Re-travail des missions

Mission 1 — Centraliser l’heure (NTP)

--> A faire sur les deux switchs et le routeur

Pourquoi : Le **routeur** donne l’heure à tous les **switchs** et hôtes (horodatages cohérents pour les logs et les tests).

Console --> passer en config :

```
enable
configure terminal
```

Fuseau horaire (France) :

```
clock timezone CET 1
clock summer-time CEST recurring
```

Routeur NTP maître (seulement dans le routeur) :

```
ntp master 3
end
write memory
```

Pour vérifier :

```
show ntp status
show clock
```

Déclarer le routeur NTP (seulement dans les switchs) :

```
conf t
ntp server (IP routeur)
clock timezone CET 1
end
write memory
```

Pour vérifier :

```
show ntp associations
show clock
```

--> Redémarre un switch --> show clock doit afficher la bonne heure (synchro)

Sans internet :

Bilan complet des commandes

Routeur

```
enable
clock set HH:MM:SS 19 March 2026
configure terminal
clock timezone CET 1
ntp master 3
end
write memory
```

Vérification :

```
show clock
show ntp status
```

Switchs (les deux)

```
enable
configure terminal
```

```
clock timezone CET 1
ntp server <IP_du_routeur>
end
write memory
```

Vérification :

```
show clock
show ntp associations
```

Points importants

- Ne pas mettre `clock summer-time CEST recurring` pour l'instant (on est encore en heure d'hiver, ça décalerait d'1h)
- Remplacer `<IP_du_routeur>` par une IP visible dans `show ip interface brief` sur le routeur
- Le `clock set` est à faire **avant** le `configure terminal`, sinon la commande n'est pas disponible

Mission 2 — Lister ce qui doit être journalisé (logs)

Objectif : Etablir quoi logger sur routeurs/switchs pour la supervision/sécurité.

1. Connexions administrateur

À journaliser :

- Connexions SSH / Telnet / Console réussies
- Tentatives de connexion échouées
- Entrée / sortie du mode enable
- Escalade de privilèges
- Identifiant, IP source, date / heure

Justification CNIL/RGPD : traçabilité des accès, enregistrement des actions d’administration

---

2. Changements d’état des interfaces

À journaliser :

- Interface up/down
- Changement speed/duplex
- Déconnexion / reconnexion
- Erreurs physiques : CRC, collisions, input/output errors

Justification : détection d’incident matériel ou intrusion réseau

---

3. Violations de sécurité L2

À journaliser :

- Port-Security : MAC inconnue, port en err-disabled
- DHCP Snooping : serveur DHCP non autorisé
- Dynamic ARP Inspection (DAI) : ARP spoofing / MITM détecté
- IP Source Guard : mismatch IP/MAC

Justification : détection d’accès non autorisé et attaques L2 ciblant des données personnelles

---

4. VLAN / trunk / Spanning-Tree

À journaliser :

- VLAN créés / supprimés / modifiés
- Changements d’affectation de port
- Perte d’un trunk 802.1Q
- Spanning-Tree : changement de root, TCN, blocage de port

Justification : actions administratives affectant le transport des données → traçabilité obligatoire

---

5. Reboot, crash, anomalies système

À journaliser :

- Reboot planifié / manuel
- Crash system / stack trace
- Panic IOS / firmware
- Événements SNMP critiques

Justification : analyse d’incident et sécurité du système d’information

---

6. Alertes matérielles (température, ventilateurs, alimentation)

À journaliser :

- Température anormale
- Ventilateur défectueux
- Panne alimentation / changement d’état PSU

Justification : mesure technique indispensable à la sécurité (art. 32 RGPD)

---

7. Violations ACL / tentatives d’accès refusées

À journaliser :

- Paquets bloqués par ACL
- Accès réseau refusé
- Tentatives d’accès à ressources interdites

Justification : traçabilité des tentatives d’accès non autorisées (CNIL)

---

8. Modifications de configuration

À journaliser :

- copy run start / write
- Modification des ACL
- Modification des routes

- Création / suppression d’interfaces
- Changement de paramètres NTP, SNMP, VLAN

Justification CNIL : journalisation obligatoire des actions *création, modification, suppression* de configuration

---

9. Événements système critiques

À journaliser :

- CPU élevé
- Mémoire saturée
- Bug matériel

Justification : détection automatique des incidents via outils de supervision (CNIL)

---

10. Journaux NTP (indispensable pour traçabilité)

À journaliser :

- Synchronisation NTP OK / KO
- Perte de synchronisation
- Modification de serveur NTP

Justification : horodatage fiable, nécessaire à la valeur probante des logs (CNIL)

---

11. SNMP / Supervision

À journaliser :

- Traps SNMP critiques
- Changements de configuration SNMPv3 (auth/priv)
- MIB système / sécurité

Justification CNIL : analyse automatique obligatoire pour détection rapide d’incidents

Sources a utiliser :

https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation

https://donnees.net/gestion-logs-rgpd

Mission 3 — Paramétrer les logs sur routeurs & switchs

Objectif : Envoyer les journaux vers un serveur central (rsyslog) tout en gardant un buffer local.
--> A le faire a chaque équipement

Sur PuTTy, sur le routeur :

1.1. Activer l'horodatage (obligatoire pour CNIL/RGPD) :

```
conf t
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

1.2. Envoyer les logs au serveur Syslog

```
logging host 192.168.99.3
logging trap informational
logging on
```

1.3. Inclure les informations critiques

Logs des tentatives administratives (SSH, console, login)

```
login on-failure log
login on-success log
ip ssh logging events
```

Logs des changements de configuration

```
archive
log config
  logging enable
  notify syslog
  hidekeys
```

1.4. Suivi des interfaces (up/down + erreurs)

```
conf t
   logging event link-status
   logging event trunk-status
```

Pour une interface spécifique :

```
interface GigabitEthernet0/1
   logging event link-status
```

1.5. Logs ACL (accés refusés)

Ajoute log à la fin des ACL :

```
ip access-list extended SECURITE
deny ip any any log
permit ip any any
```

1.6. Logs sécurité L2 (si switch - routeur hybride)

Sur routeurs L3 avec switch intégré :

```
ip dhcp snooping database write-delay 60
ip arp inspection logging
```

1.7. Logs NTP

```
ntp logging
```

1.8. Logs système

```
logging buffered 16384 warnings
```

Sur PuTTy, sur le swicth :

2.1. Activer horodatage

```
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

2.2. Envoi vers serveur Syslog

```
logging host 192.168.99.10
logging trap informational
logging on
```

2.3. Port - Security (violation des MAC)

```

```

2.4. DHCP Snooping (serveur DHCP protégé)

Activation globalement :

```
ip dhcp snooping
ip dhcp snooping vlan 10,20,30,40,50
```

Marquer les ports trusted (vers serveur DHCP ou routeur) :

```
interface GigabitEthernet0/1
ip dhcp snooping trust
```

Logs spécifiques :

```
ip dhcp snooping information option allow-untrusted
```

2.6. Spanning Tree (STP)

```
spanning-tree logging
```

2.7. Interface up/down :

Pour forcer logs :

```
interface range Fa0/1 - 48
   logging event link-status
```

Mission 4 — Mettre en place le serveur de logs (rsyslog)

Objectif : Réceptionner les logs en **UDP/TCP 514** sur une VM Debian/Ubuntu.
Sur PC Ubuntu :

