RAPPORT DE PROJET SAE 4.01 : SÉCURISER UN SYSTÈME D'INFORMATION

Auteur : Pierre FAMCHON
Formation : R&T - 2ème Année
Année : 2024-2025

Table des matières :

1.Introduction

Objectif :

Ce projet vise à renforcer la sécurité d'une infrastructure réseau multi-sites en implémentant deux mécanismes principaux :

- La protection de la résolution DNS via DNSSEC pour garantir l'authenticité des réponses DNS.
- La sécurisation des communications web (HTTP/HTTPS) à l'aide de certificats SSL/TLS et d'un Web Application Firewall (WAF).

Ces mécanismes permettent de réduire les risques d'attaques telles que l'empoisonnement de cache DNS, les attaques MITM (Man-in-the-Middle) et les injections web, que nous testerons avec OWASP ZAP et Wireshark.

Contexte :

L'infrastructure comporte deux sites reliés par un tunnel IPSEC, avec trois réseaux cloisonnés (« Service », « Production » et « Admin »).

Les serveurs critiques (DNS et Web) sont hébergés dans le réseau «Admin» pour limiter leur exposition.

Répartition des tâches :

Sécurisation DNS	BACHART Michel
Sécurisation Web	DUVAL Baptiste
Recommandation ANSSI	EDOUARD Nicolas
Tests de sécurité	FAMCHON Pierre

2.Architecture

2.1.Description du Schéma :

- Réseaux :
  - Service : Accès utilisateur standard.
  - Production : Héberge les systèmes de production.
  - Admin : Réseau sécurisé pour la gestion des serveurs.
- Serveurs critiques :
  - Serveur DNS (BIND) : Gère les zones DNS signées avec DNSSEC.
  - Serveur Web (Nginx) : Fournit des services HTTP/HTTPS et est protégé par un WAF.

2.2.Adressage :

1. VLANs et Adressage IP

VLAN ID	Nom	Subnet 1	VLAN IP (3)
VLAN 10	Admin	192.168.10.0/24	192.168.11.0/24
VLAN 20	Production	192.168.20.0/24	192.168.21.0/24
VLAN 30	Service	192.168.30.0/24	192.168.31.0/24

2. Routeurs

Routeur	Interface	Adresse IP	Masque
R1	G0/0	10.10.50.2	/24
	G0/1	60.10.50.2	/24
	Tunnel	192.168.100.1	/30
R3	G0/0	20.20.50.2	/24
	G0/1	60.10.50.6	/24
	G0/2	192.168.100.2	/30

3. Switch de niveau 3 (Multilayer)

Switch	Int	VLAN	Adresse IP	Masque
L3_Siege	F0/1	VLAN 10	192.168.10.254	/24
	F0/2	VLAN 20	192.168.20.254	/24
	F0/3	VLAN 30	192.168.30.254	/24
	G0/1	-	10.10.40.2	/24
L3_Succu	F0/1	VLAN 10	172.31.10.254	/24
	F0/2	VLAN 20	172.31.20.254	/24
	F0/3	VLAN 30	172.31.30.254	/24
	G0/1	-	20.20.40.2	/24

4. PC et Affectation d'Adresses

PC	VLAN	Adresse IP	Passerelle
Admin_Siege	VLAN 10	192.168.10.11	192.168.10.254
Production_Siege	VLAN 20	192.168.20.11	192.168.20.254
Service_Siege	VLAN 30	192.168.30.11	192.168.30.254
Admin_Succu	VLAN 10	172.31.10.11	172.31.10.254
Production_Succu	VLAN 20	172.31.20.11	172.31.20.254
Service_Succu	VLAN 30	172.31.30.11	172.31.30.254

3.Mise en oeuvre

3.1.Configuration équipements réseaux

3.1.1.Routeurs :

R1

```
! Définit un nom d'utilisateur avec un mot de passe crypté et privilège 15
username admin privilege 15 secret 5
$1$mERr$tN2nmMK5hNorN4zAZEGGz.
!
! Activation du protocole SSH pour sécuriser les connexions à distance
ip ssh version 2
! Définit le nom de domaine pour la machine
ip domain-name reseau.local
!
! Activation du mode PVST
spanning-tree mode pvst
!
! Configuration de l'interface Tunnel0 pour une connexion VPN
interface Tunnel0
ip address 192.168.100.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/1  ! Spécifie l'interface source pour le tunnel
tunnel destination 60.10.50.6  ! Spécifie l'adresse IP de destination du tunnel
!
! Configuration de l'interface GigabitEthernet0/0 avec une adresse IP
interface GigabitEthernet0/0
ip address 10.10.50.2 255.255.255.0
ip nat inside
duplex auto
speed auto
!
! Configuration de l'interface GigabitEthernet0/1 avec une adresse IP
interface GigabitEthernet0/1
ip address 60.10.50.2 255.255.255.252
ip nat inside
duplex auto
speed auto
```

```
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
! Configuration de la fonction de routage
ip classless
ip route 192.168.10.0 255.255.255.0 10.10.50.1  ! Route  192.168.10.0 via 10.10.50.1
ip route 192.168.20.0 255.255.255.0 10.10.50.1
ip route 192.168.30.0 255.255.255.0 10.10.50.1
ip route 192.168.100.0 255.255.255.0 60.10.50.1  ! Route 192.168.100.0 via
60.10.50.1
ip route 172.31.20.0 255.255.255.0 192.168.100.2  ! Route  172.31.20.0 via
192.168.100.2
ip route 172.31.30.0 255.255.255.0 192.168.100.2
ip route 172.31.10.0 255.255.255.0 192.168.100.2
ip route 10.10.40.0 255.255.255.0 10.10.50.1
ip route 10.10.50.0 255.255.255.0 10.10.50.1
ip route 10.10.50.0 255.255.255.0 GigabitEthernet0/0 ! Route vers le réseau
10.10.50.0 via l'interface GigabitEthernet0/0
ip route 60.10.50.6 255.255.255.255 60.10.50.1
ip route 20.20.40.0 255.255.255.0 192.168.100.2
ip route 20.20.50.0 255.255.255.0 192.168.100.2
ip route 10.10.50.0 255.255.255.0 192.168.100.2
ip route 172.31.25.0 255.255.255.0 10.10.50.1
!
ip flow-export version 9
!
line con 0  ! Configuration de console
!
line aux 0  ! Configuration de la ligne auxiliaire
!
line vty 0 4  ! Configuration des lignes VTY
login local  ! Utilisation de la base de données locale pour l'authentification
transport input ssh  ! Autorise uniquement les connexions SSH
```

