

ANALYSE DE MAILS MALVEILLANTS ET SÉCURISATION

DESCRIPTION DU THÈME

Propriétés	Description
Intitulé long	Analyse de mails malveillants et sécurisation
Formation(s) concernée(s)	<input type="checkbox"/> Classes de première Sciences et technologies du management et de la gestion (STMG) <input type="checkbox"/> Terminale STMG Système d'information de gestion (SIG) <input checked="" type="checkbox"/> BTS Services Informatiques aux Organisations
Matière(s)	<input type="checkbox"/> Sciences de gestion <input type="checkbox"/> SIG <input type="checkbox"/> Bloc 1 – Support et mise à disposition de services informatiques <input type="checkbox"/> Bloc 2 SISR – Administration des systèmes et des réseaux <input type="checkbox"/> Bloc 2 SLAM – Conception et développement d'applications <input checked="" type="checkbox"/> Bloc 3 SISR – Cybersécurité des services informatiques <input type="checkbox"/> Bloc 3 SLAM – Cybersécurité des services informatiques
Présentation	<p>Il s'agit ici d'apprendre à analyser l'en-tête puis le corps d'un courriel via l'utilisation d'outils spécifiques. Les courriels suspects feront l'objet d'une analyse de type bac à sable. Les attaques de type hameçonnage (<i>phishing</i>) seront présentées et les contre-mesures correspondantes abordées.</p> <p>Plus précisément, les objectifs de cette production sont les suivants :</p> <ul style="list-style-type: none"> • comprendre ce qu'est un courriel et sa structure. Les protocoles mis en œuvre lors de l'envoi et la réception d'un mail sont aussi présentés ; • apprendre à analyser un courriel suspect via l'extraction puis l'analyse des informations de l'en-tête et du corps du message ; • manipuler des outils en ligne d'analyse de courriels suspects en vue d'une analyse détaillée (pièces jointes, liens malveillants...) ; • tester une analyse dans un cadre sécurisé avec une démarche de type bac à sable ; • connaître et comprendre les outils utilisés en tant que contre-mesure pour valider la sécurité des courriels.
Savoirs	<p>Typologie des risques et leurs impacts.</p> <p>Cybersécurité : bonnes pratiques, normes et standards.</p>

Compétences	<p>Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service :</p> <ul style="list-style-type: none"> • Détecter les actions malveillantes • Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures <p>Préserver l'identité numérique de l'organisation</p> <ul style="list-style-type: none"> • Protéger l'identité numérique d'une organisation • Déployer les moyens appropriés de preuve électronique
Transversalité	
Prérequis	Connaissances de base de l'outil Wireshark.
Outils	<p>Wireshark, Thunderbird, app.anay.run et de nombreux autres outils en ligne.</p> <p>Les ressources en lignes utilisées (mails et fichier pcap) sont également fournis dans cette production dans le dossier « CapturesPCAP_et_Mails ».</p>
Mots-clés	Mail, courriel, e-mail, phishing, hameçonnage, usurpation d'identité, SPF, DKIM, DMARC
Durée	4 heures
Auteur·e·s	Patrice Dignan avec les relectures et les tests de Apollonie RAFFALLI et Yann Barrot.
Version	v1.0
Date de publication	février 2026

DERNIÈRES RÉVISIONS

Ce tableau contient les modifications apportées au document après sa publication uniquement.

Date	Auteur·e	Description

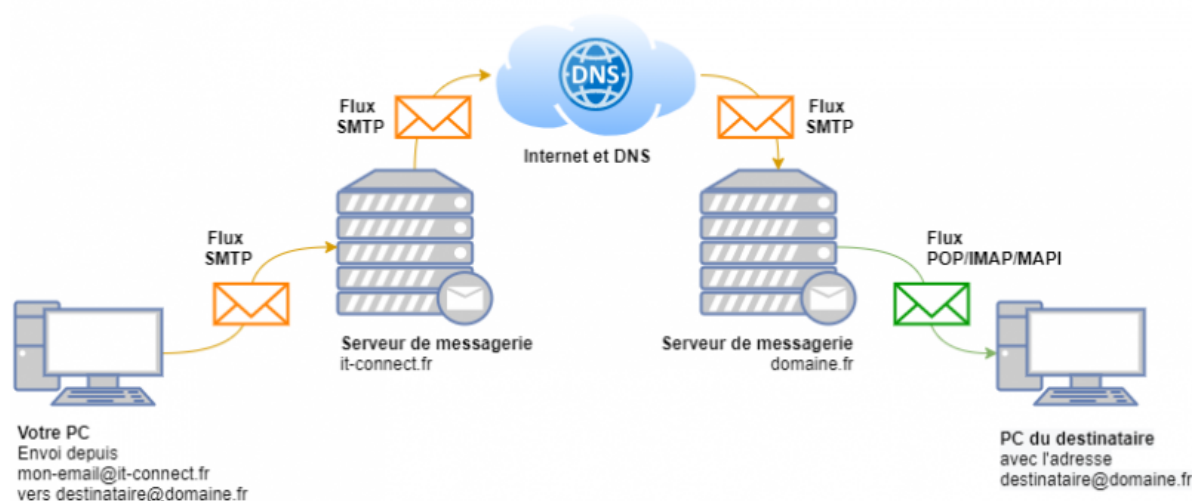
SOMMAIRE

A. Structuration des mails	5
A.1. Envoi et réception d'un mail	5
A.2. Protocoles mis en œuvre	5
A.3. Enveloppe, en-tête et corps d'un mail	6
A.4. Codes SMTP	9
B. Attaques de type hameçonnage	10
B.1. Définition	10
B.2. Caractéristiques communes	10
B.3. Type d'hameçonnage	11
B.4. Camouflage des liens	11
C. Analyse globale d'un mail malveillant	12
D. Analyse détaillée d'un mail malveillant	13
D.1. Collecte des premières informations	13
D.2. Analyse de l'en-tête	13
D.3. Analyse du corps du message	13
E. Analyse de type bac à sable	14
F. Contre-mesures	16
F.1. SPF (Sender Policy Framework)	16
F.2. DKIM (DomainKeys Identified Mails)	18
F.3. DMARC (Domain-Based Message Authentication)	19
F.4. S/MIME (Secure/ Multipurpose internet Mail Extensions)	20
G. Dossier documentaire	21
G.1. Comprendre et lire les en-têtes d'un message électronique (format IMF)	21
G.2. Fonctionnement des outils SPF, DKIM et DMARC	24

A. STRUCTURATION DES MAILS

A.1. ENVOI ET RÉCEPTION D'UN MAIL

Une adresse mail est composée d'un nom d'utilisateur, du symbole @ puis d'un nom de domaine. Le serveur DNS, via l'enregistrement MX¹, obtient l'adresse IP du serveur SMTP à joindre sur internet. Le mail passe à travers différents serveurs SMTP jusqu'à atteindre le serveur SMTP du destinataire. Le client de messagerie permet de récupérer le courrier puis de le lire.



