Année 2024-2025

SAÉ Cyber 4.0 Sécurisation d'un SI

Cahier de SAÉ

Version 1.1

Appartient à :	En équipe avec :
Nom :CHAKER Prénom : Nabil Groupe :Cyber A	Nom : DOGAN, Prénom :Eren
Nom : SULTANOVIC Prénom : Elmedin	Nom : HADDADI Prénom : ilyas
Nom de votre équipe : NETWATCH	

Informations générales

Répartition en groupes

6 équipes de 4 étudiants

Emploi du temps

Semaine 1 : 9h-12h 13h-17h, jeudi libéré pour le Forum Alternance
Semaine 2 : 9h-12h 13h-17h sauf jeudi 9h-12h
Semaine 3 : L 13h-17h, Ma 9h-12h 13h-17h, Me 9h-12h 13h-17h, jeudi libre et vendredi soutenance

Evaluation

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

Matériel par équipe

- 2 Firewalls Stormshield
- 1 Switch
- 1 Borne WiFi
- 5 PC tour et/ou portables

Documentation

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

Tâches à réaliser

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

Gestion de votre projet

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

Bilan

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

Tâches	Heures-homme	Pourcentage de réalisation
Mise en place d'une infrastructure sécurisée	2 Heures	25%
Installation et configuration d'un firewall Stormshield	0 heures	0%
Installation et configuration d'un serveur HTTP/HTTPS et d'un serveur FTP/FTPS	0 heures	0%
Authentification transparente par certificat SSL	0 heures	0%
Mettre en place un IDS	0 heures	0%
Attaque sur le Wifi	5 Heures	50%
Utilisation de scanneurs de vulnérabilité	55 Heures	100%
Attaque Man in The Middle	0 heures	0%
Contre-mesures pour le MiM	0 heures	0%
Supervision du réseau	0 heures	0%
Mise en place d'une architecture Single Sign-On	20 Heures	100%
Mise en place d'un VPN SSL pour clients distants	0 heures	0%
Mise en place d'un VPN IPSEC site à site	0 heures	0%

	A	B	C	D
1	TACHES :	Points	Répartition en %	Personnes impliquées et leur tâches
2	1.Mise en place d'une infrastructure sécurisée	1.5 pts	25/25/50%	Ilyas/Nabil/Eren (elmedin faisait le tableau)
3	2.Installation et configuration d'un firewall Stormshield	3 pts	100%	Ilyas
4	3.Installation et configuration d'un serveur HTTP/HTTPS et d'un serveur FTP/FTPS	7.35 pts	80% (5.88) / 20% (1.47)	Ilyas(FTPS, FTP, CMS + site web) / Elmedin (HTTP + HTTPS)
5	4.Authentification transparente par certificat SSL	9 pts	100%	Eren(Créer le cert, créer les utilisateurs, installation sur le client)
6	5.Mettre en place un IDS	10 pts	100%	Ilyas
7	6.Attaque sur le Wifi	4.5 pts	50%(2.25) / 50% (2.25)	Nabil/Elmedin
8	7.Utilisation de scanneurs de vulnérabilité	13.5 pts	100%	Nabil
9	8.Attaque Man in The Middle	3.75 pts	50%(1.875) / 50%	Ilyas / Elmedin
10	9.Contre-mesures pour le MiM	6 pts	100%	Elmedin
11	10.Supervision du réseau	3.75	100%	Elmedin
12	11.Mise en place d'une architecture Single Sign-On	9 pts	50%/50%	Eren/Nabil
13	12.Mise en place d'un VPN SSL pour clients distants	6 pts	100%	Eren
14	13.Mise en place d'un VPN IPSEC site à site	5.25 pts	100%	Elmedin
15				
16				
17	Nabil (20.625)			
18	Eren (20.25)			
19	Elmedin (20.595)			
20	Ilyas (21.13 pts)			

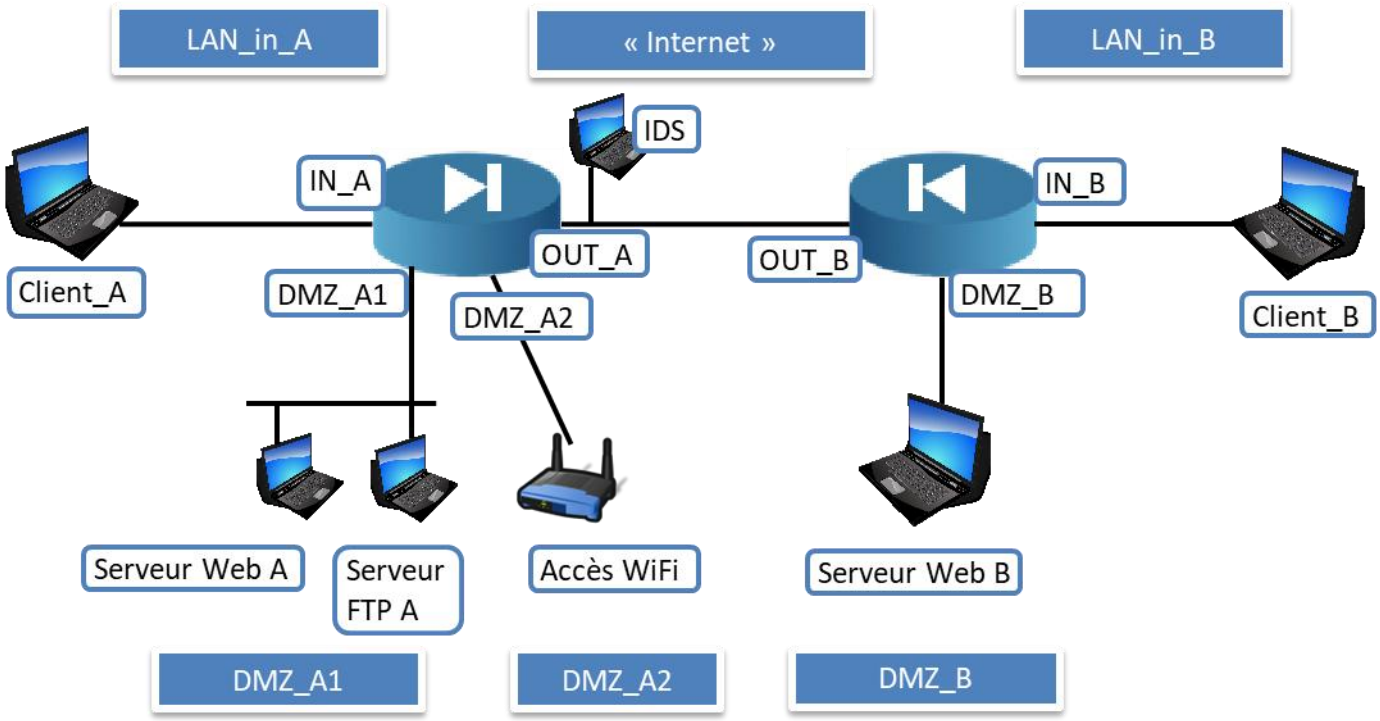
Détails des tâches à réaliser

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

Liste des personnes impliquées avec pourcentage de répartition	
CHAKER Nabil 25% HADDADI Ilyas 25% DOGAN Eren 50 %	2 Heures nabil 2 Heures Ilyas 3 Heures Eren

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

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 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
Windows Server 2022	192.168.1.10

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
Victime MiM	10.0.0.123
Hacker Kali MiM	10.0.0.111
Machine Kali Scan	10.0.0.11
VM metasploitable	10.0.0.10

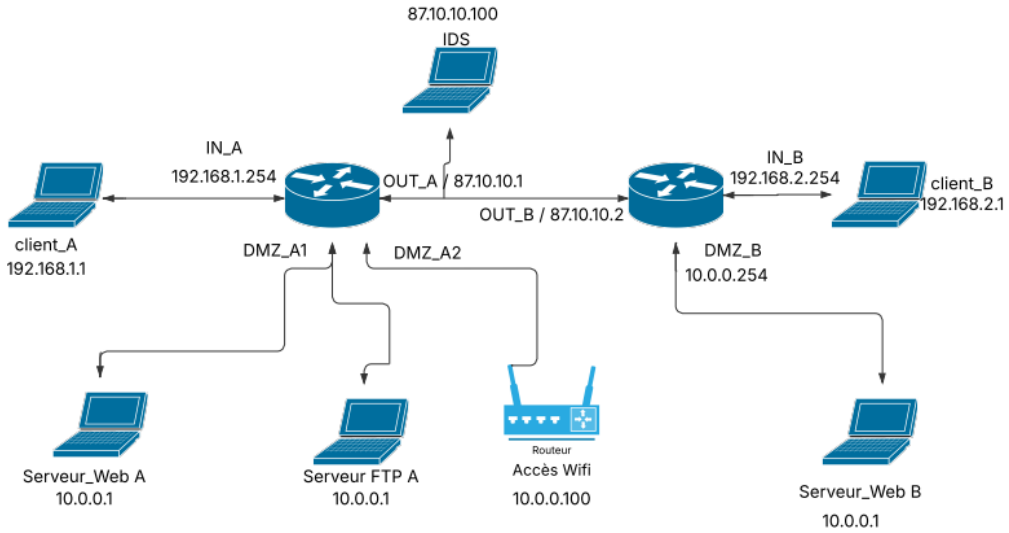
Réseau WAN	87.10.10.0/24
IDS	87.10.10.100
Firewall OUT A	87.10.10.1
Firewall OUT B	87.10.10.2
Serveur DMZ A Virtuel	87.10.10.11
Client A Virtuel	87.10.10.10
Serveur DMZ B Virtuel	87.10.10.21
Client B Virtuel	87.10.10.20
Virtual Machine Metasploitable Virtuel	87.10.10.32
Virtual Machine Kali scanner	87.10.10.30

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

Pour mettre plusieurs machines sur le réseau A dmz on a mis un switch branché à la DMZ du réseau A là où on fera tous nos tests sur réseau (scanner, attaque MiM ainsi que les contre mesure). Pour relier les deux stormshields, on a mis un deuxième switch c'est le réseau OUT.

