

TP Kali (Découverte et Scan réseau)

Ce TP a pour objectif de découvrir Kali Linux, un système utilisé pour tester la sécurité des réseaux. L'objectif est de comprendre comment les attaquants agissent pour mieux protéger un réseau.

1) Quelle commande avez-vous utilisée pour réaliser cette étape ?

Pour identifier l'IP et l'adresse MAC de ma carte réseau sous Kali Linux, j'ai utilisé la commande `ifconfig`.

```
(dulcie2014@DULCIE)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.5.85 netmask 255.255.0.0 broadcast 10.20.255.255
    inet6 fe80::215:5dff:fe01:2781 prefixlen 64 scopeid 0<*link>
    ether 00:15:5d:01:27:81 txqueuelen 1000 (Ethernet)
    RX packets 65951 bytes 4604871 (4.3 MiB)
    RX errors 0 dropped 246 overruns 0 frame 0
    TX packets 119 bytes 16858 (16.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Carte Ethernet Ethernet :
    Suffixe DNS propre à la connexion. . . . : Sio-Metz.net
    Adresse IPv6 de liaison locale. . . . . : fe80::5b7b:9a93:e10d:2e6%7
    Adresse IPv4. . . . . : 10.20.5.98
    Masque de sous-réseau. . . . . : 255.255.0.0
    Passerelle par défaut. . . . . : 10.20.0.253

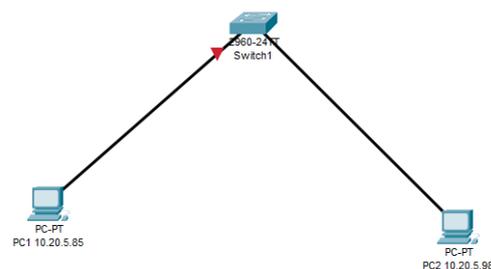
C:\Users\Dulcie>ping 10.20.5.85

Envoi d'une requête 'Ping' 10.20.5.85 avec 32 octets de données :
Réponse de 10.20.5.85 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.20.5.85:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

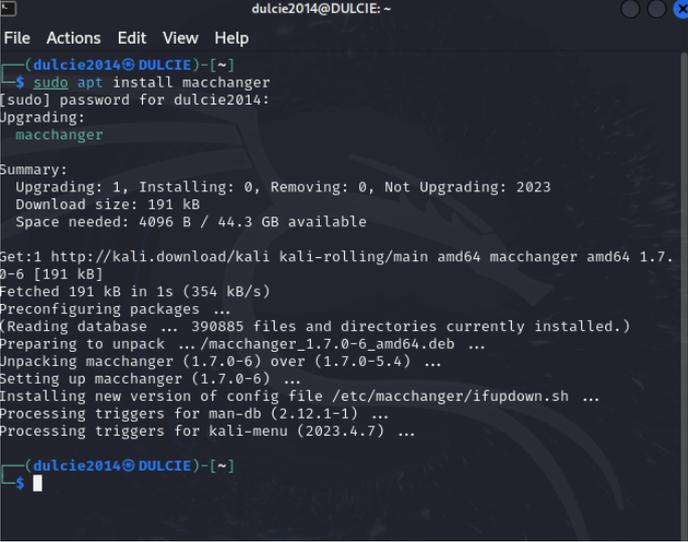
C:\Users\Dulcie>_
```

2) Réalisez un schéma de votre infrastructure avec le logiciel de votre choix



3) Dans quel dossier cette application est-elle rangée et pour quelle raison ? A quoi sert-elle ?

La commande macchanger est rangée dans le répertoire usr/bin sur ma machine Linux.



```
dulcie2014@DULCIE:~  
File Actions Edit View Help  
--(dulcie2014@DULCIE)-[~]  
--$ sudo apt install macchanger  
[sudo] password for dulcie2014:  
Upgrading:  
  macchanger  
Summary:  
  Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 2023  
  Download size: 191 kB  
  Space needed: 4096 B / 44.3 GB available  
Get:1 http://kali.download/kali kali-rolling/main amd64 macchanger amd64 1.7.0-6 [191 kB]  
Fetched 191 kB in 1s (354 kB/s)  
Preconfiguring packages ...  
(Reading database ... 390885 files and directories currently installed.)  
Preparing to unpack .../macchanger_1.7.0-6_amd64.deb ...  
Unpacking macchanger (1.7.0-6) over (1.7.0-5.4) ...  
Setting up macchanger (1.7.0-6) ...  
Installing new version of config file /etc/macchanger/ifupdown.sh ...  
Processing triggers for man-db (2.12.1-1) ...  
Processing triggers for kali-menu (2023.4.7) ...  
--(dulcie2014@DULCIE)-[~]  
--$
```

4) Combien de temps cela vous a pris ? Quels sont les dangers possibles avec une telle application ? Comment s'en protéger ?

Cela m'a pris environ 10 minutes. Les dangers incluent la possibilité de masquer l'adresse MAC, ce qui peut être utilisé pour contourner des filtres ou mener des attaques. Pour ce protéger, il faut surveiller le réseau, utiliser des filtres MAC et activer des authentifications plus sécurisées.

5) Dans quel dossier cette application est-elle rangée et pour quelle raison ? A quoi sert-elle ?

6) Quelle application se cache derrière Zenmap ? Quels sont les dangers possibles avec une telle application ? Comment s'en protéger ?

Zenmap est une interface graphique pour l'outil Nmap, utilisé pour scanner les réseaux. Les dangers incluent la découverte de vulnérabilités et les attaques potentielles. Pour se protéger, il faut utiliser des pare-feu, des systèmes de détection d'intrusions et limiter l'accès aux services réseau.

7) Tirez une conclusion sur ce que vous venez de découvrir aujourd'hui

Aujourd'hui, j'ai appris que des outils comme macchanger et Zenmap peuvent être utilisés pour scanner et modifier des réseaux, mais qu'ils présentent des risques si mal utilisés. Il est important de mettre en place des protections comme des pare-feu et des systèmes de détection d'intrusions.