R2

```
! Définit un nom d'utilisateur avec un mot de passe crypté et privilège 15
username admin privilege 15 secret 5
$1$mERr$tN2nmMK5hNorN4zAZEGGz.
!
! Activation du protocole SSH pour sécuriser les connexions à distance
ip ssh version 2
! Définit le nom de domaine pour la machine
ip domain-name reseau.local
!
! Activation du mode PVST
spanning-tree mode pvst
!
!
! Configuration de l'interface Tunnel0 pour une connexion VPN
interface Tunnel0
ip address 192.168.100.2 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/1
tunnel destination 60.10.50.2
!
! Configuration de l'interface GigabitEthernet0/0 avec une adresse IP
interface GigabitEthernet0/0
ip address 20.20.50.2 255.255.255.0
ip nat inside
duplex auto
speed auto
!
! Configuration de l'interface GigabitEthernet0/1 avec une adresse IP
interface GigabitEthernet0/1
ip address 60.10.50.6 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
```

```
no ip address
shutdown
!
! Configuration de la fonction de routage
ip classless
ip route 172.31.10.0 255.255.255.0 20.20.50.1
ip route 172.31.20.0 255.255.255.0 20.20.50.1
ip route 172.31.30.0 255.255.255.0 20.20.50.1
ip route 192.168.100.0 255.255.255.0 20.20.50.1
ip route 192.168.20.0 255.255.255.0 192.168.100.1
ip route 192.168.30.0 255.255.255.0 192.168.100.1
ip route 192.168.10.0 255.255.255.0 192.168.100.1
ip route 192.168.0.0 255.255.0.0 192.168.100.1
ip route 20.20.40.0 255.255.255.0 20.20.50.1
ip route 20.20.50.0 255.255.255.0 20.20.50.1
ip route 20.20.50.0 255.255.255.0 GigabitEthernet0/0
ip route 10.10.40.0 255.255.255.0 192.168.100.1
ip route 60.10.50.2 255.255.255.255 60.10.50.5
ip route 192.168.100.0 255.255.255.0 20.20.40.1
ip route 20.20.50.0 255.255.255.0 192.168.100.1
ip route 192.168.100.0 255.255.255.0 20.20.40.2
ip route 172.31.25.0 255.255.255.0 192.168.100.1
!
ip flow-export version 9
!
!
line con 0   ! Configuration de console
!
line aux 0   ! Configuration de la ligne auxiliaire
!
line vty 0 4   ! Configuration des lignes VTY
exec-timeout 5 0   ! Déconnecte l'utilisateur inactif au bout de 5 minutes
login local   ! Utilisation de la base de données locale pour l'authentification
transport input ssh  ! Autorise uniquement les connexions SSH
!
!
!
end
```

R3

```
! Définit un nom d'utilisateur avec un mot de passe crypté et privilège 15
username admin privilege 15 secret 5
$1$mERr$tN2nmMK5hNorN4zAZEGGz.
!
! Activation du protocole SSH pour sécuriser les connexions à distance
ip ssh version 2
! Définit le nom de domaine pour la machine
ip domain-name reseau.local
!
! Activation du mode PVST
spanning-tree mode pvst
!
!
! Configuration de l'interface GigabitEthernet0/0 avec une adresse IP
interface GigabitEthernet0/0
ip address 60.10.50.1 255.255.255.252
ip ospf 1 area 0  ! Activation du protocole OSPF dans la zone 0
ip nat inside
duplex auto
speed auto
!
! Configuration de l'interface GigabitEthernet0/1 avec une adresse IP
interface GigabitEthernet0/1
ip address 60.10.50.5 255.255.255.252
ip ospf 1 area 0  ! Activation du protocole OSPF dans la zone 0
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 10.2.1.1 255.0.0.0
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
```

```
! Activation du protocole OSPF sur le routeur, avec les réseaux spécifiés dans la zone 0
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 0  ! inclue 192.168.10.0/24 dans la zone 0
network 192.168.11.0 0.0.0.255 area 0   ! inclue 192.168.11.0/24 dans la zone 0
!
! Configuration du NAT pour permettre le partage d'adresse IP entre les machines internes et externes
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip flow-export version 9
!
!
line con 0   ! Configuration de console
!
line aux 0   ! Configuration de la ligne auxiliaire
!
line vty 0 4   ! Configuration des lignes VTY
exec-timeout 5 0   ! Déconnecte l'utilisateur inactif au bout de 5 minutes
login local   ! Utilisation de la base de données locale pour l'authentification
transport input ssh  ! Autorise uniquement les connexions SSH
!
!
!
end
```

3.1.2.Switch de couche 3 :