Schéma IP de notre réseau :



Le réseau final :

Tâche 6 Attaque sur le Wifi (4,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
CHAKER Nabil 50 % SULTANOVIC Elmedin 50 %	8h Pour le groupe

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

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

Rapport

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

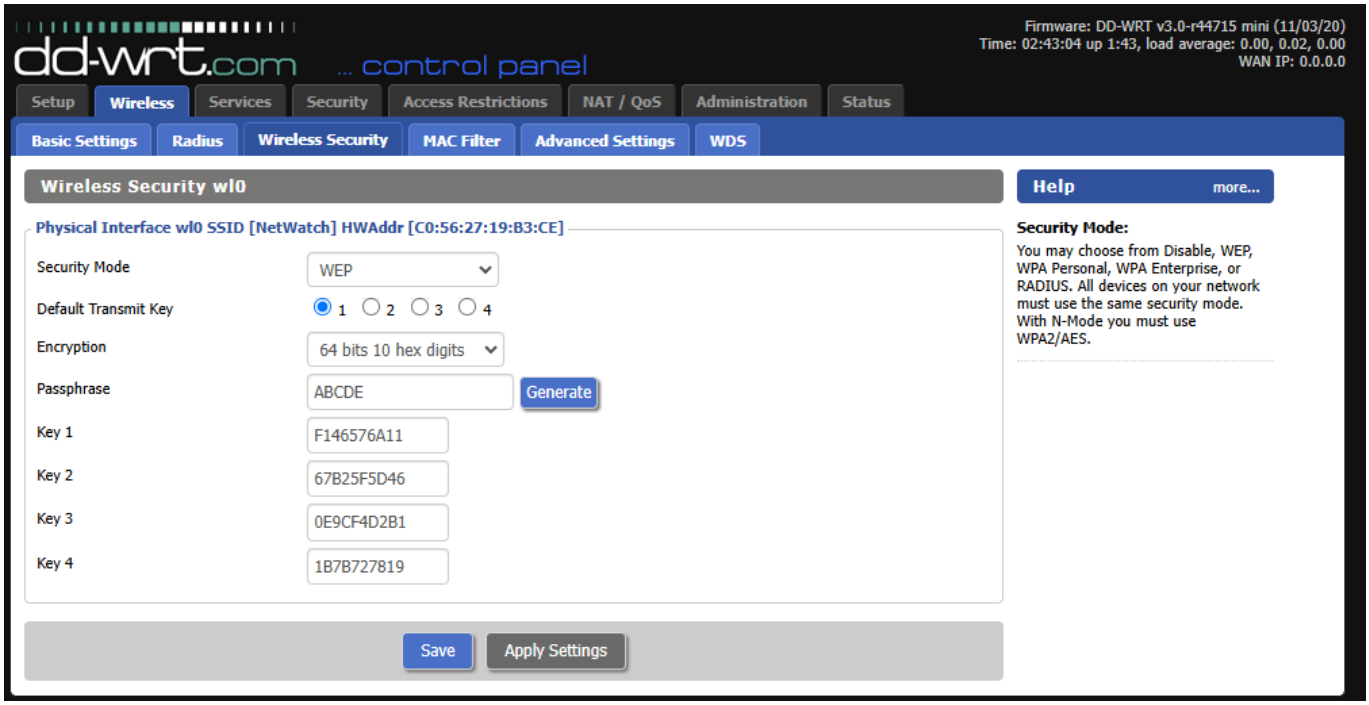
(Description de la démarche, du fonctionnement des protocoles WEP et WPA, ainsi que du principe utilisé par le cracker) :

WEP:

Le Wired Equivalent Privacy (WEP) repose sur un chiffrement symétrique aujourd'hui considéré comme obsolète. Ce protocole présente des failles importantes permettant, après une phase d'écoute prolongée (dont la durée dépend de l'intensité du trafic réseau), d'intercepter des paquets circulant sur le réseau local. Ces paquets peuvent alors être utilisés pour provoquer des collisions, ce qui permet de reconstituer la clé de chiffrement, caractère par caractère.

L'objectif de cette étape est de configurer la borne Wi-Fi Linksys en activant le protocole de sécurité WEP (Wired Equivalent Privacy). La première clé WEP définie dans les paramètres de la borne sera utilisée comme clé active pour le chiffrement. Cette configuration permet de sécuriser temporairement les échanges entre les clients et le point d'accès, tout en mettant en évidence les faiblesses inhérentes à ce protocole. Cette mise en place servira de base pour tester des techniques d'interception et de déchiffrement, dans un but pédagogique et de compréhension des vulnérabilités du WEP.

Screen de la mise en place du WEP sur la borne LinkSys avec utilisation de la première clé :



Utilisation de Fern WiFi Cracker :

Nous avons utilisé Fern WiFi Cracker car il s'agit d'un outil graphique simple et efficace permettant d'automatiser les attaques sur les réseaux sans fil. Dans le cadre de cette manipulation, il a été utilisé pour détecter les réseaux protégés par WEP et lancer une attaque de type capture de paquets IVs, afin d'extraire la clé de chiffrement. Son interface intuitive facilite la compréhension du processus de cassage de clé, tout en illustrant concrètement les failles de ce protocole.

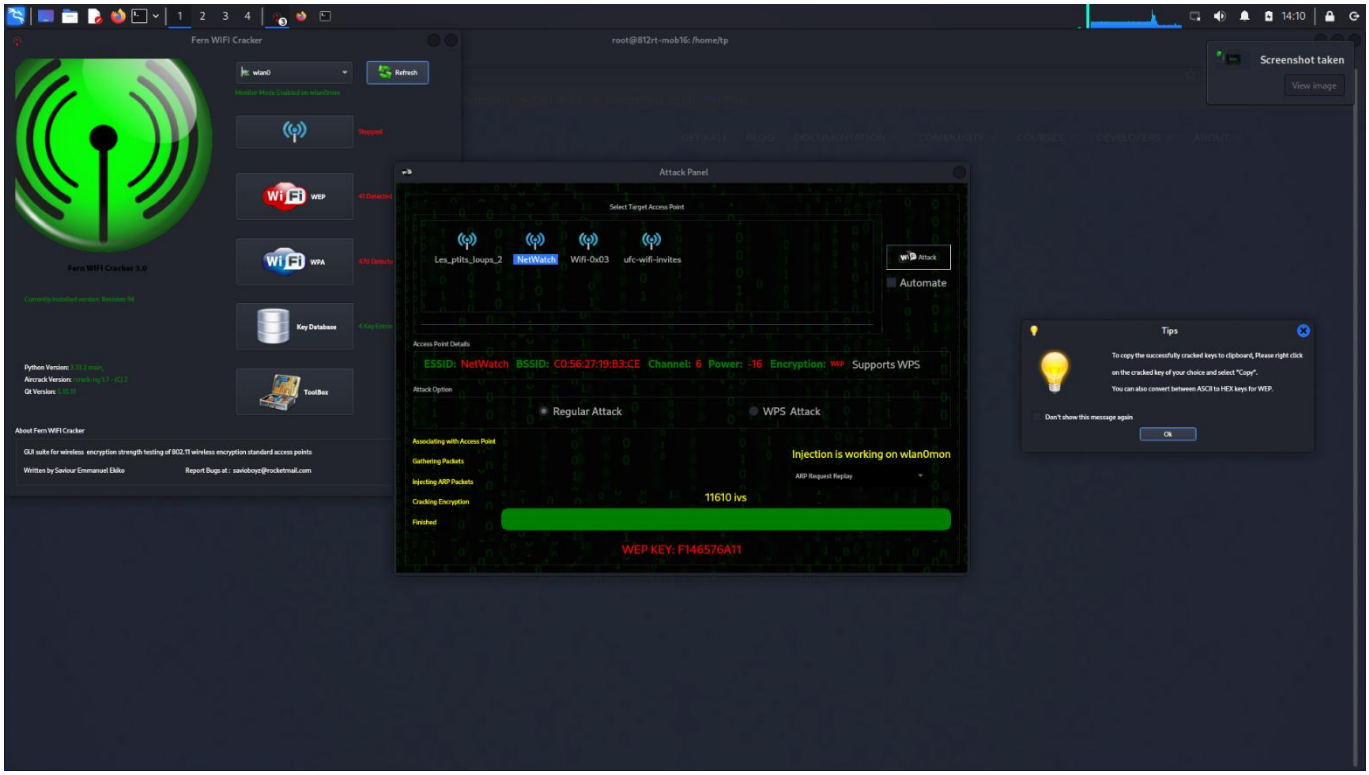
Étapes pour obtenir une clé WEP :

1. Mise en mode moniteur de la carte réseau :
   Active le mode moniteur sur ta carte Wi-Fi pour intercepter les paquets sans se connecter au réseau.
   (Ex. : airmon-ng start wlan0)
2. Scan des réseaux à portée :
   Lancement de recherche des points d'accès pour repérer un réseau protégé par WEP.
3. Sélection de la cible :
   On choisit le réseau WEP à attaquer dans la liste des réseaux détectés.
4. Capture des paquets (IVs) :

L'outil intercepte déconnecte l'utilisateur pour le forcé a se reconnecté les paquets contenant des vecteurs d'initialisation (IVs) qui sont nécessaires pour casser la clé.
Plus il y a de trafic, plus les paquets sont collectés rapidement.

