

Rapport de mini-projet

FILIERE : ICCN - INE2

Mise en place d'un service de messagerie sécurisé et développement d'un outil automatisé d'analyse des attaques par courrier électronique destiné aux analystes du SOC

Réalisé par :

M. Abdelghafour BOUHDYD

M. Zakaria HAMID

M. Amine LACHEGUR

M. Taha SAFA

M. Mouad TIGMOUTI

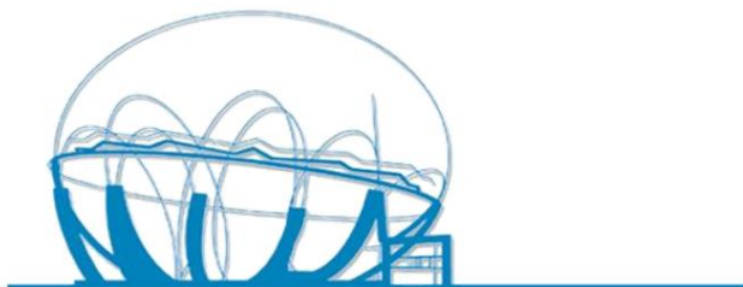
Encadrés par :

Mme. Aafaf OUADDAH

M. Abdellatif MEZRIOUI

Mme. Meryem AYACHE

Mme. Charifa HANIN



AGENCE NATIONAL DE RÉGLEMENTATION DES TÉLÉCOMMUNICATIONS

INSTITUT NATIONAL DES POSTES ET TÉLÉCOMMUNICATIONS

Année universitaire : 2023/2024

Sommaire

Chapitre 1 : Fonctionnement et Protocoles des Services de Messagerie Électronique

I. Principe de fonctionnement d'un service de messagerie

1. **Définition et concepts de base**
 - Qu'est-ce qu'un service de messagerie ?
 - Fonctionnalités principales d'un service de messagerie
2. **Architecture typique d'un système de messagerie**
 - Composants principaux (serveur de messagerie, client de messagerie, etc.)
 - Interaction entre les composants
3. **Flux de communication dans un service de messagerie**
 - Envoi et réception des messages
 - Transit des messages à travers différents serveurs

II. Protocoles de messagerie

1. **SMTP (Simple Mail Transfer Protocol)**
 - Description et historique
 - Fonctionnement du protocole SMTP
 - Commandes principales et réponses SMTP
2. **POP3 (Post Office Protocol v3)**
 - Description et historique
 - Fonctionnement du protocole POP3
 - Avantages et inconvénients du POP3
3. **IMAP (Internet Message Access Protocol)**
 - Description et historique
 - Fonctionnement du protocole IMAP
 - Comparaison entre IMAP et POP
4. **Postfix**
 - Présentation de Postfix
 - Configuration de base de Postfix
 - Fonctionnement interne de Postfix
5. **Dovecot**
 - Présentation de Dovecot
 - Configuration de base de Dovecot
 - Fonctionnalités avancées de Dovecot
6. **Chronologie de l'évolution de l'Email**

III. Structure des Emails

1. **Composants d'un mail**
 - MIME (Multipurpose Internet Mail Extensions)
 - En-tête (header)
 - Champs standards (From, To, Subject, Date, etc.)
 - Champs optionnels
 - Corps (body)
 - Texte brut vs texte formaté (HTML)
 - Pièces jointes
2. **Encodage des messages**
 - Encodage des caractères (MIME, Base64, Quoted-Printable)
 - Encodage des pièces jointes

Chapitre 2 : Attaques et Menaces dans les Services de Messagerie Électronique

Partie 1

I. Spam

1. Définition et concepts de base
2. Impacts de spam
3. Comment se protéger contre les spams ?

II. Phishing

1. Définition et concepts de base
2. Fonctionnement du phishing
3. Impacts de phishing
4. Comment se protéger contre le phishing ?

III. Virus

1. Définition et concepts de base
2. Types de virus
3. Impacts des virus
4. Comment se protéger contre les virus ?

Partie 2

IV. Des attaques avancées sur l'infrastructure email

1. Reconnaissance
2. Attaque sur S/MIME et OpenPGP
3. SPF : Allow by default
4. Attacking third-parties in "include"
5. Forger des signatures DKIM
6. DMARC : loose policy and subpolicy
7. DMARC : Poor sampling percentage
8. Conclusion

Partie 1

I. **DKIM (DomainKeys Identified Mail)**

1. Définition
2. Les principaux éléments de DKIM
3. Fonctionnement DKIM
4. Implementation DKIM
5. Les bonnes pratiques

II. **SPF (Sender Policy Framework)**

1. Définition
2. Le fonctionnement de SPF
3. Les composants de SPF
4. Implementation SPF

III. **DMARC**

1. Définition
2. Fonctionnement
3. Implémentation

IV. **SPAM ASSASSIN**

1. Définition
2. Fonctionnement
3. Custom rules

Partie 2

I. **Mxtoolbox**

1. Définition
2. Utilisation de MXToolbox pour les Emails
3. Les avantages
4. Les outils de MXtoolbox

II. **Spamhaus**

1. Définition
2. Fonctionnement
3. Listes de blocage gérées par Spamhaus
4. Défis et critiques de Spamhaus
5. Rôle de Spamhaus **dans la Sécurité**

III. **VirusTotal**

1. Définition
2. Fonctionnement

IV. **Clamav**

1. Définition
2. Fonctionnement
3. Exemple de scan

Introduction :

Il n'est un secret pour personne que l'ère numérique actuelle est construite sur un ensemble d'outils de communication rapides et efficaces, dans ce contexte, les services de courrier électronique ne font pas exception. Ils font déjà partie intégrante de toute communication électronique organisée et sont utilisés à la fois dans un environnement professionnel et pour des motifs personnels. Le document propose une description détaillée des processus sous-jacents à ce type de service, depuis la définition des notions de base, des types d'architectures et des routines de flux de messages les plus courantes. Nous allons aborder plusieurs protocoles de messagerie qui sous-tendent l'envoi et la réception d'emails : SMTP, POP3, IMAP et des outils de travail populaires tels que Postfix et Dovecot.

Enfin, il est important de connaître la structure des pourriels en tant que tels, autrement dit, des envois indésirables qui nuisent sérieusement à l'efficacité des services de messagerie. Outre les en-têtes et le corps du message, outre les différentes méthodes d'encodage, il ne faut pas oublier qu'il existe également de nombreuses menaces et attaques qui pèsent sur de tels services. Cela devrait inclure le spam, le phishing, les virus et les mesures préventives pour y faire face.

De plus, ce rapport traitera également des cyberattaques sophistiquées basées sur l'infrastructure d'emailing et des mécanismes de sécurité développés pour les atténuer, notamment DKIM, SPF, DMARC et d'autres outils de sécurité, tels que SpamAssassin, MXToolbox, Spamhaus, VirusTotal et ClamAV. Cette analyse mettra en évidence la chronologie du développement d'hier à aujourd'hui des emails et les questions de sécurité actuelles pour rendre ce domaine essentiel de la communication moderne plus compréhensible.

Chapitre 1 : Fonctionnement et Protocoles des Services de Messagerie Électronique
-Mouad Tigmouti-

I. Principe de fonctionnement d'un service de messagerie

1. Définition et concepts de base

- Qu'est-ce qu'un service de messagerie ?

Un service de messagerie est un système permettant la transmission électronique de messages écrits, de documents et de pièces jointes via Internet, directement dans la boîte de réception électronique du destinataire sélectionné par l'expéditeur. Ce service, généralement invisible pour l'utilisateur, fonctionne en continu, 24h/24, pour garantir l'envoi et la réception des courriels selon les besoins.

Le service de messagerie se compose de deux entités : un serveur mail et un client mail :

Les serveurs de messagerie sont essentiels dans le cheminement des courriels, agissant comme des intermédiaires pour transférer les messages entre les différents clients.

Le serveur, un logiciel spécialisé, assure la réception et l'envoi des courriels, englobant à la fois les agents de transfert de courrier (MTA) et les agents de distribution de courrier (MDA).

Le MTA gère la réception initiale des emails et les transfère au MDA qui les stocke de manière appropriée jusqu'à ce que l'utilisateur les récupère.

Les serveurs de messagerie transmettent des messages d'un client de messagerie à un autre. Le client de messagerie est une application web ou de bureau qui reçoit et stocke les messages électroniques. Parmi les clients de messagerie les plus couramment utilisés, on trouve Microsoft Outlook, Mozilla Thunderbird et Lotus Notes. En plus de permettre l'envoi et la réception des emails, ces clients facilitent le tri des messages dans la boîte de réception selon vos besoins.

- Fonctionnalités principales d'un service de messagerie

La messagerie électronique s'appuie sur des protocoles et des serveurs d'email pour gérer l'envoi, la réception et le stockage des messages électroniques.

L'envoi d'un courrier électronique repose sur le protocole SMTP (Simple Mail Transfer Protocol), qui assure le transfert des emails entre les serveurs de messagerie. Ce protocole utilise généralement le port 25 pour la connexion, mais ce port est parfois bloqué pour éviter le spam. Dans ce cas, les ports 587 ou 465 peuvent être utilisés à la place.

Pour la réception des emails, deux protocoles principaux sont utilisés : le POP (Post Office Protocol) et l'IMAP (Internet Message Access Protocol).

Le protocole POP permet de récupérer les emails du serveur de messagerie sur l'ordinateur local, mais il présente des limitations, notamment en termes de synchronisation et de risques de perte de données en cas de panne.

En revanche, le protocole IMAP offre une synchronisation permanente entre le serveur de messagerie et l'appareil utilisé pour consulter les emails, que ce soit un ordinateur, une tablette ou un téléphone. Les emails sont ainsi stockés en toute sécurité sur le serveur, éliminant ainsi le risque de perte de données.

2. Architecture typique d'un système de messagerie

- Composants principaux

La structure du serveur de messagerie englobe divers composants qui travaillent de concert pour acheminer, transmettre, recevoir, stocker et distribuer des courriels.

Il y a cinq composantes principales : MUA, MTA, MDA, MSA, MSS

Mail User Agent (MUA) : également appelé client de messagerie, est une application qui vous permet d'envoyer et de recevoir des emails. Il s'agit de l'interface avec laquelle vous interagissez, contrairement à un serveur de messagerie qui se charge du transport des emails. Les MUAs peuvent être des applications logicielles, telles que Microsoft Outlook, ou des services de messagerie en ligne comme ceux proposés par Gmail ou Yahoo!

Mail Transfer Agent (MTA) : Un programme exécuté sur un serveur de messagerie qui reçoit des messages des agents utilisateurs de messagerie ou d'autres MTAs et les transmet à un autre MTA, ou, si le destinataire se trouve sur le MTA, remet le message à l'agent de livraison locale (LDA) pour qu'il soit remis au destinataire.

Mail Delivery Agent (MDA) : est un programme qui reçoit les emails d'un Agent de Transfert de Courrier (MTA), puis trie et distribue les emails dans la boîte de réception du destinataire. Le destinataire accède aux emails dans sa boîte de réception en utilisant un Agent Utilisateur de Courrier (MUA).

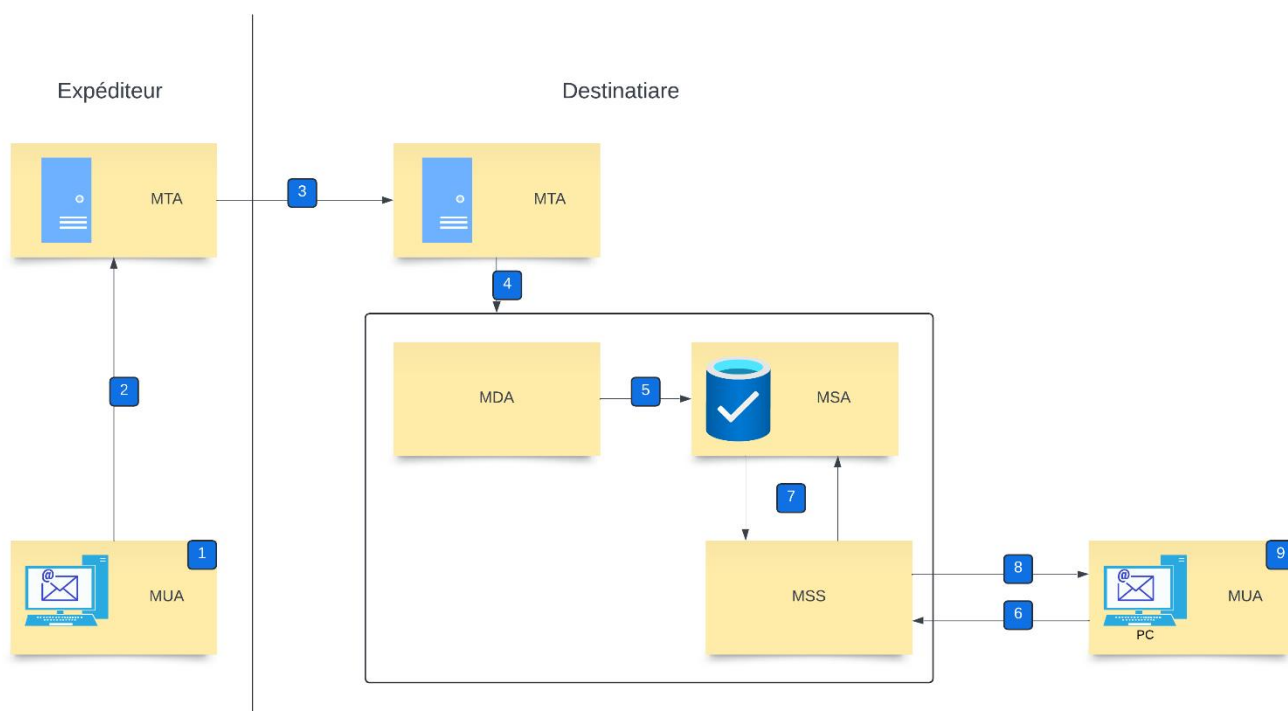
Mail Storage Area (MSA) : est un système ou un serveur local où l'application MTA stocke les courriers électroniques. Il s'agit également de l'endroit d'où le serveur MSS extrait les courriels à la demande de l'application MUA.

Mail Storage Server (MSS) : C'est une application qui récupère les courriels de la zone MSA pour les transmettre à l'application MUA.

Ci-dessous se trouve un tableau détaillant chaque composant du serveur de messagerie, accompagné d'une description de ses fonctionnalités :

Composant	Description	Exemples
Mail User Agent (MUA)	Une application qui vous permet d'envoyer et de recevoir des emails.	<ul style="list-style-type: none"> • Microsoft Outlook Express • Mozilla Thunderbird • Mutt Email Client
Mail Transfer Agent (MTA)	Reçoit des messages des agents utilisateurs de messagerie ou d'autres MTAs et les transmet à un autre MTA.	<ul style="list-style-type: none"> • Postfix • Sendmail • Lotus Domino Server • Microsoft Exchange
Mail Delivery Agent (MDA)	Reçoit les emails d'un MTA, puis trie et distribue les emails dans la boîte de réception du destinataire.	Postfix, Dovecot et Cyrus mettent en œuvre une partie ou la totalité des fonctionnalités de l'agent MDA.
Mail Storage Area (MSA)	Stocke les courriers électroniques.	<ul style="list-style-type: none"> • Mbox • Maildir • /var/mail/spool/.../
Mail Storage Server (MSS)	Récupère les courriels de la zone MSA pour les transmettre à l'application MUA	<ul style="list-style-type: none"> • Dovecot • Cyrus

○ Interaction entre les composants



1. Dans l'application MUA, l'émetteur compose un message électronique puis appuie sur "Envoyer".
2. L'application MUA utilise le protocole SMTP pour transférer le message électronique à un serveur MTA.
3. Le serveur MTA achemine le message électronique vers un autre serveur MTA dans le domaine du destinataire.
4. Le serveur MTA du domaine destinataire transmet le message électronique à un agent MDA dans le système du destinataire.
5. L'agent MDA stocke le message électronique dans la boîte aux lettres du destinataire.
6. L'application MUA du destinataire interroge un serveur MSS.
7. Le serveur MSS utilise les protocoles IMAP4 ou POP pour récupérer le message électronique du destinataire depuis sa boîte aux lettres.
8. Le serveur MSS renvoie le message électronique à l'application MUA.
9. Le destinataire consulte le message électronique envoyé par l'émetteur dans son application MUA.

3. Flux de communication dans un service de messagerie

- Envoi et réception des messages

Composition du message :

L'utilisateur rédige un message en utilisant un client de messagerie (comme Outlook, Gmail, etc.). Le message inclut l'adresse du destinataire, le sujet, le corps du message, et éventuellement des pièces jointes.

Envoi du message :

Lors de l'envoi, le client de messagerie utilise le protocole SMTP (Simple Mail Transfer Protocol) pour transmettre le message au serveur SMTP du fournisseur de services de messagerie de l'expéditeur.

Traitement par le serveur de l'expéditeur :

Le serveur SMTP de l'expéditeur vérifie le domaine du destinataire et tente de localiser le serveur de messagerie approprié. Si le destinataire se trouve sur le même domaine, le message est directement transféré au serveur de réception (serveur IMAP/POP3) du destinataire.

- Transit des messages à travers différents serveurs

Transmission à travers des serveurs intermédiaires :

Si le destinataire se trouve sur un domaine différent, le message peut passer par plusieurs serveurs intermédiaires. Chaque serveur intermédiaire utilise des protocoles de routage pour acheminer le message vers le serveur de destination. Ces serveurs peuvent inclure des serveurs de relais, des passerelles, et des filtres antispam.

Réception par le serveur du destinataire :

Le serveur SMTP du destinataire reçoit le message et le transfère à un serveur de réception (IMAP ou POP3). Le serveur de réception stocke le message jusqu'à ce que le destinataire se connecte pour récupérer ses emails.

Récupération du message par le destinataire :

Le destinataire utilise son client de messagerie pour se connecter à son serveur de réception (via IMAP ou POP3). Le protocole IMAP permet de synchroniser les messages entre le serveur et le client, permettant un accès aux messages depuis plusieurs dispositifs. Le protocole POP3 télécharge les messages sur le dispositif et les supprime généralement du serveur.

II. Protocoles de messagerie

1. SMTP (Simple Mail Transfer Protocol)

- Description et historique

Le protocole de transfert de courrier simple (SMTP) est une norme largement acceptée pour l'envoi des emails. La plupart des cadres de développement prennent en charge SMTP sans nécessiter de bibliothèques supplémentaires, ce qui en fait le moyen le plus rapide pour commencer à envoyer des emails transactionnels depuis votre application web.

En 1982, la première utilisation connue du terme « email » a eu lieu et le protocole SMTP (Simple Mail Transfer Protocol) a été créé. Ce protocole de communication est utilisé pour transférer des messages électroniques vers des serveurs de messagerie.

Le protocole SMTP, défini en 1982 par la RFC 821, permet l'envoi d'emails sur Internet et fonctionne sur le port TCP/25 pour la communication entre services MTA (Mail Transfer Agent).

Il est l'un des plus anciens protocoles d'Internet et a toujours maintenu une compatibilité ascendante. Bien qu'il ait subi quelques modifications mineures, notamment avec la RFC 2821 et l'ajout de la gestion des pièces jointes via le protocole MIME (RFC 2045 à 2049), ses principes de base sont restés inchangés. SMTP est un protocole relativement simple qui pourrait se résumer à l'utilisation de quatre commandes principales : HELO, MAIL FROM, RCPT TO, DATA.

- Fonctionnement du protocole SMTP

Les étapes nécessaires entre le client de messagerie et le serveur pour envoyer un email sont les suivantes :

Établissement de la connexion SMTP : Étant donné que le SMTP (Simple Mail Transfer Protocol) repose sur le TCP (Transmission Control Protocol) comme protocole de transport, la première étape consiste à établir une connexion TCP entre le client et le serveur. Le client de messagerie initie ensuite l'envoi de l'email en utilisant une commande spécifique appelée "Hello" (HELO ou EHLO).

Transfert des données de l'email : Le client envoie au serveur une série de commandes accompagnées du contenu de l'email, qui inclut l'en-tête (avec la destination et l'objet), le corps du message, et tout élément supplémentaire.

Fonctionnement du Mail Transfer Agent : Le serveur utilise un programme appelé Mail Transfer Agent (MTA). Ce dernier vérifie le domaine de l'adresse email du destinataire. Si celui-ci est différent de celui de l'expéditeur, le MTA interroge le DNS (Domain Name System) pour obtenir l'adresse IP du destinataire, similaire à la recherche d'un code postal par les services postaux.

Clôture de la connexion : Une fois la transmission des données terminée, le client informe le serveur, qui met alors fin à la connexion. À ce point, le serveur n'accepte plus de données supplémentaires pour cet email, sauf si une nouvelle connexion SMTP est établie par le client.

En général, ce serveur de messagerie initial n'est pas la destination finale de l'email. Après réception du message, le serveur établit une nouvelle connexion SMTP avec un autre serveur de messagerie, et ce processus est répété jusqu'à ce que l'email atteigne la boîte de réception du destinataire, hébergée par le fournisseur de messagerie du destinataire.

Pour illustrer ce processus, on peut le comparer à l'acheminement d'un courrier postal : un facteur ne livre pas directement une lettre de l'expéditeur au destinataire. Il la dépose d'abord à son bureau de poste local, qui l'envoie ensuite à un bureau dans une autre ville, et ainsi de suite, jusqu'à ce que la lettre parvienne à sa destination finale.

○ Commandes principales et réponses SMTP

Les commandes SMTP sont des instructions textuelles prédéfinies qui indiquent au client ou au serveur comment gérer les données liées à un email. Pensez à ces commandes comme des boutons sur lesquels le client peut cliquer pour assurer la bonne réception des données par le serveur.