L3_Siege (Switch) Siège

```
! Exclusion des adresses IP de la plage DHCP
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
!
! Configuration des pools DHCP pour différents VLANs
ip dhcp pool Vlan10
network 192.168.10.0 255.255.255.0  ! Plage d'adresses pour Vlan10
default-router 192.168.10.254  ! Routeur par défaut pour le VLAN 10
dns-server 10.10.10.5
ip dhcp pool Vlan20
network 192.168.20.0 255.255.255.0  ! Plage d'adresses pour Vlan20
default-router 192.168.20.254  ! Routeur par défaut pour le VLAN 20
dns-server 10.10.10.5
ip dhcp pool Vlan30
network 192.168.30.0 255.255.255.0  ! Plage d'adresses pour Vlan30
default-router 192.168.30.254  ! Routeur par défaut pour le VLAN 30
dns-server 10.10.10.5
!
! Activation du routage IP sur le switch
ip routing
!
! Définition de l'utilisateur  avec privilège administrateur) et mot de passe
sécurisé
username admin privilege 15 secret 5
$1$mERr$tN2nmMK5hNorN4zAZEGGz.
!
! Configuration de SSH pour la gestion à distance sécurisée
ip ssh version 2
ip domain-name monreseau.local  ! Définit le domaine DNS
!
! Activation du mode PVST
spanning-tree mode pvst
!
! Configuration interfaces FastEthernet pour chaque VLAN avec mode
"access"
interface FastEthernet0/1
```

```
switchport access vlan 10  ! Associe l'interface au VLAN 10
switchport mode access  ! Configure l'interface en mode "access"
!
interface FastEthernet0/2
switchport access vlan 20  ! Associe l'interface au VLAN 20
switchport mode access  ! Configure l'interface en mode "access"
!
interface FastEthernet0/3
switchport access vlan 30  ! Associe l'interface au VLAN 30
switchport mode access  ! Configure l'interface en mode "access"
!
! Configuration de l'interface FastEthernet0/4 comme un trunk
interface FastEthernet0/4
switchport trunk allowed vlan 10,20,30  ! Permet le trafic des VLANs 10, 20 et
30
!
interface FastEthernet0/5
!
! Configuration de l'interface GigabitEthernet0/1 avec une adresse IP
statique
interface GigabitEthernet0/1
no switchport
ip address 10.10.40.2 255.255.255.0  ! Attribue une adresse IP à l'interface
duplex auto
speed auto
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
! Configuration de l'interface Vlan10 avec une adresse IP et HSRP
interface Vlan10
mac-address 0006.2aec.7001
ip address 192.168.10.254 255.255.255.0  ! Adresse IP de l'interface
standby 10 ip 10.10.10.1  ! IP virtuelle HSRP pour le VLAN 10
standby 10 priority 110  ! Priorité HSRP de l'interface
standby 10 preempt  ! Permet à cette interface de prendre le rôle de
routeur actif
!
```

```
! Configuration de l'interface Vlan20 avec une adresse IP et HSRP
interface Vlan20
mac-address 0006.2aec.7002
ip address 192.168.20.254 255.255.255.0  ! Adresse IP de l'interface
standby 20 ip 10.10.20.1  ! IP virtuelle HSRP pour le VLAN 10
standby 20 priority 110  ! Priorité HSRP de l'interface
standby 20 preempt  ! Permet à cette interface de prendre le rôle de routeur actif
!
! Configuration de l'interface Vlan30 avec une adresse IP et HSRP
interface Vlan30
mac-address 0006.2aec.7003
ip address 192.168.30.254 255.255.255.0  ! Adresse IP de l'interface
standby 30 ip 10.10.30.1  ! IP virtuelle HSRP pour le VLAN 10
standby 30 priority 110  ! Priorité HSRP de l'interface
standby 30 preempt  ! Permet à cette interface de prendre le rôle de routeur actif
!
! Configuration des routes statiques
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.40.1  ! Route par défaut envoyée à 10.10.40.1
ip route 192.168.100.0 255.255.255.0 20.20.40.2  ! Route vers  192.168.100.0 via 20.20.40.2
ip route 192.168.100.0 255.255.255.0 10.10.40.1  ! Route vers  192.168.100.0 via 10.10..40.1
ip route 172.31.20.0 255.255.255.0 10.10.40.1  ! Route vers 172.31.20.0 via 10.10.40.1
!
! Configuration des ACL
ip access-list extended VLAN20_30_BLOCK ! vlan 20 et 30 siège ne peuvent pas se ping
deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
permit ip any any
ip access-list extended BLOCK_PING_VLAN20  ! permet la communication du vlan 20 siège vers le vlan 20 succursale uniquement
deny icmp 192.168.20.0 0.0.0.255 172.31.30.0 0.0.0.255
deny icmp 192.168.20.0 0.0.0.255 172.31.10.0 0.0.0.255
permit ip any any
ip access-list extended BLOCK_PING_VLAN30 ! permet la communication du vlan 30 siège vers le vlan 30 succursale uniquement
deny icmp 192.168.30.0 0.0.0.255 172.31.10.0 0.0.0.255
deny icmp 192.168.30.0 0.0.0.255 172.31.20.0 0.0.0.255
```

```
permit ip any any
!
ip flow-export version 9
!
line con 0   ! Configuration de console
!
line aux 0   ! Configuration de la ligne auxiliaire
!
line vty 0 4   ! Configuration des lignes VTY
exec-timeout 5 0   ! Déconnecte l'utilisateur inactif au bout de 5 minutes
login local   ! Utilisation de la base de données locale pour l'authentification
transport input ssh  ! Autorise uniquement les connexions SSH
!
!
!
end
```

