KALI OSINT

Sommaire :

1. Préambule

Je vais donc rédiger un compte rendu de mes analyses faite sur le réseau du groupe Pierreval, avec les autorisations des administrateurs réseaux j'ai utilisé différents outils d'analyse. Grâce à la VM kali linux qui offre une panoplie d'outils informatique très puissant et qui sont libre d'accès, il existe plusieurs guides qui explique comment débuter et comment bien s'en servir.L'étude du réseau a été Réalisé dans un cadre éthique !

*Je tiens aussi à dire que pour des raisons évidentes, **aucune vulnérabilité** ne sera citée dans ce compte rendu. Celui-ci permet seulement de comprendre comment j'ai effectué mon analyse du réseau.

2. Identification :

Version	1.0 – 01/07/2024
Objectif	Comprendre ce que veut dire OSINT, et pourquoi est-il important de mener des analyses de sécurité.
Demande complémentaire à faire auprès du service Informatique	Aucune, Toutes les autorisations ont été accordé.

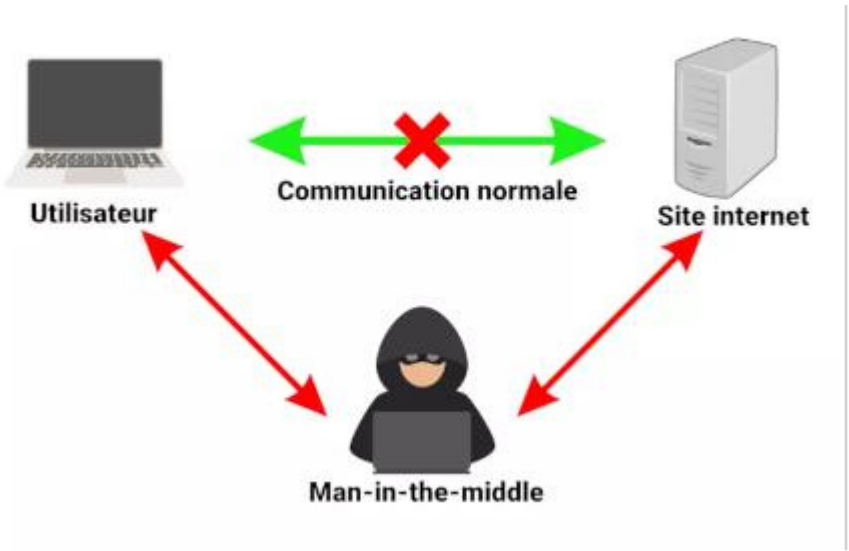
3- Serveur de Messagerie :

Les enregistrements DNS : on y retrouve SPF, DKIM, DMARC.

SPF est configuré automatiquement lorsque le Nom de Domaine est créé. Autrement il est mis en place par l'un des protocoles de la licence Microsoft365.
-J'ai pris soin de vérifier sur le site Vérification du dossier SPF | Vérificateur SPF | Mimecast qu'il était bien actif.

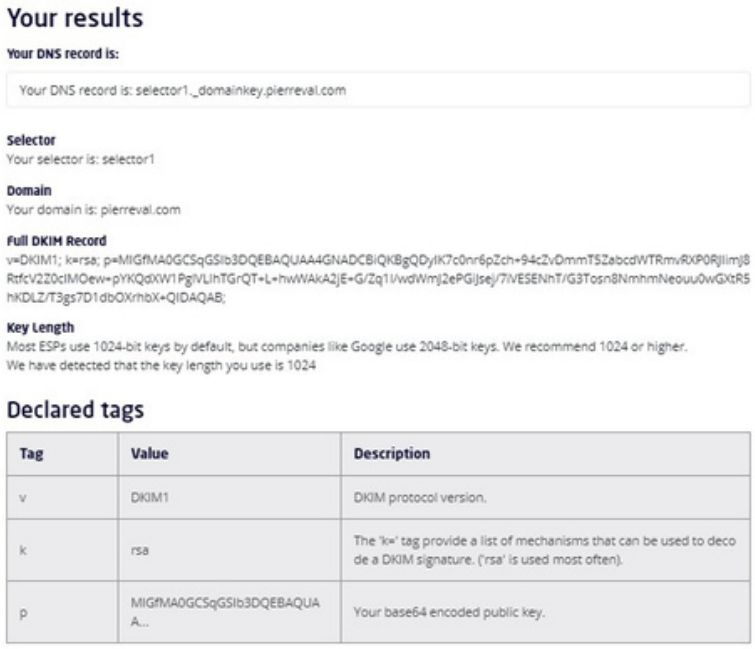
Passons maintenant à DKIM qui est un acronyme pour Domain Keys Identified Mail. Cette technologie permet d'envoyer un message chiffré, et de s'assurer que celui-ci n'a subi **aucune altération durant sa transition entre le serveur émetteur et le serveur récepteur.**
Comparé à SPF il n'est pas mis automatiquement après la configuration d'un DNS il est donc important de vérifier ou de le mettre en place.

DKIM permet d'éviter la fameuse attaque du « MAN IN THE MIDDLE ».



DKIM prouve que le contenu du mail ainsi que les en-têtes n'ont subi aucune altération : le mail est donc authentique et légitime : personne ne l'a envoyé à votre place, et le serveur de messagerie distant a maintenant la capacité de le vérifier.