HELO/EHLO : Ces commandes servent à établir la connexion SMTP entre le client et le serveur en disant "Bonjour". "HELO" est la version de base, tandis que "EHLO" est une variante spécifique à SMTP.

MAIL FROM : Cette commande informe le serveur de l'adresse email de l'expéditeur. Par exemple, si Alice envoie un email à Bob, son client enverrait la commande "MAIL FROM:alice@example.com".

RCPT TO : Cette commande liste les destinataires de l'email. Si l'email a plusieurs destinataires, le client peut envoyer cette commande plusieurs fois. Par exemple, pour envoyer un email à Bob, Alice utiliserait "RCPT TO:bob@example.com".

DATA : Cette commande précède le contenu de l'email, comme illustré ci-dessous :

DATA

Date : Lundi 4 avril 2022

De : « Alice » <alice@example.com>

Objet : Œufs Bénédicte en cocotte

Pour : « Bob » <bob@example.com>

Salut Bob,

J'apporterai la recette des œufs Bénédicte en cocotte vendredi.

— Alice

.

RSET : Cette commande réinitialise la connexion et efface toutes les informations précédemment transférées, sans terminer la connexion SMTP. Elle est utilisée si le client a envoyé des données incorrectes.

QUIT : Cette commande termine la connexion.

Pour envoyer un email, les clients de messagerie se connectent directement au serveur SMTP de leur fournisseur de messagerie. Un serveur SMTP exécute plusieurs programmes distincts :

Mail Submission Agent (MSA) : L'agent qui reçoit les emails envoyés par le client de messagerie.

Mail Transfer Agent (MTA) : L'agent de transfert de courrier transmet les emails au serveur suivant dans la chaîne de transmission. Si nécessaire, il peut interroger le DNS pour trouver l'enregistrement DNS MX (Mail Exchange) du domaine du destinataire.

Mail Delivery Agent (MDA) : L'agent de livraison de courrier reçoit les emails des MTA et les stocke dans la boîte de réception du destinataire.

Historiquement, le port 25 était le seul utilisé par le protocole SMTP. Bien qu'il soit toujours en usage aujourd'hui, le protocole SMTP peut également fonctionner sur les ports 465, 587 et 2525.

Le **port 25** est principalement réservé aux connexions entre serveurs SMTP. Cependant, il est fréquemment bloqué par les pare-feux des réseaux des utilisateurs finaux pour empêcher les spammeurs de l'exploiter pour l'envoi massif de spam.

Le **port 465** était initialement destiné à l'utilisation du SMTP avec chiffrement SSL (Secure Sockets Layer). Avec le remplacement du SSL par le protocole TLS (Transport Layer Security), ce port est devenu obsolète et n'est plus utilisé par les systèmes de messagerie modernes, bien qu'il puisse encore être trouvé dans des systèmes anciens.

Le **port 587** est maintenant le port standard pour l'envoi d'emails, utilisant le chiffrement TLS pour sécuriser les communications SMTP.

Le **port 2525**, bien qu'il ne soit pas officiellement attribué au SMTP, est parfois proposé par certains services de messagerie pour contourner le blocage des autres ports par les réseaux.

2. POP (Post Office Protocol)

- Description et historique

Le protocole POP3 (Post Office Protocol version 3) est utilisé pour la réception des emails. Il télécharge les messages du serveur de messagerie vers un ordinateur local. Après le téléchargement, les messages originaux sont supprimés de la boîte de réception du serveur.

En général, il est recommandé aux utilisateurs qui accèdent à leurs emails via un seul appareil et qui ont besoin de consulter leurs messages hors ligne d'utiliser le protocole POP3. C'est également avantageux pour ceux qui cherchent à libérer de l'espace dans une boîte de réception presque pleine.

Cependant, il est important de noter que ce protocole ne synchronise pas automatiquement les messages entre votre boîte de réception en ligne et hors ligne. Par conséquent, si l'appareil où les messages sont stockés est perdu ou endommagé, vous risquez de perdre tous les emails sauvegardés.

Le port POP3 par défaut pour établir une connexion avec un serveur de messagerie électronique est le port 110. De plus, le port 995 est utilisé pour le mode sécurisé SSL/TLS, également appelé POP3S.

- Fonctionnement du protocole POP

Les commandes de POP3 :

Commande	Fonction
USER	Il s'agit de l'identifiant du titulaire du compte. En règle générale la partie à gauche du @ dans l'adresse électronique.
PASS	Le mot de passe fourni par le FAI
STAT	Donne le nombre de messages présents dans la file d'attente, ainsi que le volume total des messages en octets.
LIST	Donne la liste des messages en attente, avec pour chaque message : * Son numéro d'ordre dans la file * Sa taille en octets
UIDL	Analogue à LIST, mis à part qu'elle retourne non pas la taille du message mais un identificateur unique
RETR n	Permet de récupérer la totalité du message "n" dans la file d'attente.
DELE n	Détruit le message "n" dans la file d'attente. Le numéro d'ordre des messages suivants demeure inchangé jusqu'à la fin de la session.
TOP n x	Permet de récupérer les x premières lignes du message "n". Les ligne d'en-tête ne sont pas comptabilisées. Cette commande est le plus souvent utilisée pour récupérer l'en-tête complet et la première ligne du message, x ne pouvant être égal à 0.
LAST	Permet de connaître le numéro d'ordre du dernier message auquel on a accédé. (Utile avec une session TELNET).
RSET	Cette commande permet d'annuler toutes les commandes de destruction de messages envoyées pendant la session. En fait, les commandes DELE ne sont rendues effectives que si la session a proprement été fermée (commande QUIT acceptée). Cette méthode permet donc d'annuler les opérations d'effacement dans la session en cours.
NOOP	Cette commande sert à ne rien faire.
QUIT	Clôture la session en cours. Le serveur ferme alors la session TCP et "fait le ménage" dans la file d'attente, en fonction des ordres DELE qui ont été donnés.

Exemple de POP3 avec TELNET :

- Authentification de l'utilisateur :

```
~# telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
user chris
+OK
pass epikoi
+OK Logged in.
```

Nous avons utilisé les commandes 'user' et 'pass' pour nous authentifier

➤ Liste des messages :

```
stat
+OK 3 6694
list
+OK 3 messages:
1 4997
2 1217
3 480
.
```

Nous avons utilisé la commande stat pour connaître le nombre de messages et la commande list pour obtenir les numéros et les tailles de chaque message.

➤ Lire les messages :

```
top 1 1
+OK
Return-Path: <logcheck@lair.nain-t.net>
X-Original-To: root
Delivered-To: root@lair.nain-t.net
Received: by lair.nain-t.net (Postfix, from userid 110)
       id 0278628B8; Sat, 19 Jul 2008 06:02:34 +0200 (CEST)
To: root@lair.nain-t.net
Subject: betelgeuse.maison.mrs 2008-07-19 06:02 System Events
Message-Id: <20080719040235.0278628B8@lair.nain-t.net>
Date: Sat, 19 Jul 2008 06:02:34 +0200 (CEST)
From: logcheck@lair.nain-t.net (logcheck system account)

This email is sent by logcheck. If you wish to no-longer receive it,
.
```

La première ligne du premier message (l'entête non incluse).

```
top 2 1
+OK
Return-Path: <prof@nain-t.net>
X-Original-To: root
Delivered-To: root@lair.nain-t.net
Received: by lair.nain-t.net (Postfix, from userid 0)
       id CCD3D10169; Sat, 19 Jul 2008 13:54:05 +0200 (CEST)
To: root@lair.nain-t.net
Subject: [Fail2Ban] ssh: banned 82.17.104.168
Message-Id: <20080719115406.CCD3D10169@lair.nain-t.net>
Date: Sat, 19 Jul 2008 13:54:05 +0200 (CEST)
From: prof@nain-t.net (root)

Hi,
.
```

La première ligne du deuxième message (l'entête non incluse).

➤ Suppression des messages :

```
dele 3
+OK Marked to be deleted.
list
+OK 2 messages:
1 4997
2 1217
.
```

dele 3 : Marquer le troisième message comme étant supprimé.

list : Afficher la liste des messages restants.

➤ Annulation de la suppression :

```
rset
+OK
list
+OK 3 messages:
1 4997
2 1217
3 480
.
```

rset : Réinitialise la session de manière à annuler toutes les opérations de suppression marquées.

➤ Termine la session :

```
quit
+OK Logging out.
Connection closed by foreign host.
```

quit : Termine la session SMTP et déconnecte l'utilisateur du serveur SMTP.

- Avantages et inconvénients du POP3

POP3	
Les avantages	Les inconvénients
Consultation hors ligne	Synchronisation limitée
Libération d'espace sur le serveur	Risque de perte de données
Simplicité	Accès unique
Gestion des emails multiples	Sécurité

Les avantages :

- Les emails sont téléchargés sur votre appareil, permettant une consultation sans connexion Internet.
- Après le téléchargement, les emails sont supprimés du serveur, ce qui aide à gérer les limites de stockage.
- POP3 est un protocole simple et facile à configurer et utiliser.
- Vous pouvez organiser vos emails localement sur votre appareil, créant des dossiers et sous-dossiers selon vos préférences.

Les inconvénients

- POP3 ne synchronise pas les emails entre différents appareils. Les actions effectuées sur un appareil (comme la suppression ou le déplacement d'un email) ne sont pas reflétées sur d'autres appareils.
- Si l'appareil où les emails sont stockés est perdu, volé ou endommagé, vous risquez de perdre tous les messages téléchargés.
- POP3 est idéal pour ceux qui accèdent à leur email depuis un seul appareil. Pour ceux qui utilisent plusieurs appareils, IMAP est souvent une meilleure option.
- POP3 peut être moins sécurisé que certains protocoles modernes, surtout s'il n'est pas configuré pour utiliser des connexions sécurisées (SSL/TLS).

3. IMAP (Internet Message Access Protocol)

- Description et historique

IMAP (Internet Message Access Protocol), contrairement à POP3, est un protocole de courrier entrant bidirectionnel qui ne récupère que les en-têtes des messages électroniques plutôt que leur contenu complet. Ainsi, les messages restent sur le serveur même après leur consultation, ce qui permet un accès depuis différentes plateformes. De plus, ce protocole assure la synchronisation des modifications effectuées par le client de messagerie avec le serveur, facilitant ainsi une communication bidirectionnelle.

Cette configuration est recommandée pour les utilisateurs qui désirent accéder à leurs emails à partir de plusieurs appareils sans craindre la perte de messages importants en cas de vol ou de panne d'un appareil. Un avantage supplémentaire de l'utilisation d'IMAP est la facilité de recherche de messages spécifiques à l'aide de mots-clés.

Cependant, il est indispensable de disposer d'une connexion Internet stable pour accéder à tous les emails stockés sur le serveur IMAP. La gestion de l'espace de stockage des emails peut également poser des problèmes, notamment en cas d'utilisation intensive.

Le port 993 est attribué à IMAPS, un protocole sécurisé utilisant SSL/TLS pour assurer la confidentialité des communications lors de l'accès aux emails via IMAP, et le port 143 est utilisé pour IMAP standard.

- Fonctionnement du protocole IMAP

Commande	Description
capability	demande la liste des possibilités que le serveur supporte.
authenticate	indique au serveur un mécanisme d'authentification. Si le serveur supporte le mécanisme d'authentification demandé, il exécute un échange protocolaire d'authentification afin d'authentifier et identifier le client. Il est aussi possible d'utiliser la commande <code>login</code> , plus rudimentaire car elle ne supporte que le nom d'utilisateur et son mot de passe en texte clair.
namespace	Pour aller vite, cette commande retourne ce qu'il faut pour que l'utilisateur puisse connaître les dossiers auxquels il peut accéder et souscrire, ce qui peut inclure les dossiers partagés, prévus dans le protocole IMAP

lsub	permet d'obtenir à partir d'un point de référence la liste de dossiers auxquels le client a souscrit (qu'il désire voir dans son client).
list	permet d'obtenir à partir d'un point de référence la liste de dossiers existants
select	sélectionne une boîte aux lettres, ainsi les messages dans la boîte aux lettres sont accessibles. Cette commande renvoie le nombre total de messages (EXISTS), et le nombre de nouveaux messages (RECENT)
getquotaroot	Comme son nom le laisse penser, cette commande renvoie l'état d'occupation de l'espace alloué, lorsque les quotas sont activés sur le serveur IMAP
uid	s'utilise avec les commandes COPY, FETCH, STORE ou encore SEARCH. Son utilité est de renvoyer un index unique plutôt qu'un numéro de séquence, comme le feraient les commandes COPY, FETCH, STORE et SEARCH
fetch	cette commande dispose d'une syntaxe assez complexe. il est possible d'obtenir par elle de nombreuses informations sur un message ou un lot de messages. Dans l'exemple, Thunderbird se contente de récupérer les drapeaux attachés à chaque message présent dans INBOX
idle	lorsque le serveur supporte cette commande, il permet au client d'être informé en temps réel de l'arrivée de nouveaux messages
close	assez similaire à EXPUNGE, cette commande détruit de façon définitive tous les messages qui ont le drapeau <code>deleted</code> . Elle ne renvoie pas de compte rendu, comme le fait <code>EXPUNGE</code> . Thunderbird n'envoie pas cette commande par défaut. Il faut le lui indiquer dans sa configuration avancée, comme expliqué dans cette astuce
logout	Logout met fin à la session IMAP

✓ Exemple de IMAP avec TELNET :

Connexion à un serveur IMAP via Telnet permettant au client d'interagir avec le serveur de messagerie pour recevoir et gérer des emails.

```
$ telnet imap-us.atmailcloud.com 143
Trying 204.145.97.25...
Connected to imap-us.atmailcloud.com.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-012mip
```

En utilisant netcat (ou nc) à la place de Telnet pour se connecter à un serveur IMAP :

```
$ nc --crlf --verbose imap-us.atmailcloud.com 143
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Connected to 204.145.97.26:143.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-012mip
```

Avec SSL :

```
$ openssl s_client -connect imap-us.atmailcloud.com:993 -crlf -quiet
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
verify return:1
depth=1 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = RapidSSL TLS RSA CA G1
verify return:1
depth=0 CN = *.atmailcloud.com
verify return:1
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-010mip
```

Pour effectuer des actions sur un serveur IMAP, il est généralement nécessaire de s'authentifier. Il existe trois méthodes pour s'authentifier :

- Login
- SASL AUTH LOGIN
- SASL AUTH PLAIN

➤ Pour s'authentifier via la méthode **Login** :

```
$ telnet imap-us.atmailcloud.com 143
Trying 204.145.97.26...
Connected to imap-us.atmailcloud.com.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-011mip
A1 login someuser@example.atmailcloud.com My_P@ssword1
A1 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL
```

➤ L'authentification via la méthode **SASL LOGIN** :

Tout d'abord, nous devons vérifier si le serveur IMAP prend en charge la méthode SASL AUTH LOGIN, comme suit :

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-011mip
```

AUTH=LOGIN" indique que le serveur IMAP prend en charge la méthode SASL LOGIN, où le nom d'utilisateur et le mot de passe sont envoyés séparément sous forme de chaînes encodées en base64.

Le serveur IMAP communique cette information en encodant la question.

Lorsque nous émettons la commande "AUTHENTICATE LOGIN", nous recevons :

En base64 nous obtenons :

```
a AUTHENTICATE LOGIN
+ VXNlcm5hbWU6
```

```
$ echo "VXNlcm5hbWU6" | openssl base64 -d
Username:
```

La méthode préférable pour encoder à la fois le nom d'utilisateur et le mot de passe est Base64 :

```
$ echo -en "someuser@example.atmailcloud.com" | openssl base64
c29tZXVzZXJAZXhxbXBsZS5hdG1haWxjbG91ZC5jb20=
$ echo -en "My_P@ssword1" | openssl base64
TX1fUEBzc3dvcnQx
```

Pour procéder à l'authentification :

```
$ telnet imap-us.atmailcloud.com 143
Trying 204.145.97.25...
Connected to imap-us.atmailcloud.com.
Escape character is '^'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-012mip
a authenticate login
+ VXNlcm5hbWU6
c29tZXVzZXJAZXhxbXBsZS5hdG1haWxjbG91ZC5jb20=
+ UGFzc3dvcnQx
TX1fUEBzc3dvcnQx
a OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL C
```

➤ L'authentification via la méthode **SASL AUTH PLAIN** :

Utilisant la méthode PLAIN, nous fournissons le nom d'utilisateur et le mot de passe sous forme d'une seule chaîne encodée en base64, séparés par le caractère NUL.

```
$ echo -en "\0someuser@example.atmailcloud.com\0My_P@ssword1" | openssl base64
AHNvbWV1c2VyQGV4YW1wbGUuYXRtYWlsY2xvdWQuY29tAE15X1BAc3N3b3JkMQ==
```

La méthode d'authentification :

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] IMAP/POP3 ready - us11-011mip
a authenticate plain
+
AHNvbWV1c2VyQGV4YW1wbGUuYXRtYWlsY2xvdWQuY29tAE15X1BAc3N3b3JkMQ==
a OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND U
```

✓ La création d'un nouveau répertoire : CREATE

```

1  c CREATE work
2  c OK Create completed (0.002 + 0.000 + 0.001 secs).
3  k2 LIST "" "*"
4  * LIST (\HasNoChildren \Trash) "." Trash
5  * LIST (\HasNoChildren) "." folder1
6  * LIST (\HasNoChildren) "." work
7  * LIST (\HasNoChildren) "." INBOX
8  k2 OK List completed (0.001 + 0.000 secs).
```

✓ Sélectionner une boîte : SELECT

Cette commande indique au serveur que le client souhaite désormais sélectionner une boîte aux lettres ou un répertoire particulier :

```

1  g21 SELECT "INBOX"
2  * FLAGS (Answered Flagged Deleted Seen Draft)
3  * OK [PERMANENTFLAGS (Answered Flagged Deleted Seen Draft *)] Flags permitted.
4  * 4 EXISTS
5  * 0 RECENT
6  * OK [UNSEEN 2] First unseen.
7  * OK [UIDVALIDITY 1536750617] UIDs valid
8  * OK [UIDNEXT 9] Predicted next UID
9  * OK [HIGHESTMODSEQ 11] Highest
10 g21 OK [READ-WRITE] Select completed (0.000 + 0.000 secs).
```

✓ Lister le contenu d'un répertoire : LIST

Affichez tous les dossiers/boîtes aux lettres auxquels vous avez le droit d'accès sur le serveur, qu'il s'agisse de vos propres dossiers, de ceux d'un autre utilisateur ou de dossiers accessibles publiquement.

```

1  A1 list "INBOX/" "*"
2  * LIST (HasNoChildren) "/" INBOX/some_other_folder
3  * LIST (HasNoChildren UnMarked Archive) "/" INBOX/Archive
4  * LIST (HasNoChildren UnMarked Sent) "/" INBOX/Sent
5  * LIST (HasNoChildren Marked Trash) "/" INBOX/Trash
6  * LIST (HasNoChildren Marked Junk) "/" INBOX/Spam
7  * LIST (HasNoChildren UnMarked Drafts) "/" INBOX/Drafts
8  A1 OK List completed (0.000 + 0.000 secs).
```


✓ Récupération des messages : FETCH

Permet à un client de récupérer des messages depuis un répertoire :

```

1  f fetch 1:4 (BODY[HEADER.FIELDS (Subject)])
2  * 1 FETCH (BODY[HEADER.FIELDS (SUBJECT)] {27}
3  Subject: Test message 1
4
5  )
6  * 2 FETCH (FLAGS (Seen) BODY[HEADER.FIELDS (SUBJECT)] {27}
7  Subject: Test message 3
8
9  )
10 * 3 FETCH (FLAGS (Seen) BODY[HEADER.FIELDS (SUBJECT)] {27}
11 Subject: Test message 5
12
13 )
14 * 4 FETCH (FLAGS (Seen) BODY[HEADER.FIELDS (SUBJECT)] {27}
15 Subject: Test Message 6
16
17 )
18 f OK Fetch completed (0.002 + 0.000 secs).
```

