre macchine virtuali non comunicassero con la macchina host. Per fare questo, dalle impostazioni di UTM è necessario selezionare la modalità di rete "RETE CONDIVISA".

Questa modalità consente di creare un collegamento fra le macchine virtuali, come necessitiamo, ma al tempo stesso isola la macchina host.

Per accertarmi con sicurezza dell'isolamento della macchina host, ho inviato una richiesta di Ping da questa macchina alle tre macchine virtuali

```
pagizza@MacBook-APPLE ~ % ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100): 56 data bytes
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 ed2a   0 0000  3f  01 d4dc 192.168.5.53  192.168.50.100

Request timeout for icmp_seq 0
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 ede9   0 0000  3f  01 d41d 192.168.5.53  192.168.50.100

Request timeout for icmp_seq 1
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 3750   0 0000  3f  01 8ab7 192.168.5.53  192.168.50.100

^C
--- 192.168.50.100 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
pagizza@MacBook-APPLE ~ %
```

```
PING 192.168.50.101 (192.168.50.101): 56 data bytes
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 0e5b   0 0000  3f  01 b3ab 192.168.5.53  192.168.50.101

Request timeout for icmp_seq 0
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 fba9   0 0000  3f  01 c65c 192.168.5.53  192.168.50.101

Request timeout for icmp_seq 1
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 0914   0 0000  3f  01 b8f2 192.168.5.53  192.168.50.101

^C
--- 192.168.50.101 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
pagizza@MacBook-APPLE ~ %
```

```
pagizza@MacBook-APPLE ~ % ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102): 56 data bytes
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 031e   0 0000  3f  01 bee7 192.168.5.53  192.168.50.102

Request timeout for icmp_seq 0
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 036e   0 0000  3f  01 be97 192.168.5.53  192.168.50.102

Request timeout for icmp_seq 1
92 bytes from 192.168.1.254: Destination Host Unreachable
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  b8 5400 82b6   0 0000  3f  01 3f4f 192.168.5.53  192.168.50.102

^C
--- 192.168.50.102 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
pagizza@MacBook-APPLE ~ %
```

Come da immagine, le tre richieste di Ping hanno dato tutte esito negativo, certificando il fatto che la macchina host non comunica con le tre macchine virtuali in esecuzione