<https://www.it-connect.fr/messagerie-decouverte-des-protocoles-smtp-pop-imap-et-mapi/>

A.2. PROTOCOLES MIS EN ŒUVRE

Protocoles	Définitions	Numéros de ports
SMTP (Simple Mail Transfer Protocol)	Protocole utilisé pour transférer des mails vers les serveurs de messagerie électronique.	25 en non chiffré et 565 ou 587 en chiffré
IMAP (Internet Message Access Protocol)	protocole où les mails et pièces jointes restent stockés sur le serveur et sont synchronisés entre tous les appareils	143 en non chiffré et 993 en chiffré
POP3 (Post office protocol)	protocole qui télécharge les messages depuis le serveur vers un appareil, avec possibilité de les supprimer du serveur après récupération.	110 en non chiffré et 995 en chiffré
MAPI (Messaging Application Programming Interface)	Protocole propriétaire développé par Microsoft qui sert à effectuer les communications entre un client de messagerie et un serveur de messagerie Exchange	Le protocole MAPI s'appuie sur des flux Web en HTTPS donc il utilise le port par défaut 443.

La ressource suivante permet d'approfondir ces notions :

<https://www.it-connect.fr/messagerie-decouverte-des-protocoles-smtp-pop-imap-et-mapi/>

1 MX (Mail eXchanger) : enregistrement DNS qui indique quel serveur mail accepte les mails destinés à un nom de domaine.

A.3. ENVELOPPE, EN-TÊTE ET CORPS D'UN MAIL

Un mail est composé d'un en-tête (header) et d'un corps (body).

Trois éléments sont importants pour comprendre un mail :

- **l'enveloppe** de transport SMTP : elle contient les informations utilisées entre serveurs pour acheminer le mail (adresse de retour MAIL FROM, destinataires RCPT TO...). Elle ne fait pas partie du message à proprement parler, mais certains éléments sont recopiés dans l'en-tête du mail : par exemple, le champ Return-Path reprend l'adresse d'expéditeur utilisée dans MAIL FROM.
- **l'en-tête** (header) : ce sont des lignes de texte qui décrivent le message. Certaines sont visibles dans le client (From, To, Subject, Date...), d'autres sont techniques et cachées par défaut (Received, Message-ID, DKIM-Signature, Authentication-Results ...) ou bien proviennent de l'enveloppe (Return-path). Elles servent au routage, à la lutte anti-spam, à la traçabilité...
- **le corps** : correspond au contenu du message : texte, images insérées, pièces jointes.

L'enveloppe, l'en-tête et le corps du message sont composés de plusieurs champs qui contiennent des informations.

Le format de fichier utilisé pour les messages électroniques est IMF (Internet Message Format).

Pour obtenir l'en-tête d'un mail, on peut extraire le fichier IMF correspondant. Sur le client Thunderbird :





 Sélectionner le message à exporter.

 Cliquer sur Fichier → Enregistrer sous → Fichier...



Thunderbird enregistre par défaut le message au format .eml, qui est en fait un message au format IMF standard.



Avec l'interface web de Gmail, il faut cliquer sur le lien suivant :

 Répondre
 Répondre à tous
 Transférer
Filtrer les messages similaires
Imprimer
Ajouter Théâtre(s) Magazine à ma liste de contacts
Supprimer ce message
Signaler comme spam
Signaler comme phishing
Afficher l'original 
Texte du message indéchiffrable ?
Traduire le message
Marquer comme non lu

 Enregistrer le fichier EML

Selon le client de messagerie utilisé, les manipulations peuvent varier.

Travail à faire 1

-  Enregistrer le fichier IMF associé à un mail de votre choix contenant au moins une pièce jointe ainsi qu'une image. Le fichier doit avoir pour extension EML.
-  Tester l'ouverture de ce fichier avec un éditeur de texte de votre choix puis avec le logiciel Thunderbird.

Les ressources suivantes donnent des explications sur les différents champs présents dans l'en-tête d'un message.

- <https://blog.mailfence.com/fr/comprendre-utiliser-en-tete-email/>
- <https://proton.me/blog/fr/what-are-email-headers>
- Un récapitulatif « Comprendre et lire les en-têtes d'un message électronique » est également fourni dans le dossier documentaire.

Travail à faire 2

Utiliser ces ressources afin de compléter le tableau suivant sur le courriel extrait précédemment.

 Sous Linux, un filtre peut être utilisé.

Champs	Valeur
From	
To	
Return-path	
Date	
Message-ID	

Travail à faire 3

i Les questions pour ce travail se basent sur le fichier « 20251029-Relecture labo messagerie-22289.eml » au format « eml » fourni.

Q3.1 Compléter le tableau à partir du courriel fourni

Champs	Valeur
From	
To	
Return Path	
Premier Received	
Content-Type	
Content-Disposition	
Content-Transfer-Encoding	

Les ressources suivantes permettent d'obtenir des informations sur une adresse IP :

- <https://www.arin/>
- <https://ipinfo.io/> (donne des résultats plus synthétiques).

Q3.2 Relever le nom DNS et l'adresse IP de l'appareil ou du serveur depuis lequel l'e-mail a été initialement envoyé ? Vous préciserez les principales informations recueillies (nom DNS, compagnie, adresse/géolocalisation).

Q3.3 Écrire le nom DNS du serveur SMTP de l'expéditeur.

Q3.4 Écrire le nom de la pièce jointe.

A.4. CODES SMTP

Les codes de réponse SMTP fournissent des indications sur la réponse du serveur à une requête SMTP. En fonction du code de réponse obtenu, il est possible de savoir comment s'est terminée la requête SMTP.