5. Affichage de la clé :
   La clé WEP est affichée en clair une fois l'attaque réussie.

Screen du fern wifi cracker après le scan

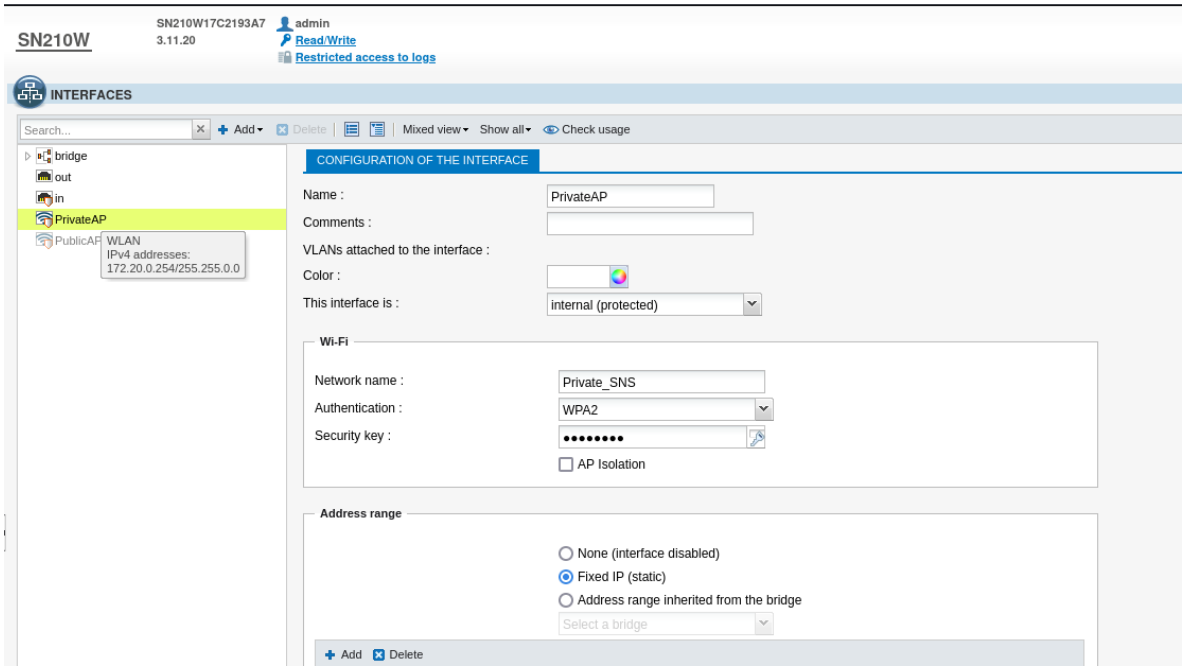


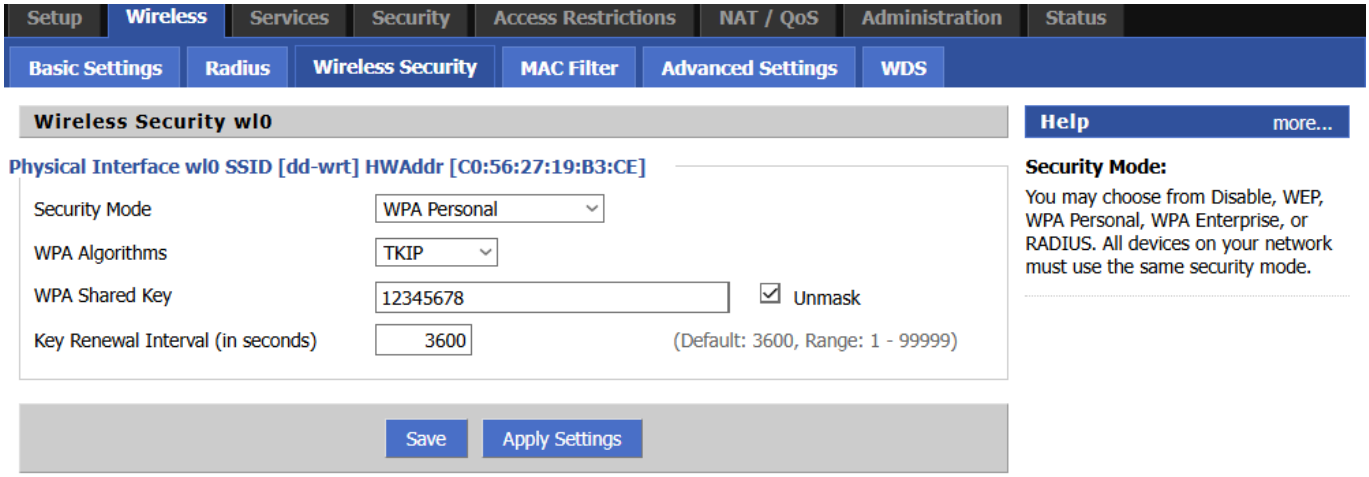
Cette image montre la réussite d'une attaque WEP sur le réseau NetWatch avec Fern WiFi Cracker. Après collecte de 11 610 paquets IVs et injection ARP, la clé WEP F146576A11 a été récupérée. Cela illustre la faiblesse du protocole WEP face aux attaques automatisées.

WPA:

Configurer un point d'accès Wi-Fi sécurisé en WPA sur une borne Linksys et sur le stormshield, puis utiliser une méthode d'attaque par capture de handshake pour tenter de récupérer la clé de sécurité. Cette étape vise à démontrer les différences entre WEP et WPA en termes de résistance aux attaques.

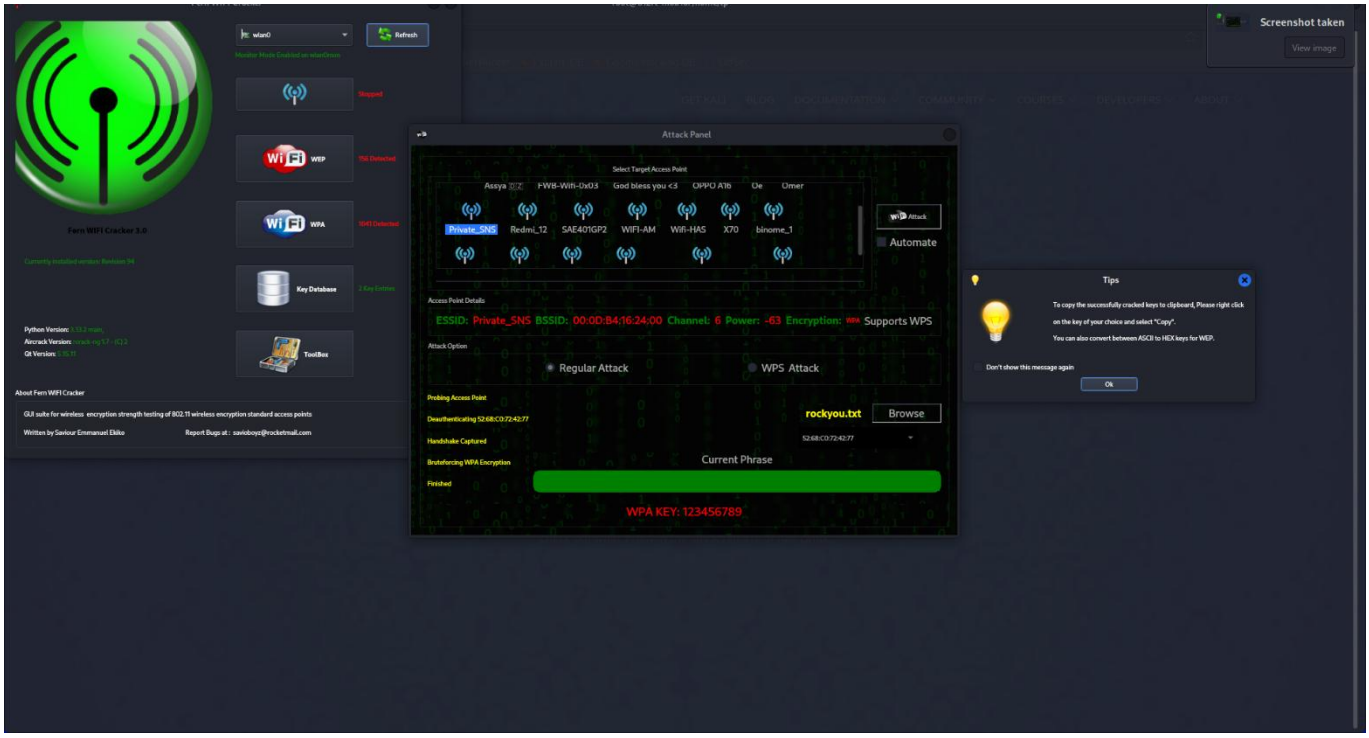
Screen de la mise en place du WPA sur le Stormshield et le Linksys





Utilisation de Fern WiFi Cracker

Fern WiFi Cracker permet de lancer facilement des attaques sur les réseaux protégés par WPA/WPA2 grâce à son interface graphique. Il automatise la capture du handshake ainsi que le craquage de la clé à l'aide d'un dictionnaire de mots de passe. Cela rend le processus accessible, rapide à mettre en œuvre, et idéal pour une démonstration pédagogique.



Étapes pour obtenir une clé WPA avec Fern WiFi Cracker

1. Mise en mode moniteur de l'interface Wi-Fi

   On met le mode moniteur pour intercepter les communications. (airmon-ng start wlan0)

2. Scan des réseaux à portée

   Détecte les points d'accès WPA/WPA2 autour.

3. Sélection du réseau cible

   Lancement de l'attaque sur notre wifi.

4. Capture du handshake

   Le handshake en forçant un client connecté à se reconnecter (attaque de désauthentification).

5. Craquage de la clé WPA

   Une fois le handshake capturé, Fern wifi tente de trouver la clé via un dictionnaire de mots de passe.

6. Affichage du mot de passe (si trouvé)
   - La clé est affichée si elle correspond à une entrée du dictionnaire utilisé.

L'interface de Fern WiFi Cracker affiche un point d'accès WPA sélectionné. L'outil a capturé un handshake valide et tente ensuite de craquer la clé via un dictionnaire. Si le mot de passe est présent dans le fichier, la clé est révélée. Cette étape met en lumière la dépendance des attaques WPA aux fichiers de mots de passe et à la robustesse du mot de passe utilisé.