Activer la réception des logs :

```
sudo nano /etc/rsyslog.conf
```

Décommenter :

```
module(load="imudp")
input(type="imudp" port="514")
```

Redémarrer :

```
sudo systemctl restart rsyslog
```

Pour voir les logs :

```
sudo tail -f /var/log/syslog
```

PuTTy routeur + switch :

Activer l'horodatage :

```
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
```

Logs interfaces (UP/DOWN) Switch et Routeur :

```
logging event link-status
```

5. ACL avec logs (seulement Routeur)

```
ip access-list extended SECURITE
   deny ip any any log
   permit ip any any

interface gi0/0/0
   ip access-group SECURITE in

interface gi0/0/1
   ip access-group SECURITE in
```

Port-Security (Switch) :

Téléphone + PC téléphone :

```
interface range fa0/6 , fa0/7, fa0/8
   switchport mode access
   switchport port-security
   switchport port-security maximum 2
   switchport port-security mac-address sticky
   switchport port-security violation restrict
```

CaméraIP :

```
interface range fa0/19 , fa0/20
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security mac-address sticky
   switchport port-security violation shutdown
```

Sur PC Ubuntu :

Activer la réception des logs :

```
sudo nano /etc/rsyslog.conf
```

Décommenter :

```
module(load="imudp")
input(type="imudp" port="514")
```

Redémarrer :

```
sudo systemctl restart rsyslog
```

Pour voir les logs :

```
sudo tail -f /var/log/syslog
```


Mission 5 — Déployer NTP + logs sur toute l’infra

Objectif : Appliquer NTP et logging sur tous les routeurs & switchs de la maquette (plan d’E3)
--> Utilisation des missions 1 et 3.
Le contrôler :

```
show run | include ntp|logging
show clock
```

Vérifier coté rsyslog --> OK ?
avec --> sudo tail -f /var/log/syslog

Mission 6 — NAS Synology (stockage & sauvegardes)

Objectif : Mettre en place du stockage réseau (partages), pour sauvegardes de configs et vidéo.

--> https://www.cnil.fr/fr/la-videosurveillance-au-travail

--> https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf

Étapes

1. **Brancher** le NAS sur le **switch** (VLAN défini par E3). Obtenir l'IP (DHCP ou statique).
2. **Accéder** à **DSM** : navigateur → `http://IP_NAS:5000`.
3. **Créer volumes** (SHR/RAID1 selon nb de disques), **Btrfs** recommandé.
4. **Créer partages** :
   - `Cisco_logs`
   - `cameras`
5. **Activer protocoles** : **SMB** (Windows), **NFS** si nécessaire.
6. **Comptes & droits** : créer groupes/profils.
7. **Rétention** : activer **snapshots** / quotas si Btrfs.

Installation et configuration un NAS

1. Objectif
Le but du NAS est de regrouper toutes les données et de garder les vidéos des caméras de surveillance. On peut regarder les vidéos jusqu'à une semaine en arrière, comme demandé dans le projet IRS-SI.

NAS utilisé : Synology DS920+

2. Matériels
• NAS Synology DS920+ avec des disques durs faits pour ça

• Caméras IP qui marchent avec ONVIF
• Switch et routeur pour le réseau
• Adresse IP fixe pour le NAS

3. Installer le système DSM
Après avoir installé le NAS et branché au réseau, on installe DSM via le site suivant :

```
https://find.synology.com
```

Une fois le NAS déctecté :

- Installation automatique de DSM
- Création d'un compte administrateur bien protégé pendant cette étape (mot de passe fort).

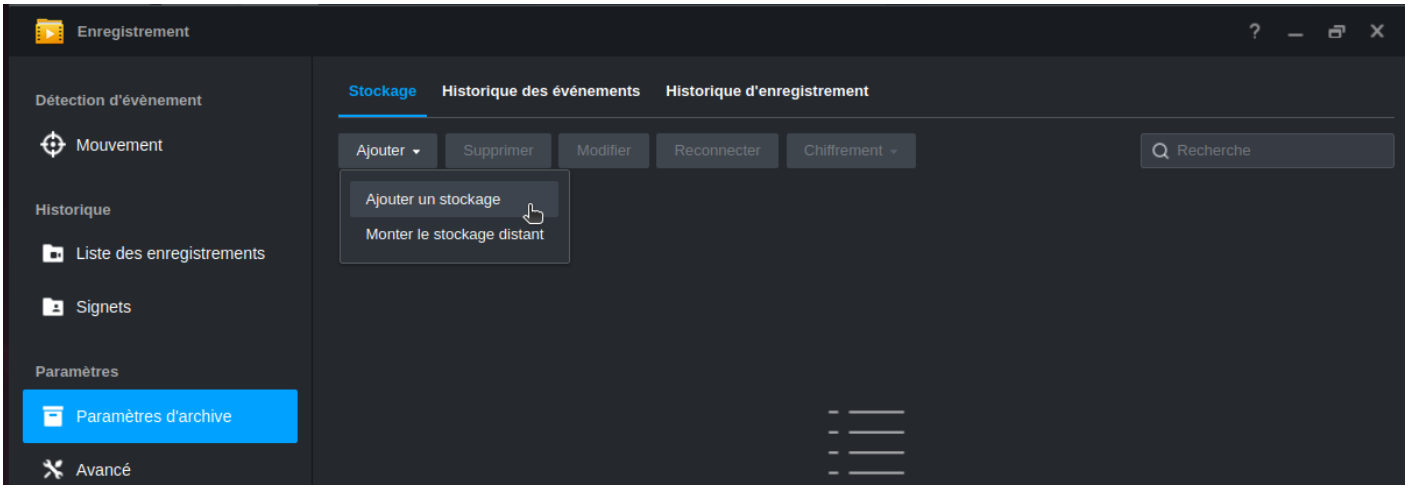
4. Régler l'heure et le NTP
On met le fuseau horaire sur Europe/Paris. L'heure se règle avec le serveur NTP, comme ça les vidéos et les infos du système ont la bonne heure. --> Si internet fonctionnel