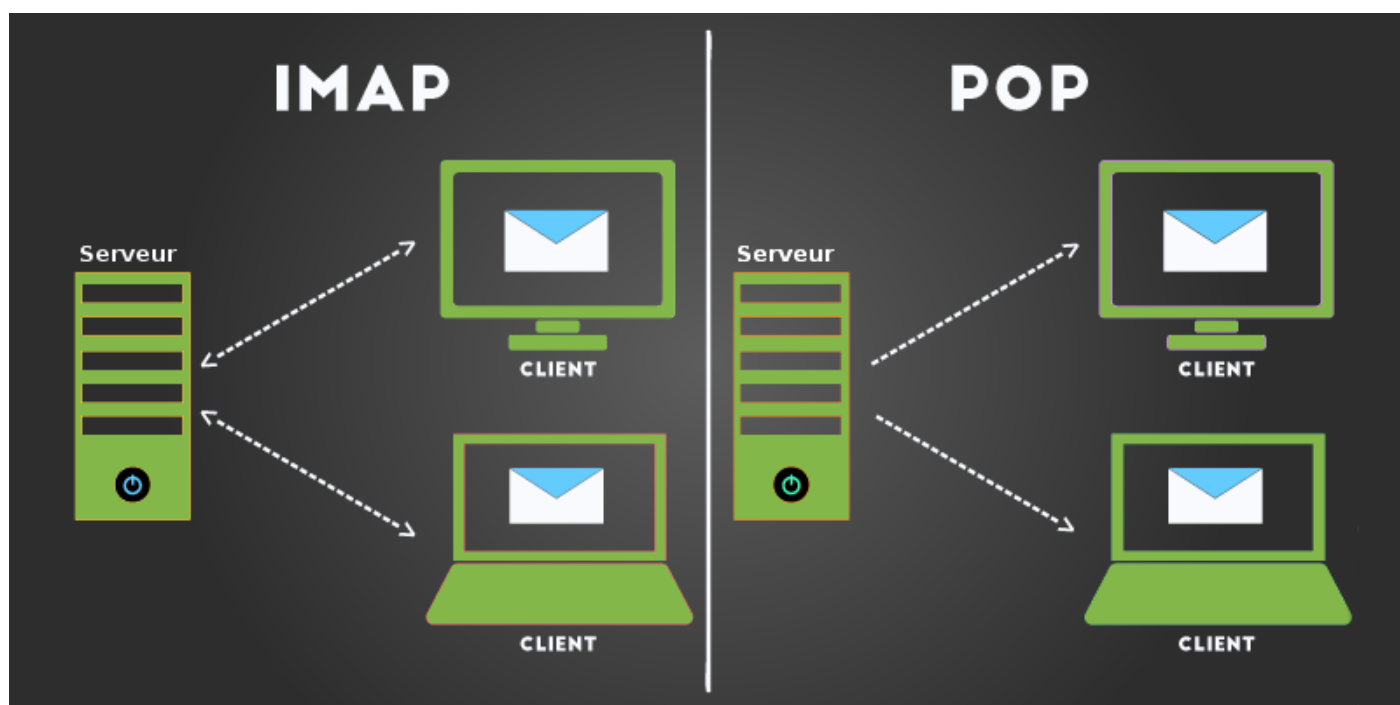
✓ Suppression d'un message : DELETE

Cette commande supprime la boîte aux lettres ou le répertoire spécifié par son nom :

```

1  A682 LIST "" *
2  * LIST () "/" blurdybloop
3  * LIST (\Noselect) "/" foo
4  * LIST () "/" foo/bar
5  A682 OK LIST completed
6  A683 DELETE blurdybloop
7  A683 OK DELETE completed
8  A684 DELETE foo
9  A684 NO Name "foo" has inferior hierarchical names
10 A685 DELETE foo/bar
11 A685 OK DELETE Completed
12 A686 LIST "" *
13 * LIST (\Noselect) "/" foo
14 A686 OK LIST completed
15 A687 DELETE foo
16 A687 OK DELETE Completed
```

- Comparaison entre IMAP et POP



Fonctionnalité	POP3	IMAP
Téléchargement des emails	Télécharge les emails du serveur vers le client local. Les emails sont généralement supprimés du serveur après téléchargement.	Permet de visualiser, organiser et gérer les emails directement sur le serveur. Les actions effectuées sont synchronisées entre le client et le serveur.
Gestion des répertoires	Les répertoires sur le client sont distincts de ceux sur le serveur.	Permet d'accéder aux répertoires du serveur et de gérer les emails de manière interactive. Les modifications sont reflétées sur le serveur et accessibles depuis différents appareils.
Type de connexion	Établit une connexion ponctuelle pour télécharger les emails, puis se déconnecte.	Maintient une connexion active, permettant une interaction continue pour rechercher, accéder et gérer les emails en temps réel.
Flexibilité et accessibilité	Convient généralement lorsque les emails doivent être téléchargés sur un seul appareil et consultés localement.	Idéal pour une gestion flexible des emails sur plusieurs appareils, avec une synchronisation en temps réel entre le client et le serveur.

1. Postfix

○ Présentation de Postfix

Le courrier électronique a été introduit sur le réseau ARPANET dans les années 1970, établissant le protocole SMTP comme l'un des premiers dans l'architecture TCP/IP.

Avec l'essor d'Internet, les systèmes de messagerie ont gagné en importance. En 1980, Sendmail est devenu le premier serveur de messagerie majeur, utilisant déjà le protocole SMTP.

Postfix est apparu en 1998, avec le soutien d'IBM, pour résoudre les problèmes de sécurité de Sendmail tout en introduisant une gestion plus flexible et modulaire de l'administration des serveurs de messagerie.

Postfix est un logiciel libre conçu pour gérer la livraison des messages électroniques de manière rapide, sécurisée et facile à administrer, se distinguant ainsi de Sendmail. Il offre une solution complète pour les besoins professionnels en remplaçant avantageusement d'autres solutions propriétaires.

Pour améliorer la gestion des emails, Postfix permet l'intégration avec des processus externes chargés de décider de l'acceptation ou du rejet des courriels, notamment dans les systèmes anti-spam.

○ Configuration de base de Postfix

Pour configurer Postfix :

1. L'installation se fait avec la commande pour les machines Ubuntu :

```
sudo apt update  
sudo apt install postfix
```

2. Configuration principale :

Dans le fichier : `/etc/postfix/main.cf`, voila un exemple de la configuration minimale :

```
myhostname = mail.example.com  
mydomain = example.com  
myorigin = $mydomain  
inet_interfaces = all  
inet_protocols = ipv4
```

3. Redémarrage du service Postfix :

```
sudo systemctl restart postfix
```

4. Vérification du statut du service :

```
sudo systemctl status postfix
```

5. Tests d'envoi d'email :

```
echo "Test email " | mail -s "Test Subject" mail.iccn@inpt.com
```

○ Fonctionnement interne de Postfix

Postfix est un système de messagerie très modulaire.

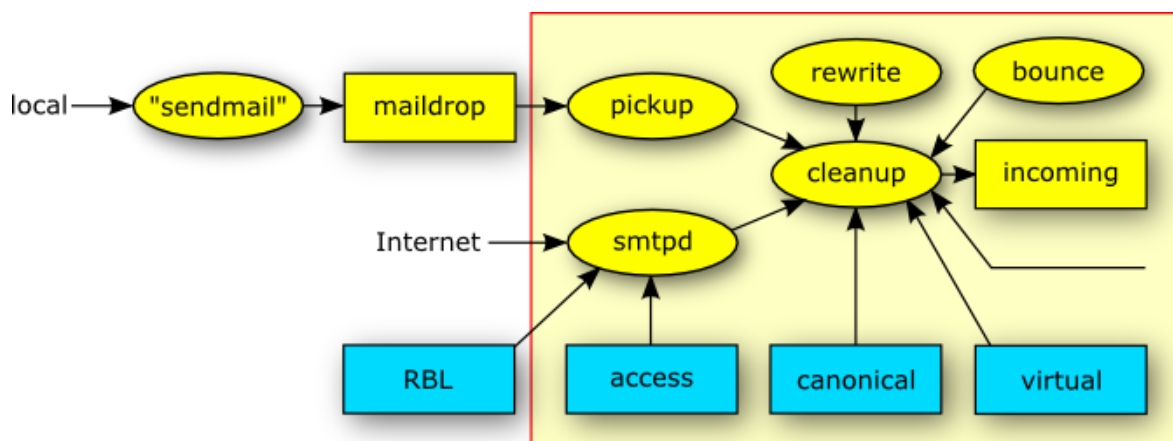
Les files d'attente de Postfix :

Il existe cinq files d'attente pour la gestion des messages :

- « maildrop » : reçoit les messages postés localement, c'est-à-dire à partir de l'hôte lui-même.
- « incoming » : reçoit à la fois les messages postés localement et ceux arrivant du réseau (par exemple, lorsque l'hôte est utilisé comme serveur SMTP pour un réseau local). Les messages dans cette file ont déjà subi certains traitements, détaillés ultérieurement.
- « active » : contient les messages en cours d'envoi.
- « deferred » : regroupe les messages qui n'ont pas pu être envoyés pour diverses raisons. Conformément au protocole SMTP, ces messages ne sont pas abandonnés immédiatement. Ils seront réessayés plusieurs fois et réintégrés dans la file « active ».
- « mailbox » : file d'attente des messages destinés aux utilisateurs locaux, dont l'utilisation précise sera discutée plus tard.

Réception d'un email :

À son arrivée dans le système Postfix, un message, quelle que soit sa provenance initiale, est d'abord dirigé vers la file d'attente appelée « incoming ».



Origine du message :

Message posté localement :

Pour le message posté localement, le programme Postfix appelé « sendmail » dépose le message dans la file « maildrop », où il est ensuite récupéré par le service « pickup ». Ce processus inclut des contrôles sanitaires visant à sécuriser le système Postfix. Les permissions du répertoire contenant « maildrop » permettent à tout utilisateur d'écrire dans le dossier, mais aucun utilisateur ne peut effacer son contenu.

Le message vient du réseau :

Lorsque le message provient du réseau, le serveur SMTP de Postfix le reçoit et applique également des contrôles sanitaires pour protéger l'intégrité du système. Ce serveur SMTP peut être configuré pour effectuer des vérifications anti-spam basées sur une liste noire locale, des requêtes DNS concernant le domaine de l'expéditeur, ou d'autres informations relatives à l'émetteur.

Traitement du message :

Le message n'est pas livrable :

Lorsqu'un message n'est pas livrable, le système Postfix génère automatiquement un email pour informer l'expéditeur. Cette notification est gérée par les démons « bounce » (rebond) ou « defer » (différé) qui communiquent le statut du message.

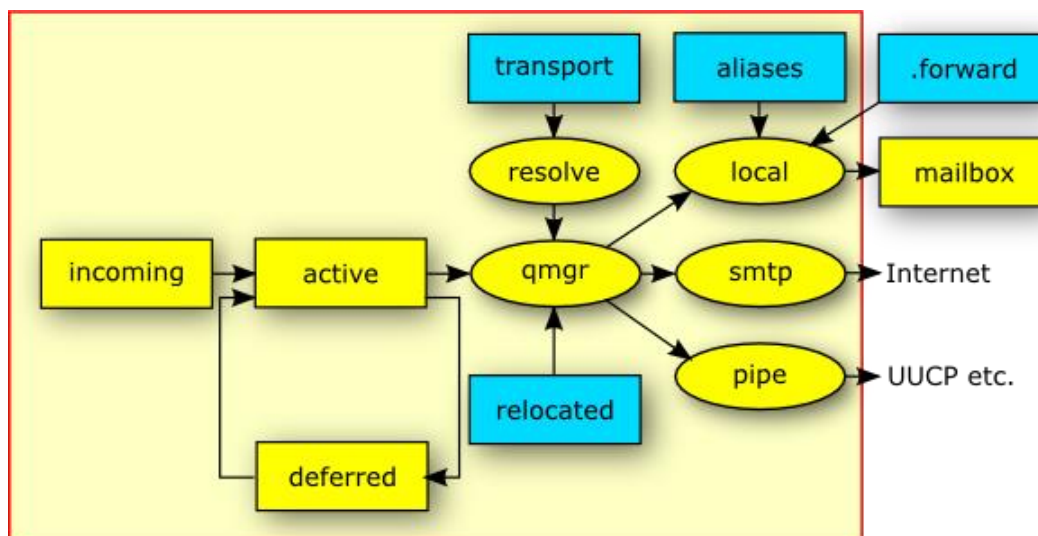
De plus, le système Postfix envoie automatiquement un email d'alerte au responsable de la messagerie en cas de problème, comme des violations de protocole SMTP, des infractions aux règles de sécurité UCE, etc. Ce mécanisme d'alerte peut être configuré pour signaler divers incidents relatifs à la gestion des emails.

Le message est livrable :

Le message est acheminé par l'agent de livraison local, soit via une entrée de la base de données des « alias » au niveau du système, soit via le fichier « .forward » au niveau de l'utilisateur. Ces concepts seront explorés plus en détail lors de la configuration de Postfix.

Le daemon « cleanup » effectue le dernier traitement du message en ajoutant des en-têtes comme « From: », en normalisant les adresses de réponse au format « user@fully.qualified.domain », et facultativement en extrayant les adresses des destinataires de l'en-tête. Le résultat est placé dans la file d'attente « incoming », et une notification est envoyée au « queue manager » (qmgr) pour signaler l'arrivée d'un nouveau message. Le daemon « cleanup » peut être configuré pour modifier les adresses en fonction des tables de consultation «canonical » et « virtual », un aspect qui sera également abordé dans la configuration de Postfix.

Livraison du message :



Lorsqu'un message est placé dans la file d'attente « incoming » de Postfix, la prochaine étape est sa livraison, comme illustré dans le schéma ci-contre qui présente les composants principaux du processus de livraison de Postfix.

Le gestionnaire de file d'attente, au cœur du système de messagerie, communique avec les agents de livraison « local », « smtp », ou « pipe », en fournissant les informations nécessaires telles que le chemin d'accès au fichier contenant la file d'attente, l'adresse de l'expéditeur, le nom de l'hôte destinataire si celui-ci n'est pas local, ainsi qu'une ou plusieurs adresses de destinataires.

Pour chaque message non livré, le gestionnaire maintient une file d'attente « deferred » distincte afin de prévenir tout impact négatif sur les performances dues à des rapports de livraison trop volumineux, préservant ainsi l'accès aux autres files d'attente.

De plus, le gestionnaire maintient une petite file d'attente « active » contenant uniquement quelques messages prêts pour la livraison. Cette approche limite le risque de débordement de mémoire en cas de charge élevée sur le serveur.

En option, le gestionnaire peut renvoyer le message pour les destinataires répertoriés dans la table « relocated », laquelle contient des informations sur les utilisateurs ayant changé d'adresse email.

5. Dovecot

- Présentation de Dovecot

Dovecot est un serveur qui supporte les protocoles "Internet Message Access Protocol" (IMAP) et "Post Office Protocol" (POP), conçu avec une forte emphase sur la sécurité. Dovecot est un choix idéal pour les installations de petite et grande envergure. Il est rapide, facile à configurer, ne nécessite pas d'administration spéciale et consomme très peu de mémoire.

Dovecot est conçu pour être léger et efficace en termes de consommation de ressources système. Il utilise des techniques de caching pour améliorer les performances lors de l'accès aux boîtes aux lettres et aux messages.

- Configuration de base de Dovecot

1. Installation de Dovecot :

```
sudo apt update  
sudo apt install dovecot-core dovecot-imapd dovecot-pop3d
```

2. Configuration de Dovecot :

La configuration de Dovecot est généralement située dans le répertoire `/etc/dovecot/`. Les principaux fichiers de configuration sont **dovecot.conf**, **10-auth.conf**, **10-mail.conf**, et **10-master.conf**.

Pour le fichier : `/etc/dovecot/dovecot.conf` :

```
# Dovecot configuration file  
  
# Enable installed protocols  
protocols = imap pop3  
  
# A more verbose logging for debugging  
log_path = /var/log/dovecot.log  
info_log_path = /var/log/dovecot-info.log
```

Pour le fichier : /etc/dovecot/conf.d/10-auth.conf :

```
# Authentication configuration

# Disable plain text authentication without SSL/TLS
disable_plaintext_auth = yes

# Authentication mechanisms
auth_mechanisms = plain login


# User database
userdb {
    driver = passwd
}


# Password database
passdb {
    driver = pam
}
```

Pour le fichier : /etc/dovecot/conf.d/10-mail.conf :

```
# Mailbox configuration


# Mail location
mail_location = maildir:~/Maildir


# Mailbox namespaces
namespace inbox {
    inbox = yes
}


# Mailbox formats
mail_uid = vmail
mail_gid = vmail
```


Pour le fichier : /etc/dovecot/conf.d/10-master.conf :

```
# Service configuration
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
}
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    port = 995
    ssl = yes
  }
}

# Disable unnecessary services
service dict {
  unix_listener dict {
    mode = 0600
    user = vmail
    group = vmail
  }
}
```

Pour appliquer la configuration :

```
sudo systemctl restart dovecot
```

6. Chronologie de l'évolution de l'Email

1965 : À l'Institut de technologie du Massachusetts (MIT), le programme « Mailbox » marque la première apparition de l'email. Les utilisateurs peuvent laisser des messages sur les ordinateurs de l'université pour que d'autres puissent les consulter.

1971 : Ray Tomlinson, ingénieur américain, développe le système de messagerie pour le réseau ARPANET, ancêtre de l'Internet moderne, et introduit l'utilisation de l'arobase (@) dans les adresses email.

1977 : La proposition du RFC 733 établit un format standard pour l'envoi de messages électroniques sur Internet. Le service postal américain commence à percevoir l'email comme une menace.

1982 : Le terme « email » est utilisé pour la première fois et le Simple Mail Transfer Protocol (SMTP) est créé pour faciliter le transfert de messages électroniques entre serveurs.

1988 : Steve Dorner, ingénieur logiciel américain, crée Eudora, une application qui popularise l'email grâce à son interface utilisateur graphique. Simultanément, Microsoft lance Microsoft Mail pour Mac.

1989 : CompuServe devient la première entreprise à offrir un accès limité à Internet et un service de messagerie à ses abonnés.

Début des années 90 : L'apparition des pourriels (spams) commence avec des envois massifs de messages non sollicités à des fins lucratives.

1992 : Microsoft lance Microsoft Outlook pour MS-DOS, et CompuServe introduit le premier email WYSIWYG, permettant l'utilisation de polices, couleurs et émoticônes.

1993 : AOL et Delphi connectent leurs systèmes d'email propriétaires à Internet, standardisant ainsi l'email Internet.

1996 : Sabeer Bhatia et Jack Smith lancent Hotmail, l'un des premiers services de messagerie en ligne gratuits. La startup attire rapidement l'attention de Microsoft, qui la rachète un an plus tard.

1997 : Microsoft présente Outlook 97, qui, associé à Internet Explorer 4, devient un leader du marché des logiciels de messagerie. Yahoo! acquiert Four11 et propose un webmail gratuit, RocketMail, ainsi qu'un annuaire d'adresses email.

1998 : Microsoft lance Outlook 2000 et finalise le rachat de Hotmail pour une somme estimée entre 300 et 400 millions de dollars. À cette époque, plus de 36 millions de machines sont connectées à Internet.

Chapitre 1 : Fonctionnement et Protocoles des Services de Messagerie Électronique -Mouad Tigmouti-

Fin des années 90 : L'email devient de plus en plus populaire, avec l'apparition de messages au format HTML intégrant différentes polices, couleurs, images et formats.

2003 : Microsoft commercialise Exchange Server 2003 (Outlook 2003), incluant un dossier « courrier indésirable ».

2004 : Google annonce le lancement de Gmail, un service de messagerie gratuit. Parallèlement, la Federal Trade Commission des États-Unis codifie les lois anti-spam.

2006 : Microsoft lance Outlook 2007, renomme Outlook Express en Windows Mail, et rebaptise MSN Hotmail en Windows Live Mail. À cette époque, près de 439 millions de machines sont connectées à Internet.

2007 : Google rend Gmail accessible au public. L'Internet Engineering Task Force adopte le protocole DKIM pour réduire les risques de phishing (hameçonnage).

2010 : Microsoft déploie Outlook 2010 et enrichit le module Outlook Social Connector en intégrant des fonctionnalités sociales provenant de LinkedIn, Facebook et MySpace.

2011 : Le guide de grammaire Associated Press Stylebook recommande l'utilisation du mot « Email » sans trait d'union. À cette époque, on compte 3,1 milliards d'adresses email dans le monde.

2012 : Avec l'avènement du Responsive Design, l'email connaît un renouveau et devient un mode de communication principal sur smartphone.

2013 : Le marketing mobile, l'email retargeting et l'email-to-store deviennent des tendances majeures, modifiant la manière de concevoir les campagnes.

2015 : L'affaire des courriels d'Hillary Clinton émerge, devenant l'une des plus grandes controverses de l'histoire de l'email.

2018 : Le Règlement Général sur la Protection des Données (RGPD) entre en vigueur dans les 28 pays de l'Union Européenne, impactant directement l'email marketing.

2019 : Les sites web doivent se conformer aux exigences du Référentiel Général d'Accessibilité pour les Administrations, et les emails tendent à suivre cette direction.

2020 : Profitant de la pandémie de coronavirus, les cybercriminels augmentent les attaques par email de 667 % par rapport à l'année précédente.

III. Structure des Emails

1. Composants d'un mail

- MIME (Multipurpose Internet Mail Extensions)

MIME, ou Multipurpose Internet Mail Extensions, est une norme Internet qui permet d'étendre le format des emails pour inclure :

- Texte dans différents jeux de caractères au-delà de l'ASCII
- Texte formaté en HTML
- Contenu multimédia (images, audio, vidéo)
- Messages multipartites
- Pièces jointes binaires (documents, images, etc.)
- Un email se compose principalement de deux parties : l'en-tête et le corps.

À l'origine, les emails étaient limités au texte brut en ASCII. MIME a été développé pour surmonter ces limites, permettant l'envoi de contenus plus riches et variés par email.

Composants de MIME :

1. Type MIME (MIME Type)

Le type MIME indique la nature et le format d'un document, structuré en deux parties : type et sous-type, séparés par une barre oblique. Par exemple :

- text/plain : texte brut
- text/html : texte HTML
- image/jpeg : image JPEG
- application/pdf : document PDF

2. Encodage du Contenu (Content-Transfer-Encoding)

MIME définit plusieurs méthodes pour encoder les données afin qu'elles soient adaptées à la transmission par email :

- 7bit : données ASCII standard
- 8bit : données étendues au-delà de l'ASCII
- binary : données binaires pures
- base64 : encodage des données binaires en texte ASCII
- quoted-printable : encodage des caractères non-ASCII en séquences ASCII

3. Disposition du Contenu (Content-Disposition)

Ce champ spécifie la manière dont le contenu doit être présenté. Les valeurs courantes incluent :

- inline : contenu intégré directement dans le corps de l'email.
- attachment : contenu ajouté en tant que pièce jointe.

Structure des Messages MIME

Un email MIME peut être composé de plusieurs parties, chacune définie par une frontière (boundary).

Exemple d'un message multipart :

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary-string"

--boundary-string
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 7bit

Bonjour,

Veuillez trouver ci-joint le document demandé.