L'attaque WPA via Fern WiFi Cracker a permis de capturer le handshake du réseau ciblé. Contrairement au WEP, la clé n'a été trouvée que si elle figurait dans le dictionnaire utilisé, ce qui souligne que la sécurité WPA dépend fortement de la complexité du mot de passe. Bien que plus sécurisé que WEP, WPA reste vulnérable aux attaques par dictionnaire ou brute-force si le mot de passe est faible

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

Liste des personnes impliquées avec pourcentage de répartition	
CHAKER Nabil 100%	55 Heures

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

Objectif : Réaliser plusieurs évaluations de la sécurité des serveurs

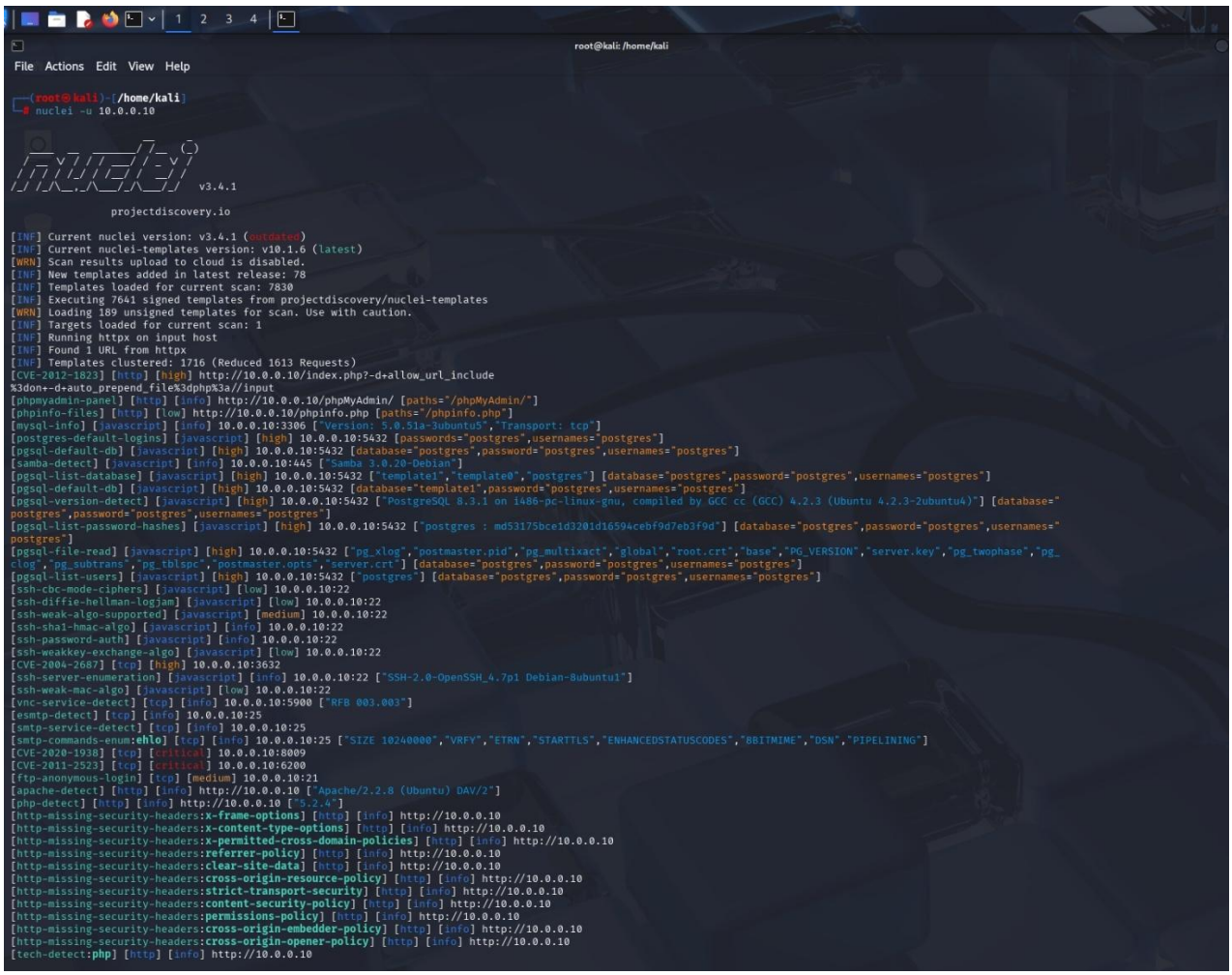
Sous-tâches	Evaluation prof
Installez dans la DMZ une machine/VM metasploitable	100%
Installez et utilisez SCNR	100%
Installez et utilisez Legion	100%
Installez et utilisez Nuclei	100%
Installez et utilisez Nikto	100%
Placez les scanners dans la DMZ, puis à l'extérieur	100%

Rapport

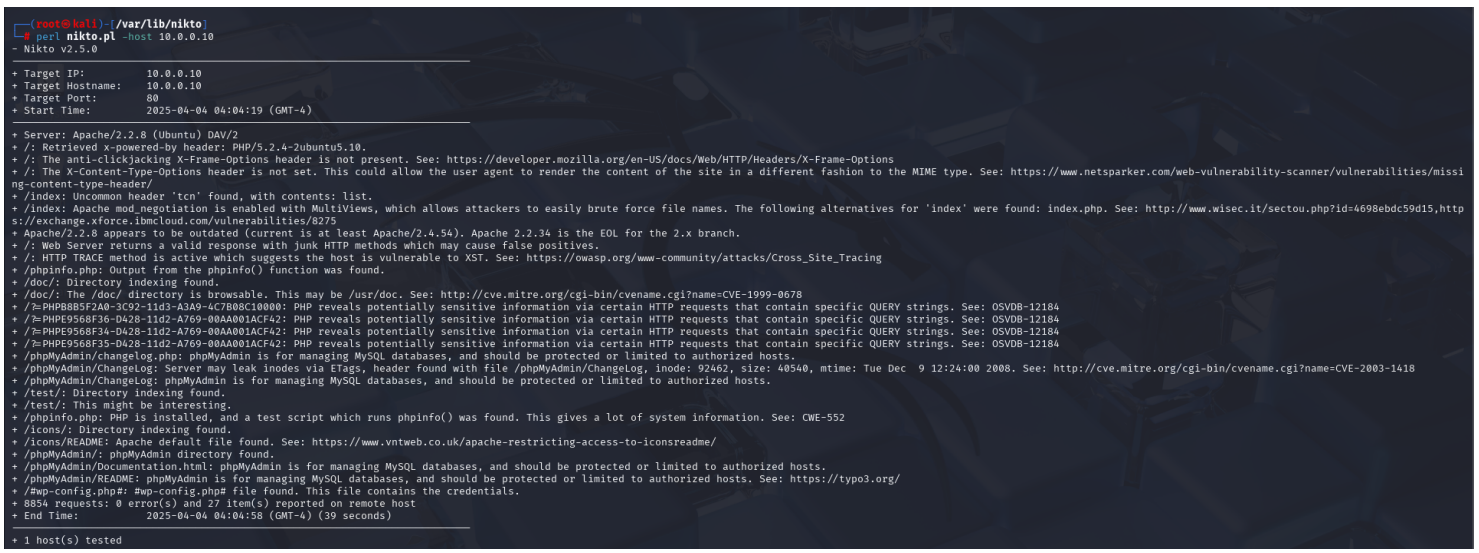
Dans cette nouvelle phase, l'objectif est de mettre en place un environnement de test orienté cybersécurité au sein de la DMZ (zone démilitarisée). Plusieurs outils de scanning de vulnérabilités seront installés et utilisés afin d'analyser le comportement d'une machine vulnérable, en l'occurrence Metasploitable.
Les sous-tâches consisteront à déployer et tester différents scanners (SCNR, Legion, Nuclei, Nikto) dans des contextes variés : en interne (DMZ) puis depuis l'extérieur, afin de comparer les résultats et évaluer l'exposition des services.

Un scan a été réalisé depuis la machine Kali (IP : 10.0.0.11) placée dans la DMZ, à l'aide des outils Nuclei, SCNR, Nikto et Legion. La cible était la machine Metasploitable (IP : 10.0.0.10), également située dans la DMZ. Cette configuration permet de tester les outils de scan dans un environnement isolé, tout en ayant un accès direct à la machine vulnérable. Puis sur le réseau public nous avec les IP Kali en 87.10.10.30 et Metasploitable en 87.10.10.32

Scan nuclei dans la DMZ :