L3_Succu (Switch) Succursale

```
! Exclusion des adresses IP de la plage DHCP
ip dhcp excluded-address 172.31.10.1 172.31.10.10
ip dhcp excluded-address 172.31.20.1 172.31.20.10
ip dhcp excluded-address 172.31.30.1 172.31.30.10
!
! Configuration des pools DHCP pour différents VLANs
ip dhcp pool Vlan10
network 172.31.10.0 255.255.255.0 ! Plage d'adresses pour Vlan10
default-router 172.31.10.254  ! Routeur par défaut pour le VLAN 10
dns-server 8.8.8.8
ip dhcp pool Vlan20
network 172.31.20.0 255.255.255.0  ! Plage d'adresses pour Vlan20
default-router 172.31.20.254  ! Routeur par défaut pour le VLAN 20
dns-server 8.8.8.8
ip dhcp pool Vlan30
network 172.31.30.0 255.255.255.0  ! Plage d'adresses pour Vlan30
default-router 172.31.30.254  ! Routeur par défaut pour le VLAN 30
!
! Activation du routage IP sur le switch
ip routing
!
! Définition de l'utilisateur  avec privilège administrateur et mot de passe
sécurisé
username admin privilege 15 secret 5
$1$mERr$tN2nmMK5hNorN4zAZEGGz.
!
! Configuration de SSH pour la gestion à distance sécurisée
ip ssh version 2
ip domain-name monreseau.local   ! Définit le domaine DNS
!
! Activation du mode PVST
spanning-tree mode pvst
!
! Configuration interfaces FastEthernet pour chaque VLAN avec mode
“accès”
interface FastEthernet0/1  ! Associe l'interface au VLAN 10
switchport access vlan 10  ! Configure l'interface en mode "access"
!
interface FastEthernet0/2  ! Associe l'interface au VLAN 20
```

```
switchport access vlan 20  ! Configure l'interface en mode "access"
!
interface FastEthernet0/3  ! Associe l'interface au VLAN 30
switchport access vlan 30  ! Configure l'interface en mode "access"
!
! Configuration de l'interface FastEthernet0/4 comme un trunk
interface FastEthernet0/4
switchport trunk allowed vlan 10,20,30  ! Permet le trafic des VLANs 10, 20 et
30
!
interface FastEthernet0/5
!
! Configuration de l'interface GigabitEthernet0/1 avec une adresse IP
statique
interface GigabitEthernet0/1
no switchport
ip address 20.20.40.2 255.255.255.0  ! Attribue une adresse IP à l'interface
duplex auto
speed auto
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
! Configuration de l'interface Vlan10 avec une adresse IP et HSRP
interface Vlan10
mac-address 0004.9aeb.4501
ip address 172.31.10.254 255.255.255.0    ! Adresse IP de l'interface
!
! Configuration de l'interface Vlan20 avec une adresse IP et HSRP
interface Vlan20
mac-address 0004.9aeb.4503
ip address 172.31.20.254 255.255.255.0   ! Adresse IP de l'interface
!
! Configuration de l'interface Vlan30 avec une adresse IP et HSRP
interface Vlan30
mac-address 0004.9aeb.4504
ip address 172.31.30.254 255.255.255.0   ! Adresse IP de l'interface
!
```

```
! Configuration des routes statiques
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.40.1  ! Route par défaut envoyée à 20.20.40.1
ip route 192.168.100.0 255.255.255.0 10.10.40.2  ! Route vers  192.168.100.0 via 10.10.40.2
ip route 192.168.100.0 255.255.255.0 20.20.40.1  ! Route vers  192.168.100.0 via 20.20.40.1
ip route 172.31.20.0 255.255.255.0 20.20.40.1  ! Route vers  172.31.20.0 via 20.20.40.1
!
! Configuration des ACL
ip access-list extended VLAN20_30_BLOCK  ! vlan 20 et 30 succursale ne peuvent pas se ping
deny ip 172.31.20.0 0.0.0.255 172.31.30.0 0.0.0.255
deny ip 172.31.30.0 0.0.0.255 172.31.20.0 0.0.0.255
permit ip any any
ip access-list extended BLOCK_PING_VLAN20  ! permet la communication du vlan 20 succursale vers le vlan 20 siège uniquement
deny icmp 172.31.20.0 0.0.0.255 192.168.10.0 0.0.0.255
deny icmp 172.31.20.0 0.0.0.255 192.168.30.0 0.0.0.255
deny icmp 172.31.20.0 0.0.0.255 172.31.10.0 0.0.0.255
permit ip any any
ip access-list extended BLOCK_PING_VLAN30 ! permet la communication du vlan 30 succursale vers le vlan 30 siège uniquement
deny icmp 172.31.30.0 0.0.0.255 192.168.10.0 0.0.0.255
deny icmp 172.31.30.0 0.0.0.255 192.168.20.0 0.0.0.255
deny icmp 172.31.30.0 0.0.0.255 172.31.10.0 0.0.0.255
permit ip any any
ip flow-export version 9
!
line con 0  ! Configuration de console
!
line aux 0  ! Configuration de la ligne auxiliaire
!
line vty 0 4  ! Configuration des lignes VTY
exec-timeout 5 0  ! Déconnecte l'utilisateur inactif au bout de 5 minutes
login local  ! Utilisation de la base de données locale pour l'authentification
transport input ssh  ! Autorise uniquement les connexions SSH
!
!
!
end
```

3.1.3.Firewalls ASA-cisco :

ASA_Siege (Firewall)

```
! Définition du nom de domaine
domain-name sh  ! Définit le nom de domaine "sh"
! Définition des mots de passe
enable password NGG7hxXFlbbN77XF encrypted  ! Définit le mot de passe d'activation (enable) crypté
passwd NGG7hxXFlbbN77XF encrypted  ! Définit le mot de passe d'accès utilisateur crypté
names
!
! Définition des interfaces réseau avec leurs adresses IP et niveaux de sécurité
interface GigabitEthernet1/1
nameif outside  ! Nom de l'interface : "outside"
security-level 0   ! Niveau de sécurité de l'interface "outside" (0 = faible sécurité)
ip address 10.10.50.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif inside   ! Nom de l'interface : "inside"
security-level 100  ! Niveau de sécurité de l'interface "inside" (100 = haute sécurité)
ip address 10.10.40.1 255.255.255.0
!
interface GigabitEthernet1/3
nameif dmz   ! Nom de l'interface : "dmz"
security-level 50  ! Niveau de sécurité de l'interface "dmz" (niveau moyen)
ip address 172.31.25.1 255.255.255.0
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
!
! Configuration des routes statiques pour différents réseaux
```

```
route outside 10.10.50.0 255.255.255.0 10.10.50.2 1
route outside 10.10.40.0 255.255.255.0 10.10.40.2 1
route outside 10.10.40.0 255.255.255.0 192.168.100.1 1
route outside 20.20.40.0 255.255.255.0 192.168.100.2 1
route outside 192.168.100.0 255.255.255.0 10.10.50.2 1
route outside 172.31.10.0 255.255.255.0 192.168.100.2 1
route inside 10.10.40.0 255.255.255.0 10.10.40.2 1
route inside 192.168.10.0 255.255.255.0 10.10.40.2 1
route inside 192.168.20.0 255.255.255.0 10.10.40.2 1
route inside 192.168.30.0 255.255.255.0 10.10.40.2 1
route outside 20.20.50.0 255.255.255.0 10.10.50.2 1
route outside 172.31.20.0 255.255.255.0 192.168.100.2 1
route outside 172.31.30.0 255.255.255.0 192.168.100.2 1
route outside 172.31.25.0 255.255.255.0 10.10.50.2 1
route outside 172.31.25.0 255.255.255.0 192.168.100.2 1
!
! Définition de la liste de contrôle d'accès (ACL) pour filtrer le trafic
access-list ACL-FILTRE extended permit ip any any
access-list ACL-FILTRE extended permit icmp 192.168.10.0 255.255.255.0 any
echo
access-list ACL-FILTRE extended permit icmp 192.168.10.0 255.255.255.0 any
echo-reply
access-list ACL-FILTRE extended deny icmp any 192.168.10.0 255.255.255.0
!
! Applique l'ACL sur les interfaces "outside" et "inside"
access-group ACL-FILTRE in interface outside
access-group ACL-FILTRE in interface inside
!
! Configuration de l'authentification AAA pour Telnet et SSH
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
!
! Définition de l'utilisateur  avec privilège administrateur et mot de passe
sécurisé
username admin password NGG7hxXFlbbN77XF encrypted
!
! Configuration des politiques de sécurité pour les inspections
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
```

```
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect http
inspect icmp
inspect tftp
!
! Applique la politique d'inspection globale
service-policy global_policy global
!
! Configuration des délais de timeout pour Telnet et SSH
telnet timeout 5
ssh timeout 5
ssh 192.168.10.0 255.255.255.0 inside  ! Autorise SSH depuis le réseau
192.168.10.0/24 vers "inside"
ssh 192.168.20.0 255.255.255.0 inside
ssh 192.168.30.0 255.255.255.0 inside
ssh 172.31.10.0 255.255.255.0 outside  ! Autorise SSH depuis le réseau
172.31.10.0/24 vers "outside"
ssh 172.31.20.0 255.255.255.0 outside
ssh 172.31.30.0 255.255.255.0 outside
```