Cordialement,
John

--boundary-string
Content-Type: application/pdf; name="document.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="document.pdf"

JVBERi0xLjQKJdP0zOEKMSAwIG9iago8PC9UeXBIL1BhZ2UvUGFyZW50IDIgMCBS...
--boundary-string--
```

Types MIME courants

- text/plain : texte brut
- text/html : texte formaté en HTML
- image/jpeg : images JPEG
- image/png : images PNG
- application/pdf : fichiers PDF
- application/zip : fichiers compressés ZIP
- audio/mpeg : fichiers audio MPEG
- video/mp4 : fichiers vidéo MP4

- En-tête (header)

L'en-tête (header) contient plusieurs champs essentiels et additionnels. Les champs principaux incluent l'expéditeur (From), le destinataire (To), le sujet (Subject) et la date d'envoi (Date). Il peut également comporter des champs optionnels tels que copie carbone (CC), copie carbone invisible (BCC) et répondre à (Reply-To).

L'en-tête d'un email contient des informations cruciales pour la transmission et l'identification du message. Il comprend les champs suivants :

➤ Champs principaux :

- From (Expéditeur) : Adresse email de l'expéditeur.
- To (Destinataire) : Adresse email du ou des destinataires principaux.
- Subject (Objet) : Objet de l'email, résumant le contenu du message.
- Date (Date d'envoi) : Date et heure à laquelle l'email a été envoyé.

➤ Champs additionnels :

- CC (Copie carbone) : Adresses email des destinataires secondaires qui recevront une copie visible de l'email.
- BCC (Copie carbone invisible) : Adresses email des destinataires secondaires qui recevront une copie invisible de l'email.
- Reply-To (Répondre à) : Adresse email à laquelle les réponses doivent être envoyées, si différente de l'adresse de l'expéditeur.
- Message-ID : Identifiant unique du message, utilisé pour le suivi et la gestion des emails.
- MIME-Version : Version du standard MIME (Multipurpose Internet Mail Extensions) utilisé, généralement "1.0".
- Content-Type : Indique le type de contenu du corps de l'email, par exemple "text/plain" pour du texte brut ou "text/html" pour du HTML.
- Content-Transfer-Encoding : Spécifie le type d'encodage utilisé pour le contenu du message, comme "7bit", "8bit", "base64" ou "quoted-printable".

- Corps (body)

Le corps (body) de l'email est constitué du contenu principal, qui peut être en texte brut ou en format HTML. Il permet aussi l'inclusion de pièces jointes, ajoutant ainsi des fichiers supplémentaires à l'email.

➤ Texte brut vs texte formaté (HTML) :

- Texte brut (text/plain) : Contenu simple sans formatage, compatible avec tous les clients de messagerie.
- Texte formaté (text/html) : Contenu formaté utilisant le langage HTML, permettant l'inclusion de styles, images, liens et autres éléments multimédia.

➤ Multipart Messages :

- Les emails peuvent être envoyés en tant que messages multipart pour inclure plusieurs parties de contenu. Par exemple, un email peut contenir une partie en texte brut et une partie en HTML pour assurer la compatibilité avec différents clients de messagerie.
- Multipart/alternative : Utilisé pour inclure des versions alternatives du contenu (par exemple, texte brut et HTML).
- Multipart/mixed : Utilisé pour joindre plusieurs parties différentes, telles que le contenu principal et les pièces jointes.

➤ Pièces jointes :

- Les pièces jointes sont ajoutées au corps de l'email à l'aide du standard MIME.
- Disposition des pièces jointes : Les pièces jointes peuvent être intégrées directement dans le contenu (inline) ou ajoutées en tant que fichiers séparés (attachment).
- Content-Disposition : Indique comment la pièce jointe doit être présentée (inline ou attachment).
- Content-Type : Spécifie le type MIME de la pièce jointe (par exemple, "image/jpeg" pour une image JPEG).
- Content-Transfer-Encoding : Détermine l'encodage utilisé pour transmettre la pièce jointe (souvent "base64" pour les fichiers binaires).

Exemples de champs d'en-tête

```
From: john.doe@example.com
To: jane.smith@example.com
CC: manager@example.com
BCC: ceo@example.com
Subject: Réunion de projet
Date: Tue, 1 Jan 2024 10:00:00 +0000
Message-ID: <unique-message-id@example.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="boundary-string"
```

Exemple de corps en texte brut :

```
--boundary-string
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 7bit

Bonjour Jane,

Nous avons une réunion de projet prévue pour demain à 10h. Merci de préparer les documents nécessaires.

Cordialement,
John
```

Exemple de corps en HTML :

```
--boundary-string
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 7bit

<html>
<body>
<p>Bonjour Jane,</p>
<p>Nous avons une réunion de projet prévue pour demain à 10h. Merci de préparer les documents
nécessaires.</p>
<p>Cordialement,<br>John</p>
</body>
</html>
```

Exemple avec pièce jointe :

```
--boundary-string
Content-Type: multipart/mixed; boundary="mixed-boundary-string"

--mixed-boundary-string
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 7bit

Bonjour Jane,
Veuillez trouver ci-joint les documents pour la réunion de projet.
Cordialement,
John

--mixed-boundary-string
Content-Type: application/pdf; name="document.pdf"
Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename="document.pdf"

JVBERi0xLjQKJdP0zOEKMSAwIG9iago8PC9UeXBIL1BhZ2ZUvUGFyZW50IDlgMCBSL1Jlc291cmNlcyA...
--mixed-boundary-string--
```


1. Encodage des messages

L'encodage des messages est essentiel pour s'assurer que les données sont correctement transmises et reçues, en particulier lorsque des caractères spéciaux, des contenus multimédias ou des pièces jointes sont inclus. Voici un aperçu des principales méthodes d'encodage utilisées pour les emails.

- Encodage des caractères (MIME, Base64, Quoted-Printable)

Pour transmettre des caractères spéciaux et des données binaires via email, il existe plusieurs méthodes d'encodage :

MIME (Multipurpose Internet Mail Extensions) :

- MIME permet de définir divers types de contenu dans les emails et de spécifier comment ces contenus doivent être encodés et décodés. Cela inclut le texte en différentes langues, les images, les vidéos, les fichiers audio, etc.
- MIME utilise des en-têtes pour décrire le type de contenu et l'encodage.

Par exemple :

```
Content-Type: text/plain; charset=UTF-8  
Content-Transfer-Encoding: 7bit
```

Base64 :

- Utilisé pour convertir des données binaires en texte ASCII. Couramment utilisé pour les pièces jointes comme les images et les fichiers PDF.
- Base64 convertit les données binaires en un format de texte lisible utilisant 64 caractères ASCII.

Exemple d'encodage Base64 :

```
Content-Transfer-Encoding: base64  
VGhpcyBpcyBhbiBlbmNvZGVkIHNoZy4=
```

Quoted-Printable :

- Utilisé pour encoder du texte contenant des caractères non-ASCII tout en restant lisible pour les humains. Efficace pour les textes avec peu de caractères spéciaux.
- Les caractères non-ASCII sont représentés par un signe égal (=) suivi du code hexadécimal du caractère.

Exemple d'encodage Quoted-Printable :

```
Content-Transfer-Encoding: quoted-printable  
Ceci est un texte =E9crit en Quoted-Printable.
```

- Encodage des pièces jointes

Les pièces jointes, qu'il s'agisse de documents, d'images, de fichiers audio ou vidéo, doivent être encodées pour être incluses dans les emails. Les méthodes courantes incluent :

Base64 :

- La méthode la plus courante pour encoder des pièces jointes binaires.
- Convertit les fichiers binaires en texte ASCII pour garantir une transmission sans corruption

Exemple de pièce jointe encodée en Base64 :

```
--boundary-string  
Content-Type: application/pdf; name="document.pdf"  
Content-Transfer-Encoding: base64  
Content-Disposition: attachment; filename="document.pdf"  
  
JVBERi0xLjQKJdP0zOEKMSAwIG9iago8PC9UeXBIL1BhZ2UvUGFyZW50IDlgMCBS...  
--boundary-string--
```

Quoted-Printable :

- Utilisé principalement pour des fichiers textuels où peu de caractères doivent être encodés. Moins efficace pour les fichiers binaires volumineux.

UUEncode :

- Une méthode plus ancienne et moins courante aujourd'hui.
- Transforme des fichiers binaires en texte ASCII.

Chapitre 2 : Attaques et Menaces dans les Services de Messagerie Électronique

-partie 1-

-Amine Lachegur-

I. Spam

1. Définition et concepts de base

Le spam, également connu sous le nom de courrier indésirable ou pourriel, se définit comme une communication électronique non sollicitée, principalement diffusée via le courrier électronique à des fins publicitaires. Cette pratique, qualifiée de technique de prospection par internet, consiste à envoyer massivement des informations publicitaires non désirées par les destinataires.

Au Maroc, la législation pertinente inclut la Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, qui régit ce phénomène. Un email est considéré comme du spam pour les boîtes de messagerie privées s'il est envoyé sans consentement préalable (opt-in). Toutefois, pour les adresses professionnelles, un email non sollicité n'est pas nécessairement du spam si son contenu est pertinent par rapport à la fonction du destinataire au sein de son organisation.

2. Impacts de spam

- **Surcharge des Boîtes de Réception :**

Les spams remplissent rapidement les boîtes de réception, rendant difficile pour les utilisateurs de trouver et de gérer les emails légitimes.

- **Perte de Productivité :**

Les employés passent beaucoup de temps à trier et supprimer les spams, ce qui réduit leur efficacité et leur productivité.

- **Consommation de Ressources :**

Les serveurs de messagerie et les réseaux peuvent être surchargés par le volume de spams, entraînant des ralentissements et des interruptions de service.

- **Risque de Sécurité :**

Certains spams peuvent contenir des liens malveillants ou des pièces jointes infectées, servant de vecteurs pour des logiciels malveillants.

3. Comment se protéger contre les spams ?

Se protéger contre le spam nécessite une combinaison de bonnes pratiques et l'utilisation de divers outils :

1. Utilisation de filtres anti-spam :

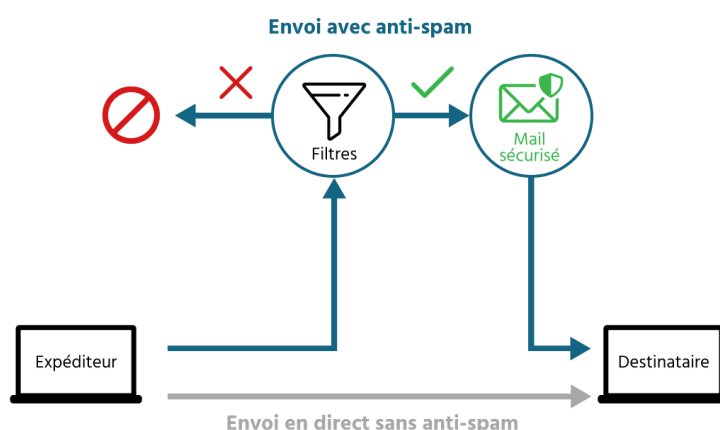
- **Configurer les filtres anti-spam :**

La plupart des services de messagerie offrent des filtres anti-spam intégrés qui détectent et déplacent les courriels indésirables dans un dossier dédié.

- **Mettre à jour régulièrement :**

Assurez-vous que ces filtres sont régulièrement mis à jour pour détecter les dernières techniques de spam

Fonctionnement d'un anti-spam



2. Bloquer et signaler :

- **Bloquer les expéditeurs :**

Utilisez les options de votre service de messagerie pour bloquer les expéditeurs indésirables.

- **Signaler le spam :**

Aidez les fournisseurs de services à améliorer leurs filtres en signalant les emails non sollicités comme spam.

3. Logiciels de sécurité :

- **Utiliser un logiciel antivirus :**

Certains logiciels antivirus offrent également des fonctionnalités anti-spam.

- **Mises à jour régulières :**

Maintenez tous les logiciels de sécurité à jour pour bénéficier des dernières protections.

4. Bonnes pratiques en ligne :

- **Ne pas répondre au spam :**

Répondre aux emails de spam peut confirmer à l'expéditeur que votre adresse est active.

- **Ne pas cliquer sur les liens :**

Évitez de cliquer sur des liens ou de télécharger des pièces jointes provenant d'emails suspects.

5. Réglementation et droits au Maroc :

- **Connaître ses droits :**

Informez-vous sur les lois marocaines concernant la protection contre le spam. Le Maroc a des réglementations visant à protéger les utilisateurs contre le spam, notamment à travers la Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

- **Utiliser des services de protection des consommateurs :**

En cas de spam persistant, il est possible de signaler les abus à des organismes compétents au Maroc, comme la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP).

III. Phishing

1. Définition et concepts de base

Le phishing, ou hameçonnage en français, est une technique malveillante qui consiste à envoyer des emails conçus pour tromper les utilisateurs et leur soutirer des informations sensibles. Ces informations peuvent inclure des données financières, des identifiants de connexion, des numéros de carte de crédit ou d'autres données personnelles. Les escrocs utilisent des méthodes d'ingénierie sociale pour manipuler la psychologie humaine, comme la falsification, la désorientation et le mensonge, pour réussir leurs attaques.

En se faisant passer pour une source légitime et en utilisant des demandes attractives, les attaquants attirent les victimes dans un piège, similaire à un pêcheur utilisant un appât pour attraper un poisson. L'objectif est de voler des informations sensibles pour les utiliser ou les vendre.

2. Fonctionnement du phishing

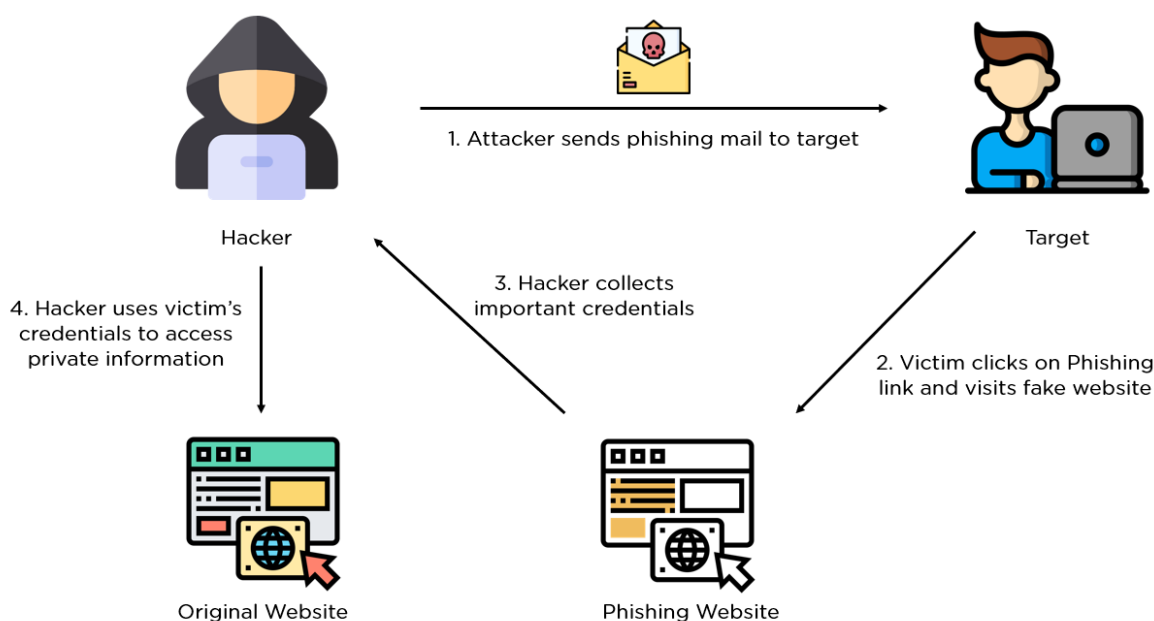
Toute campagne de phishing, qu'elle cible spécifiquement une personne ou soit diffusée à un grand nombre de victimes, débute toujours par l'envoi d'un email malveillant, déguisé en message provenant d'une entreprise légitime.

Plus ce message imite les caractéristiques de l'entreprise réelle, plus les chances de succès de l'attaquant augmentent. Les objectifs des hackers varient, mais ils visent généralement à dérober des informations personnelles ou des identifiants.

Pour ce faire, ils suscitent un sentiment d'urgence dans leurs messages, menaçant de suspendre des comptes, de perdre de l'argent ou de mettre en danger l'emploi de la victime. Les utilisateurs, pressés ou effrayés, ne prennent pas le temps de vérifier la plausibilité des demandes.

Ce n'est que plus tard qu'ils reconnaissent les signes d'alerte et les demandes irrationnelles. Évoluant constamment pour échapper aux mesures de sécurité et à la vigilance humaine, le phishing nécessite une formation continue des employés pour les armer contre les dernières techniques.

Une seule victime peut provoquer une grave violation de données, rendant le phishing l'une des menaces les plus critiques à maîtriser, car elle repose sur des défenses humaines.



3. Impacts de phishing

- **Vol d'Identité :**

Les attaques de phishing visent à obtenir des informations sensibles telles que des identifiants de connexion, des numéros de carte de crédit et d'autres données personnelles, pouvant être utilisées pour usurper l'identité des victimes.

- **Fraude Financière :**

Les informations obtenues par phishing peuvent être utilisées pour effectuer des transactions frauduleuses, vider des comptes bancaires et causer des pertes financières importantes.

- **Atteinte à la Réputation :**

Les entreprises victimes de phishing peuvent subir des dommages à leur réputation, perdant la confiance de leurs clients et partenaires.

- **Accès Non Autorisé :**

Les attaquants peuvent utiliser les informations obtenues pour accéder à des systèmes internes, voler des données sensibles et compromettre la sécurité de l'organisation.

4. Comment se protéger contre le phishing ?

Pour se protéger contre le phishing, il est important d'adopter une combinaison de bonnes pratiques et d'utiliser divers outils de sécurité :

1. Sensibilisation et formation :

- **Éduquez-vous et vos proches :**

Apprenez à reconnaître les signes courants de phishing, comme les emails qui demandent des informations personnelles ou financières, les messages urgents ou alarmants, et les liens suspects.

- **Participez à des formations :**

Si possible, suivez des formations en ligne ou en entreprise sur la sécurité informatique et la détection des tentatives de phishing.

2. Vérification des sources :

- **Vérifiez l'expéditeur :**

Avant de cliquer sur un lien ou de télécharger une pièce jointe, vérifiez que l'expéditeur est légitime en examinant attentivement l'adresse email et en recherchant des signes de falsification.

- **Ne cliquez pas sur les liens directement :**

Passez la souris sur les liens pour voir l'adresse URL réelle avant de cliquer. Si elle semble suspecte, ne cliquez pas dessus.

3. Logiciels de sécurité :

- **Installez un logiciel antivirus :**

Utilisez un logiciel antivirus fiable qui inclut une protection contre le phishing.

- **Activez les filtres anti-phishing :**

De nombreux navigateurs web et services de messagerie offrent des filtres anti-phishing qui peuvent bloquer les sites web frauduleux et les emails suspects.

4. Bonnes pratiques en ligne :

- **Mettez à jour vos logiciels :**

Vérifiez-vous que l'ensemble de vos systèmes d'exploitation, vos navigateurs et vos applications sont à jour, bien sûr avec les derniers correctifs de sécurité.

- **Utilisez les dernières versions des navigateurs :**

Les navigateurs modernes offrent des protections intégrées contre le phishing.

5. Utilisation de l'authentification à deux facteurs (2FA):

- **Activez 2FA :**

Pour vos comptes en ligne importants, activez l'authentification à deux facteurs, qui ajoute une couche de sécurité supplémentaire en demandant une deuxième forme d'identification.

V. Virus

1. Définition et concepts de base

Une attaque par virus en messagerie électronique désigne un type de cyberattaque où des programmes malveillants, souvent appelés virus, sont distribués via des emails. Ces virus sont conçus pour infecter les systèmes informatiques des destinataires lorsqu'ils ouvrent des pièces jointes infectées ou cliquent sur des liens dangereux inclus dans le corps du message.

L'objectif principal d'une attaque par virus est de compromettre la sécurité des données, d'endommager les systèmes informatiques ou de dérober des informations confidentielles. Les victimes peuvent être ciblées individuellement ou à grande échelle, faisant de la messagerie électronique un vecteur courant pour la propagation de logiciels malveillants.

2. Types de virus

Virus de fichier :

Infecte les fichiers exécutables (comme les .exe) et se propage lorsque le fichier infecté est exécuté, altérant ou corrompant des fichiers et programmes.

Macrovirus :

Écrit en langage de macro, souvent trouvé dans des fichiers de traitement de texte ou des feuilles de calcul (comme ceux de Microsoft Word ou Excel), et s'exécute lorsque le fichier infecté est ouvert.

Cheval de Troie (Trojan) :

Se présente comme un logiciel légitime pour tromper l'utilisateur et, une fois installé, exécute des actions malveillantes comme voler des données ou installer d'autres malwares.

Ver informatique (Worm) :

Programme autonome qui se propage à travers les réseaux en exploitant des vulnérabilités, causant des dommages en surchargeant les réseaux et les systèmes.

Ransomware :

Prend en otage les données d'un utilisateur en les chiffrant et demande une rançon pour les déchiffrer, paralysant potentiellement des entreprises en bloquant l'accès à leurs données critiques.

3. Impacts des virus

- **Dommages aux Systèmes Informatiques :**

Les virus peuvent endommager ou détruire des fichiers et des systèmes, rendant les ordinateurs inutilisables et entraînant des pertes de données.

- **Perte de Données :**

Les virus peuvent corrompre ou supprimer des fichiers importants, entraînant la perte de données critiques pour les individus et les entreprises.

- **Exfiltration de Données Sensibles :**

Certains virus sont conçus pour voler des informations sensibles, telles que des mots de passe, des documents financiers et d'autres données confidentielles.

- **Interruption des Activités :**

Les attaques de virus peuvent paralyser les opérations d'une entreprise en rendant les systèmes indisponibles, entraînant des pertes financières et opérationnelles.

- **Coûts de Réparation et de Récupération :**

La détection, la suppression des virus et la récupération des données perdues ou endommagées peuvent entraîner des coûts importants pour les individus et les entreprises.

4. Comment se protéger contre le phishing ?

Pour se protéger contre les attaques par virus en messagerie électronique, il est essentiel d'adopter plusieurs mesures de sécurité :

- **Méfiance face aux emails non sollicités :**

Soyez prudent lors de l'ouverture d'emails provenant d'expéditeurs inconnus ou suspects. Ne cliquez pas sur les liens ni n'ouvrez les pièces jointes à moins d'être certain de leur légitimité.

Vérification de l'expéditeur :

Assurez-vous que l'adresse email de l'expéditeur semble authentique et correspond à celle attendue. Méfiez-vous des adresses email qui semblent similaires à celles d'entreprises légitimes mais comportent des erreurs typographiques ou des domaines suspects.

Analyse des pièces jointes :

Avant d'ouvrir une pièce jointe, scannez-la avec un logiciel antivirus à jour pour détecter d'éventuels virus ou malware. Évitez d'ouvrir des fichiers exécutables (par exemple, avec les extensions .exe, .bat) à moins d'être certain de leur origine et de leur sécurité.

Prudence avec les liens inclus dans les emails :

Ne cliquez pas sur les liens présents dans les emails suspects ou non sollicités. Passez votre curseur sur le lien pour vérifier l'URL réelle avant de cliquer, et assurez-vous qu'elle correspond à celle attendue.

Utilisation de filtres anti-spam et anti-phishing :

Activez les filtres anti-spam dans votre client de messagerie pour bloquer les emails indésirables. De même, utilisez des outils anti-phishing qui peuvent détecter les tentatives d'hameçonnage et les emails malveillants.

Formation et sensibilisation :

Sensibilisez-vous et formez vos collaborateurs aux bonnes pratiques en matière de sécurité informatique, notamment en identifiant les signes d'emails suspects et en comprenant les techniques courantes utilisées par les attaquants.

Mises à jour régulières :

Maintenez votre logiciel de messagerie, votre système d'exploitation et votre antivirus à jour avec les derniers correctifs de sécurité pour protéger votre système contre les vulnérabilités connues.

Chapitre 2 : Attaques et Menaces dans les Services de Messagerie Électronique

-partie 2-

-Hamid Zakariaa-

IV. Des attaques avancées sur l'infrastructure email

Dans cette section, nous allons aborder des attaques peu connues. Avec un peu de recherche, on peut trouver que l'outil linux cURL peut négocier des sessions SMTP ce qui rend l'envoi des mails très facile ainsi que le mode "verbose" permet d'afficher toutes les commandes SMTP envoyées pour le débogage.