Exemple : **553 Requested action not taken: mailbox name not allowed** :

Exemples de codes :

Codes d'erreur	Description
421	Le service n'est pas disponible, réessayer plus tard.
451	Message non envoyé en raison d'une erreur sur le serveur.
501	Erreur de syntaxe dans les paramètres de la commande.
552*	Message non envoyé. Généralement car la boîte aux lettres du destinataire ne dispose pas de suffisamment d'espace de stockage mais d'autres raisons sont possibles.
553	Adresse e-mail rejetée en raison d'une syntaxe incorrecte ou d'un format invalide. Cela peut également indiquer que l'adresse est sur une liste noire.

* un message de code « 552 5.7.0 » renvoyé par 'google' signale la présence de pièces jointes et/ou liens suspects ou malveillants dans les e-mails. Cela inclut les liens vers des domaines connus pour héberger des logiciels malveillants, des sites de *phishing*, voire des domaines légitimes compromis. Les filtres de Gmail sont constamment mis à jour pour identifier ces menaces.

Dans l'exercice qui suit, nous allons travailler sur une analyse de trame, incluant la récupération de plusieurs e-mails, issue du site <https://www.malware-traffic-analysis.net/index.html> et plus particulièrement de la page <https://www.malware-traffic-analysis.net/2018/12/19/index.html>. Cette page documente une campagne de *malspam*² active en décembre 2018 diffusant le ver MyDoom, incluant des :

- Échantillons d'e-mails
- Fichiers malveillants
- Captures réseau d'infection
- Indicateurs techniques (hash, IP, ports, objets, expéditeurs usurpés)

 Extraire le fichier pcap de capture de trames associé à la ressource suivante puis l'enregistrer sur votre ordinateur : <https://www.malware-traffic-analysis.net/2018/12/19/index.html>



Le mot de passe de l'archive est infected_20181219.

En utilisant les deux ressources suivantes :

- <https://www.wireshark.org/docs/dfref/s/smtp.html>
- <https://www.wireshark.org/docs/dfref/i/imf.html>

² Malspam (malicious spam) : E-mails de spam contenant un malware en pièce jointe ou via un lien malveillant,

Répondre aux questions.

Q3.5 Quel est le port utilisé pour le trafic SMTP ?

Q3.6 Combien de paquets liés au trafic SMTP la capture de trames contient-elle ?

Q3.7 Repérez les adresses IP des serveurs SMTP associés à cette capture

Q3.8 Repérez les noms des pièces jointes

Q3.9 Quelle est l'extension de ces pièces jointes ?

Q3.10 Les messages électroniques ont-ils été délivrés ?

B. ATTAQUES DE TYPE HAMEÇONNAGE

B.1. DÉFINITION

D'après economie.gouv.fr

« L'hameçonnage (*phishing* en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. »

Ce type de fraude se réalise en envoyant un mail frauduleux qui contient un lien malveillant. Lorsque la victime clique sur ce lien, elle se trouve redirigée vers une page de connexion frauduleuse. L'attaquant cherche ainsi à récupérer les identifiants de connexion de la victime. La page de connexion est généralement une copie qui reprend le logo et la présentation de la page d'une organisation existante (banque par exemple).

B.2. CARACTÉRISTIQUES COMMUNES

La plupart des mails de type hameçonnage présentent les caractéristiques suivantes :

- Le sujet du mail ou son message fait référence à une urgence à répondre à ce mail ;
- Le mail usurpe le logo et le nom d'une entreprise connue ;
- Le mail est parfois mal rédigé avec des fautes d'orthographe et de syntaxe ;
- Les liens présents sont souvent raccourcis afin de dissimuler la véritable destination malveillante ;
- Une pièce jointe malveillante est présente via un lien sur un document qui semble légitime.

La ressource suivante donne plus de détails sur les techniques d'identification de ce type de mail frauduleux.

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage>

B.3. TYPE D'HAMEÇONNAGE

Travail à faire 4

À l'aide de vos recherches sur internet, compléter le tableau suivant :

Spam	
Spear phishing	
Whaling	
Smishing	
Vishing	
Mail spoofing	

B.4. CAMOUFLAGE DES LIENS

L'attaquant peut camoufler les liens présents dans le mail frauduleux afin d'optimiser l'efficacité de son attaque. Les liens peuvent être réduits et camouflés afin de ne pas attirer l'attention de la victime. Le typosquattage (noms de domaine modifiés ou mal orthographiés) peut aussi être utilisé afin de tromper la victime.

La ressource suivante permet de générer facilement un lien mini : <https://urlr.me>.

En contre-mesure, afin d'éviter un clic accidentel sur un lien malveillant, la technique de masquage des liens et des adresses IP peut être utilisée. Cette technique rend inopérant le clic accidentel sur un lien en modifiant son contenu. Afin d'accéder au lien d'origine, l'utilisateur destinataire doit donc effectuer une opération de conversion volontaire. Cette technique peut être utilisée lors de certains envois de mails qui nécessitent un haut niveau de sécurité.

- http est remplacé par hxxp ;
- Des crochets sont ajoutés dans les noms de domaines (www[.]example[.]com) ;
- Des crochets sont ajoutés dans les adresses IP (8[.]8[.]8[.]8).

Des outils permettent de retrouver le lien d'origine.

<https://gchq.github.io/CyberChef/>

Les ressources suivantes donnent plus d'indications sur cette technique :

<https://privacymatters.ubc.ca/news/blocking-email-links-why-we-use-hxxp-emails>

<https://infuse.quest/fr/learning-path/1/module-3/#neutraliser-les-url>

C. ANALYSE GLOBALE D'UN MAIL MALVEILLANT

En tant que technicien membre du centre de sécurité des opérations, on vous transmet des mails suspects pour étude.

Travail à faire 5

 Se rendre sur la ressource <https://www.malware-traffic-analysis.net/2020/05/05/index.html>

Cette ressource contient des exemples de mails frauduleux ainsi que des fichiers de capture de trames associés à l'ouverture de ces mails. Le mot de passe pour accéder à l'archive est infected_20200505. Pour des raisons de sécurité, le contenu des liens a été modifié. Les archives contiennent quatre mails (fichiers EML) ainsi que les quatre captures de trames correspondantes (fichiers PCAP).

 Télécharger puis extraire ces fichiers sur votre ordinateur et répondre aux questions.