ASA Succu (Firewall)

```
! Définition du nom de domaine
domain-name sh  ! Définit le nom de domaine "sh"
! Définition des mots de passe
enable password NGG7hxXFlbbN77XF encrypted  ! Définit le mot de passe d'activation (enable) crypté
passwd NGG7hxXFlbbN77XF encrypted  ! Définit le mot de passe d'accès utilisateur crypté
names
!
! Définition des interfaces réseau avec leurs adresses IP et niveaux de sécurité
interface GigabitEthernet1/1
nameif outside  ! Nom de l'interface : "outside"
security-level 0  ! Niveau de sécurité de l'interface "outside" (0 = faible sécurité)
ip address 20.20.50.1 255.255.255.0
!
interface GigabitEthernet1/2
nameif inside  ! Nom de l'interface : "inside"
security-level 100  ! Niveau de sécurité de l'interface "inside" (100 = haute sécurité)
ip address 20.20.40.1 255.255.255.0
!
interface GigabitEthernet1/3
nameif dmz  ! Nom de l'interface : "dmz"
security-level 50  ! Niveau de sécurité de l'interface "dmz" (niveau moyen)
ip address 172.31.25.1 255.255.255.0
!
interface GigabitEthernet1/4
no nameif
no security-level
no ip address
shutdown
!
!
! Configuration des routes statiques pour différents réseaux
route outside 20.20.50.0 255.255.255.0 20.20.50.2 1
route outside 20.20.40.0 255.255.255.0 20.20.40.2 1
route outside 20.20.40.0 255.255.255.0 192.168.100.2 1
```

```
route outside 10.10.40.0 255.255.255.0 192.168.100.1 1
route outside 192.168.10.0 255.255.255.0 192.168.100.1 1
route inside 172.31.10.0 255.255.255.0 20.20.40.2 1
route inside 172.31.20.0 255.255.255.0 20.20.40.2 1
route inside 172.31.30.0 255.255.255.0 20.20.40.2 1
route inside 20.20.40.0 255.255.255.0 20.20.40.2 1
route outside 192.168.100.0 255.255.255.0 20.20.50.2 1
route inside 20.20.40.0 255.255.255.0 20.20.50.2 1
route inside 10.10.50.0 255.255.255.0 20.20.50.2 1
route inside 10.10.50.0 255.255.255.0 192.168.100.1 1
route outside 192.168.20.0 255.255.255.0 192.168.100.1 1
route outside 192.168.30.0 255.255.255.0 192.168.100.1 1
route inside 10.10.50.0 255.255.255.0 20.20.40.2 1
route inside 192.168.10.0 255.255.255.0 20.20.40.2 1
route outside 192.168.10.0 255.255.255.0 20.20.40.2 1
route outside 10.10.50.0 255.255.255.0 20.20.40.2 1
route outside 172.31.25.0 255.255.255.0 20.20.40.2 1
route outside 172.31.25.0 255.255.255.0 192.168.100.1 1
!
! Définition de la liste de contrôle d'accès (ACL) pour filtrer le trafic
access-list OUTSIDE_IN extended permit icmp any any
!
! Applique l'ACL sur les interfaces "outside" et "inside"
access-group OUTSIDE_IN in interface outside
!
! Configuration de l'authentification AAA pour Telnet et SSH
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
!
! Définition de l'utilisateur  avec privilège administrateur et mot de passe
sécurisé
username admin password NGG7hxXFlbbN77XF encrypted
!
! Configuration des politiques de sécurité pour les inspections
class-map inspection_default
match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
```

```
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect http
inspect icmp
inspect tftp
!
! Applique la politique d'inspection globale
service-policy global_policy global
!
telnet timeout 5
ssh timeout 5
ssh 172.31.20.0 255.255.255.0 inside
ssh 172.31.10.0 255.255.255.0 inside  ! Autorise SSH depuis le réseau
172.31.10.0/24 vers "inside"
ssh 172.31.30.0 255.255.255.0 inside
ssh 192.168.10.0 255.255.255.0 outside  ! Autorise SSH depuis le réseau
192.168.10.0/24 vers "outside"
ssh 192.168.20.0 255.255.255.0 outside
ssh 192.168.30.0 255.255.255.0 outside
```

3.2.1.Configuration du DNS :

- *Installation du service DNS sur un Windows Server*

1. Ouvrir le Gestionnaire de serveur sur le serveur cible.
2. Cliquer sur Gérer > Ajouter des rôles et fonctionnalités.
3. Sélectionner Installation basée sur un rôle ou une fonctionnalité, puis cliquer sur Suivant.
4. Sélectionner le serveur sur lequel installer le rôle et cliquer sur Suivant.
5. Dans la liste des rôles, cocher Serveur DNS.
6. Accepter l'installation des fonctionnalités requises et cliquer sur Suivant.
7. Lire les informations sur le rôle DNS, puis cliquer sur Suivant.
8. Cliquer sur Installer et patienter jusqu'à la fin de l'installation.
9. Une fois l'installation terminée, fermer l'assistant.