```
1 $ curl -v smtp://<recipient> --mail-from hamid@sender.com --mail-rcpt zakariaa@receiver.com --upload-file mail.txt
```

Envoyer un mail avec curl

Le fichier mail.txt doit avoir la forme suivante :

```
1 From: hamid@sender.com
2 To: zakariaa@receiver.com
3 Subject: test
4
5 Bonjour Zakariaa,
6
7 envoyé avec cURL
8
9 test,
10
11 Hamid
```

Format d'un mail

Il est important de souligner le fait qu'une nouvelle ligne doit être faite avec "\r\n" car les données sont envoyées sous forme brute.

Nmap est un autre outil intéressant pour évaluer la sécurité d'une infrastructure mail. Cet outil comprend plusieurs scripts pour auditer comme :

- **smtp-commands** : Exécute des commandes SMTP.
- **smtp-enum-users** : Enumère les utilisateurs SMTP.
- **smtp-brute** : Effectue une attaque brute force sur SMTP.
- **smtp-ntlm-info** : Récupère des informations NTLM SMTP.
- **smtp-open-relay** : Détecte les relais SMTP ouverts.
- **smtp-strangeport** : Identifie les ports SMTP inhabituels.

L'usage de nmap se fait comme-ci :

```
1 $ nmap -sSV -p 25,465,587 -script smtp-commands smtp.example.com
```

Usage de nmap pour scan smtp

1. Reconnaissance

Afin d'attaquer une infrastructure mail, on doit collecter des informations sur celle-ci afin de procéder à lancer plusieurs attaques :

- Détecter, identifier et contourner les passerelles de messagerie électronique
- Identifier les exploits fonctionnels contre les serveurs SMTP
- Avoir une idée globale du niveau de sécurité des emails
- Falsifier des emails de phishing convaincants

Parmi les informations de valeurs qu'on peut exploiter :

- Noms de domaine MX et adresses IP
- Logiciels et versions des serveurs SMTP
- Une liste d'adresses email valides
- Présence de chiffrement
- Type d'authentification SMTP
- Présence de défenses basées sur DNS ou liées à DNS : SPF, DKIM, DMARC, DANE, MTA-STS, etc.
- Présence de passerelles de sécurité (souvent déduites uniquement lors de l'envoi d'emails à un destinataire connu à l'intérieur de l'infrastructure cible)
- Présence de mécanismes de chiffrement de bout en bout

Les domaines MX peuvent être facilement récupérés à l'aide de la commande "dig" comme suit :

```
zoroark@zoroark:~$ dig +short mx inpt.ac.ma
20 mail2.inpt.ac.ma.
```

Domaine MX à partir de dig

D'autres commandes peuvent être lancées sur la cible comme :

```
zoroark@zoroark:~$ nc -Cv mail2.inpt.ac.ma 25
Connection to mail2.inpt.ac.ma (196.12.232.102) 25 port [tcp/smtp] succeeded!
220 mail2.inpt.ac.ma ESMTP Postfix
EHLO test
250-mail2.inpt.ac.ma
250-PIPELINING
250-SIZE 52428800
250-VERFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 XXXXXXXX
```

Netcat sur smtp

Donc on peut envoyer des commandes SMTP au serveur. On peut utiliser “openssl” si TLS est obligatoire.

Un scénario potentiel pour éviter l’usage de TLS est d’avoir Man-in-the-Middle est changer la commande STARTTLS par quelque chose afin de tromper la victime à ne pas utiliser TLS. Parfois le TLS est activé par le serveur mais pas en général.

2. Attaque sur S/MIME et OpenPGP

Dans un article de recherche, des chercheurs de Rhur University Bochum et Münster University of Applied Science, ont abordé une vulnérabilité pour forger les signatures des emails. L’article peut être consulté via <https://github.com/RUB-NDS/Johnny-You-Are-Fired/blob/master/paper/johnny-fired.pdf>

Juste parce qu’on utilise un chiffrement de bout en bout et un logiciel pour les signatures, cela ne veut pas dire qu’on est sécurisé.

Les chercheurs n’ont pas cassé les chiffrements utilisés, mais plutôt ils ont exploité la faiblesse au niveau de la vérification des signatures S/MIME et OpenPGP au niveau du client email. Ils ont défini 5 classes d’attaques :

- **CMS attacks:**

La Cryptographic Message Syntax (CMS) est une norme polyvalente pour les messages signés et chiffrés dans l’infrastructure à clé publique X.509. Nous avons trouvé des défauts dans le traitement des emails avec des structures de données contradictoires ou inhabituelles (telles que plusieurs signataires) et dans la présentation des problèmes dans la chaîne de confiance X.509.

- **GPG API attacks:**

GnuPG est la mise en œuvre OpenPGP la plus largement utilisée, mais elle offre seulement une interface en ligne de commande très restreinte pour la validation des signatures. Cette interface est vulnérable aux attaques par injection.

- **MIME attacks:**

Le corps d'un email est conceptuellement un arbre MIME, mais généralement l'arbre n'a qu'une seule feuille qui est signée. Nous construisons des arbres MIME non standard qui trompent les clients en affichant un texte non signé tout en vérifiant une signature non liée dans une autre partie.

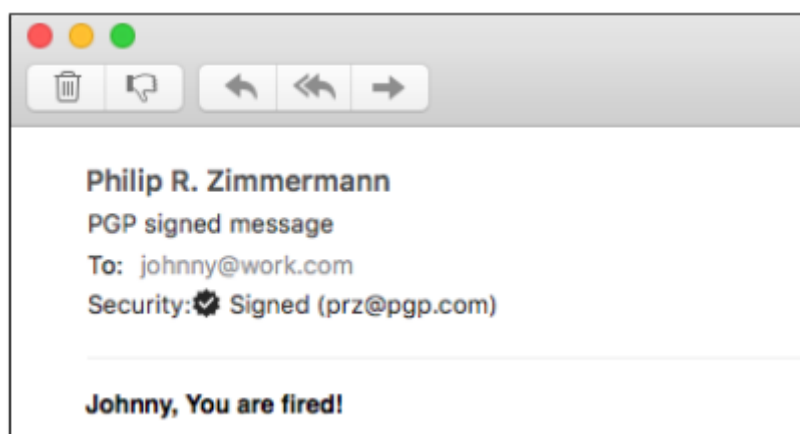
- **ID attacks:**

L'objectif de cette classe d'attaque est d'afficher une signature valide à partir de l'identité (ID) d'un partenaire de communication de confiance situé dans l'en-tête du courrier, bien que l'email manipulé soit en réalité signé par l'attaquant.

- **UI attacks:**

Les clients de messagerie indiquent une signature valide en affichant certains indicateurs de sécurité dans l'interface utilisateur (UI), par exemple, une lettre avec un sceau. Cependant, plusieurs clients permettent l'imitation d'éléments d'UI importants en utilisant HTML, CSS et d'autres contenus intégrés.

La figure suivante est extraite de l'article précédent :



Mail signé par exploitation de l'arbre MIME

3. SPF : Allow by default

L'idée est d'exploiter les serveurs SMTP avec une directive SPF qui n'est pas bien configurée.

Imaginons que l'organisation propriétaire de victim.com ait un enregistrement SPF défini comme suit :

```
$ dig +short txt victim.com | grep spf
```

```
"v=spf1 mx ipv4:1.2.3.4/30 +all"
```

Remarquez-le +all, indiquant que le comportement par défaut pour les adresses IP ne correspondant pas aux conditions SPF précédentes est une autorisation, permettant à l'ensemble de la plage d'adresses IP d'Internet d'envoyer des courriers utilisant le nom de domaine victim.com. C'est une sorte de politique SPF "autoriser par défaut". Nous pouvons envoyer un courrier en tant que ceo@victim.com depuis un serveur illégitime contrôlé par nous vers une boîte aux lettres test jeff@test-mailbox.com également contrôlée par nous pour exploiter la technique :

```
$ curl smtp://qlq-chose.com --mail-from 'abcd@example.com' --mail-rcpt hamid.zakariaa@qlq-chose.com' --upload-file mail.txt"
```

La forme du fichier mail.txt est la même que celle de la première partie.

Il y a tout un article un article par un chercheur qui s'appelle Sebastian Salla sur ce type d'attaque : <https://caniphish.com/phishing-resources/blog/scanning-spf-records>

Cette configuration de la directive all est dangereuse et peut sembler rare, mais dans son article, Salla a constaté qu'elle n'était pas si rare que ça. Que la cause soit une mauvaise configuration ou un acte volontaire des propriétaires de domaines vulnérables est cependant impossible à déterminer. La solution consiste à remplacer le +all du record SPF par -all. La politique SPF passe alors de "autoriser par défaut" à "interdire par défaut". Je ne suis pas favorable à l'option softfail ~all et je ne recommande pas son utilisation.

Salla a indiqué dans son article que plusieurs organisations importantes sont vulnérables à ce type d'attaques:

1	DomainName	Organisation	Code	Title	Severity
46	REDACTED.law REDACTED.edu	REDACTED Law School - REDACTED University	3	SPF "+all" mechanism set	Severe
94	cttso.gov	Combating Terrorism Technical Support Office (USA)	3	SPF "+all" mechanism set	Severe
305	mil.gov.ua	Ministry of Defense (Ukraine)	3	SPF "+all" mechanism set	Severe
389	li. REDACTED .it.edu	REDACTED Institute of Technology	3	SPF "+all" mechanism set	Severe
748	mpwt.gov.kh	Ministry of Public Works (Cambodia)	3	SPF "+all" mechanism set	Severe
868	civilservice.gov.uk	Civil Service (United Kingdom)	3	SPF "+all" mechanism set	Severe
903	justice.gov.lb	Ministry of Justice (Lebanon)	3	SPF "+all" mechanism set	Severe
986	com.miami.edu	School of Communication - University of Miami	3	SPF "+all" mechanism set	Severe
1103	rcfl.gov	Regional Computer Forensics Laboratory (USA)	3	SPF "+all" mechanism set	Severe

Des organisations .gov sont vulnérables à l'attaque SPF allow by default

4. Attacking third-parties in "include":

SPF dispose d'un mécanisme pour déléguer la vérification à d'autres domaines à travers la directive "include". Lorsqu'un destinataire rencontre cette directive, il effectue une évaluation récursive de son contenu et renvoie le résultat à l'évaluation SPF de niveau supérieur.

L'idée de l'attaque est d'exploiter les directives "include" SPF définies sur des domaines tiers vulnérables. En effet, il est important de faire attention aux domaines étrangers publiés dans une directive "include" de votre enregistrement SPF, car cela délègue essentiellement le résultat SPF à ceux-ci :

Si vous avez une organisation avec un enregistrement SPF publié comme suit :

```
$ dig +short txt victim.org | grep spf
```

```
"v=spf1 mx include:thirdparty.com -all"
```

Où thirdparty.com est un fournisseur de services de messagerie. Ensuite, le récepteur interrogera le SPF de thirdparty.com en raison de la directive "include" :

```
$ dig +short txt thirdparty.com | grep spf
```

```
"v=spf1 ipv4:203.0.0.0/8 +all"
```

La plage 203.0.0.0/8 est assez large et cela devrait déjà paraître suspect à vos yeux. Cela signifie que tout serveur avec une adresse IP dans cette plage envoyant un email passera SPF pour thirdparty.com et donc victim.org. Maintenant, imaginez que thirdparty.com propose également des services d'hébergement, tels que des serveurs privés virtuels (VPS), et que les serveurs loués dans leur infrastructure obtiennent une adresse IP publique à l'intérieur de la plage IP 203.0.0.0/8. N'importe qui peut louer un serveur chez thirdparty.com, ce qui signifie que n'importe qui peut se faire passer pour victim.org.

Afin de protéger contre ce type d'attaques :

- Vérifiez régulièrement les directives "include" SPF pour vous assurer qu'elles sont définies sur des tiers de confiance et que ceux-ci n'incluent pas de larges plages d'adresses IP englobant des hôtes non administrés par eux.
- Ne pas inclure de larges plages d'adresses IP dans vos enregistrements SPF.

5. Forger des signatures DKIM

Une méthode assez rusée pour accéder à la boîte aux lettres d'une cible est de signer des emails avec des noms de domaine qui ne sont pas ceux de l'expéditeur. Les filtres anti-spam faibles vérifient simplement si un email est signé, peu importe le domaine utilisé. Il est donc possible d'envoyer un email à destinataire@exemple.com tout en signant avec un domaine de attacker.com et de contourner ainsi les défenses.

On peut générer une clé privée d'une signature DKIM avec :

```
$ openssl genrsa -out dkim_private.pem 2048
```

Puis récupérer la clé publique correspondante :

```
$ openssl rsa -in dkim_private.pem -pubout -outform der 2>/dev/null | openssl base64 -A Ayw[...]zkWA
```

6. DMARC : loose policy and subpolicy :

Une attaque de base contre les politiques DMARC consiste à exploiter les directives de politique et de sous-politique (p= et sp=) qui ont une valeur lâche de none. Rencontrer des politiques telles que celles-ci :

```
$ dig +short txt _dmarc.victimtime.com
```

```
"v=DMARC1; p=none; sp=none; rua=mailto:dmarc.report@victimtime.com"
```

Est un bon indicateur que les emails pour le domaine exemple.com peuvent être falsifiés. Essayons en envoyant un email simple en utilisant un serveur contrôlé :

```
$ curl smtp://test-boitemail.com --mail-from 'pdg@victime.com' --mail-rcpt 'jeff@test-boitemail.com' --upload-file mail.txt
```

7. DMARC : Poor sampling percentage

Si nous considérons maintenant la politique DMARC suivante :