Il peut être plus pratique d'ouvrir les fichiers .eml dans un client de messagerie.

Q5.1 Quels éléments apparents dans le corps du message permettent de soupçonner que ces mails sont frauduleux ?

Q5.2 En vous appuyant sur un des mails fourni, décrire le principe de l'attaque.

Q5.3 Utiliser la première capture de trame du premier mail malveillant afin de récupérer le login et le mot de passe saisi par la victime.

Travail à faire 6

Valider votre niveau de détection des mails malveillants en réalisant le questionnaire suivant :

<https://phishingquiz.withgoogle.com/>



Vous pouvez indiquer n'importe quelle adresse mail pour commencer le test.

D. ANALYSE DÉTAILLÉE D'UN MAIL MALVEILLANT

D.1. COLLECTE DES PREMIÈRES INFORMATIONS

Un premier niveau d'analyse consiste à collecter les informations suivantes :

- adresse IP de l'expéditeur ;
- résolution inverse de l'adresse IP de l'expéditeur ;
- sujet du mail ;
- destinataire du mail ;
- présence d'une adresse mail de retour (reply-to) ;
- date et heure du mail.

Par la suite, vérifier la présence de pièces jointes et de liens notamment :

- présence de minis liens ;
- nom des pièces jointes ;
- somme de contrôle (hashé³) des pièces jointes.

D.2. ANALYSE DE L'EN-TÊTE

L'outil Messageheader de Google permet d'analyser le contenu des en-têtes via le lien suivant :

<https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

Après avoir récupéré le fichier IMF du mail, Il suffit de copier/coller son contenu puis de lancer l'analyse. Ceci évite de faire des recherches manuelles dans un fichier IMF.

D'autres outils permettent aussi d'extraire les informations de l'en-tête.

<https://mha.azurewebsites.net/>



Pour rappel, afin d'obtenir plus d'informations sur l'adresse IP de l'expéditeur, l'outil suivant peut être utilisé : <https://ipinfo.io/>

D.3. ANALYSE DU CORPS DU MESSAGE

Le corps du message peut contenir des liens malveillants. Les outils suivants permettent de collecter automatiquement les liens d'un mail en vue d'une analyse ultérieure.:

- <https://www.convertcsv.com/url-extractor.htm>
- <https://gchq.github.io/CyberChef/>
- <https://mxtoolbox.com/EmailHeaders.aspx>

Une fois les URL obtenues, leur réputation peut être étudiée via les outils d'analyse suivants :

- [virustotal.com](https://www.virustotal.com)
- <https://urlscan.io/>
- <https://talosintelligence.com/>

³ Code produit par une fonction de hachage informatique.

Analyse des pièces jointes :

Afin d'analyser les pièces jointes, il convient de les enregistrer sur une machine dédiée (clic droit avec Thunderbird par exemple) puis de calculer leur hashé afin de les comparer à une liste de hashés reconnus comme malveillants.

Sous Linux, on peut également utiliser la commande 'sha256sum'.

Ensuite, il faut vérifier si le hashé obtenu est reconnu comme malveillant. Les outils suivants sont disponibles :

- https://talosintelligence.com/talos_file_reputation
- <https://www.virustotal.com/gui/>

Travail à faire 7

En vous appuyant sur les outils cités, réaliser l'analyse détaillée du 4^e mail précédemment téléchargé : <https://www.malware-traffic-analysis.net/2020/05/05/index.html> :

Q7.1 Réaliser l'analyse détaillée de l'en-tête du message en récupérant les champs suivants : sujet, date de création, expéditeur, destinataire.

Q7.2 Réaliser l'analyse détaillée du corps du message : liste des noms de domaines, liste des URL, réputation des hashés de ces URL (si pertinent).

E. ANALYSE DE TYPE BAC À SABLE

Une analyse bac à sable permet d'exécuter un fichier malveillant afin d'observer son comportement et de voir les conséquences sur une machine dédiée.


Les outils suivants peuvent être utilisés :

- <https://app.any.run/submissions>
- <https://www.hybrid-analysis.com/>
- <https://www.joesecurity.org/>

Dans cette activité, c'est l'outil app.any.run qui sera utilisé.

L'outil app.any.run est une ressource en ligne qui permet de réaliser une analyse de type bac à sable sur un mail suspect. L'outil permet, entre autres, de suivre les interactions engendrées par l'ouverture d'un mail suspect dans un cadre sécurisé. App.any.run permet une interaction humaine afin d'observer les conséquences de l'ouverture d'un mail malveillant. Les informations de protocoles et de trafic réseau sont affichées en direct afin de suivre le trafic généré par l'ouverture du mail suspect.

ANY.RUN est une entreprise de cybersécurité qui propose un environnement interactif d'analyse des logiciels malveillants et des services de veille sur les menaces pour l'analyse et l'investigation en temps réel des menaces de logiciels malveillants et de phishing

-  L'outil permet aussi d'extraire les informations d'en-tête et de corps du message manipulé afin d'établir un rapport d'activité via l'onglet « Text export ».

Bac à sable n°1

Travail à faire 8

Réaliser l'analyse détaillée du mail disponible dans le bac à sable suivant :

<https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59/>

Q8.1 Comment AnyRun classe-t-il ce mail ?

Q8.2 Quel est le nom de la pièce jointe PDF ?

Q8.3 Quel est le hashé sha256 de cette pièce jointe ?

Q8.4 Quelles sont les deux adresses IP classées comme malveillantes présentes dans ce mail ?

Q8.5 Quel est le nom du processus étiqueté comme potentiel trafic malveillant ?

Bac à sable n°2

Travail à faire 9

Réaliser l'analyse détaillée du mail disponible dans le bac à sable suivant :

<https://app.any.run/tasks/82d8adc9-38a0-4f0e-a160-48a5e09a6e83>

Q9.1 Comment AnyRun classe-t-il ce mail ?

Q9.2 Quel est le nom du fichier Excel présent dans ce mail ?

Q9.3 Quel est le hashé de ce fichier Excel ?

Q9.4 Quels sont les domaines classés comme malveillants présents dans ce mail ?

Q9.5 Quelles sont les trois adresses IP classées comme malveillantes présentes dans ce mail ?

Q9.6 À quel type de vulnérabilité CVE est associée la pièce jointe ?