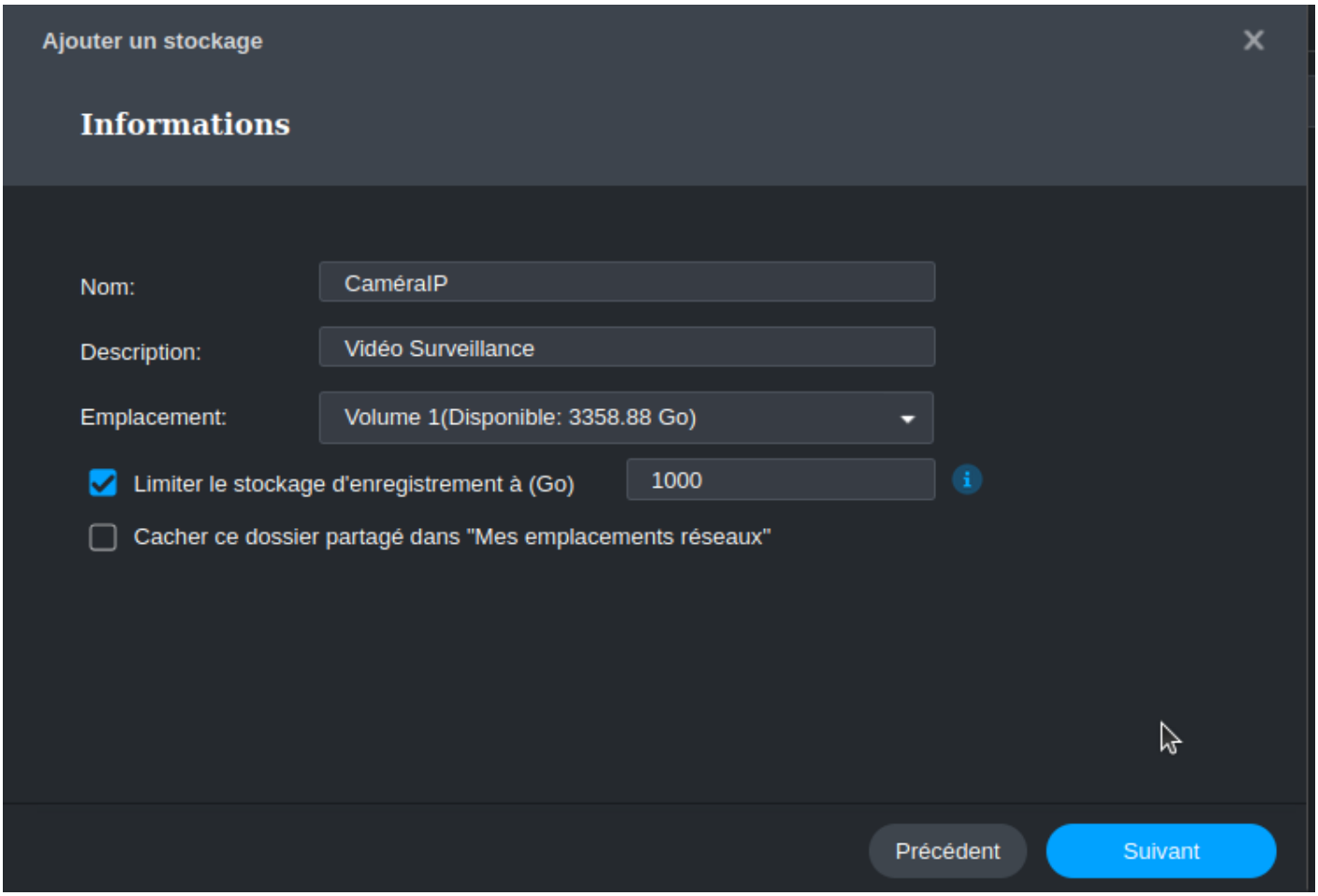
```
fr.pool.ntp.org
```

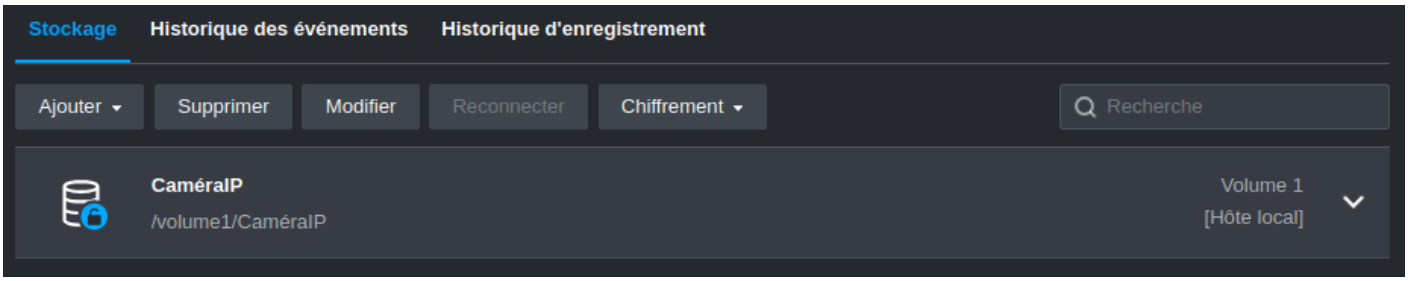
Cette configuration garantit un horodatage fiable des vidéos et des journaux système.

5. Configurer le stockage

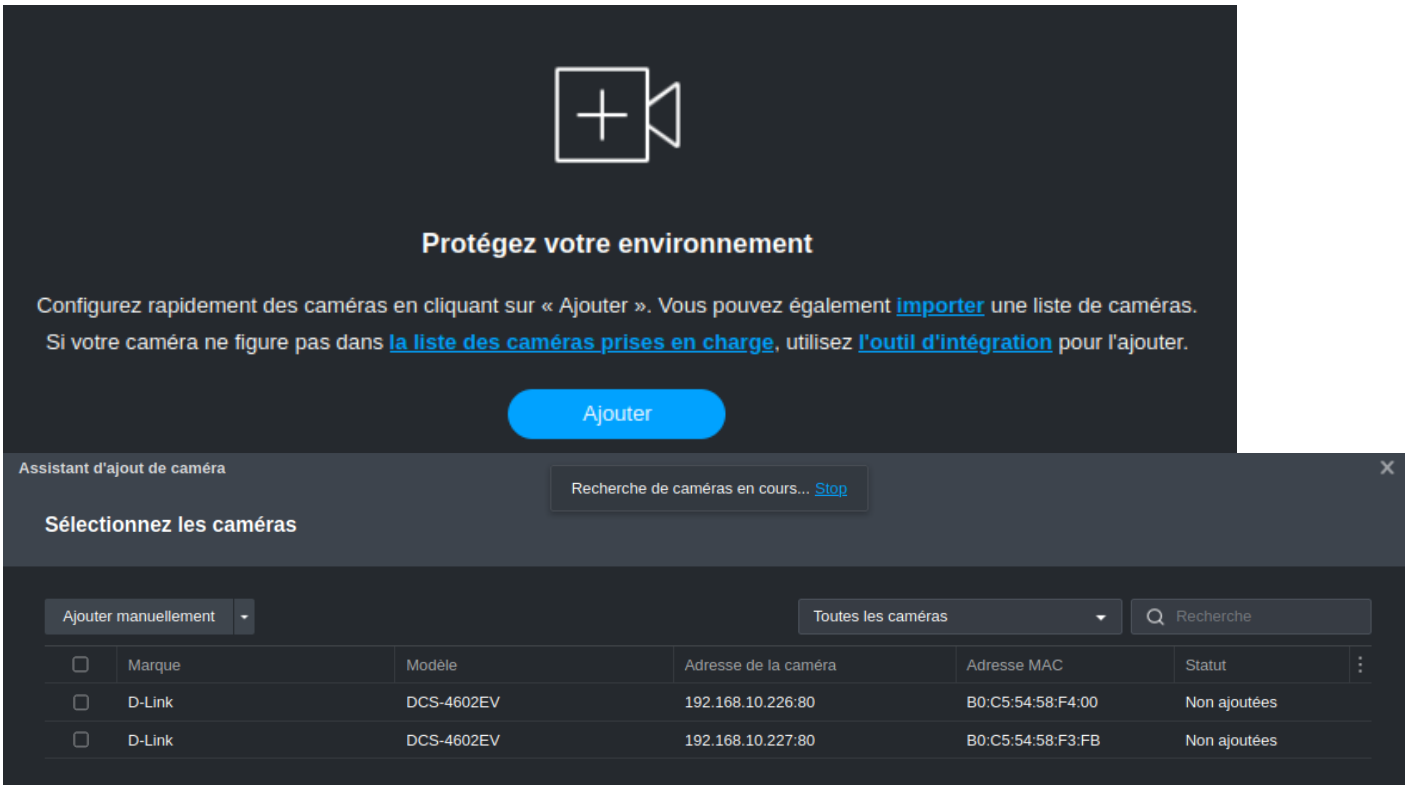
On installe Surveillance Station depuis le Centre de paquets DSM (dans le NAS).
On ouvre l'application "Enregistrement", on crée un espace de stockage SHR avec un volume en Btrfs, pour éviter de perdre des données en cas de problème.