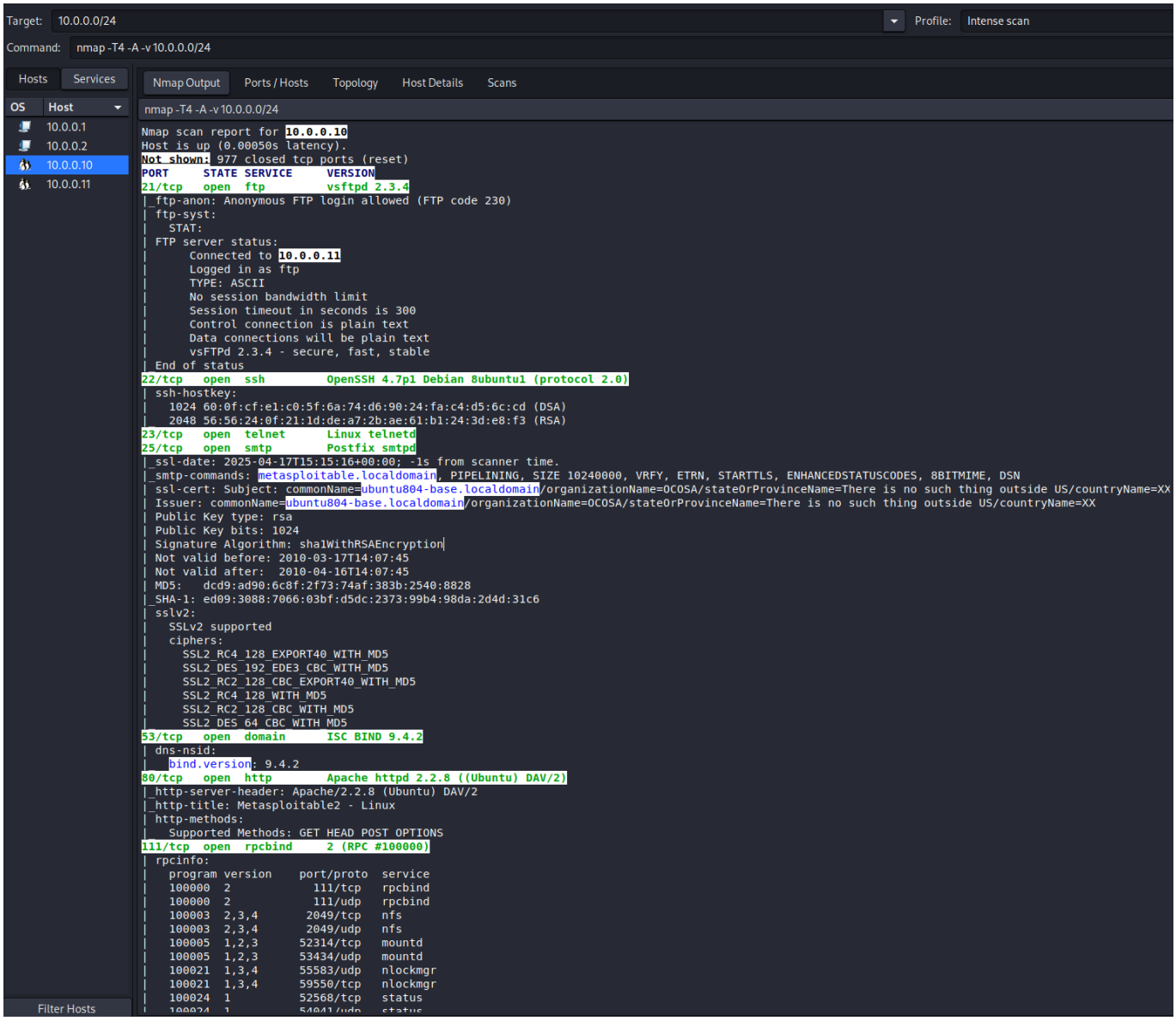
Scan nikto dans la DMZ :



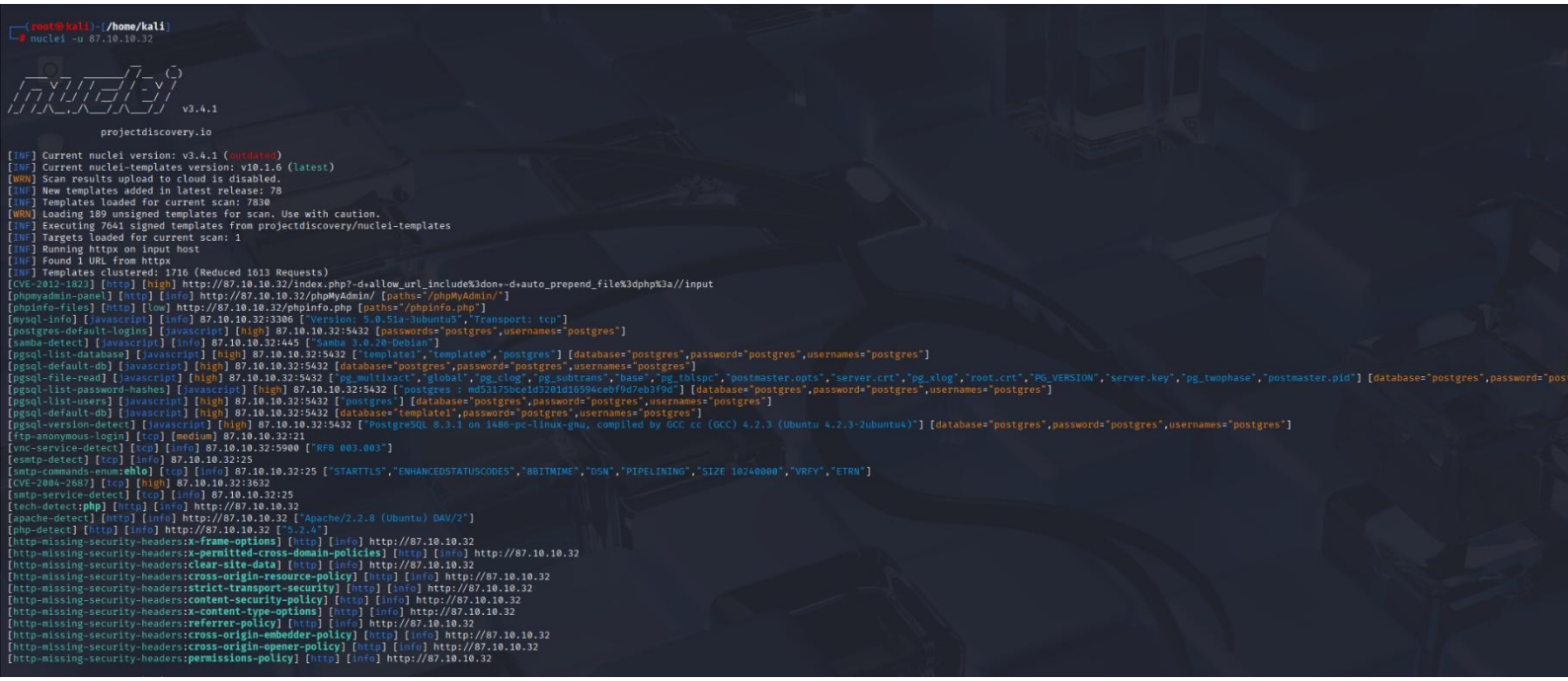
Scan scnr dans la DMZ :

```
SCNR::Engine has discovered that the affected page permits the HTTP `TRACE` method.

[~] Tags: xst, methods, trace, server

[~] CWE: http://cwe.mitre.org/data/definitions/693.html
[~] References:
[~]   CAPEC - http://capec.mitre.org/data/definitions/107.html
[~]   OWASP - http://www.owasp.org/index.php/Cross_Site_Tracing

[~] URL:        http://10.0.0.10/
[~] Element:    server

[~] Proof:     "HTTP/1.1 200 OK"

[~] Referring page: http://10.0.0.10/

[~] Affected page:  http://10.0.0.10/
[~] HTTP request
TRACE / HTTP/1.1
Host: 10.0.0.10
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Gecko) SCNR::Engine/v0.1.2
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: 2c41ab0ecc06a69f8c8c756bef3c1f6d
X-Scnr-Request-Id: 697
X-Scnr-Introspector-Trace: 1



[+] [9] Private IP address disclosure (Trusted)
[~] ~~~~~~~~~~~~~~~~~~~~
[~] Digest:     1739033593
[~] Severity:   Low
[~] Description:
[~]
Private, or non-routable, IP addresses are generally used within a home or
company network and are typically unknown to anyone outside of that network.
```

Scan legion remplacé par zenmap dans la DMZ :



Scan nuclei sur le réseau public :



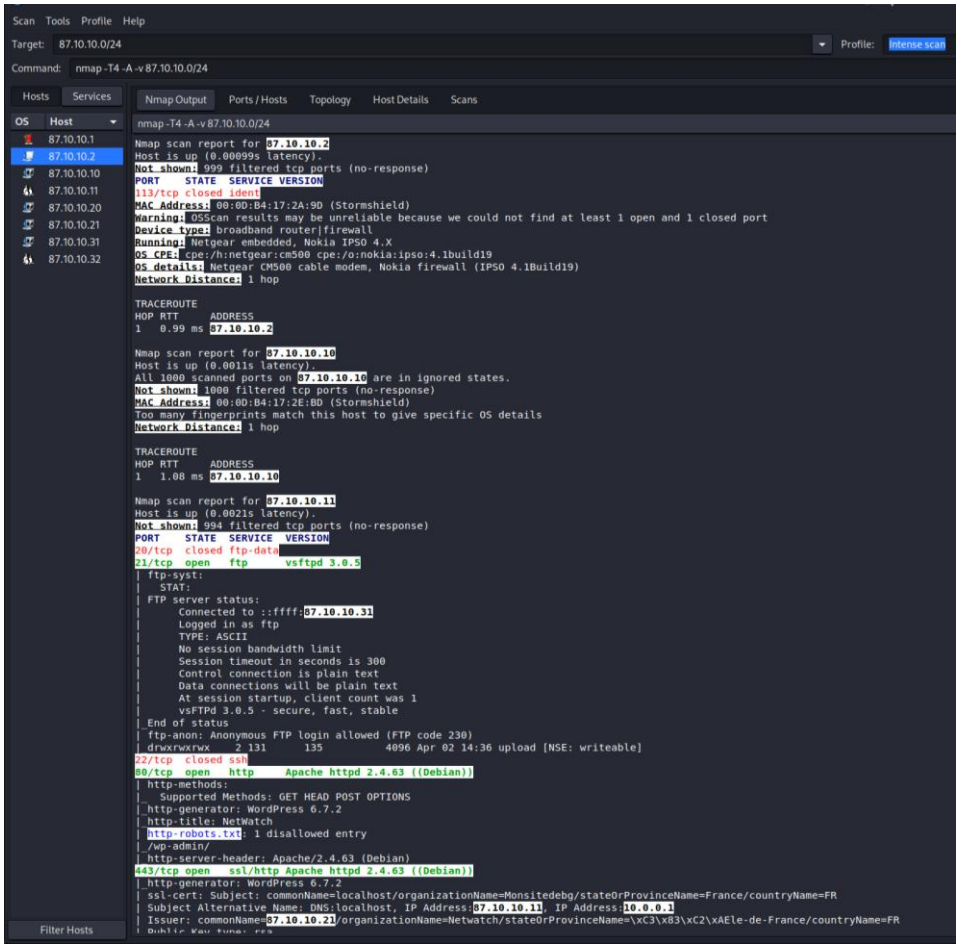
Scan nikto sur le réseau public :

```
┌──(root㉿kali)-[/var/lib/nikto]
└─# perl nikto.pl -host 87.10.10.32
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          87.10.10.32
+ Target Hostname:    87.10.10.32
+ Target Port:        80
+ Start Time:         2025-04-08 05:19:18 (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-vu
nerability-scanner/vulnerabilities/missing-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.w
isec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: 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
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See: http://cve.mitre.org/cgi-bi
n/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /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.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8882 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-04-08 05:20:26 (GMT-4) (68 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Scan scnr dans le réseau public :