F. CONTRE-MESURES

Selon **MITRE ATT&CK Framework**, le [Phishing](#) a plusieurs classifications dont : Technique ID 1566 (T1566) et 1598 (T1598). Ci dessous, un extrait des contre-mesures.

Mitigations

ID	Mitigation	Description
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation. ^{[6][9]}
M1017	User Training	Users can be trained to identify social engineering techniques and spearphishing attempts.

Plusieurs contre-mesures permettent de se protéger des risques liés au phishing. Nous nous intéresserons ici aux **contre mesures liées à la messagerie** :

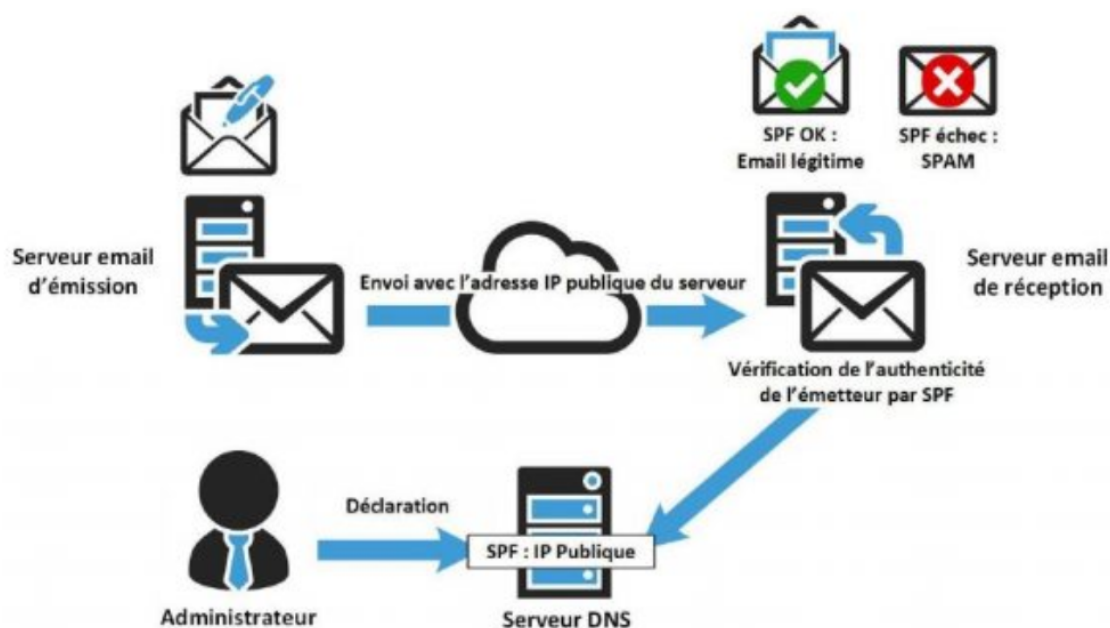
- Sécurisation des mails avec les indicateurs de sécurité (SPF, DKIM et DMARC) ;
- Filtre anti-spam et anti-virus ;
- Blocage de certains noms de domaine ;
- Blocage automatique de certaines pièces jointes ;
- Sensibilisation des utilisateurs.

Dans la suite des activités, nous détaillerons les outils SPF, DKIM et DMARC.

Un récapitulatif du fonctionnement de ces outils est fourni dans le document « Fonctionnement des outils SPF, DKIM et DMARC ».

F.1. SPF (SENDER POLICY FRAMEWORK)

Avec un enregistrement SPF en place, les fournisseurs de services Internet peuvent vérifier qu'un serveur de messagerie est autorisé à envoyer des mails pour un domaine spécifique. **Un enregistrement SPF est un enregistrement DNS TXT** contenant une liste des adresses IP autorisées à envoyer des mails au nom d'un domaine.



Source : <https://blog.devensys.com/2020/06/07/spf-dkim-dmarc-securite-mail/>

Exemple d'enregistrement SPF :

```
v=spf1 ip4:127.0.0.1 include:_spf.google.com -all
```

- v=spf1 → début de l'enregistrement SPF (Indique la version du protocole SPF utilisée) ;
- ip4 : 127.0.0.1 → Types d'adresses IP autorisées à envoyer le mail ;
- include :_spf.google.com → considère aussi comme **autorisées** toutes les IP qui passent le SPF du domaine spf.google.com ;
- -all : → toutes les autres adresses IP (all) sont rejetées (-)..

Travail à faire 10

Q10.1 À l'aide de la ressource <https://dmarcian.com/spf-survey/>, récupérer le SPF du domaine cisco.com.

Q10.2 En utilisant les liens suivants

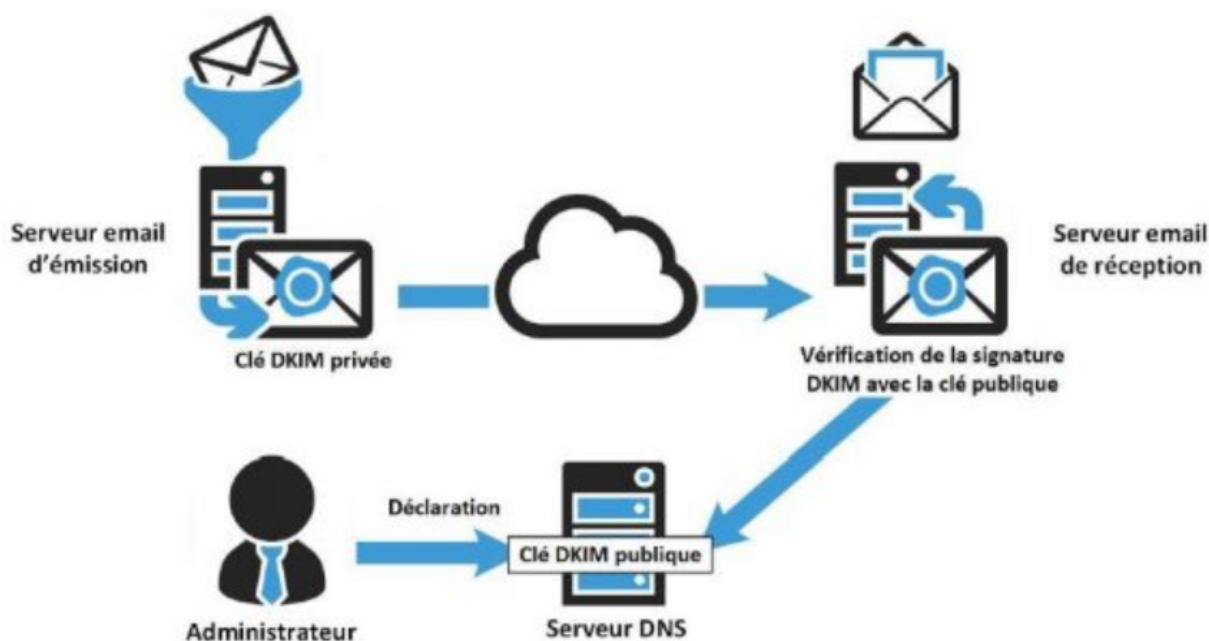
- <https://dmarcian.com/spf-syntax-table/>
- <https://dmarcian.com/what-is-the-difference-between-spf-all-and-all/>