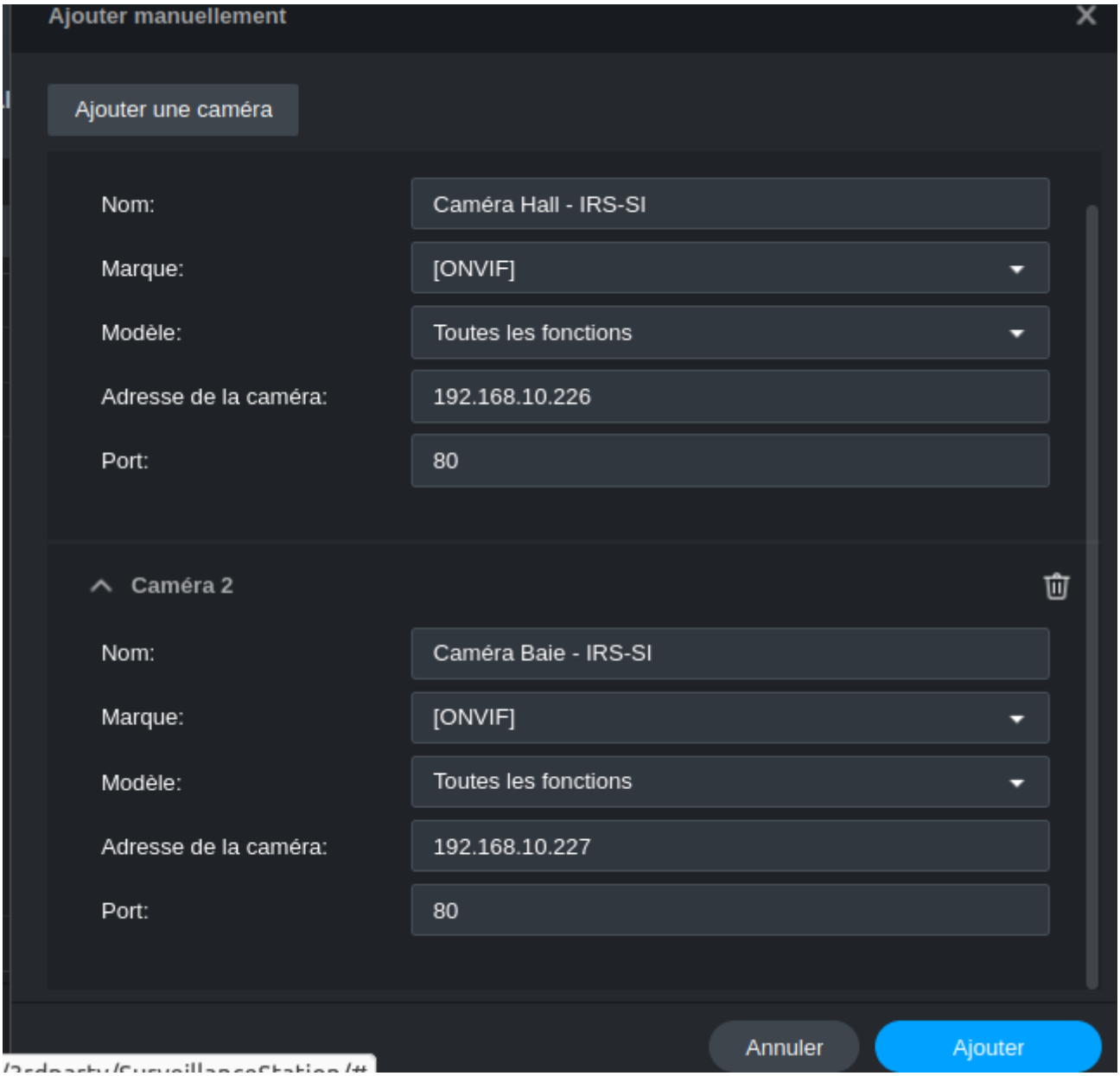


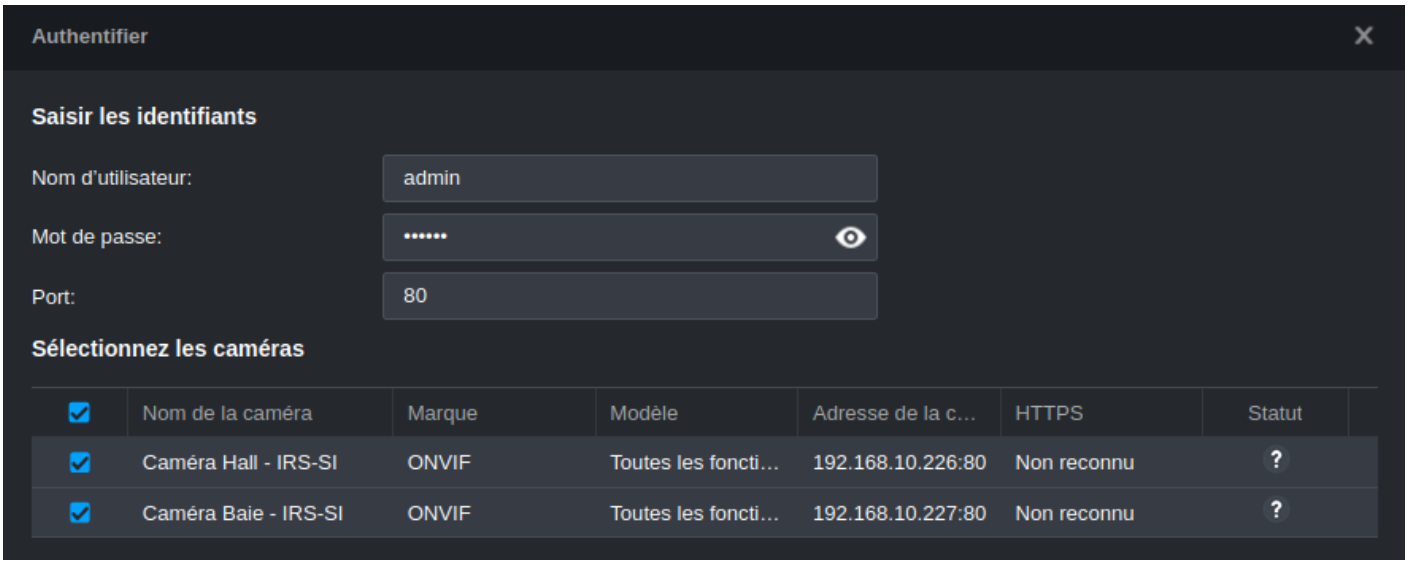
6. Installer la vidéosurveillance
On ajoute les caméras IP :