```
 [~] Tags: path, directory, common, discovery

 [~] CWE: http://cwe.mitre.org/data/definitions/538.html
 [~] References:
 [~]   CWE - http://cwe.mitre.org/data/definitions/538.html
 [~]   OWASP - https://www.owasp.org/index.php/Forced_browsing

 [~] URL:        http://87.10.10.32/doc/login/
 [~] Element:    server

 [~] Proof:     "HTTP/1.1 200 OK"



 [~] Referring page: http://87.10.10.32/doc/

 [~] Affected page:  http://87.10.10.32/doc/login/
 [~] HTTP request
GET /doc/login/ HTTP/1.1
Host: 87.10.10.32
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Gecko) SCNR::Engine/v0.1.2
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: 9b48ee0a4d03ce5ab858a453efd005de
X-Scnr-Request-Id: 2618
X-Scnr-Introspector-Trace: 1



 [+] [4] Common directory (Trusted)
 [~] ~~~~~~~~~~~~~~~~~~~
 [~] Digest:     2668727389
 [~] Severity:   Medium
 [~] Description:
 [~]
```

Scan légion remplacé par zenmap réseau public :



Différences entre scan LAN et scan externe

Lors de mes analyses, j'ai constaté des différences notables entre les scans réalisés en interne (LAN) et ceux effectués depuis l'extérieur (Internet). Ces écarts s'expliquent par le filtrage mis en place par le pare-feu, qui limite l'accès aux services internes depuis l'extérieur.

Pour un attaquant, cela complique la tâche dès la première phase d'une attaque, à savoir l'énumération, en ralentissant la découverte des services exposés et en réduisant ainsi la surface d'attaque accessible.

SCNR

L'installation de SCNR a été particulièrement compliquée : la documentation est peu claire, ce qui n'a pas facilité sa mise en place.
En revanche, son efficacité est impressionnante, aussi bien depuis le LAN que depuis l'extérieur. Son principal avantage est aussi sa limite : SCNR est très rigoureux et fouille en profondeur, ce qui peut entraîner des scans très longs si les cibles ne sont pas restreintes.
Dans notre cas, en lançant simplement, ./scnr http://ip sans options spécifiques, l'outil a entrepris un scan exhaustif de toutes les pages et sous-domaines détectés, en testant l'ensemble de ses méthodes.
Le scan a duré 9 heures, la machine cible étant vulnérable pour voir les différentes failles de sécurité.

Nikto :

Nikto s'est montré facile à installer et à utiliser. Il suffit de lancer la commande :
perl nikto.pl -host IP
Spécialisé dans les scans web, Nikto détecte notamment des vulnérabilités telles que les failles XSS.
Il propose également un paramètre de niveau d'analyse, permettant d'adapter la profondeur du scan en