```
$ dig +short txt _dmarc.victime.com  
"v=DMARC1; p=reject; sp=reject; rua=mailto:dmarc.report@victim.com pct=10"
```

Nous voyons que p=reject et sp=reject constituent un obstacle pour utiliser la technique d'attaque DMARC précédente qui était moins stricte. Cependant, le pct=10 nous sera utile.

Cela indique le pourcentage d'échantillonnage des emails sur lesquels la politique DMARC est appliquée, soit 10 %. En d'autres termes, si une adresse email pour le domaine victime.com est usurpée, il y a 90 % de chances qu'elle ne soit pas rejetée en raison de DMARC.

8. Conclusion

La plupart des attaques qui peuvent avoir lieu sont causées par des erreurs de configuration et pas plus. Même si on implémente le meilleur chiffrement, on reste vulnérable car ce sont d'autres humains qui font la configuration. Voici quelques pratiques pour renforcer sa défense :

Chiffrement partout

Le déploiement du chiffrement est nécessaire pour prévenir les scénarios décrits dans la section des mécanismes de sécurité des emails. Partout où cela est possible, un niveau de chiffrement devrait être imposé et non seulement activé de manière opportuniste.

Interdiction par défaut

En règle générale, tout ce qui peut être configuré sous forme de liste d'instructions devrait toujours être utilisé avec une approche "interdiction par défaut". Cela signifie que, sauf autorisation explicite, les serveurs de sécurité des emails et les expéditeurs pour un domaine donné doivent être bloqués et les politiques des mécanismes de protection des emails doivent être restrictives

Audits réguliers

Les défenses mises en place doivent être régulièrement auditées pour s'assurer qu'elles respectent la politique de sécurité choisie. Voici quelques exemples de choses à auditer :

- **Les communications par email pour s'assurer qu'elles sont chiffrées.**
- **Les enregistrements DNS SPF pour les directives "include" supplémentaires au fil du temps, en veillant à ce qu'aucune d'entre elles ne pointe vers des enregistrements de tiers risqués.**
- **Les clés DKIM doivent être régulièrement changées, de même que les enregistrements DNS DKIM associés.**
- **Les enregistrements DNS des serveurs MX ne doivent pas pointer vers des adresses IP utilisées.**
- **Les enregistrements DNS CNAME de la zone ne doivent pas pointer vers des domaines inutilisés, car cela permettrait des prises de contrôle de sous-domaines.**

Chapitre 3 : Les techniques et les outils de sécurité des services

-partie 1-

-Abdelghafour Bouhdyd-

I. DKIM (DomainKeys Identified Mail)

1. Définition

DKIM (DomainKeys Identified Mail) est une norme d'authentification des emails par leur domaine expéditeur. Grâce à la cryptographie asymétrique, il permet de signer un message afin de garantir son intégrité de l'expéditeur au destinataire. Comme DomainKey, DKIM précise comment signer les messages en utilisant un chiffrement asymétrique, en publiant les clés publiques via le DNS et en confiant le processus de signature aux serveurs de messagerie. La différence entre DomainKey et DKIM est que le signataire peut être distinct de l'auteur et de l'expéditeur, le champ de signature est autosigné et la signature peut inclure une durée de validité. DomainKey a été abandonné par Yahoo au profit de DKIM, qui est devenu un standard.

La signature cryptographique DKIM permet d'authentifier le nom de domaine de l'expéditeur d'un email. Les signatures des messages assurent aux serveurs destinataires que l'expéditeur est bien associé à l'organisme émetteur et que le message n'a pas été modifié durant son transit.

2. Les principaux éléments de DKIM

Signature : Lorsqu'un email est envoyé, le serveur de messagerie de l'expéditeur signe l'email avec une clé privée unique. Cette signature est ajoutée aux en-têtes de l'email.

DNS et clé publique : Le domaine de l'expéditeur publie une clé publique dans son DNS. Cette clé publique correspond à la clé privée utilisée pour signer les emails.

Vérification : Lorsque le destinataire reçoit l'email, son serveur de messagerie utilise la clé publique (disponible dans le DNS de l'expéditeur) pour vérifier la signature. Si la signature correspond, cela signifie que l'email n'a pas été altéré et qu'il provient bien du domaine annoncé.

Intégrité et Authenticité : Grâce à ce mécanisme, DKIM assure que l'email n'a pas été modifié après avoir été signé et qu'il est bien envoyé par le domaine qu'il prétend représenter.

3. Fonctionnement DKIM

Avant de comprendre le fonctionnement de DKIM, il est essentiel de se familiariser avec le concept des deux clés DKIM. Il s'agit d'une clé publique publiée dans le DNS, qui aide le serveur récepteur à vérifier un email, et d'une clé privée utilisée par votre serveur de messagerie pour le processus d'authentification.

Tous les processus DKIM se déroulent en interne, au sein des serveurs de messagerie.

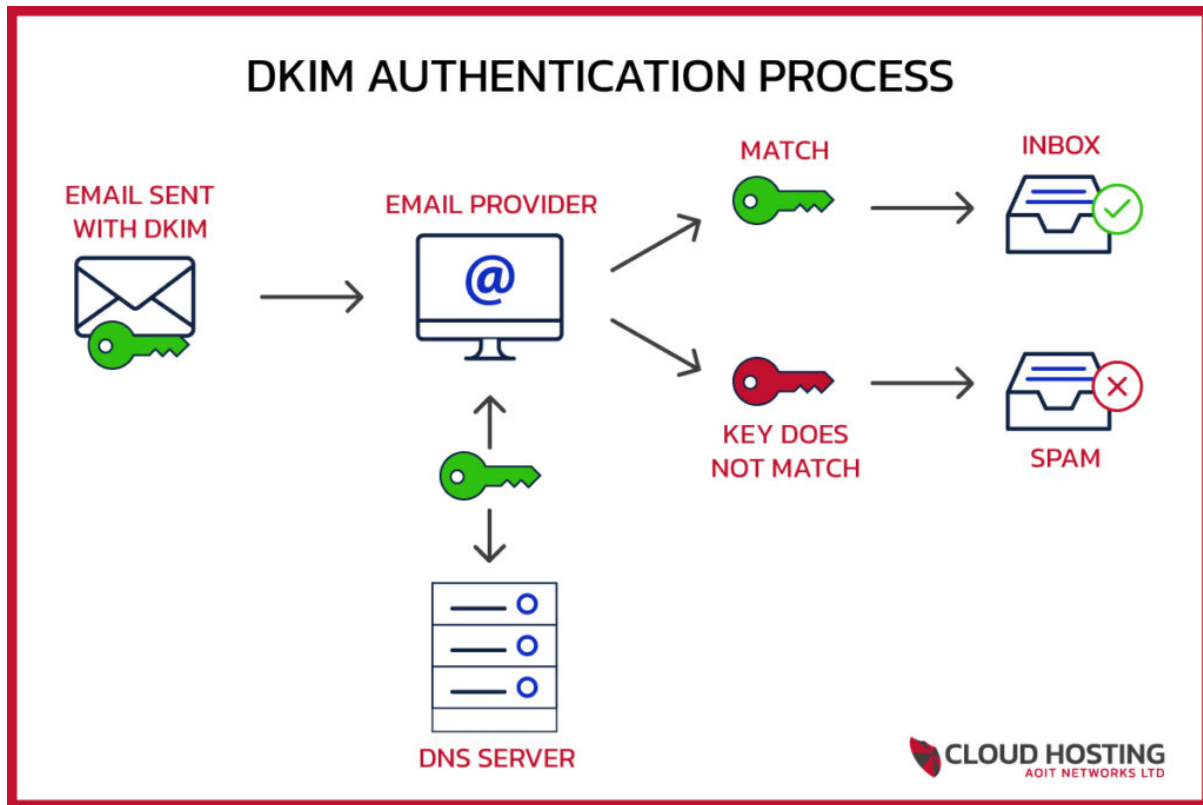
Par exemple, lorsque vous envoyez un email via test@example.com, le serveur de messagerie génère un en-tête de signature DKIM en utilisant une clé privée avant d'envoyer le message.

Le système de messagerie vérifie ensuite la signature DKIM pour s'assurer qu'elle correspond aux informations de l'expéditeur.

Lorsque le message est reçu, le serveur de messagerie récepteur obtient l'enregistrement DKIM à partir du DNS de example.com. Le serveur utilise ensuite la clé publique de l'enregistrement DNS pour vérifier la signature DKIM du message.

Si la clé publique DKIM correspond aux informations de la signature, l'authenticité du message est confirmée et il est placé dans la boîte de réception. Cela prouve que le message n'a pas été modifié en transit.

Si la clé DKIM ne correspond pas aux informations, le message sera probablement dirigé vers le dossier des spams ou des courriers indésirables.



Fonctionnement DKIM

4. Implémentation DKIM

Implémenter DKIM (DomainKeys Identified Mail) pour votre domaine implique plusieurs étapes. Voici un guide pour vous aider à configurer DKIM sur votre serveur de messagerie :

a) Générer les Clés DKIM

- **Clé Privée** : Utilisée par votre serveur de messagerie pour signer les emails.
- **Clé Publique** : Publiée dans votre DNS pour permettre aux serveurs récepteurs de vérifier les signatures des emails.

b) Ajouter la Clé Publique au DNS

- Accédez à votre gestionnaire de DNS.
- Ajoutez un nouvel enregistrement TXT pour votre domaine.
- Le nom de l'enregistrement est généralement une combinaison d'un sélecteur (que vous définissez) et du domaine, par exemple : selector._domainkey.example.com.
- La valeur de l'enregistrement sera la clé publique générée.

c) Configurer votre Serveur de Messagerie pour Signer les Emails

- Configurez votre serveur de messagerie pour utiliser la clé privée pour signer les emails sortants.
- Les instructions varient en fonction du serveur de messagerie que vous utilisez (Postfix, Exim, Microsoft Exchange, etc.).

d) Tester la Configuration DKIM

- Envoyez un email de test à un service de vérification DKIM comme DKIM Core ou utilisez les outils intégrés de votre serveur de messagerie.
- Assurez-vous que la signature DKIM est valide et que les serveurs récepteurs peuvent vérifier les emails.

L'implémentation de DKIM implique la génération de clés cryptographiques, la configuration des enregistrements DNS, et l'ajustement de votre serveur de messagerie pour signer les emails. Suivre ces étapes aidera à assurer que vos emails sont correctement authentifiés et réduira le risque qu'ils soient marqués comme spam.

5. Les bonnes pratiques

a. Utiliser des Sélecteurs Uniques

- **Sélecteurs Uniques** : Utilisez des sélecteurs uniques pour chaque domaine ou sous-domaine. Cela permet de gérer plus facilement les clés et de les renouveler sans affecter les autres configurations.

b. Renouveler Régulièrement les Clés

- **Renouvellement Régulier** : Renouvelez régulièrement les clés DKIM pour améliorer la sécurité. Une clé compromise peut permettre à des attaquants de signer des emails frauduleux.

- **Plan de Rotation** : Mettez en place un plan de rotation des clés, en incluant des dates spécifiques pour générer de nouvelles clés et mettre à jour les enregistrements DNS.

c. Configurer les Enregistrements DNS Correctement

- **Enregistrement TXT** : Assurez-vous que l'enregistrement TXT pour la clé publique DKIM est correctement configuré et accessible.
- **Longueur de Clé Suffisante** : Utilisez des clés d'une longueur suffisante (au moins 1024 bits, mais de préférence 2048 bits) pour assurer une sécurité adéquate.

d. Utiliser des Protocoles de Sécurité Complémentaires

- **SPF (Sender Policy Framework)** : Configurez également SPF pour définir les serveurs autorisés à envoyer des emails pour votre domaine.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance)** : Implémentez DMARC pour indiquer aux serveurs récepteurs comment gérer les emails échouant les vérifications DKIM et SPF.

e Tester la Configuration

- **Outils de Test** : Utilisez des outils de test DKIM comme DKIM Core ou des services en ligne pour vérifier que vos emails sont correctement signés et que les signatures sont valides.
- **Emails de Test** : Envoyez régulièrement des emails de test pour vérifier la validité des signatures DKIM et assurer que les configurations sont à jour.

f. Configurer les Serveurs de Messagerie Correctement

- **Serveurs internes et externes** : Configurez tous les serveurs de messagerie internes et externes pour signer les emails sortants et vérifier les signatures des emails entrants.
- **En-Têtes et Signatures** : Assurez-vous que les en-têtes et les signatures ne sont pas modifiés par des systèmes intermédiaires, ce qui pourrait invalider la signature DKIM.

g. Maintenir une Documentation à Jour

- **Documentation** : Maintenez une documentation détaillée de la configuration DKIM, des sélecteurs utilisés, des clés générées, et des procédures de rotation des clés.
- **Procédures de Sauvegarde** : Documentez les procédures de sauvegarde et de récupération des clés DKIM pour éviter toute interruption en cas de perte de données.

h. Formation et Sensibilisation

- **Formation du Personnel** : Formez le personnel technique sur l'importance de DKIM, la gestion des clés, et les meilleures pratiques en matière de sécurité des emails.
- **Sensibilisation à la Sécurité** : Sensibilisez l'ensemble du personnel à l'importance de la sécurité des emails et aux mesures à prendre pour éviter le phishing et les emails frauduleux.

i. Utiliser des Clés Différentes pour Différents Services

- **Clés Spécifiques aux Services** : Utilisez des clés différentes pour les différents services (ex. marketing, support) afin de mieux gérer les autorisations et la sécurité.

II. SPF (Sender Policy Framework)

1. Définition

Le SPF (Sender Policy Framework) est un protocole utilisé pour prévenir le spoofing d'adresses email en permettant aux domaines de spécifier quels serveurs de messagerie sont autorisés à envoyer des emails en leur nom. Cela aide à réduire les risques de recevoir des emails frauduleux qui semblent provenir de sources légitimes.

2. Le fonctionnement de SPF

Au cœur du Sender Policy Framework (SPF) se trouve un processus technique simple : une méthode permettant aux serveurs de messagerie de vérifier qu'un hôte autorisé par les administrateurs de ce domaine est à l'origine de l'email entrant.

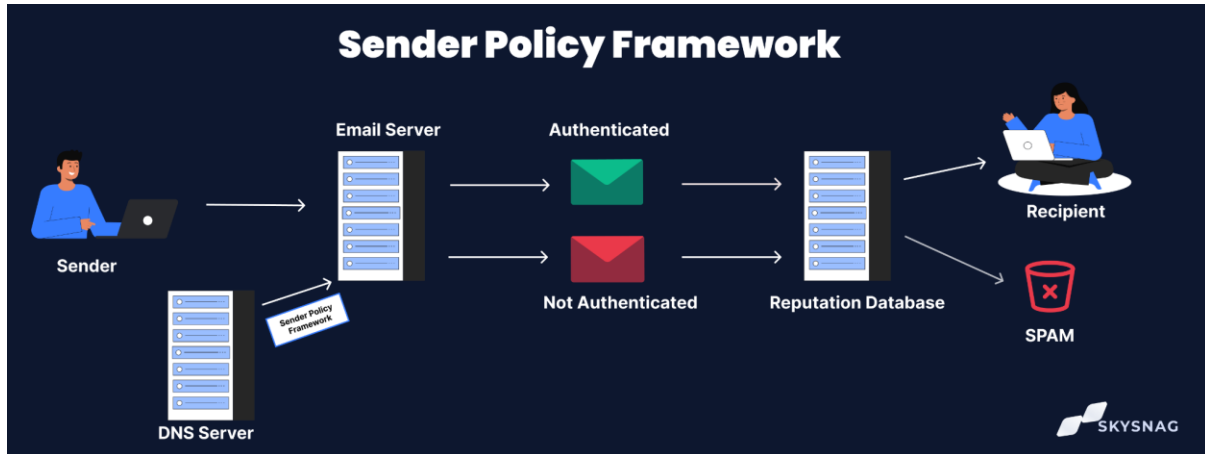
Les enregistrements DNS répertorient les hôtes d'envoi autorisés et les adresses IP d'un domaine.

Lorsqu'un email est reçu, le protocole SPF permet au serveur de réception de vérifier que le propriétaire du domaine a autorisé l'email prétendant provenir de ce domaine spécifique. Une fois vérifié, l'email est accepté.

En cas d'échec, l'email est considéré comme usurpé et est généralement marqué comme spam ou rejeté.

Bien que le SPF puisse améliorer efficacement la sécurité des emails d'une organisation, il n'est pas suffisant à lui seul.

Il doit faire partie d'une approche de sécurité des emails en plusieurs couches, combinant d'autres techniques telles que DKIM (Domain Keys Identified Mail) et DMARC (Domain-based Message Authentication, Reporting & Conformance).



Fonctionnement SPF

3. Les composants de SPF

Les composants principaux d'un enregistrement SPF comprennent différents mécanismes et modificateurs qui définissent quelles adresses IP et quels domaines sont autorisés à envoyer des emails pour un domaine spécifique. Voici une explication détaillée des composants d'un enregistrement SPF :

1. Version SPF

v=spf1 : Indique la version du SPF utilisée. Actuellement, c'est toujours "v=spf1".

2. Mécanismes (Méthodes d'Authentification)

Les mécanismes spécifient les règles pour déterminer si une adresse IP est autorisée à envoyer des emails pour le domaine spécifié. Les principaux mécanismes sont :

- **ip4 : 192.0.2.0/24** : Autorise les adresses IPv4 dans la plage spécifiée (par exemple, 192.0.2.0 à 192.0.2.255).
- **ip6 : 2001:db8::/32** : Autorise les adresses IPv6 dans la plage spécifiée.
- **a** : Autorise les adresses IP associées aux enregistrements A du domaine.
- **mx** : Autorise les adresses IP des serveurs de messagerie (MX records) du domaine.
- **Include : spf.example.com** : Inclut les mécanismes SPF du domaine _spf.example.com.

- **ptr** : Déprécié et pas recommandé pour des raisons de sécurité.
- **exists**
.com : Autorise une adresse IP si un enregistrement spécifique (par exemple, un A ou AAAA record) existe pour le domaine example.com.

3. Modificateurs (Actions à Prendre)

Les modificateurs définissent ce qu'il faut faire si une adresse IP ne correspond pas aux mécanismes autorisés :

- **+** (**Pass**) : L'adresse IP est autorisée à envoyer des emails au nom du domaine. Exemple : +ip4:192.0.2.0/24.
- **-** (**Fail**) : L'adresse IP n'est pas autorisée à envoyer des emails au nom du domaine. Exemple : -all.
- **~** (**SoftFail**) : L'adresse IP n'est pas autorisée, mais l'email peut être accepté avec un avertissement. Exemple : ~all.
- **?** (**Neutral**) : Aucune indication claire sur l'autorisation de l'adresse IP. Exemple : ?all.

Exemple d'Enregistrement SPF Complet

```
v=spf1 ip4:192.0.2.0/24 ip6:2001:db8::/32 a mx include:_spf.example.com -all
```

v=spf1 : Version SPF utilisée.

ip4:192.0.2.0/24 : Autorise les adresses IPv4 de la plage 192.0.2.0/24.

ip6:2001:db8::/32 : Autorise les adresses IPv6 de la plage 2001:db8::/32.

a : Autorise les adresses IP associées aux enregistrements A du domaine.

mx : Autorise les adresses IP des serveurs de messagerie (MX records) du domaine.

include:_spf.example.com : Inclut les mécanismes SPF du domaine _spf.example.com.

-all : Rejette tous les emails qui ne correspondent à aucun des mécanismes autorisés.

Lorsqu'un serveur de messagerie reçoit un email, il vérifie l'enregistrement SPF du domaine de l'expéditeur pour voir si l'adresse IP de l'expéditeur est autorisée à envoyer des emails pour ce domaine. En fonction des mécanismes et modificateurs spécifiés, le serveur de réception prendra une décision sur la manière de traiter l'email (accepter, rejeter, marquer comme suspect).

En utilisant SPF, les organisations peuvent renforcer la sécurité de leurs emails en réduisant le risque de spoofing et en aidant à identifier les emails légitimes. Cependant, SPF seul n'est pas suffisant et doit être combiné avec d'autres techniques comme DKIM et DMARC pour une protection complète contre les abus d'emails.

4. Implémentation SPF

L'implémentation du Sender Policy Framework (SPF) pour un domaine implique plusieurs étapes clés, principalement basées sur la modification et la configuration des enregistrements DNS du domaine concerné. Voici un guide étape par étape pour mettre en œuvre SPF :

a. Définir les Règles SPF

Avant de commencer l'implémentation, déterminez quelles adresses IP et quels serveurs sont autorisés à envoyer des emails pour votre domaine. Cela peut inclure les serveurs de messagerie de votre domaine, les services de marketing par email que vous utilisez, ou d'autres tiers de confiance.

b. Créer l'Enregistrement SPF

Une fois les règles SPF définies, créez l'enregistrement SPF approprié pour votre domaine. Voici comment créer un enregistrement SPF :

- Ouvrez un éditeur de texte ou utilisez l'interface de gestion DNS de votre fournisseur de domaine.
- Écrivez l'enregistrement SPF en commençant par la version (v=spf1) et en spécifiant les mécanismes et les modificateurs selon vos besoins.

Exemple d'enregistrement SPF basique :

makefile

Copier le code