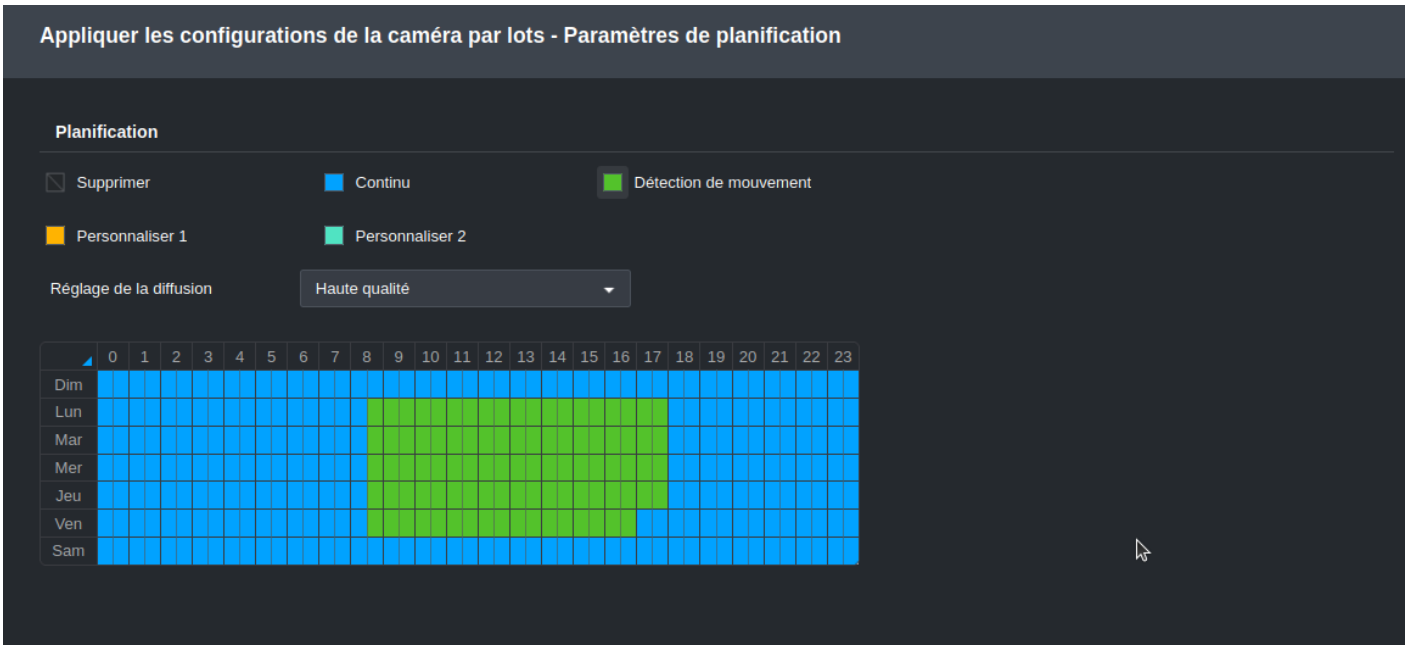


On les sélectionne, et puis on les configurent :

- Via le protocole ONVIF
- Avec leurs adresses IP et identifiants (Authentifier)
- Test de connexion validé

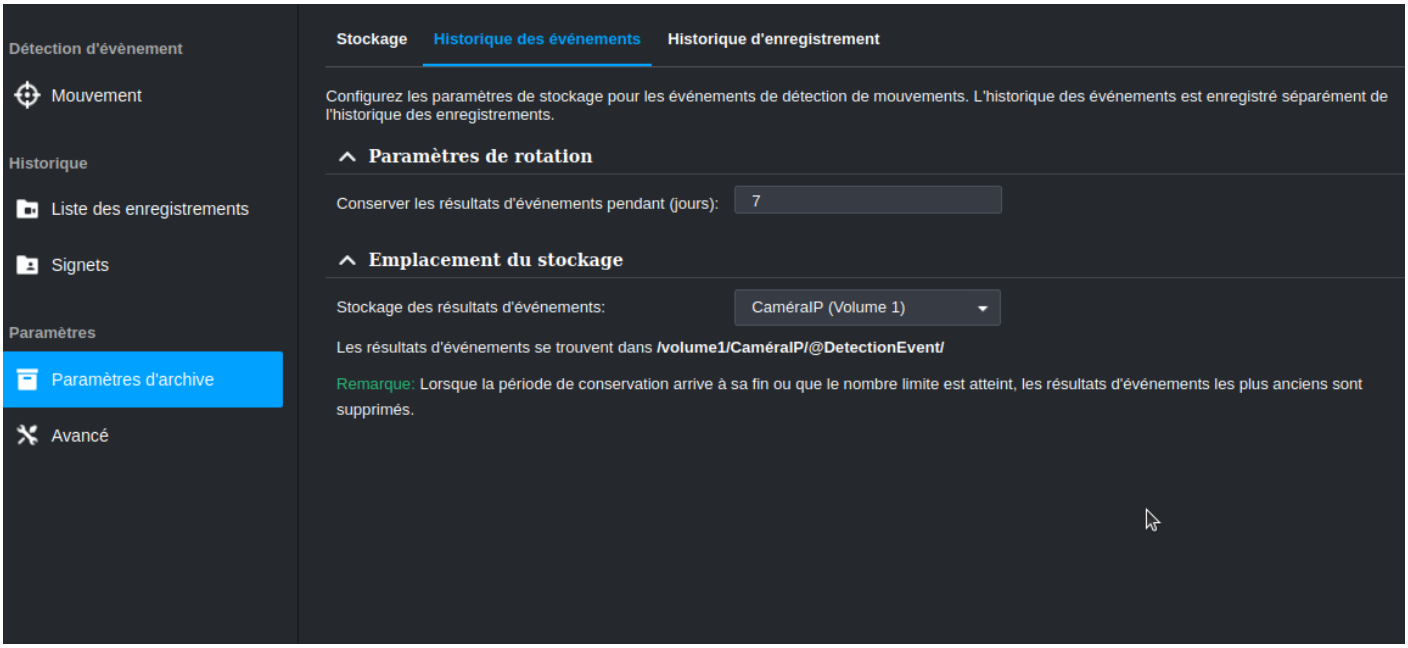

Ajouter manuellement
Ajouter une caméra
Nom:
Caméra Hall - IRS-SI
Marque:
[ONVIF]
Modèle:
Toutes les fonctions
Adresse de la caméra:
192.168.10.226
Port:
80
Caméra 2
Nom:
Caméra Baie - IRS-SI
Marque:
[ONVIF]
Modèle:
Toutes les fonctions
Adresse de la caméra:
192.168.10.227
Port:
80
Annuler
Ajouter


Authentifier
Saisir les identifiants
Nom d'utilisateur:
admin
Mot de passe:
Port:
80
Sélectionnez les caméras
Nom de la caméra
Marque
Modèle
Adresse de la c…
HTTPS
Statut
Caméra Hall - IRS-SI
ONVIF
Toutes les foncti…
192.168.10.226:80
Non reconnu
Caméra Baie - IRS-SI
ONVIF
Toutes les foncti…
192.168.10.227:80
Non reconnu