Et vos recherches sur internet, expliquer chacun des éléments constituant le SPF de cisco.com.

F.2. DKIM (DOMAINKEYS IDENTIFIED MAILS)

DKIM (DomainKeys Identified Mail) est un mécanisme d'authentification qui signe les mails pour prouver qu'ils viennent bien du domaine indiqué. Le SPF peut limiter les adresses IP utilisées pour l'envoi de mails alors que le DKIM vérifie cryptographiquement l'identité de l'expéditeur et l'intégrité du mail selon les principes suivants :

- signature numérique : l'expéditeur calcule un hashé à partir de certaines parties du message et le signe avec sa clé privée ;
- vérifications :
 - le destinataire utilise une clé publique, publiée dans le DNS du domaine expéditeur, pour vérifier la signature.
 - il recalcule le hashé à partir du message reçu et utilise la clé publique pour vérifier la signature : si la vérification réussit, le message n'a pas été altéré et il a bien été signé par le détenteur de la clé privée correspondante.
- authentification : une signature valide montre que le mail provient bien du domaine revendiqué et qu'il n'a pas été altéré pendant le transfert.



Source : <https://blog.devensys.com/2020/06/07/spf-dkim-dmarc-securite-mail/>

Exemple d'enregistrement DKIM dans le DNS :

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAXtQIC7vZAHHZ7wVv/5x  
/qH1RagMQI+y6Xtsn73rW0geBQjHKbmIEIlgrebyWFCXjnzIP0NYJrGehenmPWK5bF/TRDstbM8uVQCWpoRAHzuhIxPSYw6k  
/w2+HdCECF2gnGmmw1cT6nHjfcyKGS00n0HDvxP8I5YQIILzNigP32n1hVnQP+UuInj0wLI0B1WkHdnFewzGK2+qjF2wmEjx+vqHDnxdUTay5DfTgaqgA9AKjgXNjLEbK1Ewvy  
0tj7UzQRHd24a5+2X/R4Pc7PF/y60xAWYBZnEP00sJwio4uqL9CYZcvaHGCL0IMwQmNTPMKGC9nt3PSjUjFHUBX3wIDAQAB
```

- v=DKIM1 → Version de DKIM ;
- k=rsa → type de clé utilisée ;
- p= → clé publique qui devra correspondre à la clé privée créée lors du process DKIM.

Travail à faire 11

Q11.1 Relever la signature DKIM associée au mail fourni ou à un de vos mails et vérifier le statut de ce DKIM.

Q11.2 En utilisant les liens suivants et vos recherches sur internet, expliquer chacun des éléments constituant le DKIM précédent.

<https://dmarcian.com/dkim-selectors/>

<https://help.returnpath.com/hc/en-us/articles/222481088-DKIM-DNS-record-overview>

F.3. DMARC (DOMAIN-BASED MESSAGE AUTHENTICATION)

DMARC, (Domain-based Message Authentication Reporting, & Conformance) est une norme open source qui lie le résultat des deux normes SPF et DKIM au contenu d'un mail. La mise en place d'un enregistrement DMARC pour un domaine donnera des informations qui permettront de dépanner les configurations SPF et DKIM si nécessaire.