fonction des besoins. Nikto nous a fourni une liste claire des failles détectées, ce qui le rend très utile pour une analyse rapide.

Nuclei :

Comme Nikto, Nuclei ne pose aucune difficulté d'installation ou d'utilisation. La commande de base est : nuclei -u IP
Cet outil offre une portée de détection très large, en scannant une grande variété de protocoles et services, tout en gardant un fort accent sur les vulnérabilités web.
Sa rapidité et sa polyvalence en font un excellent outil pour un premier aperçu général des failles potentielles.

Legion

Parmi tous les outils testés, Legion est celui qui m'a posé le plus de problèmes. L'outil n'est plus maintenu, ce qui entraîne plusieurs erreurs d'exécution et des incompatibilités avec les versions récentes de certaines bibliothèques. Malgré une interface graphique intéressante, ces dysfonctionnements ont rendu son utilisation impossible pour se faire j'ai décidé d'utilisé zenmap pour avoir un scan…

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

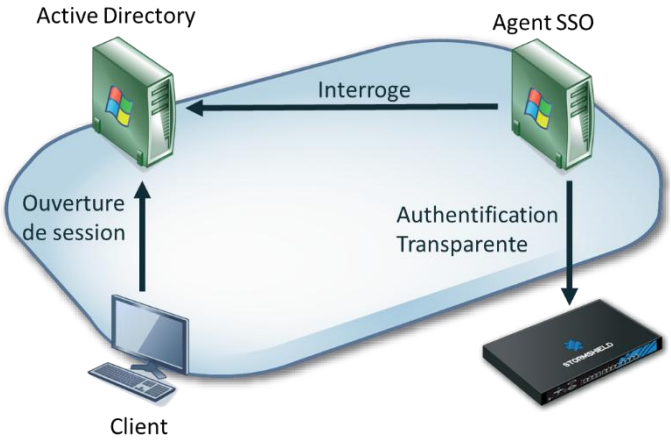
Liste des personnes impliquées avec pourcentage de répartition	
CHAKER Nabil 50% DOGAN Eren 50%	20 heures pour le groupes

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

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

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

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



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

Les échanges entre l'agent et le firewall utilisent le port 1301/TCP et sont chiffrés grâce au protocole

SSL, algorithme PSK-AES256-CBC-SHA.

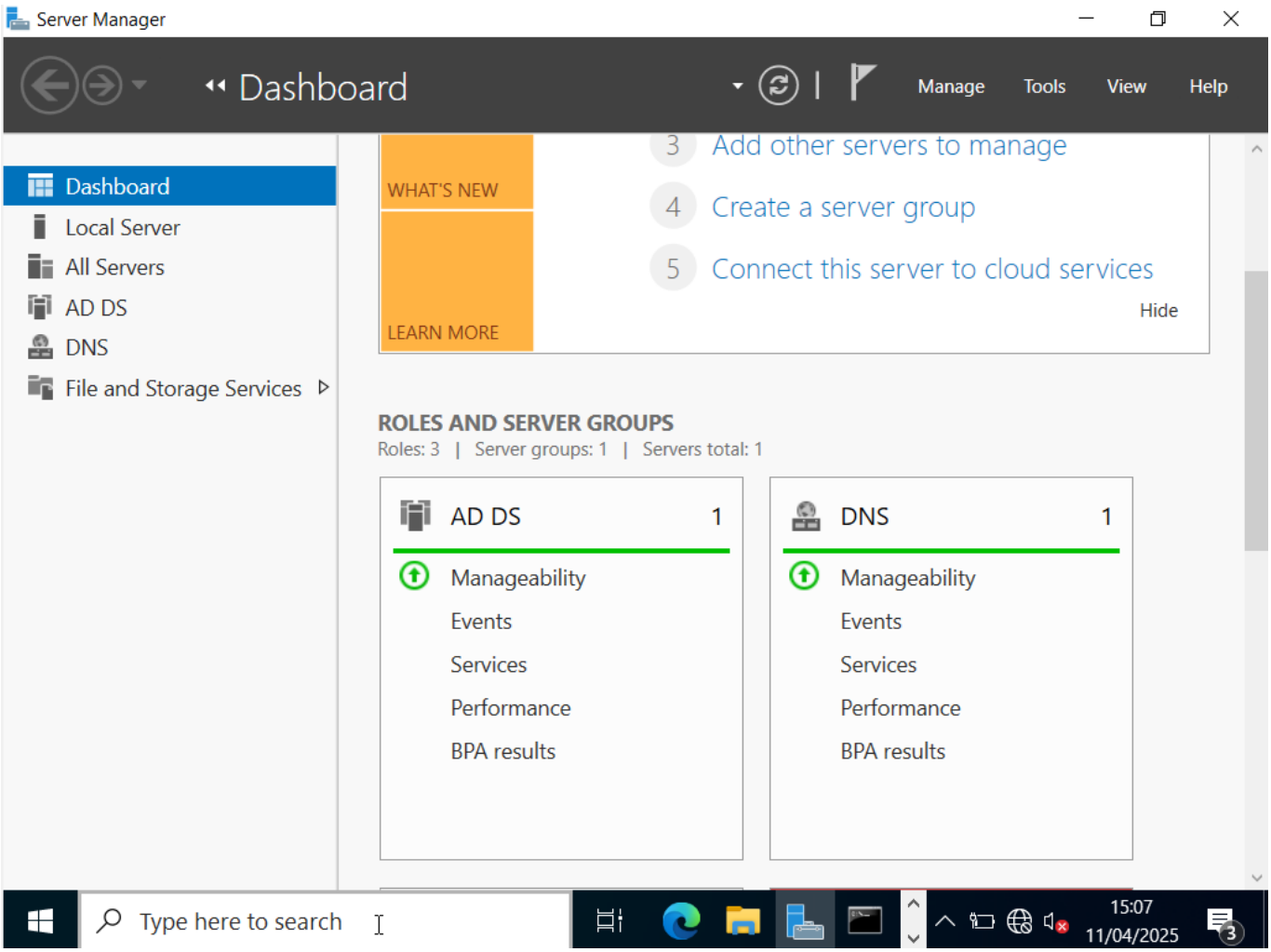
L'authentification doit être robuste au changement de l'adresse IP de la machine client.

Sous-tâches	Evaluation prof
Installation d'un serveur Active Directory	100%
Installation d'un agent SSO sur une machine	100%
Configuration de la machine de client	100%
Changement de l'adresse IP de la machine	100%

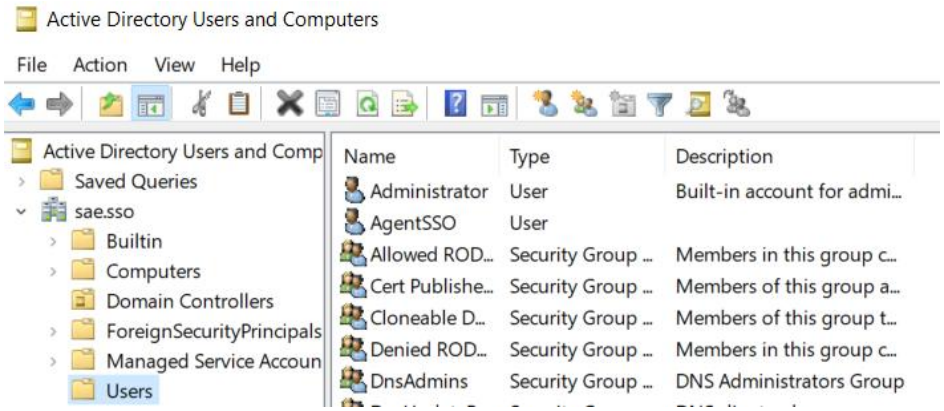
Pour mettre en place l'Agent SSO avec l'Active Directory, nous avons utilisé une machine virtuelle hébergées localement sur VirtualBox :

- Une VM Windows Server 2022
- Un PC

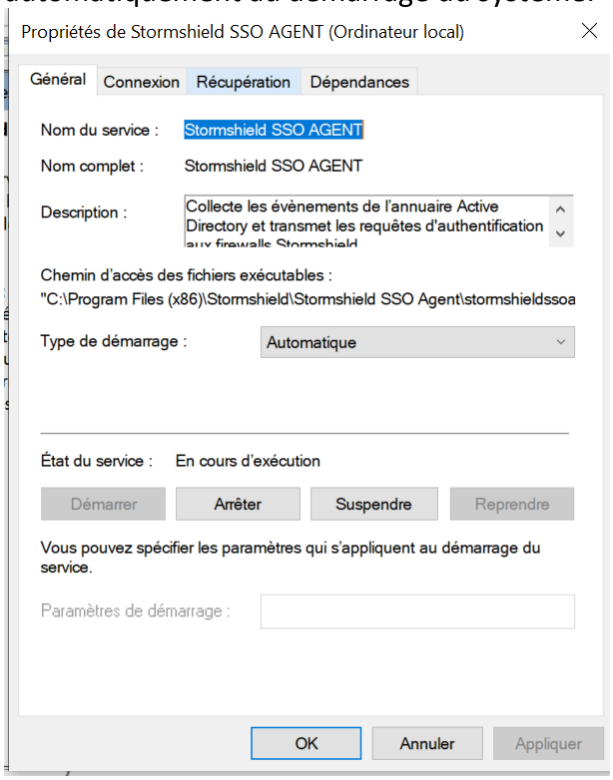
Nous avons installé et configuré un contrôleur de domaine Active Directory ainsi qu'un serveur DNS, indispensables pour que l'Agent SSO puisse s'intégrer correctement au réseau.



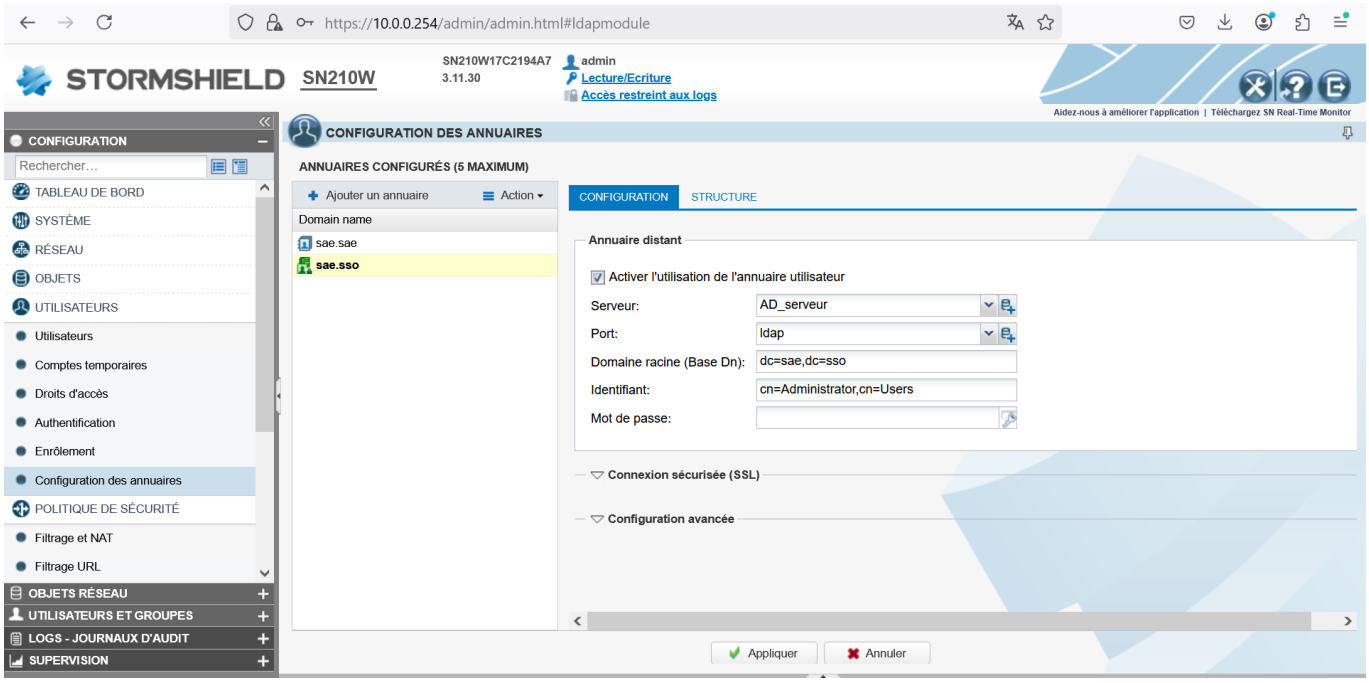
Un compte utilisateur dédié, nommé AgentSSO, a également été créé et configuré pour fonctionner en tant que compte de service.

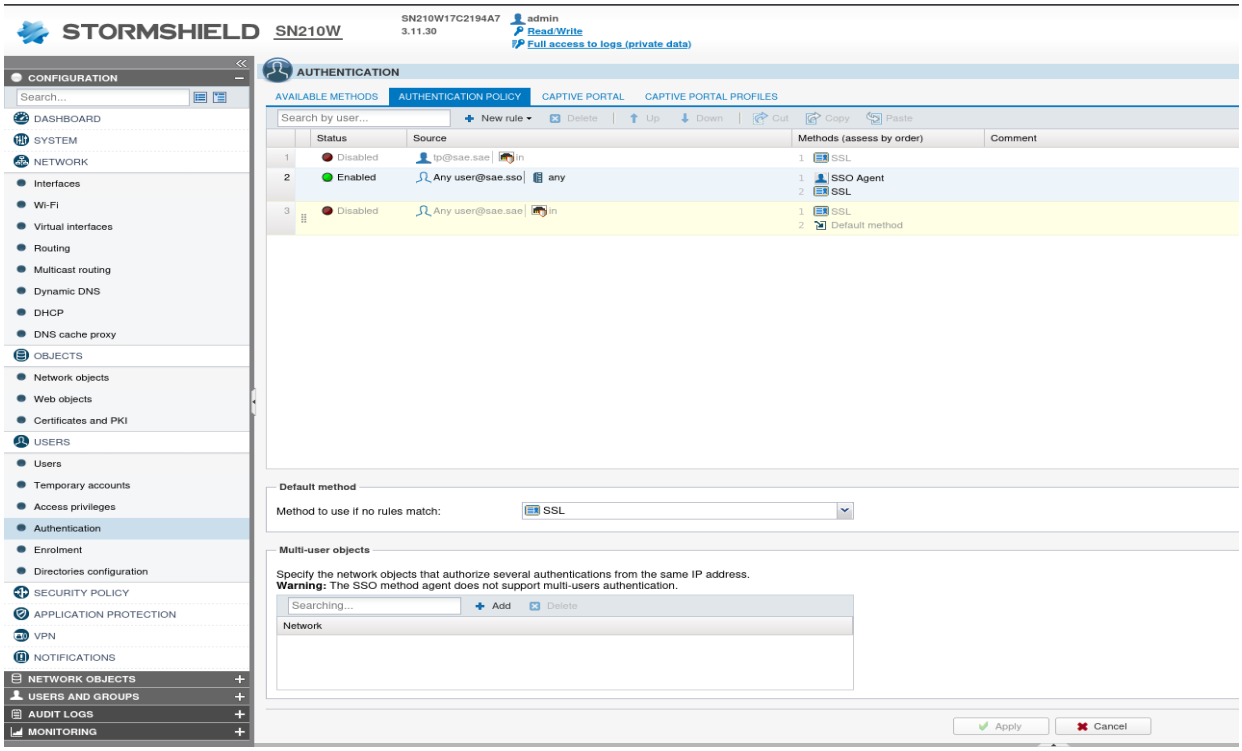