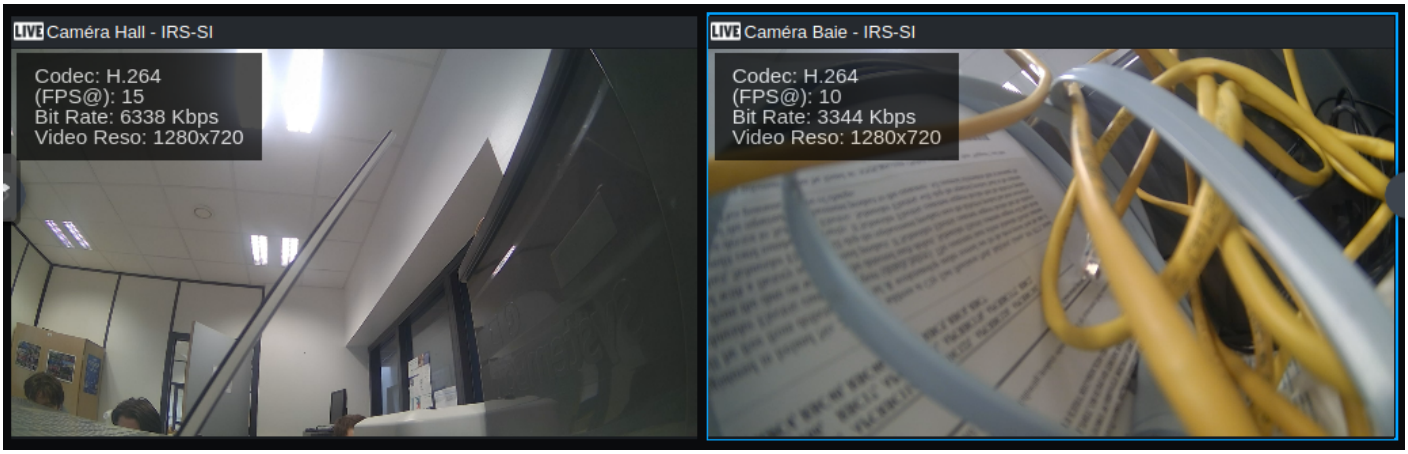
On ajoute la plage horaire les comportement des caméras IP souhaitées.
On prend en compte les horaire de la PME fictive, selon les règles de la CNIL et les recommandation de l'ANSSI, avec citations.

7. Garder les vidéos
On met une règle pour garder les vidéos une semaine max (7 jours), après elles s'effacent automatiquement.



8. Sécuriser l'accès
On crée des comptes pour chaque personne avec des droits limités pour la consultation des vidéos. Seules les personnes autorisées peuvent accéder à DSM et Surveillance Station.

9. Vérifications
On vérifie que les vidéos s'enregistrent bien, qu'on peut les regarder, qu'elles s'effacent après une semaine et que l'heure est bonne.



Note : Utilisation d'une basse qualité de caméra pour en garde une visibilité pour économiser du stockage.

Mission 7 — Caméra IP D-Link DCS-4602EV (rétention 7 jours)

Objectif :
Le but du NAS est de regrouper toutes les données et de garder les vidéos des caméras de surveillance. On peut regarder les vidéos jusqu'à une semaine en arrière, comme demandé dans le projet IRSISI.
Sources à utiliser :

--> https://www.cnil.fr/fr/la-videosurveillance-au-travail

--> https://www.cnil.fr/sites/cnil/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf

Alimentation : switch **PoE** (ou injecteur).

Découverte IP : via DHCP/switch (`show dhcp binding` si relay) ou scan.

Connexion web : `http://IP_CAMERA` → **changer mot de passe** admin, vérifier **firmware**.

Intégration NAS :

- NAS → **Surveillance Station** → **Ajouter** caméra → modèle **D-Link DCS-4602EV** → saisir IP/login.
- **Définir rétention** : 7 jours pour le dossier `cameras`.

Test : déclencher mouvement, vérifier lecture et purge > 7 jours.

---

2. Matériels
• NAS Synology DS920+ avec des disques durs faits pour ça
• Caméras IP qui marchent avec ONVIF
• Switch et routeur pour le réseau
• Adresse IP fixe pour le NAS

3. Installer le système DSM
Après avoir installé le NAS et branché au réseau, on installe DSM via le site suivant :

```
https://find.synology.com
```

Une fois le NAS déctecté :

- Installation automatique de DSM
- Création d'un compte administrateur bien protégé pendant cette étape (mot de passe fort).

4. Régler l'heure et le NTP
On met le fuseau horaire sur Europe/Paris. L'heure se règle avec le serveur NTP, comme ça les vidéos et les infos du système ont la bonne heure.

```
fr.pool.ntp.org
```

Cette configuration garantit un horodatage fiable des vidéos et des journaux système.

5. Configurer le stockage
On crée un espace de stockage SHR avec un volume en Btrfs, pour éviter de perdre des données en cas de problème.

6. Installer la vidéosurveillance
On installe Surveillance Station depuis le Centre de paquets DSM.

Les caméras IP sont ajoutées :

- Via le protocole ONVIF
- Avec leurs adresses IP et identifiants
- Test de connexion validé

7. Garder les vidéos
On met une règle pour garder les vidéos une semaine max (7 jours), après elles s'effacent automatiquement.

8. Sécuriser l'accès
On crée des comptes pour chaque personne avec des droits limités pour la consultation des vidéos. Seules les personnes autorisées peuvent accéder à DSM et Surveillance Station.

9. Vérifications
On vérifie que les vidéos s'enregistrent bien, qu'on peut les regarder, qu'elles s'effacent après une semaine et que l'heure est bonne.

Pour conclure
Le NAS Synology DS920+ est top pour garder et utiliser les vidéos de surveillance du projet IRSI-SI. Il est fiable, bien protégé et fait ce qu'on lui demande.

Mission 8 — Fiches outils Kali (étude & documentation)

Objectif : Pour chaque outil (Nmap, Wireshark, arp-scan/DAI, DHCP tools, Aircrack-ng, Hydra), fournir une fiche simple : pourquoi dans IRS, comment l’utiliser, risques/éthique, preuves.

--> Kali Linux MV

```
# Nmap (exemples)
nmap -sn 172.16.10.0/24
nmap -sS -sV -p 22,80,443 172.16.10.1
```

Risques/limites : bruit réseau si scans agressifs → faire ça sur VLAN de test uniquement.
Éthique/légalité : périmètre maquette, accord prof
Preuves : captures de sortie + entrée syslog correspondante (horodatée via NTP)

Mission 9 — Tester les protections avec Kali

Objectif : Prouver que Port-Security, DHCP Snooping, Dynamic ARP Inspection, ACL/pare-feu, Wi-Fi résistent, et que tout est journalisé sur le serveur de logs.
Cas de test :

Port-Security

1. Brancher PC-A (MAC-1) → OK.
2. Remplacer par Kali (MAC-2) → violation attendue.
3. Vérifier :

```
show port-security interface GiX/Y
show logging
```

--> Sur rsyslog, il doit y avoir une alerte !!!

DHCP Snooping
Sur Kali :

```
sudo dhclient -v eth0
```

--> Tenter faux serveur (sur port non-trusted) --> Il doit échouer côté client

Vérifier dans Wireshark --> Filtrer "bootp" + logs switch.