```
v=spf1 include:_spf.example.com -all
```

Cet exemple inclut tous les mécanismes SPF définis dans `_spf.example.com` et rejette (-all) tout autre serveur d'envoi qui ne correspond pas aux règles définies.

c. Ajouter l'Enregistrement SPF dans le DNS

Une fois que vous avez créé l'enregistrement SPF, ajoutez-le à votre DNS en suivant ces étapes :

- Connectez-vous à votre compte de gestion DNS avec votre fournisseur de domaine.
- Trouvez la section où vous pouvez ajouter ou modifier des enregistrements DNS.
- Ajoutez un nouvel enregistrement de type TXT avec le contenu de votre enregistrement SPF.

Assurez-vous de respecter la syntaxe SPF et de ne pas introduire d'erreurs de format lors de l'ajout de l'enregistrement TXT dans votre DNS.

d. Vérifier l'Enregistrement SPF

Après avoir ajouté l'enregistrement SPF dans le DNS, vérifiez sa validité à l'aide d'outils en ligne tels que les validateurs SPF ou en envoyant des emails de test et en vérifiant les résultats SPF dans les en-têtes des emails.

e. Configuration et Surveillance

Une fois l'implémentation SPF terminée, configurez votre serveur de messagerie pour utiliser SPF dans le processus d'authentification des emails entrants. Surveillez régulièrement les journaux SPF pour détecter tout problème potentiel ou toute tentative d'usurpation d'identité par email.

f. Compléter avec DKIM et DMARC

Bien que SPF aide à vérifier l'authenticité de l'adresse IP de l'expéditeur, il est recommandé de compléter votre stratégie de sécurité des emails avec DKIM et DMARC pour une protection plus robuste contre le phishing et le spoofing.

En résumé, l'implémentation SPF nécessite de définir les règles SPF appropriées, de créer et d'ajouter l'enregistrement SPF dans votre DNS, de vérifier sa configuration et de surveiller son efficacité. Cela contribue à renforcer la sécurité des emails sortants de votre domaine en réduisant les risques de spoofing et de phishing.

III. DMARC

1. Définition

DMARC (Domain-based Message Authentication, Reporting & Conformance) est un protocole d'authentification des emails conçu pour donner aux propriétaires de domaine la possibilité de protéger leur domaine contre l'utilisation non autorisée, souvent appelée usurpation d'identité ou phishing. DMARC s'appuie sur deux autres mécanismes d'authentification des emails, SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail), et ajoute un mécanisme de reporting qui permet aux administrateurs de domaine de recevoir des rapports sur l'activité de messagerie utilisant leur domaine.

2. Fonctionnement

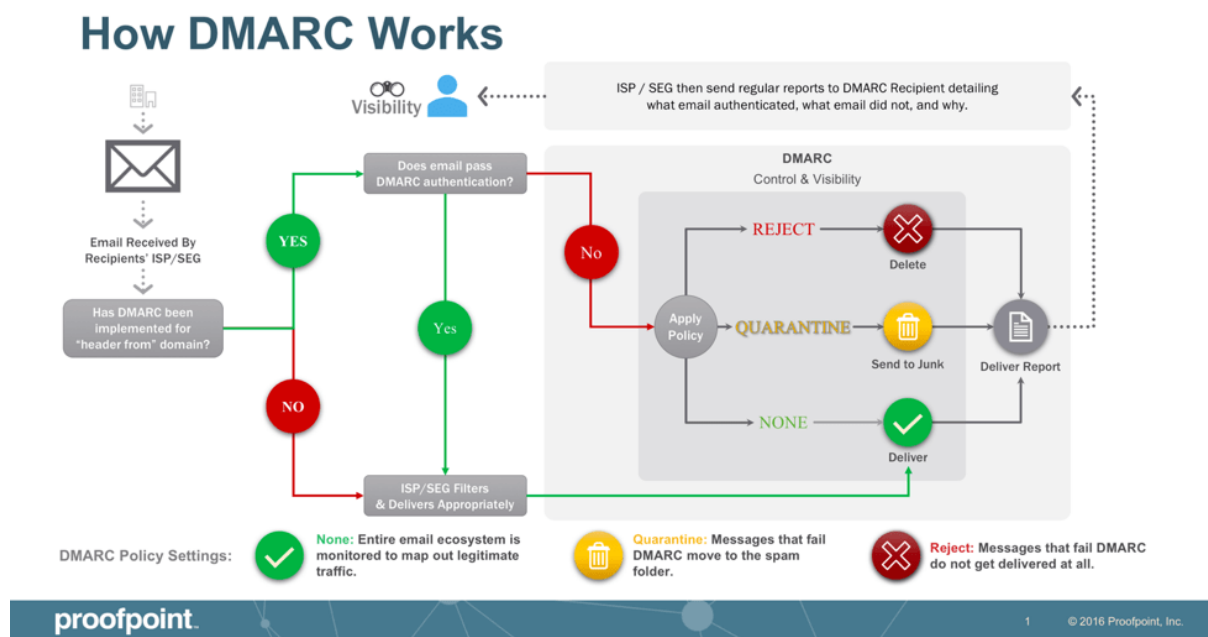
Pour qu'un message passe l'authentification DMARC, il doit réussir l'authentification SPF et l'alignement SPF et/ou réussir l'authentification DKIM et l'alignement DKIM.

Si un message échoue à l'authentification DMARC, les expéditeurs peuvent indiquer aux destinataires comment traiter ce message via une politique DMARC. Le propriétaire du domaine peut choisir parmi trois politiques : aucune (le message est remis au destinataire et un rapport DMARC est envoyé au propriétaire du domaine), quarantaine (le message est déplacé dans un dossier de quarantaine), et rejet (le message n'est pas du tout remis).

La politique DMARC "none" est une bonne étape initiale. Elle permet au propriétaire du domaine de s'assurer que tous les emails légitimes s'authentifient correctement. Le propriétaire reçoit des rapports DMARC qui l'aident à vérifier que tous les emails légitimes sont identifiés et passent l'authentification.

Une fois que le propriétaire du domaine est certain d'avoir identifié tous les expéditeurs légitimes et résolu les problèmes d'authentification, il peut adopter une politique de "rejet" pour bloquer les attaques de phishing, les compromissions d'emails d'entreprise et autres fraudes par email.

En tant que destinataire de courrier électronique, une organisation peut s'assurer que sa passerelle de messagerie sécurisée applique la politique DMARC mise en œuvre par le propriétaire du domaine. Cela protégera les employés contre les menaces provenant des courriels entrants.



Fonctionnement DMARC

3. Implémentation

Étape 1 : Comprendre DMARC

Familiarisez-vous avec le protocole DMARC et son fonctionnement. DMARC s'appuie sur les méthodes d'authentification du courrier électronique existantes, telles que SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail).

Étape 2 : Évaluer votre infrastructure de messagerie

Évaluez votre infrastructure de courrier électronique actuelle pour déterminer si vous avez le contrôle des domaines d'envoi et si vous pouvez mettre en œuvre SPF et DKIM. Assurez-vous d'avoir accès aux enregistrements DNS (Domain Name System) pour votre domaine.

Étape 3 : Configurer SPF ou DKIM ou les deux

Mettez en œuvre SPF et/ou DKIM pour votre domaine. SPF définit les serveurs de messagerie autorisés à envoyer des courriels au nom de votre domaine, tandis que la norme DKIM ajoute une signature numérique aux en-têtes des courriels, vérifiant ainsi leur authenticité.

Étape 4 : Créer un enregistrement DMARC

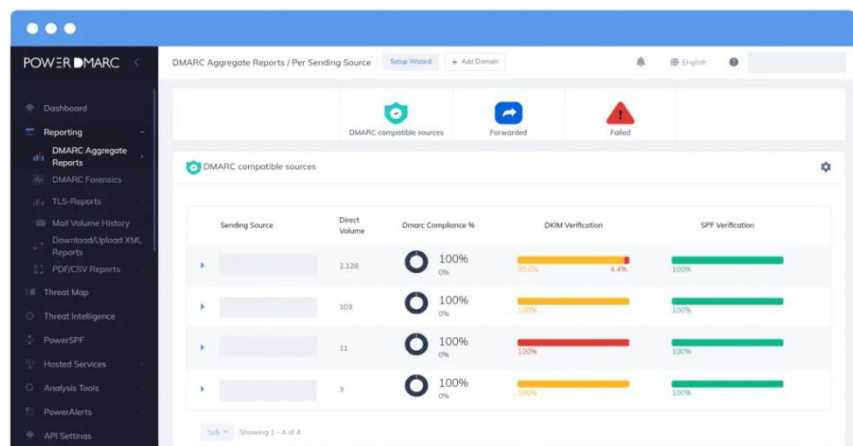
Étape 5 : Définir votre politique DMARC

Dans un premier temps, définissez votre politique sur "none" afin de collecter des données et de surveiller le trafic de courrier électronique sans affecter la distribution des messages. Une fois que vous avez examiné les rapports et que vous vous êtes assuré que les sources de courrier électronique légitimes sont alignées sur SPF et DKIM, appliquez progressivement une politique plus stricte, telle que la "quarantaine" ou le "rejet", afin de limiter les courriers électroniques non autorisés ou frauduleux.

Étape 6 : Analyser les rapports DMARC

- Recevoir et analyser les rapports : Configurez une boîte de réception pour recevoir les rapports DMARC. Utilisez des outils comme DMARCian, Agari, ou d'autres pour analyser les rapports et comprendre les sources des emails.
- Identifier les expéditeurs légitimes : Assurez-vous que tous les expéditeurs légitimes de votre domaine sont correctement configurés pour SPF et DKIM.

Contrôle des rapports DMARC :



IV. SPAM ASSASSIN

1. Définition

SpamAssassin est un filtre de messagerie destiné à identifier les spams. Il s'agit d'un filtre intelligent qui utilise une gamme variée de tests pour identifier les courriels en masse non sollicités, plus communément appelés spam. Ces tests sont appliqués aux en-têtes et au contenu des courriels pour les classer en utilisant des méthodes statistiques avancées. De plus, SpamAssassin possède une architecture modulaire qui permet d'utiliser rapidement d'autres technologies contre le spam et est conçu pour une intégration facile dans pratiquement n'importe quel système de messagerie.

2. Fonctionnement

SpamAssassin fonctionne en utilisant une combinaison de techniques pour analyser et attribuer un score à chaque courriel, afin de déterminer s'il s'agit de spam. Voici un aperçu de son fonctionnement :

- a. Analyse des en-têtes de courriel : SpamAssassin examine les en-têtes des courriels pour des indices de spam. Les en-têtes contiennent des informations sur l'expéditeur, le chemin parcouru par le message, et d'autres métadonnées.
- b. Analyse du contenu : Le contenu du courriel est analysé pour détecter des caractéristiques communes au spam. Cela peut inclure des mots-clés, des phrases typiques de spam, et des structures de message suspectes.
- c. Tests heuristiques : SpamAssassin utilise des règles heuristiques, basées sur l'expérience et les pratiques courantes de détection de spam, pour attribuer des points de score à différents aspects du message.
- d. Filtrage bayésien : Une méthode statistique qui utilise des modèles probabilistes pour estimer la probabilité qu'un message soit du spam en se basant sur l'analyse de messages précédemment classifiés.
- e. Listes noires (DNSBL) : SpamAssassin vérifie les adresses IP et les domaines de l'expéditeur contre des listes noires connues pour être des sources de spam.
- f. Listes blanches : À l'inverse des listes noires, les listes blanches contiennent des adresses ou des domaines réputés sûrs et fiables.

- g. Modules et plugins : SpamAssassin a une architecture modulaire, ce qui permet d'ajouter facilement des plugins et des modules pour utiliser des technologies supplémentaires ou des règles de filtrage spécifiques.
- h. Score combiné : Chaque test et vérification attribue un score au message. Les scores de tous les tests sont ensuite combinés pour obtenir un score total. Si ce score dépasse un certain seuil, le message est marqué comme spam.
- i. Actions automatisées : En fonction du score final, SpamAssassin peut marquer le message comme spam, le déplacer vers un dossier de courrier indésirable, le supprimer ou effectuer d'autres actions configurées par l'administrateur.

3. Custom rules

Les "custom rules" (règles personnalisées) dans SpamAssassin sont des règles définies par l'utilisateur ou l'administrateur pour adapter le filtrage du spam aux besoins spécifiques de leur environnement de messagerie. Ces règles personnalisées permettent d'ajouter, de modifier ou de supprimer des règles existantes pour mieux détecter les spams en fonction de critères spécifiques.

Pourquoi utiliser des règles personnalisées ?

- a. Adapter aux besoins spécifiques : Chaque environnement de messagerie est unique, avec différents types de courriels légitimes et de spam. Les règles personnalisées permettent d'adapter le filtrage pour mieux correspondre à ces particularités.
- b. Améliorer la précision : En ajoutant des règles spécifiques à certains types de spam que vous recevez fréquemment, vous pouvez améliorer la précision de la détection.
- c. Réagir rapidement aux nouvelles menaces : Les spams évoluent constamment. Les règles personnalisées permettent une réponse rapide aux nouvelles formes de spam avant qu'elles ne soient intégrées dans les mises à jour officielles de SpamAssassin.

Structure d'une règle :

Une règle dans SpamAssassin suit généralement une structure spécifique, qui comprend plusieurs éléments permettant de définir comment le logiciel doit traiter un courriel. Voici une explication des différentes parties d'une règle typique dans SpamAssassin :

1. Type de règle : La règle peut être de différents types, tels que "header", "body", "uri", etc., indiquant quelle partie du courriel elle examine. Par exemple, une règle "header" examine les en-têtes du courriel, tandis qu'une règle "body" recherche dans le corps du message.
2. Identifiant de la règle : Chaque règle est identifiée par un nom unique qui la distingue des autres règles. Cet identifiant est utilisé pour référencer la règle dans d'autres parties de la configuration ou des rapports.
3. Expression régulière : Une expression régulière est utilisée pour spécifier le motif que la règle recherche dans le contenu du courriel. Cette expression peut être simple ou complexe, et elle est souvent encadrée par des délimiteurs, tels que des barres obliques ("/") pour une expression régulière simple.
4. Score attribué : Chaque règle est associée à un score qui est attribué au courriel si la règle correspond au contenu du message. Ce score peut être positif ou négatif, et il peut être ajusté pour refléter l'importance de la règle dans la détection du spam.
5. Description : Une description est fournie pour expliquer la raison de la règle et ce qu'elle cherche à détecter. Cette description est utilisée à des fins de référence et de documentation, et elle peut être incluse dans les rapports de diagnostic pour aider à comprendre pourquoi un courriel a été marqué comme spam.

Exemple :