Après l'installation de l'Agent SSO sur la machine Windows 10, le service a été activé pour qu'il démarre automatiquement au démarrage du système.

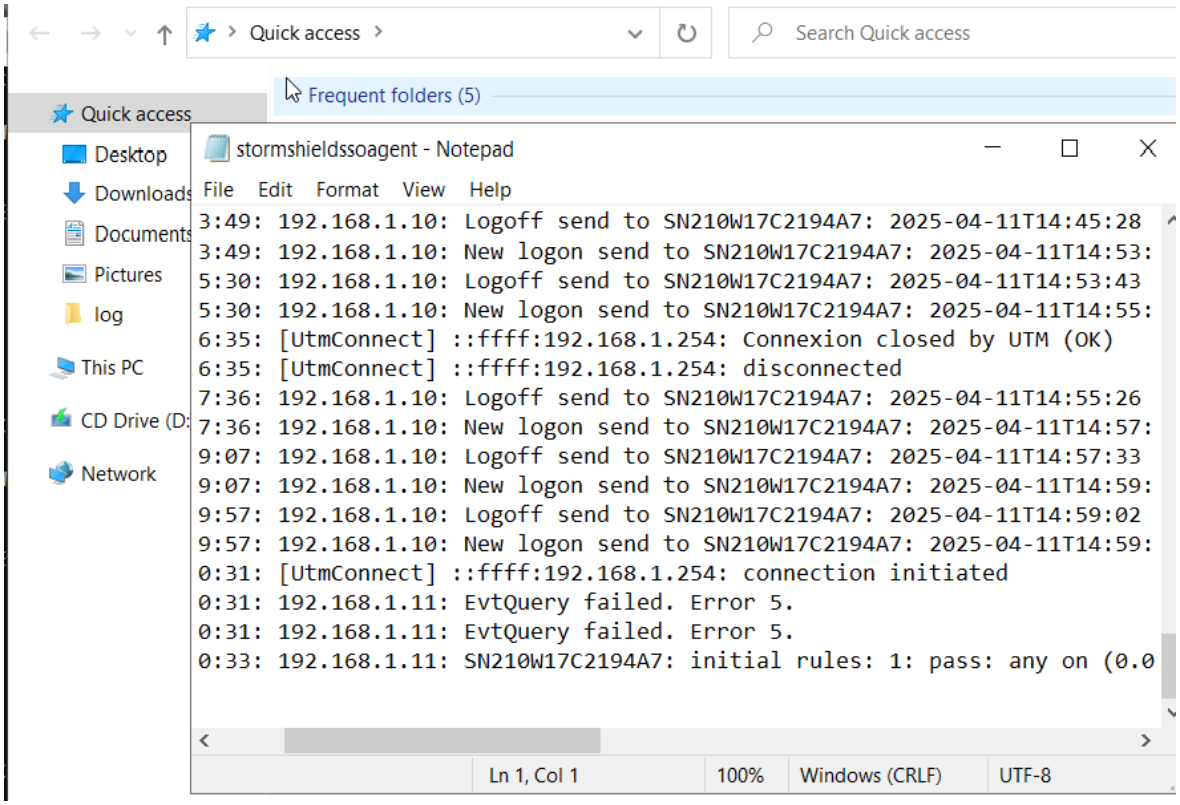


Côté Stormshield, on a configuré l'accès à l'annuaire Active Directory puis mis en place une règle d'authentification basée sur l'Agent SSO.

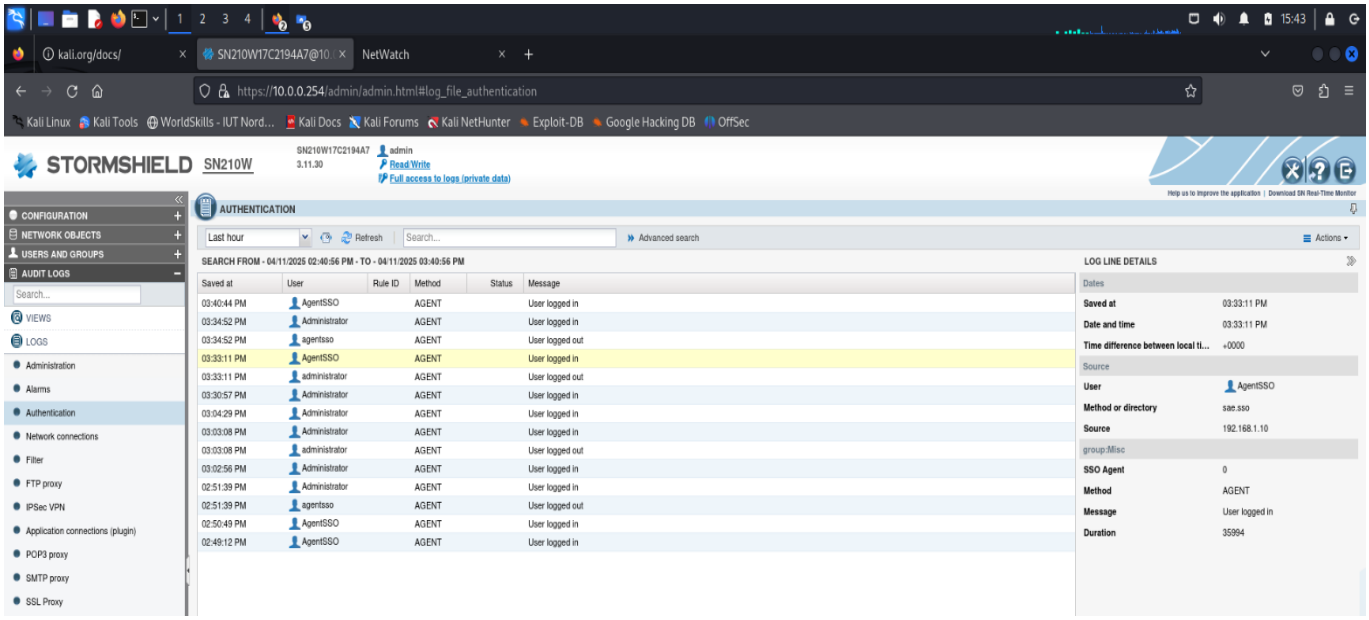




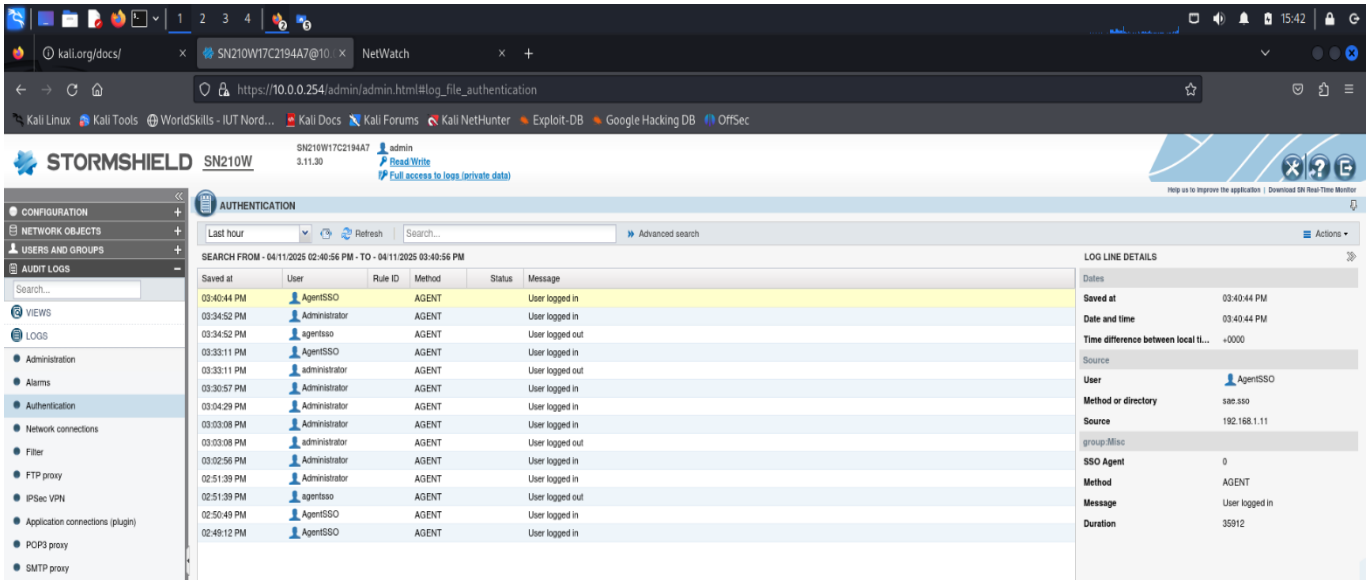
Les logs du Stormshield confirment que l'agent est bien connecté une premier fois en 192.168.1.10, et reste fonctionnel même après un changement d'adresse IP en 192.168.1.11, ce qui valide le bon fonctionnement de la solution.



Nous avons ensuite regardé les logs du Stormshield où nous voyons la connexion de l'utilisateur AgentSSO avec son adresse IP en 192.168.1.10.



Après avoir changé l'adresse IP du client en passant de 192.168.1.10 à 192.168.1.11. Nous voyons que l'utilisateur est toujours connecté mais cette fois-ci avec l'adresse IP en 192.168.1.11. Cela montre que l'Agent SSO fonctionne.


kali.org/docs/
SN210W17C2194A7@10.
NetWatch
https://10.0.0.254/admin/admin.html#log_file_authentication
Kali Linux
Kali Tools
WorldSkills - IUT Nord...
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
STORMSHIELD
SN210W
SN210W17C2194A7
3.11.30
admin
Read/Write
Full access to logs (private data)
CONFIGURATION
NETWORK OBJECTS
USERS AND GROUPS
AUDIT LOGS
VIEWS
LOGS
Administration
Alarms
Authentication
Network connections
Filter
FTP proxy
IPSec VPN
Application connections (plugin)
POP3 proxy
SMTP proxy
AUTHENTICATION
Last hour
Refresh
Search...
Advanced search
Actions
SEARCH FROM - 04/11/2025 02:40:56 PM - TO - 04/11/2025 03:40:56 PM
Saved at
User
Rule ID
Method
Status
Message
03:40:44 PM AgentSSO AGENT User logged in
03:34:52 PM Administrator AGENT User logged in
03:34:52 PM agentsso AGENT User logged out
03:33:11 PM AgentSSO AGENT User logged in
03:33:11 PM administrator AGENT User logged out
03:30:57 PM Administrator AGENT User logged in
03:04:29 PM Administrator AGENT User logged in
03:03:08 PM Administrator AGENT User logged in
03:03:08 PM administrator AGENT User logged out
03:02:56 PM Administrator AGENT User logged in
02:51:39 PM Administrator AGENT User logged in
02:51:39 PM agentsso AGENT User logged out
02:50:49 PM AgentSSO AGENT User logged in
02:49:12 PM AgentSSO AGENT User logged in
LOG LINE DETAILS
Dates
Saved at 03:40:44 PM
Date and time 03:40:44 PM
Time difference between local ti... +0000
Source
User AgentSSO
Method or directory sae.sso
Source 192.168.1.11
group:Misc
SSO Agent 0
Method AGENT
Message User logged in
Duration 35912