DAI (ARP Inspection)
Observation de l'ARP :

```
sudo arp-scan --interface eth0 --localnet
```

Tenter ARP spoof (poste de test) --> DAI doit le bloquer

Pour le contrôler :

```
show ip arp inspection statistics
show logging
```

--> Faire une capture Wireshark filtre arp

ACL/Pare-feu routeur

Depuis Kali (VLAN test), scanner services admin routeur/NAS :

```
nmap -sS -p 22,23,80,443,161,514 (IP routeur)
```

Essais directs (doivent normalement échouer) :

```
ssh admin@172.16.0.1
curl -k https://172.16.0.1
```

→ Attendu : **inaccessible** (filtré). Logs côté routeur/rsyslog

Borne de test
Recon :

```
sudo airmon-ng start wlan0
airodump-ng wlan0mon
```

Traçabilité
Test

```
sudo tail -f /var/log/syslog
```

Heure (NTP) cohérent et avec des événements (routeur + switch).

BONUS (IL FAUT DEMANDER) :

- **Ettercap/Bettercap** (démonstration DAI)
- **John the Ripper** (hash fourni)

Pour effectuer un test de pénétration sur une borne WiFi en utilisant Kali Linux, vous pouvez suivre ces étapes et utiliser les commandes appropriées. Ces étapes simulent une attaque pour évaluer les vulnérabilités du réseau WiFi.

1. **Analyse du réseau WiFi**

Commande : `airodump-ng`

Description : Cette commande permet de scanner les réseaux WiFi disponibles et de capturer les paquets pour analyser les trames de données.

Exemple :

airodump-ng wlan0

2. **Détection des clients connectés**

Commande : `airodump-ng`

Description : Vous pouvez utiliser `airodump-ng` pour détecter les clients connectés à un réseau WiFi spécifique.

Exemple :

```
airodump-ng --bssid <BSSID> -c <channel> wlan0
```

3. **Capture des paquets de données**

Commande : `airodump-ng`

Description : Capturez les paquets de données pour analyser les trames de données et détecter les vulnérabilités.

Exemple :

```
airodump-ng --bssid <BSSID> -c <channel> -w capture wlan0
```

4. **Déchiffrement des paquets WEP**

Commande : `aircrack-ng`

Description : Utilisez `aircrack-ng` pour déchiffrer les paquets WEP capturés.

Exemple :

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

5. **Attaque de type Deauthentication**

Commande : `aireplay-ng`

Description : Forcez les clients à se reconnecter pour capturer des paquets de données.

Exemple :

```
aireplay-ng --deauth 10 -a <BSSID> wlan0
```

6. **Attaque de type WPA/WPA2 PSK**

Commande : `aircrack-ng`

Description : Utilisez `aircrack-ng` pour attaquer les réseaux WPA/WPA2 en utilisant une attaque par force brute.

Exemple :

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

7. **Analyse des vulnérabilités**

Commande : `nmap`

Description : Utilisez `nmap` pour scanner les ports ouverts et détecter les vulnérabilités sur les périphériques connectés.

Exemple :

```
nmap -sV <target_ip>
```

8. **Exploitation des vulnérabilités**

Commande : `metasploit`

Description : Utilisez Metasploit pour exploiter les vulnérabilités détectées.

Exemple :

```
msfconsole
use exploit/<path_to_exploit>
set RHOST <target_ip>
run
```

9. **Post-exploitation**

Commande : `metasploit`

Description : Après avoir exploité une vulnérabilité, vous pouvez utiliser Metasploit pour effectuer des actions post-exploitation, telles que l'installation de backdoors ou le vol de données.

Exemple :

```
use post/windows/gather/credentials
set SESSION <session_id>
run
```

Ces commandes et étapes vous permettront de réaliser un test de pénétration complet sur une borne WiFi, en identifiant et exploitant les vulnérabilités potentielles.

10. **Capture des paquets avec Wireshark**

Commande : `wireshark`
Description : Utilisez Wireshark pour capturer et analyser les paquets réseau en temps réel. Cela peut aider à identifier des vulnérabilités spécifiques et à comprendre le trafic réseau.
Exemple :

```
wireshark
```

11. **Attaque de type Evil Twin**

Commande : `hostapd`
Description : Créez un faux point d'accès WiFi pour capturer les données des clients connectés.
Exemple :

```
hostapd /etc/hostapd.conf
```

12. **Analyse des fichiers de configuration**

Commande : `cat`
Description : Examinez les fichiers de configuration des réseaux WiFi pour identifier des informations sensibles ou des vulnérabilités.
Exemple :

```
cat /etc/hostapd.conf
```

13. **Utilisation de Kismet**

Commande : `kismet`
Description : Kismet est un outil de détection et d'analyse des réseaux sans fil. Il peut être utilisé pour scanner les réseaux WiFi et détecter les vulnérabilités.
Exemple :

```
kismet
```

14. **Attaque de type Man-in-the-Middle (MitM)**

Commande : `ettercap`

Description : Utilisez Ettercap pour intercepter et manipuler le trafic réseau entre deux parties.
Exemple :

```
ettercap -G
```

15. **Analyse des vulnérabilités avec Nessus**

Commande : `nessus`
Description : Nessus est un outil de scan de vulnérabilités qui peut être utilisé pour identifier les failles de sécurité sur les réseaux WiFi.
Exemple :

```
nessus
```

16. **Exploitation des vulnérabilités avec Metasploit**

Commande : `metasploit`
Description : Utilisez Metasploit pour exploiter les vulnérabilités identifiées. Metasploit offre une large gamme d'exploits et de payloads pour différentes vulnérabilités.
Exemple :

```
msfconsole

use exploit/<path_to_exploit>

set RHOST <target_ip>
run
```

17. **Post-exploitation avec Metasploit**

Commande : `metasploit`
Description : Après avoir exploité une vulnérabilité, vous pouvez utiliser Metasploit pour effectuer des actions post-exploitation, telles que l'installation de backdoors ou le vol de données.
Exemple :

```
use post/windows/gather/credentials

set SESSION <session_id>
run
```

18. **Analyse des logs**

Commande : `tail`
Description : Examinez les logs des systèmes pour identifier des activités suspectes ou des vulnérabilités.
Exemple :

```
tail -f /var/log/syslog
```

19. **Utilisation de Reaver**

- **Commande** : `reaver`

- **Exemple :**

- **Commande :** `wireshark`
- **Description :** Utilisez Wireshark pour capturer et analyser les paquets réseau en temps réel. peut aider à identifier des vulnérabilités spécifiques et à comprendre le trafic réseau.

Mission 10 — Scripts d’automatisation (optionnels mais utiles)

Objectif : Gagner du temps et produire des preuves horodatées automatiquement.
Script auto 1 :

```
#!/usr/bin/env bash
TS=$(date +%F_%H%M%S)
nmap -sS -p 22,80,443 172.16.10.0/24 -oN scan_$TS.txt
```

Script auto 2 :

```
#!/usr/bin/env bash
TS=$(date +%F_%H%M%S)
grep -Ei 'SEC|ARP|DAI|DHCP|PORT-SEC|ACL' /var/log/syslog > events_$TS.log
```

9.2 Kali video / doc

Utilisés pour décoder ou récupérer un mot de passe
Ex : **John the Ripper**, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, et Medusa

--> https://www.youtube.com/watch?v=wj-moIzMJtI

Vulnérabilité du résolveur DNS Outils de piratage sans fil
Ex : **Aircrack-ng**, Kismet, InSSIDer, KisMAC, Firesheep et NetStumbler

--> https://www.youtube.com/watch?v=9bEovGdMPtc

Analyse et de piratage réseau sonder les périphériques réseau, les serveurs et hôtes pour les ports TCP ou UDP ouverts
Ex : Nmap, SuperScan, Angry IP Scanner, et NetScanTools