- *Configuration de la zone DNS*

1. Ouvrir la console Gestionnaire DNS (DNS Manager) via le menu Outils du Gestionnaire de serveur.
2. Faire un clic droit sur Zones de recherche directes et sélectionnez Nouvelle zone.
3. Dans l'assistant de création de zone :
    a. Sélectionner Zone principale.
    b. Spécifier un nom de zone (ex : societe2.pepiniere.rt).
    c. Choisir les options de réplication selon le contexte (ex : Ne pas stocker dans Active Directory pour un serveur autonome).
    d. Activer ou non les mises à jour dynamiques selon les besoins de l'infrastructure.
4. Ajouter les enregistrements DNS nécessaires :
    a. Enregistrement A (Adresse IPv4) : Associe un nom de domaine à une adresse IP.
    b. Enregistrement NS (Name Server) : Définit les serveurs DNS responsables de la zone.
5. Appliquer et vérifier la configuration.

3.2.2.Activation de DNSSEC

- *Signature de la zone*

1. Ouvrir la console Gestionnaire DNS.
2. Sélectionner la zone précédemment créée (societe2.pepiniere.rt).
3. Faire un clic droit et choisir Signer la zone.
4. Dans l'assistant de signature de zone :
    a. Sélectionner Configurer des paramètres personnalisés pour un contrôle avancé.
    b. Choisir un algorithme de signature recommandé (ex : RSA/SHA-256).
    c. Définir les clés KSK et ZSK avec des longueurs appropriées (ex : 2048 bits pour KSK et 1024 bits pour ZSK).
    d. Spécifier une périodicité de renouvellement des signatures.
    e. Terminer l'assistant et appliquer la signature de la zone.
5. Vérifier la présence des enregistrements DS et DNSKEY après signature.

- Publication des clés DNSSEC

1. Exporter les enregistrements DS pour une transmission à l'opérateur de zone parent (si applicable).
2. Vérifier la publication correcte avec la commande PowerShell suivante :

    - Get-DnsServerDnsSecZoneSetting -ZoneName societe2.pepiniere.rt

3.3.1.Configuration du serveur Web :

- *Installation des prérequis*

1. Installer Nginx sur le serveur :
   sudo apt update && sudo apt install nginx -y
2. Vérifier que le service est actif :
   sudo systemctl status nginx
3. Installer Python et les dépendances :
   sudo apt install python3 python3-pip python3-venv -y
4. Installer MySQL :
   sudo apt install mysql-server -y

- *Fichiers de configuration et code source*
- *Application Flask (app.py) :*

```
from flask import Flask, render_template, request, redirect,
url_for, session
import mysql.connector

### génère un mot de passe hashé
from werkzeug.security import generate_password_hash,
check_password_hash

app = Flask(__name__)
app.secret_key = "secret123"

# Connexion à MySQL
db = mysql.connector.connect(
    host="localhost",
    user="flask_user",
    password="FlaskP@ss123",
    database="flask_auth"
)
cursor = db.cursor()
```

```
### permet à l'utilisateur d'accès au site
@app.route('/')
def home():
    return render_template('index.html')

### permet à l'utilisateur de se connecter
@app.route('/login', methods=['GET', 'POST'])
def login():
    message = ""
    if request.method == 'POST':
        username = request.form['username']
        password = request.form['password']

        cursor.execute("SELECT password FROM users WHERE
username=%s", (username,))
        user = cursor.fetchone()

        if user and check_password_hash(user[0], password):
            session['user'] = username
            return redirect(url_for('dashboard'))
        else:
            message = "Identifiants incorrects !"

    return render_template('login.html', message=message)

### permet à l'utilisateur de s'inscrire
@app.route('/register', methods=['GET', 'POST'])
def register():
    message = ""
    if request.method == 'POST':
        username = request.form['username']
        email = request.form['email']
        password = request.form['password']

        cursor.execute("SELECT * FROM users WHERE username=%s
OR email=%s", (username, email))
        existing_user = cursor.fetchone()
```

```
        if existing_user:
            message = "L'utilisateur existe déjà !"
            return render_template('register.html',
message=message)

        hashed_password = generate_password_hash(password)
        cursor.execute("INSERT INTO users (username, email,
password) VALUES (%s, %s, %s)", (username, email,
hashed_password))
        db.commit()

        return redirect(url_for('login'))

    return render_template('register.html', message=message)

### interface de connexion pour l'utilisateur
@app.route('/dashboard')
def dashboard():
    if 'user' in session:
        return f"<h1>Bienvenue {session['user']} !</h1><br><a
href='/logout'>Se déconnecter</a>"
    return redirect(url_for('login'))

### permet de déconnecter l'utilisateur
@app.route('/logout')
def logout():
    session.pop('user', None)
    return redirect(url_for('home'))

### hébergement du flask
if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8000)
```

render_template : Permet d'afficher un modèle HTML en y injectant des données dynamiques.
request : Utilisé pour accéder aux données d'une requête HTTP (champs de formulaire, paramètres d'URL, cookies, etc.).
redirect : Permet de rediriger l'utilisateur vers une autre page ou route.

werkzeug.security import generate_password_hash : Génère un mot de passe haché pour le stocker de manière sécurisée

mysql.connector.connect : Établit une connexion avec une base de données MySQL.
db.cursor : Crée un objet curseur permettant d'exécuter des requêtes SQL.

request.method : Permet de vérifier si la requête HTTP est de type GET, POST, etc.
request.form : Récupère les données envoyées par un formulaire via une requête POST.

cursor.execute : Exécute une requête SQL.
cursor.fetchone : Récupère une seule ligne du résultat d'une requête SQL.
db.commit : Valide les modifications effectuées dans la base de données (INSERT, UPDATE, DELETE).

session.pop : Supprime une variable de session.
app.run : Lance l'application Flask.