```
v=DMARC1; p=quarantine; rua=mailto:postmaster@website.com
```

Le détail des enregistrements DMARC est disponible via la ressource suivante :

<https://dmarc.org/overview/>

Exemple d'enregistrement DMARC :

- v=DMARC1 → début de l'enregistrement DMARC ;
- p=quarantine → En cas d'échec de vérification DMARC, l'email est signalé comme SPAM ;
- rua=mailto:postmaster... → Les rapports d'informations sont envoyés à cette adresse.

Travail à faire 12

 Se rendre sur la ressource <https://dmarcian.com/domain-checker/>, puis vérifier le DMARC du domaine cisco.com.

Q12.1 Quels sont les résultats obtenus sur les items SPF et DKIM pour le domaine cisco.com ?

 Tester avec le domaine microsoft.com.

Q12.2 Relever puis expliquer en détail le contenu des enregistrements DMARC associé à ce domaine.

Q12.3 À partir du fichier « eml » fourni, identifier la politique DMARC appliquée et le résultat de la vérification DMARC.

Q12.4 Analyser la politique générale quant aux mails du domaine considéré.

F.4. S/MIME (SECURE/ MULTIPUROPOSE INTERNET MAIL EXTENSIONS)

Selon Microsoft, S/MIME est un protocole pour l'envoi de mails signés et chiffrés.


S/MIME garantit l'intégrité et la non répudiation du message.

Concernant la non-répudiation, l'unicité d'une signature empêche le propriétaire de la signature de renier la signature. L'expéditeur d'un message peut le signer en utilisant sa clé privée. Le destinataire déchiffre ce message en utilisant la clé publique de l'expéditeur afin de vérifier l'expéditeur. Le destinataire fait de même au moment de répondre à ce message. La garantie de l'identité des correspondants est alors assurée.

G. DOSSIER DOCUMENTAIRE

G.1. COMPRENDRE ET LIRE LES EN-TÊTES D'UN MESSAGE ÉLECTRONIQUE (FORMAT IMF)

Les messages électroniques (courriels en français ou e-mails en anglais) sont stockés et transmis selon le format IMF (Internet Message Format), défini par la RFC 5322. Chaque message contient un corps (le contenu) et un en-tête (*header*) qui renferme des informations techniques sur l'expéditeur, le destinataire, la date, le chemin d'acheminement, et les mécanismes d'authentification (SPF, DKIM, DMARC).

 En dehors du corps du message, les clients de messagerie affichent généralement, par défaut, les champs Objet (*Subject*), De (*From*), À/Pour (*To*) et Date.

 Les spammeurs ou fraudeurs peuvent falsifier le champ 'De' qui s'affiche pour faire croire que l'expéditeur est quelqu'un qui vous inspire confiance, ainsi que le champ 'To'.

L'analyse de l'en-tête complète d'un mail permet notamment de :


- vérifier l'authenticité du message et l'identité de l'expéditeur ;
- repérer un éventuel *phishing* ou spam ;
- retracer le chemin d'acheminement d'un message entre serveurs ;
- identifier des erreurs de configuration ou des délais de transmission.

Pour visualiser les en-têtes complètes d'un courriel, il n'est pas forcément nécessaire de le télécharger au format « eml ». Sur Thunderbird :

 Ouvrir le message.

 Cliquer sur le menu « Affichage ».


 Sélectionner « Affichage → En-tête → Complet » ou utiliser le raccourci clavier Ctrl+U.

 Dans le cas d'utilisation du raccourci (plus pratique), une nouvelle fenêtre s'ouvre avec tout le contenu du message au format IMF.



Plutôt que de rechercher manuellement le texte de l'en-tête d'un mail, il est plus facile de trouver les champs clés en utilisant un analyseur d'en-tête de mail, comme celui de [MxToolbox](#) (très bon rendu visuel).

 Copier et coller un en-tête de mail dans l'outil d'analyse et lancer l'analyse.

 Les en-têtes d'un mail comprennent également des X-headers qui sont des champs ajoutés par, notamment, les fournisseurs de messagerie pour inclure, par exemple, les résultats d'authentification et des informations sur le filtrage des spams.

Principaux champs d'un en-tête

Champs	Signification	Exemple (extraits)
From (de)	Nom et adresse mail de l'expéditeur	Marie Dupont <m.dupont@exemple.fr>
To (à ou pour)	Nom et adresse mail de tous les destinataires, y compris ceux en Cc	Pierre Durand <p.durand@exemple.com> Romain Pic <romain.pic@exemple.com>
Date	Heure et date d'envoi du message	Mon, 13 Oct 2025 11:25:03 +0200 (CEST)
Subject (objet)	Le titre qui apparaît dans la ligne Objet	Rapport de mission
Message-ID	Identifiant unique créé pour chaque message électronique.	<1112720409.8133552.1760347503802.JavaMail.zimbra@msg.exemple.fr>
Return-Path (chemin de retour)	Adresse mail de retour en cas d'échec de transmission.	<mailer-daemon@exemple.fr>
Reply-To (répondre à)	Adresse optionnelle de réponse pour les destinataires. <i>S'il n'y a pas de champ Reply-To, l'adresse Return-Path est utilisée.</i>	<m.dupont@exemple.fr>
Received (reçu)	Noms et adresses IP de tous les serveurs SMTP par lesquels le message est passé pour arriver au destinataire. Un en-tête Received est ajouté automatiquement en tête de liste après qu'un serveur a accepté un mail. Il faut donc lire de bas en haut : l'adresse IP de l'expéditeur d'origine figure donc dans le champ Received en bas. Ici ⇒ 86.229.85.167. On peut lire également l'adresse IP privée de la machine – 192.168.0.141 – ayant envoyé le mail) et le premier serveur SMTP sollicité (smtp.exemple.fr).	from [192.168.0.141] ([86.229.85.167]) by smtp.exemple.fr with ESMTPA id DpKovlUTGsXzwDpKovKI4G; Tue, 28 Oct 2025 20:26:22 +0100
MIME-Version	version du protocole MIME ⁴ (Multipurpose Internet Mail Extensions) utilisée pour formater le message	1.0
Content-Type	Les différents types de contenu du message tels que texte brut,	text/plain; charset="UTF-8"

⁴ *MIME : extension du protocole de messagerie Internet qui vous permet d'envoyer et de recevoir divers types de fichiers de données tels que des photos, des fichiers audio et vidéo en ligne.*

	HTML ou pièce jointe.	application/zip; name="Fiches.zip"
Content-Disposition	Nom de la ou les pièces jointes attachées	attachment; filename="Fiches.zip"
Content-Transfer-Encoding	Type d'encodage appliqué au corps du message afin permettre la transmission de données non-ASCII et binaires.	BASE64
DKIM-Signature Signature DKIM (Domain Keys Identified Mail)	Méthode d'authentification qui vérifie de manière cryptographique que le message n'a pas été modifié depuis qu'il a été signé par DKIM, ce qui permet de détecter les messages falsifiés. Le champ Authentication-Results doit se lire dkim=pass avec l'en-tête d=[domaine de l'expéditeur].	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=exemple.fr; s=default; h=... bh=2wi/TIPNjxAfUuHjUAWL1v2uD7t0UMsoygLmaom5I ... t4ctbfCQ==;
Received-SPF (Sender Policy Framework)	Protocole d'authentification qui vérifie qu'un mail a été envoyé à partir d'une adresse IP autorisée. Comme pour DKIM, le champ Authentication-Results doit indiquer spf=pass.	pass (domain of m.dupont@exemple.fr designates 109.234.163.243 as permitted sender) ... <i>109.234.163.243 représente l'adresse IP du serveur SMTP qui a envoyé cet e-mail</i>
DMARC (Domain-based Message Authentication Reporting and Conformance)	Protocole d'authentification qui empêche l'usurpation d'adresse mail en combinant les résultats des vérifications DKIM et SPF. Il permet aux expéditeurs de définir ce qui arrive à leurs messages électroniques s'ils échouent aux contrôles DKIM et SPF.	<i>La vérification DMARC n'apparaît pas directement comme une ligne dédiée. Elle apparaît notamment dans « Authentication-Results »</i>
Authentication-Results (résultats d'authentification)	Résultats des vérifications d'authentification comme DKIM, SPF et DMARC (voir plus haut). Pour 'dmarc' : <ul style="list-style-type: none"> • dmarc=pass : Indique que la vérification DMARC a réussi. • p= quarantine : Politique DMARC appliquée sur le domaine (ici, mettre dans les spams les e-mails non authentifiés). • sp=reject : Politique DMARC appliquée sur le sous-domaine (ici, rejeter les e-mails non authentifiés). • dis=none : politique appliquée par le serveur destinataire. 	mx.exemple.fr; dkim=pass header.i=@exemple.fr header.s=default header.b=Vm70uALm; spf=pass (domain of m.dupont@exemple.fr designates 109.234.163.243 as permitted sender) smtp.mailfrom=m.dupont@exemple.fr; dmarc=pass (p=quarantine sp=reject dis=none) header.from=exemple.fr>

G.2. FONCTIONNEMENT DES OUTILS SPF, DKIM ET DMARC

Les mails sont l'un des vecteurs principaux d'attaques informatiques (phishing, usurpation d'identité, spam). Les protocoles **SPF**, **DKIM** et **DMARC** permettent de :

- **vérifier l'authenticité** de l'expéditeur ;
- **limiter le spoofing** (usurpation d'adresse mail) ;
- assurer l'intégrité des mails ;
- **améliorer la délivrabilité** des mails légitimes.

Pour plus d'informations voir le côté labo associé à ce thème sur le site du réseau Certa.

SPF (Sender Policy Framework)

Définition

SPF est un protocole qui permet de **lister les serveurs autorisés à envoyer des mails pour un domaine**. Il est publié sous forme d'un enregistrement DNS de type **TXT**.

Fonctionnement

- Le serveur de réception vérifie l'enregistrement SPF du domaine de l'expéditeur. Plus précisément, SPF vérifie que l'adresse IP de l'expéditeur est autorisée à envoyer des mails pour le domaine indiqué dans le champ MAIL FROM (équivalent à Return-Path).
- Si l'IP du serveur expéditeur est dans la liste autorisée, le mail est accepté.
- Sinon, il peut être rejeté ou marqué comme spam.

Exemple d'enregistrement SPF dans le DNS du domaine