--> https://www.youtube.com/watch?v=dkmTVVmiG5A

Outils de création de paquets peut nécessiter le redémarrage du résolveur ouvert DNS ou des services
sonder et tester robustesse d'un pare-feu en utilisant des paquets spécialement conçus
Ex : Hping, Scapy, **Socat**, Yersinia, Netcat, Nping, et Nemesis

--> https://www.youtube.com/watch?v=vX5YZ1jO7Zo

Renifleurs de paquets l'acteur de menace envoie deux réponses ARP usurpées gratuitement en utilisant sa propre adresse MAC pour les adresses IP de destination indiquées.
Utilisés pour capturer et analyser les paquets au sein de LAN Ethernet ou WLAN
Ex : Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, et SSLstrip

--> https://www.youtube.com/watch?v=M0hZ5ko32is

Détecteurs de rootkit vérificateur d'intégrité des répertoires et des fichiers utilisé par les chapeaux blancs pour détecter les root kits installés.
Ex : AIDE, Netfilter et PF: OpenBSD Packet Filter

--> https://www.youtube.com/watch?v=ZtI4QhOZLNM

Fuzzers Générateurs de bruits pour rechercher des vulnérabilités
Ex : Skipfish, Wapiti, et W3af

--> https://www.youtube.com/watch?v=kIIeLA78E-k

Outils d'investigation : Utilisés par les pirates à chapeau blanc pour flairer toute trace de preuves existant dans un ordinateur
Ex : Maltego, Helix, Maltego, et Encase

-->

Débogueurs
Utilisés par les chapeaux noirs pour faire de l'ingénierie inverse sur des fichiers binaires lors de l'écriture d'exploits.
Attaquant doit usurper l'adresse IP d'un hôte prédire le numéro de séquence suivant et envoyer un ACK à l'autre hôte
également utilisés par les chapeaux blancs lors de l'analyse des logiciels malveillants
Ex : GDB, WinDbg, IDA Pro et **Immunity Debugger**

--> https://www.youtube.com/watch?v=iQf1OvTREvg

OS de piratage
OS spécialement conçus, préchargés avec des outils optimisés pour le piratage
Ex : Kali Linux, Knoppix, BackBox Linux

-->

Outils de chiffrement
coder les données afin d'empêcher tout accès non autorisé aux données cryptées
Ex : VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN et Stunnel

--> https://www.youtube.com/watch?v=J2JKh9mOy8U

--> https://www.youtube.com/watch?v=6CqT96d4-8Y

Outils d'exploitation des vulnérabilités
Déterminer si un hôte distant est vulnérable à une attaque de sécurité
Ex : Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, et Netsparker

--> https://www.youtube.com/shorts/jBTW8wWnkqU

Analyseurs devulnérabilité
Analysent un réseau ou un système pour identifier les ports ouverts
utilisé également pour rechercher vulnérabilités connues et analyser les MV, BYOD périphériques et BDD client
Ex : Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, et Open VAS

--> https://www.youtube.com/watch?v=EaA5pLAwnkc
--> https://www.youtube.com/watch?v=vvp_OnKjhik

Kali linux sans internet

1. **Scan des réseaux WiFi**

- **Commande :** `airodump-ng`
- **Description :** Utilisez `airodump-ng` pour scanner les réseaux WiFi disponibles et capturer les paquets pour analyser les trames de données.
- **Exemple :**

```
airodump-ng wlan0
```

2. **Détection des clients connectés**

- **Commande :** `airodump-ng`
- **Description :** Vous pouvez utiliser `airodump-ng` pour détecter les clients connectés à un réseau WiFi spécifique.
- **Exemple :**

```
airodump-ng --bssid <BSSID> -c <channel> wlan0
```

3. **Capture des paquets de données**

- **Commande :** `airodump-ng`
- **Description :** Capturez les paquets de données pour analyser les trames de données et détecter les vulnérabilités.
- **Exemple :**

```
airodump-ng --bssid <BSSID> -c <channel> -w capture wlan0
```

4. **Déchiffrement des paquets WEP**

- **Commande :** `aircrack-ng`
- **Description :** Utilisez `aircrack-ng` pour déchiffrer les paquets WEP capturés.
- **Exemple :**

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

5. **Attaque de type Deauthentication**

- **Commande :** `aireplay-ng`
- **Description :** Forcez les clients à se reconnecter pour capturer des paquets de données.
- **Exemple :**

```
aireplay-ng --deauth 10 -a <BSSID> wlan0
```

6. **Attaque de type WPA/WPA2 PSK**

- **Commande :** `aircrack-ng`
- **Description :** Utilisez `aircrack-ng` pour attaquer les réseaux WPA/WPA2 en utilisant une attaque par force brute.
- **Exemple :**

```
aircrack-ng -b <BSSID> -w <wordlist> capture-01.cap
```

7. **Analyse des vulnérabilités**

- **Commande :** `nmap`
- **Description :** Utilisez `nmap` pour scanner les ports ouverts et détecter les vulnérabilités sur les périphériques connectés.
- **Exemple :**

```
nmap -sV <target_ip>
```

8. **Exploitation des vulnérabilités**

- **Commande :** `metasploit`
- **Description :** Utilisez Metasploit pour exploiter les vulnérabilités détectées.
- **Exemple :**

```
msfconsole

use exploit/<path_to_exploit>

set RHOST <target_ip>
run
```

9. **Post-exploitation**

- **Commande :** `metasploit`
- **Description :** Après avoir exploité une vulnérabilité, vous pouvez utiliser Metasploit pour effectuer des actions post-exploitation, telles que l'installation de backdoors ou le vol de données.
- **Exemple :**

```
use post/windows/gather/credentials

set SESSION <session_id>
run
```

10. **Capture des paquets avec Wireshark**

- **Commande :** `wireshark`

- **Description :** Utilisez Wireshark pour capturer et analyser les paquets réseau en temps réel. Cela peut aider à identifier des vulnérabilités spécifiques et à comprendre le trafic réseau.
- **Exemple :**

```
wireshark
```

11. **Attaque de type Evil Twin**

- **Commande :** `hostapd`
- **Description :** Créez un faux point d'accès WiFi pour capturer les données des clients connectés.
- **Exemple :**

```
hostapd /etc/hostapd.conf
```

12. **Analyse des fichiers de configuration**

- **Commande :** `cat`
- **Description :** Examinez les fichiers de configuration des réseaux WiFi pour identifier des informations sensibles ou des vulnérabilités.
- **Exemple :**

```
cat /etc/hostapd.conf
```

13. **Utilisation de Kismet**

- **Commande :** `kismet`
- **Description :** Kismet est un outil de détection et d'analyse des réseaux sans fil. Il peut être utilisé pour scanner les réseaux WiFi et détecter les vulnérabilités.
- **Exemple :**

```
kismet
```

14. **Attaque de type Man-in-the-Middle (MitM)**

- **Commande :** `ettercap`
- **Description :** Utilisez Ettercap pour intercepter et manipuler le trafic réseau entre deux parties.
- **Exemple :**

```
ettercap -G
```

15. **Analyse des logs**

- **Commande :** `tail`
- **Description :** Examinez les logs des systèmes pour identifier des activités suspectes ou des vulnérabilités.
- **Exemple :**

```
tail -f /var/log/syslog
```