- *Base de donnée MySQL :*

```
CREATE DATABASE flask_auth;
USE flask_auth;

CREATE TABLE users (
    id INT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) UNIQUE NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,
    password TEXT NOT NULL
);

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| flask_auth         |
| information_schema |
| mysql              |
| performance_schema |
| postfix            |
| sys                |
| test               |
+--------------------+
7 rows in set (0,35 sec)

id : un identifiant unique pour chaque utilisateur, généré
automatiquement (AUTO_INCREMENT)
username : un nom d'utilisateur, qui doit être unique (UNIQUE
NOT NULL).
email : une adresse e-mail unique pour chaque utilisateur.
password : un mot de passe stocké sous forme chiffrée
(hashée).
```

```
mysql> use flask_auth;
Reading table information for completion of table and column
names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users;
+----+----------+-----------------------------------------------
-----------------------------------------------------------------
-------------------------------------------------------+----
-----------+
| id | username | password
     | email         |
+----+----------+-----------------------------------------------
-----------------------------------------------------------------
-------------------------------------------------------+----
-----------+
|  1 | admin    |
scrypt:32768:8:1$NEaI9FRAZIENTySz$5d2a1778811273fd346878fa458c
10d7b8a85a05c1b2b7bf2ea78ac1d581ec94f6d3888b28cb41197ec02fdf17
69a2ae77da9705f64d7e121303d356022b79c7 |               |
|  3 | test     |
scrypt:32768:8:1$udkEKhK33dm4ccOu$24de3f276c310818c67f720082a6
c88e27eee2654dd05df520f33f18cd457384deed2ba7b565cc74bf26b84ea8
68113d2b0d39fd08c456780fd2244035aa2a90 | test@test.com |
```

On observe que la base de données contient bien des mots de passe hachés.

- *Configuration de Nginx :*
- *Configuration de la redirection HTTP vers HTTPS*

Nginx est utilisé comme reverse proxy pour rediriger le trafic vers Flask.

/etc/nginx/sites-available/flask_app

Modifier la configuration Nginx pour forcer l'utilisation de HTTPS :

```
server {
    ### Le serveur écoute sur le port 443 avec SSL
    listen 443 ssl;

    ### Redirige tout le trafic HTTP vers HTTPS
    server_name baptisteduval.com;

    ### Définit le certificat SSL et sa clé privée.
    ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;

    ### Il s'agit d'un certificat auto-signé
    ssl_certificate_key
    /etc/ssl/private/nginx-selfsigned.key;

    ### Active HSTS (HTTP Strict Transport Security) pour
    forcer l'utilisation de HTTPS.
    add_header Strict-Transport-Security "max-age=31536000;
    includeSubDomains; preload" always;

    ### Empêche les navigateurs d'interpréter un fichier
    autrement que son type MIME déclaré (protection contre
    certains types d'attaques).
    add_header X-Content-Type-Options "nosniff" always;

    ### Active la protection contre les attaques XSS
    (Cross-Site Scripting).
    add_header X-XSS-Protection "1; mode=block" always;
```

```
        ### Empêche l'affichage du site dans un iframe sauf s'il
        est sur le même domaine (protection contre les attaques
        de clickjacking).
        add_header X-Frame-Options "SAMEORIGIN" always;

        ### Gère la façon dont les référents (URL précédentes)
        sont envoyés entre HTTP et HTTPS.
        add_header Referrer-Policy "no-referrer-when-downgrade"
        always;

        ### Tout le trafic est redirigé vers une application
        tournant en local sur le port 8000.
        location / {
        proxy_pass http://0.0.0.0:8000;

        ### Transmet le nom de domaine original.
        proxy_set_header Host $host;

        ### Passe l'IP réelle du client.
        proxy_set_header X-Real-IP $remote_addr;

        ### Garde une trace de l'IP du client à travers les
        proxys.
        proxy_set_header X-Forwarded-For
        $proxy_add_x_forwarded_for;

        ### Indique si la connexion est HTTP ou HTTPS.
        proxy_set_header X-Forwarded-Proto $scheme;
        }
}

server {
        ### Écoute sur le port 80 (HTTP).
        listen 80;
        ### Redirige tout le trafic HTTP vers HTTPS
        server_name baptisteduval.com;
        ### 301 signifie une redirection permanente.
        return 301 https://$host$request_uri;
```

- *Fichiers HTML :*
- *index.html :*

```
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
initial-scale=1.0">
    <title>Accueil</title>
</head>
<body>
    <h1>Bienvenue sur l  e site</h1>
    <form action="/login">
        <button type="submit">Se connecter</button>
    </form>
    <p>Pas encore de compte ? <a href="/register">Inscris-toi
ici</a></p>
</body>
</html>
```

Formulaire de connexion avec nom d'utilisateur et mot de passe.
CAPTCHA dynamique généré en JavaScript pour éviter les soumissions automatiques.
Vérification avant envoi : si le CAPTCHA est incorrect, l'envoi est bloqué.
Possibilité de régénérer un nouveau CAPTCHA.

- *login.html :*

```
<!DOCTYPE html>
<html lang="fr">

<body>
     <div>
     <h1>Connexion</h1>
     <form id="loginForm" method="POST">
          <input type="text" name="username" placeholder="Nom
d'utilisateur" required><br>
          <input type="password" name="password"
placeholder="Mot de passe" required><br>

     <!-- Affichage du CAPTCHA -->
          <div id="captcha">
               <span id="captchaText"></span><br>
               <input type="text" id="captchaInput"
placeholder="Entrez le texte ci-dessus" required><br>
               <button type="button"
onclick="generateCaptcha()">Régénérer le CAPTCHA</button>
          </div>

          <button type="submit">Se connecter</button>
     </form>
     <p id="message"></p>
     </div>

     <script>
     // Fonction pour générer un texte CAPTCHA aléatoire
     function generateCaptcha() {
          var characters =
'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789';
          var captchaText = '';
          for (var i = 0; i < 6; i++) {
               var randomIndex = Math.floor(Math.random() *
characters.length);
               captchaText += characters[randomIndex];
          }
```

```
            document.getElementById('captchaText').textContent =
captchaText;
            // Sauvegarder le texte CAPTCHA dans le localStorage
            sessionStorage.setItem('captchaText', captchaText);
      }

      // Fonction de validation du formulaire

document.getElementById("loginForm").addEventListener("submit"
, function(event) {
            var captchaInput =
document.getElementById("captchaInput").value;
            var captchaStored =
sessionStorage.getItem('captchaText'); // Récupérer le texte
CAPTCHA

            // Vérifier si le CAPTCHA saisi est correct
            if (captchaInput !== captchaStored) {
                  event.preventDefault();  // Empêcher l'envoi du
formulaire
                  document.getElementById("message").innerText =
"Le CAPTCHA est incorrect.";
                  document.getElementById("message").style.color
= "red";
            }
      });

      // Initialisation du CAPTCHA au chargement de la page
      window.onload = function() {
            generateCaptcha();
      };
      </script>
</body>
</html>
```