```
v=spf1 ip4:192.0.2.1 include:_spf.google.com ~all
```

- `v=spf1` : Version du protocole.
- `ip4:192.0.2.1` : Autorise l'IP 192.0.2.1 à envoyer des mails.
- `include:_spf.google.com` : Inclut les serveurs de Google (utile si on utilise Gmail).
- `~all` : Politique par défaut pour les serveurs non autorisés (ici, "soft fail" : le mail est accepté mais marqué comme suspect).

Intérêt principal

Si un attaquant envoie un mail depuis une IP non autorisée (ex: 192.0.2.2), le serveur de réception détecte que l'IP n'est pas dans l'enregistrement SPF et peut rejeter le mail.

DKIM (DomainKeys Identified Mail)

Définition

DKIM ajoute une **signature numérique** aux mails, permettant de vérifier que le contenu n'a pas été altéré et que l'expéditeur est bien le propriétaire du domaine qui a signé.

Fonctionnement

1. Le serveur expéditeur signe le mail avec une **clé privée**.
2. Le serveur de réception récupère la **clé publique** dans l'enregistrement DNS du domaine.
3. Il vérifie la signature avec la clé publique. Si la signature est valide, le mail est authentifié.

La signature contient aussi un hashé du message d'origine qui permet au destinataire de contrôler l'intégrité du message reçu.

Exemple d'enregistrement DKIM

v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC...

- v=DKIM1 : Version du protocole.
- k=rsa : Type de clé (RSA).
- P=... : Clé publique utilisée pour vérifier la signature.

Intérêt principal

Si un attaquant modifie le contenu d'un mail en transit, la signature DKIM ne correspondra plus, et le serveur de réception rejettera le mail.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

Définition

DMARC est un protocole qui **combine SPF et DKIM** et qui vérifie en plus que le domaine de l'expéditeur apparent correspond bien au domaine authentifié. Il fournit aussi des rapports sur les tentatives d'usurpation.

Fonctionnement

1. Le propriétaire du domaine publie un enregistrement DMARC dans son DNS.
2. Le serveur de réception vérifie SPF et DKIM.
3. Le serveur de réception vérifie la correspondance entre le domaine du From et le domaine authentifié par SPF ou par DKIM. Selon la politique DMARC (none, quarantine, reject), il traite le mail (accepter, mettre en quarantaine, rejeter).
4. Des rapports sont envoyés au propriétaire du domaine pour surveiller les activités suspectes.

Exemple d'enregistrement DMARC

v=DMARC1; p=reject; rua=mailto:dmarc-reports@exemple.fr;
ruf=mailto:dmarc-failures@exemple.fr

- v=DMARC1 : Version du protocole.
- p=reject : Politique pour les e-mails non authentifiés (ici, rejeter).
- rua=mailto:...: Adresse pour recevoir les rapports agrégés.
- ruf=mailto:...: Adresse pour recevoir les rapports d'échecs.

Intérêt principal

Si un attaquant envoie un mail en usurpant le domaine exemple.fr, le serveur de réception vérifie SPF et DKIM. Si la vérification échoue, il rejette le mail et envoie un rapport à dmarc-reports@exemple.fr.

Comment ces protocoles fonctionnent-ils ensemble ?

Lorsqu'un message prétend provenir de **contact@exemple.fr**, le serveur de réception effectue plusieurs vérifications :

1. Vérification SPF

Le serveur vérifie si **l'adresse IP de l'émetteur** est autorisée pour le domaine indiqué dans le **Return-Path** (enveloppe SMTP).

Il contrôle ensuite si **ce domaine est aligné** avec le domaine affiché dans le champ **From:** (exemple.fr).

2. Vérification DKIM

Le serveur vérifie la **signature DKIM** intégrée au message :

- la signature est-elle valide ?
- le **domaine DKIM** utilisé pour signer le message correspond-il (est-il aligné) avec le domaine du champ **From:** ?

3. Application de DMARC

Pour qu'un message soit considéré comme *conforme DMARC*, **au moins un des deux mécanismes suivants doit réussir ET être aligné** :

- SPF
- ou DKIM

Si **aucun** ne réussit avec un alignement correct, le serveur applique la **politique DMARC** du domaine (*reject*, *quarantine*, ou *none*).

Cela peut entraîner le rejet ou le classement en spam du message.

4. Rapport DMARC

Le serveur de réception peut ensuite envoyer un **rapport DMARC** au propriétaire du domaine *exemple.fr*, afin de l'informer des envois conformes ou des tentatives d'usurpation.