Après vérification sur le site suivant, on sait que DKIM est bien mis en place et que la clé publique de pierreval.com encodé sur 1024 bits.



Your results

Your DNS record is:

Your DNS record is: selector1._domainkey.pierreval.com

Selector
Your selector is: selector1

Domain
Your domain is: pierreval.com

Full DKIM Record
v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDyIK7c0nr6pZch+94cZvDmmT5ZabcdWTRmvRXP0RjIimJ8RtfcV2Z0cIMOew+pYKQdXW1PgiVLIhTGrQT+L+hwWAkA2jE+G/Zq1i/wdWmJ2ePGijsej/7IVESENhT/G3Tosn8NmhmNeouu0wGXtR5hKDLZ/T3gs7D1dbOXrhbX+QIDAQAB;

Key Length
Most ESPs use 1024-bit keys by default, but companies like Google use 2048-bit keys. We recommend 1024 or higher.
We have detected that the key length you use is 1024

Declared tags

Tag	Value	Description
v	DKIM1	DKIM protocol version.
k	rsa	The 'k=' tag provide a list of mechanisms that can be used to decode a DKIM signature. ('rsa' is used most often).
p	MIGfMA0GCSqGSIb3DQEBAQUAA...	Your base64 encoded public key.

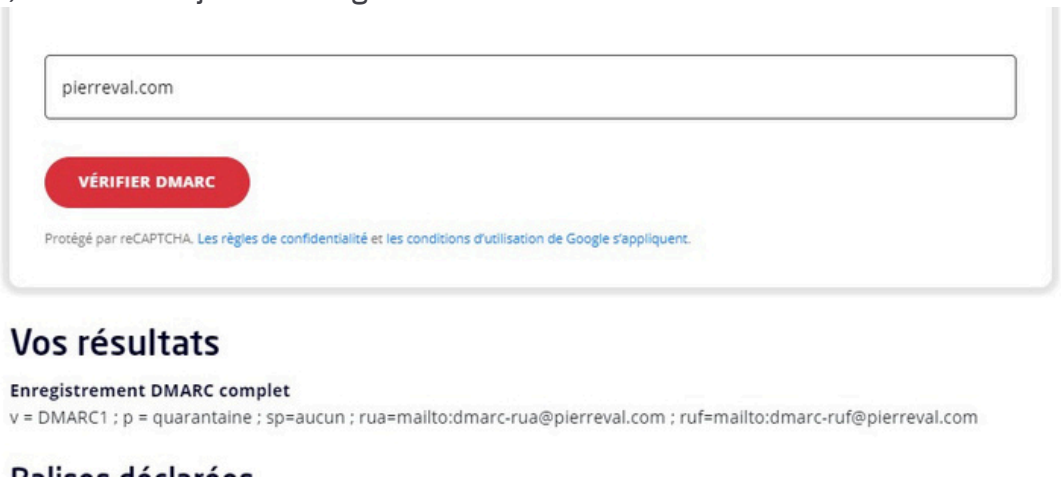
On va Maintenant passer à DMARC :

DMARC est un acronyme pour Domain-based Message Authentication, Reporting, and Conformance. **DMARC utilise SPF et DKIM pour authentifier les expéditeurs d'emails**, et fournit une protection supplémentaire. En effet, SPF et DKIM permettent d'authentifier un expéditeur (ou non). Mais ils ne donnent aucune indication sur la conduite à tenir dans le cas d'une usurpation d'identité avérée.

C'est là que DMARC entre en jeu : lorsqu'on configure cet enregistrement DNS, on lui indique une politique à tenir. Cela permet au serveur de messagerie de savoir quoi faire de ces mails : faut-il les rejeter ? les mettre en quarantaine ? Ne rien faire mais l'historiser ?

A Nous de le décider, et ça se passe dans DMARC.

Pareil ici, DMARC a déjà été configuré :



4 – Analyse Nmap

J'ai effectué plusieurs test très simple grâce aux logiciels nmap, qui m'ont permis de scanner plusieurs port TCP/UDP.

Il existe des versions avec des interfaces graphiques, cependant pour comprendre comment ça marche, j'ai préféré utiliser le logiciel en ligne de commande sur la VM Kali.

Je vais lister un maximum de commande que j'ai pu rentrer sur le logiciel sans trop rentrer dans les détails, ainsi je n'afficherais pas le résultat des commandes passé, pour des raisons de sécurité envers le groupe Pierreval.

Commandes :

- `nmap -v -A -sV 192.168.0.0 /16`
- `nping --tcp -p --flags --ttl`
- nmap -T4 -A -v 192.168.2.232
- nmap -T4 -A -v -Pn 192.168.2.232
- nmap -p 1-65535 -T4 -A -v 192.168.2.0
- nmap -sS -sU -T4 -A -v 192.168.2.0

Tout cela m'a permis de voir les ports ouvert ou fermé et ainsi par la suite faire des recherches afin de « localiser » les services mis à disposition sur les ports identifiés.

5. Analyse Amass :

- Amass est un outil inclus dans la distribution Kali Linux . Il aide les professionnels de la sécurité informatique à effectuer une cartographie réseau des surfaces d'attaque et à découvrir des actifs externes. Amass utilise des techniques de collecte d'informations open source et d'identification active.

Commandes :

- Intel
- Enum

6 – Fin Procédure :