- *register.html :*

```
<!DOCTYPE html>
<html lang="fr">

<body>
     <div>
     <h1>Inscription</h1>
     <form method="POST">
          <input type="text" name="username" placeholder="Nom
d'utilisateur" required><br>
          <input type="email" name="email" placeholder="Email"
required><br>
          <input type="password" name="password"
placeholder="Mot de passe" required><br>
          <button type="submit">S'inscrire</button>
     </form>
     <p>{{ message }}</p>
     </div>
</body>
</html>
```

3.3.2.Sécurisation Web :

- *Cacher les informations sensibles*

Désactiver l'affichage de la version de Nginx dans /etc/nginx/nginx.conf :

```
server_tokens off;
```

- *Ajouter des en-têtes de sécurité*

```
add_header Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload" always;

add_header X-Content-Type-Options "nosniff" always;

add_header X-XSS-Protection "1; mode=block" always;

add_header X-Frame-Options "SAMEORIGIN" always;

add_header Referrer-Policy "no-referrer-when-downgrade"
always;
```

- *Renforcement du chiffrement*

```
ssl_protocols TLSv1.2 TLSv1.3;

ssl_prefer_server_ciphers on;

ssl_ciphers
"ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384
:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305
";

ssl_session_cache shared:SSL:10m;

ssl_session_timeout 10m;

ssl_stapling on;

ssl_stapling_verify on;

resolver 8.8.8.8 8.8.4.4 valid=300s;

resolver_timeout 5s;
```

- *Restriction des méthodes HTTP*

```
if ($request_method !~ ^(GET|POST)$) {
    return 405;
}
```

- *Protection contre les attaques avec Fail2Ban*

Configurer Fail2Ban pour limiter les tentatives de connexion :

```
[nginx-http-auth]
enabled = true
filter = nginx-http-auth
logpath = /var/log/nginx/error.log
maxretry = 3
```

- *Protection des fichiers sensibles*

Restreindre l'accès aux fichiers cachés :

```
location ~ /\. {
  deny all;
}
```

3.3.3.Gestion des utilisateurs et journalisation

- *Système de cookies*

Un système de cookies est mis en place pour demander à l'utilisateur d'accepter les cookies. Les informations enregistrées incluent la date, l'heure et l'IP du visiteur.

- *Sécurisation de l'authentification*

Dans la page de connexion, un mécanisme bloque l'adresse IP d'un utilisateur après plusieurs tentatives échouées pendant une minute.

Uniquement les ports http et https d’ouverts, pas de ssh ni ri

4.Tests de Sécurité

4.1.Résultats obtenues :

DNS :

- *Résolution avec validation DNSSEC*

Depuis un client Windows :

1. Ouvrir PowerShell (Windows+R, taper "powershell").
2. Exécuter la commande suivante pour tester la résolution DNSSEC :
   `Resolve-DnsName societe2.pepiniere.rt -Server 192.168.10.5 -Dnssec`
   Cette commande permet de vérifier que la résolution du domaine est correctement signée.

- *Vérification des clés DNSSEC*

Pour afficher les enregistrements DNSKEY :

```
Resolve-DnsName societe2.pepiniere.rt -Server 192.168.10.5 -Type DNSKEY -DnssecOk
```

Cette commande permet de confirmer que les clés DNSSEC sont correctement publiées et accessibles.

- *DNS SPOOFING :*

On utilise l'outil bettercap 2

Spécifie les noms de domaine à spoofing pour les attaques de phishing ou de redirection DNS

```
set societe2.pepiniere.rt hacked_by_M3

dns.spoof on

dns.spoof hacked_by_M3 -> 192.168.10.5

ping hacked_by_M3
```

Cela renvoie : `ping : hacked_by_M3: Echec temporaire dans la résolution du nom`

Ce qui veut dire qu'il est impossible d'obtenir la résolution du nom, par mesure de sécurité ce ping est bloqué.

WEB :

- *Injection sql avec :*

```
' OR 1=1 --
```

Ne fonctionne pas grâce au système de blocage SQL.

- Injection XSS

Ne fonctionne pas ni sur formulaire, ni grâce à l'URL, ni par la console du F12, ni par la page login. Un système de brute force ne marche pas a cause du système de captcha

Impossible de faire des injections sql avec :

```
sqlmap -u "https://192.31.25.13:80/login.html" --form
--dbs --risk=3 --level=5 --threads=4 --batch
```

- *Scan des ports avec :*

```
nmap -sS -p- 172.20.10.11
```

Ne fonctionne pas car les ports de la machine sont fermés à part pour les ports http et le https respectivement les ports 80 et 443, qui sont ouverts pour permettre la connexion au serveur web.

5.Recommandation ANSSI

5.1. Explication du document de l'ANSSI :

Les documents de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) sont des guides, des recommandations pour améliorer la sécurité d'un système informatique. Ces documents sont destinés aux entreprises, aux administrations ainsi qu'aux particuliers qui souhaitent renforcer leur cybersécurité.

Ils comportent entre autres des aides pour mettre en place les bonnes pratiques en cybersécurité, donner des référentiels normatifs pour les infrastructures sensibles, accompagner les experts en sécurité dans l'application de règles strictes ainsi que sensibiliser des organisations aux cybermenaces.

5.2. Termes essentiels à comprendre :

Dans ce document il y a des termes qui peuvent être difficile à comprendre voici quelque exemple avec les explications :

- SI (Système d'information) : Ensemble des ressources informatiques d'une organisation.
- SOC (Security Operations Center) : Centre chargé de la surveillance et de la gestion des incidents de sécurité
- PSSI (Politique de Sécurité des Systèmes d'Information) : Règles et mesures définissant la sécurité informatique d'une organisation

5.3. Liste de recommandation :

Dans ce projet, nous avons dû remplir un tableur comprenant toutes les règles du document de l'ANSSI et expliquer lesquels nous avons respecté ou non.

Voici le tableur que nous avons complété qui est un complément du document de l'ANSSI pour les entreprises, les particuliers, etc.

Lien du tableur