```
body      CUSTOM_DEMO_RULE    /example\.com/i
score     CUSTOM_DEMO_RULE    2.0
describe  CUSTOM_DEMO_RULE    "Email containing 'example.com' in the body"
```

- Type de règle : "body"
- Identifiant de la règle : "CUSTOM_DEMO_RULE"
- Expression régulière : "/example.com/i"
- Score attribué : 2.0

Le score nécessaire pour qu'un courriel soit classé comme spam est déterminé par un seuil prédéfini dans SpamAssassin, généralement appelé le "seuil de spam". Ce seuil est configuré par l'administrateur du système en fonction des besoins spécifiques de leur environnement de messagerie.

Le seuil de spam représente la limite au-delà de laquelle un courriel est considéré comme suffisamment probable pour être du spam. Si le score total d'un courriel, calculé en additionnant les scores attribués par chaque règle correspondante, dépasse ce seuil, le courriel est marqué comme spam.

Par exemple, si le seuil de spam est fixé à 5.0, tout courriel ayant un score total de 5.0 ou plus sera considéré comme spam par SpamAssassin. Ce seuil peut être ajusté en fonction des besoins de l'environnement de messagerie et des préférences de l'administrateur

Chapitre 3 : Les techniques et les outils de sécurité des services

-partie 2-

-Taha Safa-

I. Mxtoolbox

1. Définition

MXtoolbox est une plateforme en ligne qui propose des outils performants pour optimiser la sécurité de nos courriels et améliorer leur efficacité. Grâce à MXtoolbox, nous disposons de fonctionnalités avancées qui nous permettent de vérifier les enregistrements MX, de chercher la réputation des serveurs de messagerie, de tester les blacklists, de consulter les enregistrements DNS et bien d'autres encore. Ces outils ont été créés afin de nous assister dans la détection et la résolution des problèmes susceptibles de compromettre la confidentialité de nos courriels.



Comment peut-on utiliser MXtoolbox afin d'améliorer la sécurité de nos courriels ?

2. Utilisation de MXToolbox pour les Emails

Vérification du Serveur de Messagerie

SMTP Test : Utilisez l'outil SMTP Test pour vérifier la configuration de votre serveur de messagerie. Cet outil vous aide à identifier des problèmes courants tels que les erreurs de configuration, les listes noires et les problèmes de connectivité.

Accédez à MXToolbox SMTP Test.

Entrez l'adresse de votre serveur de messagerie et lancez le test.

Analysez les résultats pour corriger les problèmes identifiés.

Analyse des Enregistrements DNS

DNS Lookup : Assurez-vous que vos enregistrements DNS (MX, SPF, DKIM, DMARC) sont correctement configurés.

Allez sur MXToolbox DNS Lookup.

Entrez votre domaine et examinez les enregistrements DNS retournés.

Vérifiez que vos enregistrements MX pointent vers les bons serveurs de messagerie.

Confirmez que vos enregistrements SPF, DKIM et DMARC sont correctement configurés pour prévenir le spoofing et améliorer la délivrabilité.

Vérification des Listes Noires (Blacklist)

Blacklist Check : Vérifiez si votre serveur de messagerie ou votre domaine est répertorié sur des listes noires, ce qui peut affecter la délivrabilité de vos emails.

Accédez à MXToolbox Blacklist Check.

Entrez l'adresse IP de votre serveur de messagerie ou votre domaine.

Si vous êtes listé, suivez les instructions pour demander le retrait de la liste noire.

Analyse de la Configuration SPF, DKIM et DMARC

SPF Lookup : Vérifiez votre enregistrement SPF pour s'assurer qu'il est configuré correctement.

Utilisez MXToolbox SPF Lookup pour entrer votre domaine et vérifier les résultats.

DKIM Lookup : Vérifiez vos enregistrements DKIM pour vous assurer que vos signatures cryptographiques sont en place.

Allez sur MXToolbox DKIM Lookup pour entrer votre domaine et sélectionner le sélecteur DKIM.

DMARC Lookup : Assurez-vous que votre politique DMARC est correctement configurée pour superviser et protéger vos emails contre l'usurpation d'identité.

Utilisez MXToolbox DMARC Lookup pour entrer votre domaine et vérifier la configuration.

Monitoring de la Réputation

Email Health Check : Utilisez l'outil Email Health Check pour une analyse globale de la santé de votre email.

Accédez à MXToolbox Email Health.

Entrez votre domaine pour recevoir un rapport complet sur la santé de votre email, incluant des recommandations d'amélioration.

Résolution des Problèmes d'Envoi et de Réception d'Emails

SMTP Diag Tool : Diagnostic des problèmes d'envoi et de réception d'emails.

Utilisez MXToolbox SMTP Diag Tool pour tester votre serveur SMTP.

Entrez l'adresse IP de votre serveur de messagerie ou le domaine pour vérifier la connectivité SMTP et diagnostiquer les problèmes potentiels.

Surveillance et Alertes

MXToolbox Monitoring : Configurez des alertes et une surveillance pour recevoir des notifications en cas de problèmes de serveur de messagerie, de mise en liste noire ou de défaillances de DNS.

Créez un compte sur MXToolbox et configurez des alertes pour surveiller en continu la santé et la réputation de votre infrastructure de messagerie.

3. Les avantages

Outils de diagnostic email complets :

MXToolbox fournit une suite d'outils pour analyser et dépanner les problèmes liés aux serveurs de messagerie, notamment les tests MX, les vérifications SPF, DKIM et DMARC, ainsi que les contrôles de blacklisting.

Surveillance en temps réel :

L'outil permet de suivre en continu l'état de votre infrastructure email et de recevoir des alertes en cas de problèmes potentiels.

Rapports et analyses détaillés :

MXToolbox génère des rapports détaillés sur la configuration et la santé de vos serveurs de messagerie, vous aidant à identifier et résoudre rapidement les problèmes.

Compatibilité avec de nombreux fournisseurs :

L'outil est compatible avec les principaux fournisseurs de services de messagerie, tels que Microsoft 365, Google G Suite, Amazon SES, etc.

Interface intuitive et conviviale :

L'interface utilisateur de MXToolbox est facile à utiliser et permet d'accéder rapidement aux différents outils.

Historique des résultats :

Vous pouvez consulter l'historique des analyses effectuées et suivre l'évolution de la configuration de vos serveurs de messagerie.

APIs et intégrations :

MXToolbox propose des APIs et des intégrations avec des outils tiers, permettant d'automatiser certaines tâches.



4. Les outils de MXtoolbox

Vérificateur MX (MX Lookup) :

Cet outil permet de vérifier les enregistrements MX (Mail Exchanger) d'un domaine et d'analyser leur configuration.

Testeur SPF (SPF Lookup) :

Permet de tester et d'analyser les enregistrements SPF (Sender Policy Framework) d'un domaine.

Vérificateur DKIM (DKIM Lookup) :

Analyse la configuration DKIM (DomainKeys Identified Mail) d'un domaine.

Testeur DMARC (DMARC Lookup) :

Vérifie et interprète les paramètres DMARC (Domain-based Message Authentication, Reporting and Conformance) d'un domaine.

Outil de blacklisting (Blacklist Lookup) :

Permet de vérifier si l'adresse IP ou le domaine est inscrit sur des listes noires.

Testeur de connectivité email (Email Test) :

Envoie un email de test depuis différents points du globe pour vérifier la deliverability.

Analyseur de serveur de messagerie (Mail Server Test) :

Analyse en profondeur la configuration d'un serveur de messagerie.

Outil de surveillance (Monitoring) :

Permet de suivre en temps réel l'état de votre infrastructure email et reçoit des alertes en cas de problèmes.

Rapports et analyses (Reports) :

Génère des rapports détaillés sur la configuration et la santé de votre système de messagerie.

API et intégrations (API & Integrations) :

Offre des APIs et des possibilités d'intégration avec d'autres outils.

Exemple de gmail.com

The screenshot shows the MXToolbox website interface. At the top, there's a navigation bar with links like Pricing, Tools, Delivery Center, and Monitoring. Below that, a search bar contains 'gmail.com' and a dropdown menu is set to 'MX Lookup'. The main content area displays the results for 'mx:gmail.com'. It includes a table with columns: Pref, Hostname, IP Address, TTL, and Blacklist Check / SMTP Test. The table lists several mail servers for gmail-smtp-in.l.google.com. Below the table, there's a section for DMARC and DNS records. The DMARC record shows 'DMARC Policy Not Enabled' with a warning icon. The DNS record shows 'DNS Record Published' with a green checkmark.

Pref	Hostname	IP Address	TTL	Blacklist Check	SMTP Test
5	gmail-smtp-in.l.google.com	142.251.163.26 Unknown (AS15159)	60 min	Blacklist Check	SMTP Test
5	gmail-smtp-in.l.google.com	2607:f8b0:4004:c1b::1b	60 min	Blacklist Check	
10	alt1.gmail-smtp-in.l.google.com	209.85.202.27 Unknown (AS15159)	60 min	Blacklist Check	SMTP Test
10	alt1.gmail-smtp-in.l.google.com	2a00:1450:400b:c00::1b	60 min	Blacklist Check	
20	alt2.gmail-smtp-in.l.google.com	64.233.184.26 Unknown (AS15159)	60 min	Blacklist Check	SMTP Test
20	alt2.gmail-smtp-in.l.google.com	2a00:1450:400c:c0b::1b	60 min	Blacklist Check	
30	alt3.gmail-smtp-in.l.google.com	142.250.27.27 Unknown (AS15159)	60 min	Blacklist Check	SMTP Test
30	alt3.gmail-smtp-in.l.google.com	2a00:1450:4025:401::1b	60 min	Blacklist Check	
40	alt4.gmail-smtp-in.l.google.com	142.250.153.27 Unknown (AS15159)	60 min	Blacklist Check	SMTP Test
40	alt4.gmail-smtp-in.l.google.com	2a00:1450:4013:c16::1b	60 min	Blacklist Check	

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DMARC Record Published	DMARC Record found	
✓	DNS Record Published	DNS Record found	

Les résultats suivants sont obtenus :

- **Préf (Préférence)** : Cela signifie que les serveurs de messagerie ont la priorité. En cas de faible nombre, la priorité sera élevée. Lorsque le serveur avec la priorité la plus élevée n'est pas disponible, les emails seront transmis en ligne au serveur suivant.
- **Le nom d'hôte (Hostname)** correspond à l'adresse du serveur de messagerie qui reçoit les courriels pour le domaine. Les serveurs de Google utilisés pour le routage des emails sont appelés hôtes.
- **L'adresse IP** correspondante pour chaque nom d'hôte MX est l'adresse IP.
- **TTL (Time To Live)** : La durée en minutes pendant laquelle l'enregistrement reste dans le cache DNS avant d'être à nouveau interrogé.

En bref, MXToolbox est une ressource précieuse pour la gestion et l'optimisation de la délivrabilité des messages électroniques et des configurations DNS. Il fournit un ensemble complet d'outils et de capacités de surveillance pour garantir que votre infrastructure de messagerie est sécurisée, fiable et qu'elle fonctionne de manière optimale.

II. Spamhaus

1. Définition

Steve Linford a fondé **Spamhaus** en 1998 pour combattre l'augmentation du spam en ligne en regroupant les adresses IP associées au spam. L'initiative s'est rapidement transformée en un projet international grâce à l'engagement de personnes du monde entier qui partagent la même vision. **Spamhaus** est devenue une organisation internationale à but non lucratif qui apporte une aide cruciale aux fournisseurs d'accès Internet, aux fournisseurs de services de messagerie électronique, aux entreprises et aux fournisseurs de sécurité. Elle joue un rôle positif dans la lutte contre les spammeurs, en diminuant de manière significative la quantité de courriels et de logiciels malveillants diffusés en ligne.

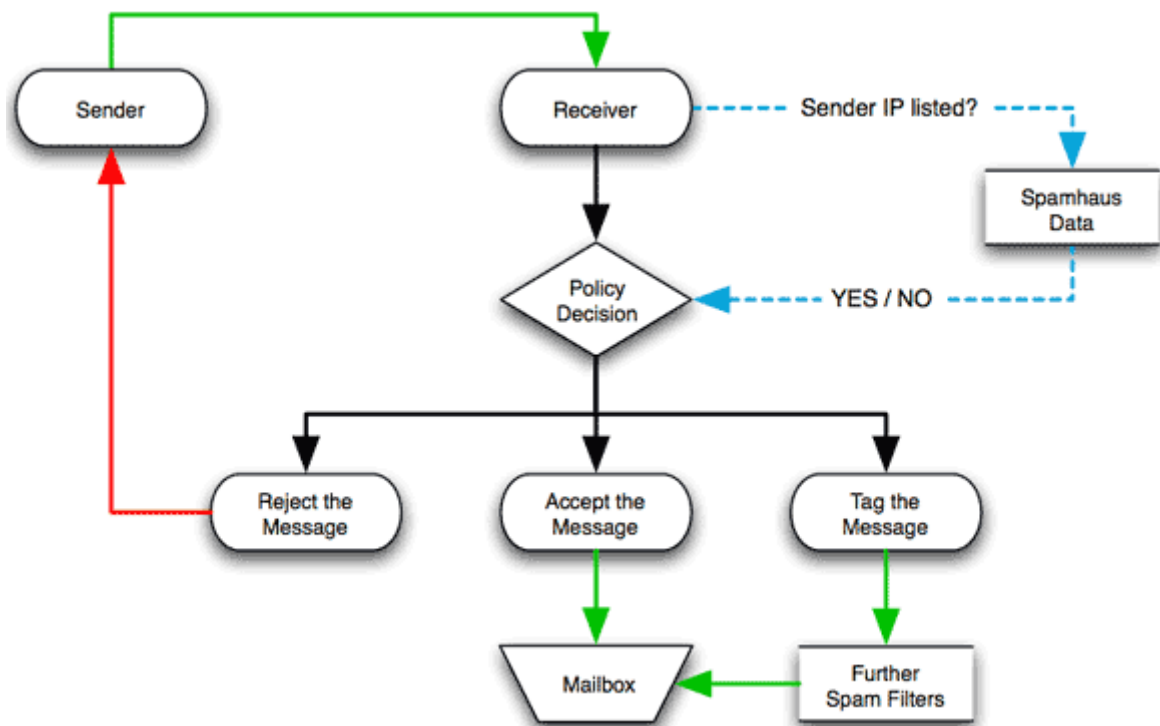
En 24 heures, **Spamhaus** analyse et gère environ trois millions de domaines, quatre milliards de connexions SMTP et environ dixhuit mille échantillons de logiciels malveillants. Des listes de domaines et d'adresses IP évaluées par **Spamhaus** sont utilisées par les spécialistes de la technologie de l'information et de la sécurité.



2. Fonctionnement

Spamhaus collabore avec la communauté mondiale du web et utilise un réseau mondial de détecteurs pour collecter des données de connexion sur divers réseaux. Ces informations sont principalement issues de collaborations avec les principaux fournisseurs d'accès à Internet, des autorités gouvernementales internationales, ainsi que des spécialistes et des chercheurs en matière de cybersécurité. On collecte également des informations en utilisant des dispositifs anti-spam et des honeypots installés sur des réseaux privés.

Avec le temps, le projet Spamhaus a créé et maintenu des listes de réputation qui répertorie les adresses IP et les domaines, largement utilisées par les fournisseurs de services de messagerie à travers le monde.

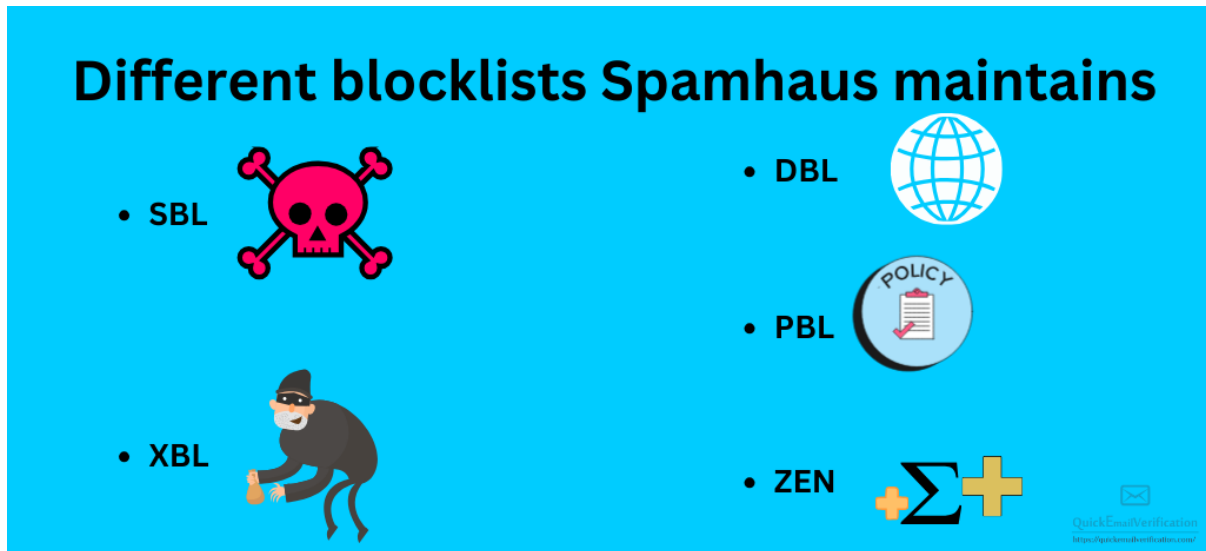


3. Listes de blocage gérées par Spamhaus

Spamhaus propose plusieurs listes noires utilisées par les fournisseurs de services de messagerie pour se protéger contre les spams :

- **SBL (Spamhaus Block List)** : La SBL recense les adresses IP que Spamhaus déconseille pour la réception d'emails. Elle est régulièrement mise à jour par une équipe d'enquêteurs passionnés de divers pays.
- **XBL (Exploit Block List)** : La XBL est une liste constamment mise à jour des adresses IP de machines compromises par des logiciels malveillants ou utilisées illégalement. Cela inclut des proxies ouverts, des virus, des vers avec capacités d'envoi de spam, et d'autres malwares comme les chevaux de Troie.
- **PBL (Policy Block List)** : La PBL est une liste DNSBL qui répertorie les segments d'adresses IP attribuées aux utilisateurs finaux, qui ne devraient pas envoyer d'emails SMTP non authentifiés directement aux serveurs de messagerie sur Internet, sauf via les services fournis par un FAI. Elle permet aux réseaux d'appliquer leur politique d'utilisation des IP dynamiques et des clients n'utilisant pas de MTA.

- **DBL (Domain Block List)** : La DBL est une liste dynamique qui identifie les domaines souvent associés à des spams. Les serveurs de messagerie peuvent analyser les URL dans les emails et utiliser la DBL pour détecter, filtrer ou bloquer les courriels indésirables contenant ces domaines.
- **ZEN** : ZEN est une compilation des différentes listes de blocage de Spamhaus, englobant les fonctionnalités des SBL, XBL et PBL. Il est recommandé d'utiliser zen.spamhaus.org pour éviter les doublons et réduire la charge sur les requêtes DNS, optimisant ainsi le traitement des emails.



4. Défis et critiques de Spamhaus

Manque de transparence et de responsabilité : Spamhaus a été critiqué pour son manque de transparence dans ses processus de listing et de radiation des domaines et adresses IP. Certains estiment que Spamhaus manque de responsabilité dans ses décisions.

Erreurs de listing : Il y a eu de nombreux cas où des domaines ou adresses IP légitimes se sont retrouvés à tort sur les listes noires de Spamhaus, causant des dommages importants aux entreprises concernées.

Abus de pouvoir : Certains accusent Spamhaus d'avoir un pouvoir trop important sur l'écosystème du courrier électronique, avec la capacité de bloquer ou perturber des entreprises à sa discrétion.

Manque de recours : Les entreprises listées par Spamhaus ont souvent du mal à obtenir un processus d'appel ou de réclamation efficace pour être retirées des listes noires.

Juridiction contestée : La légalité des activités de Spamhaus a été remise en question dans certains pays, en particulier concernant la façon dont il exerce sa juridiction à l'échelle mondiale.

Coûts et impact économique : Le fait d'être inscrit sur les listes noires de Spamhaus peut avoir des conséquences financières importantes pour les entreprises, avec des pertes de revenus et de clients.

Ciblage des petits acteurs : Certains estiment que Spamhaus se concentre davantage sur les petits expéditeurs que sur les plus gros spammeurs, ayant un impact disproportionné sur les petites entreprises.

5. Rôle de Spamhaus dans la Sécurité

Spamhaus va au-delà de la lutte contre le spam et occupe une position clé dans la sécurité numérique mondiale. En tant que référence pour l'évaluation de la réputation des adresses IP et des domaines, l'organisation joue un rôle essentiel dans l'identification des menaces et la protection de milliards de personnes. Ses nombreux partenariats l'aident à élaborer et mettre en œuvre des politiques de sécurité renforcées, favorisant une cybersécurité préventive et efficace.

L'influence de Spamhaus se manifeste également dans l'établissement de normes et de meilleures pratiques pour gérer les abus en ligne, en offrant conseils et expertise aux entités gouvernementales. Ainsi, Spamhaus contribue à créer un cadre réglementaire qui favorise une gouvernance d'Internet sûre et responsable. De plus, ses initiatives de sensibilisation et d'éducation améliorent la compréhension des enjeux de la sécurité informatique auprès des décideurs et du public.

Enfin, Spamhaus joue un rôle crucial dans la gestion des incidents, coordonnant les efforts contre les menaces cybernétiques majeures et facilitant le partage rapide d'informations vitales entre les professionnels de la sécurité. En somme, Spamhaus est un pilier indispensable pour la résilience d'Internet face aux cybermenaces.

III. VirusTotal

1. Définition

VirusTotal est un site web qui fonctionne en tant qu'agrégateur et analyste de fichiers suspects ou potentiellement malveillants. Les utilisateurs ont la possibilité de fournir des fichiers, des URL ou des adresses IP afin d'effectuer une analyse approfondie de la présence de logiciels malveillants ou d'autres menaces potentielles.

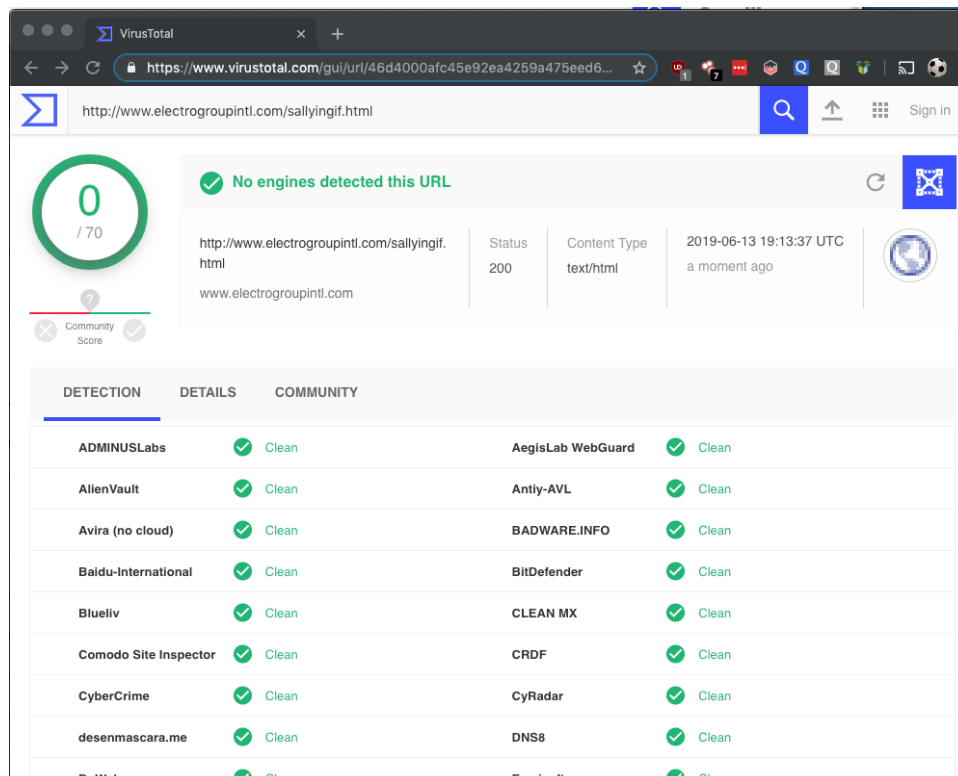


2. Fonctionnement

Pour garantir la sécurité de la messagerie, en utilisant **VirusTotal**, il est possible de :

- Lorsqu'un email contient une pièce jointe suspecte, il est possible de la télécharger sur VirusTotal afin de l'analyser en détail.
- La présence de logiciels malveillants ou d'autres menaces potentielles dans le fichier sera détectée par VirusTotal en utilisant ses moteurs antivirus et d'autres outils.
- S'il y a des liens suspects ou douteux dans un email, il est également possible de les soumettre à VirusTotal pour une analyse de la réputation.
- Le lien sera analysé par VirusTotal afin de repérer d'éventuels sites malveillants ou frauduleux.

- Analyser les adresses IP : Il est possible que les emails contiennent également des adresses IP suspectes, comme dans les en-têtes ou les liens. VirusTotal a la capacité d'examiner ces adresses IP afin de détecter toute activité malveillante liée à celles-ci.
- Observer de façon proactive : En ajoutant l'API de VirusTotal à notre système de messagerie, il est possible de soumettre automatiquement les pièces jointes ou les liens dans les messages.
- Les courriels qui arrivent à VirusTotal sont analysés en temps réel. Cela nous permet de repérer les attaques avant qu'elles ne provoquent des dégâts.



En bref, VirusTotal est particulièrement utile pour les utilisateurs individuels, les administrateurs système, et les chercheurs en sécurité qui souhaitent vérifier rapidement la sécurité de fichiers ou de liens web.

IV. CLAMAV

1. Définition

Le logiciel antivirus open source Clamav est spécialement conçu pour détecter et éliminer les logiciels malveillants, tels que les virus, les chevaux de Troie, les vers et d'autres menaces.



2. Fonctionnement

Base de données de signatures : **ClamAV** utilise une base de données de signatures constamment mise à jour pour détecter les logiciels malveillants. Ces signatures sont des empreintes spécifiques de logiciels malveillants connus, permettant à **ClamAV** de les identifier rapidement lors des analyses. FreshClam télécharge automatiquement les mises à jour pour garantir une protection contre les menaces les plus récentes.

Analyse de fichiers : ClamAV peut analyser divers types de fichiers :

Mode d'analyse :

- **Analyse à la demande :**

Les utilisateurs peuvent lancer manuellement une analyse de fichiers ou de répertoires spécifiques en utilisant ClamScan.

- **Analyse en temps réel :**

Grâce à ClamD, il est possible de configurer une surveillance continue des fichiers pour détecter les menaces dès leur apparition.

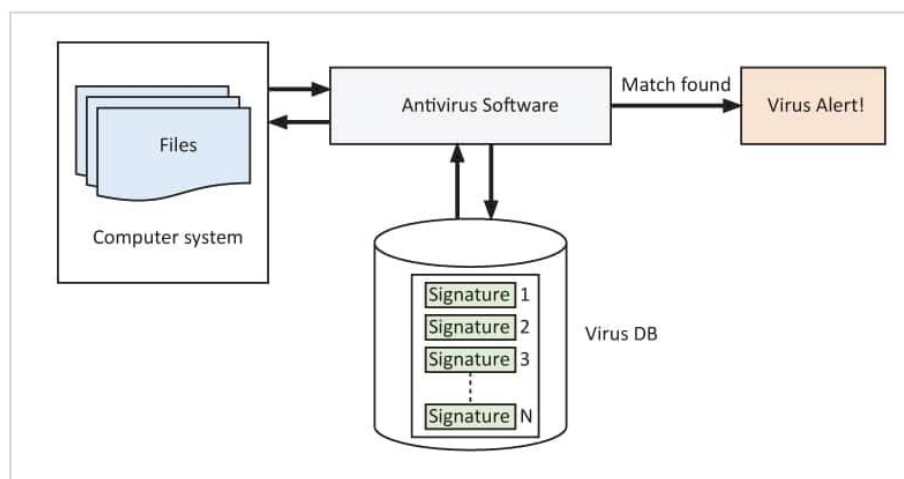
Prétraitement : Identification du type et du contenu des fichiers.

Analyse des signatures : Comparaison des fichiers avec la base de données de signatures pour détecter les menaces connues.

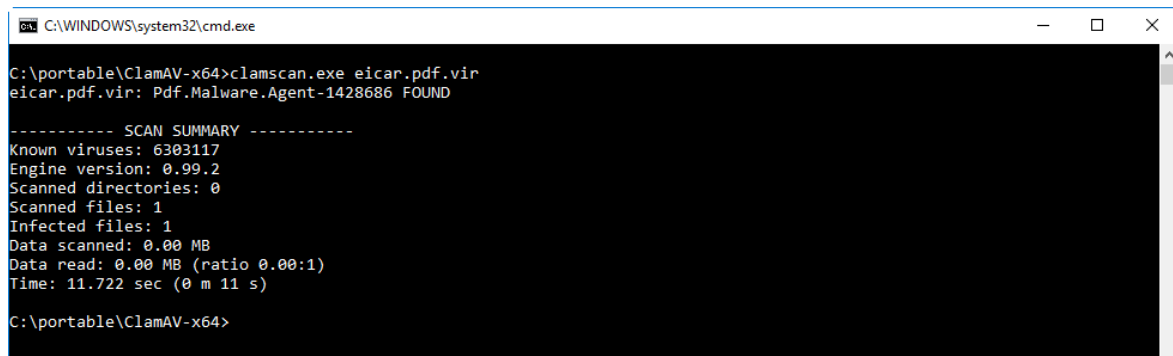
Analyse heuristique : Utilisation de techniques heuristiques pour détecter des comportements suspects ne correspondant pas à des signatures connues.

Mises à jour du logiciel : ClamAV est régulièrement mis à jour pour améliorer ses fonctionnalités et corriger les vulnérabilités.

Intégration avec d'autres systèmes : ClamAV peut être intégré à divers systèmes et logiciels pour une protection étendue.



3. Exemple de scan



```
C:\WINDOWS\system32\cmd.exe

C:\portable\ClamAV-x64>clamscan.exe eicar.pdf.vir
eicar.pdf.vir: Pdf.Malware.Agent-1428686 FOUND

----- SCAN SUMMARY -----
Known viruses: 6303117
Engine version: 0.99.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 11.722 sec (0 m 11 s)

C:\portable\ClamAV-x64>
```

En bref, ClamAV est un outil puissant et flexible pour la protection contre les menaces informatiques, bénéficiant de la communauté open source pour son développement et ses mises à jour.

Références bibliographiques :

➤ Chapitre 1 :

<https://www.coursinfo.fr/decouverte/messagerie-electronique/quest-ce-quune-messagerie-electronique/>

<https://www.cloudflare.com/learning/email-security/what-is-a-mail-server/>

<https://www.altospam.com/glossaire/mta-mda/>

<https://www.logiciels-informatiques.com/fonctionnement-client-messagerie-explications/#:~:text=Outre%20envoyer%20et%20recevoir%20votre,et%20de%20g%C3%A9rer%20votre%20agenda.>

<https://www.ibm.com/docs/fr/linux-on-systems?topic=linuxonibm/liaaz/mailflow.htm>

[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiAz5ni5tWGAXcVaQEHeaUDr8QFnoECBIQAw&url=https%3A%2F%2Fknowledge.validity.com%2Fs%2Farticles%2FWhat-is-a-Mail-User-Agent-MUA%23%3A~%3Atext%3DEmail%2520Glossary-%2CWhat%2520is%2520a%2520Mail%2520User%2520Agent%2520\(MUA\)%253F%2CEmail%2520server%252C%2520which%2520transports%2520email.&usg=AOvVaw1xKOFj39QF-Vq0NE4peUSK&opi=89978449](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiAz5ni5tWGAXcVaQEHeaUDr8QFnoECBIQAw&url=https%3A%2F%2Fknowledge.validity.com%2Fs%2Farticles%2FWhat-is-a-Mail-User-Agent-MUA%23%3A~%3Atext%3DEmail%2520Glossary-%2CWhat%2520is%2520a%2520Mail%2520User%2520Agent%2520(MUA)%253F%2CEmail%2520server%252C%2520which%2520transports%2520email.&usg=AOvVaw1xKOFj39QF-Vq0NE4peUSK&opi=89978449)

https://csrc.nist.gov/glossary/term/mail_transfer_agent#:~:text=A%20program%20running%20on%20a,for%20delivery%20to%20the%20recipient.

https://knowledge.validity.com/s/articles/What-is-a-Mail-Delivery-Agent-MDA?language=en_US

<https://www.twilio.com/docs/sendgrid/for-developers/sending-email/getting-started-smtp>

<https://mailchimp.com/developer/transactional/docs/smtp-integration/>

<https://postmarkapp.com/blog/smtp-relay-services>

<https://medium.com/@shunxianou/how-does-email-work-5964aec2d314>

<https://support.microsoft.com/fr-fr/office/que-sont-les-protocoles-pop-et-imap-ca2c5799-49f9-4079-aeef-ddca85d5b1c9#:~:text=IMAP%20et%20POP%20sont%20deux,ordinateur%20portable%20et%20une%20tablette.>

Protocoles de messagerie

SMTP

<https://postmarkapp.com/smtp-service>

<https://www.altospam.com/glossaire/smtp/#:~:text=Le%20protocole%20SMTP%20a%20%C3%A9t%C3%A9,ascendante%20a%20toujours%20%C3%A9t%C3%A9%20respect%C3%A9.>

<https://www.cloudflare.com/fr-fr/learning/email-security/what-is-smtp/>

Pop

<https://www.hostinger.fr/tutoriels/mail-pop3-smtp-imap#:~:text=Le%20POP3%20est%20un%20protocole,les%20stocke%20sur%20le%20serveur.>

https://irp.nain-t.net/doku.php/180pop3:020_commandes

IMAP

<https://www.hostinger.fr/tutoriels/mail-pop3-smtp-imap#:~:text=Le%20POP3%20est%20un%20protocole,les%20stocke%20sur%20le%20serveur.>

https://irp.nain-t.net/doku.php/190imap:030_commandes

<https://www.atmail.com/blog/imap-101-manual-imap-sessions/>

<https://www.atmail.com/blog/imap-commands/>

Différence entre imap pop3

<https://support.mozilla.org/fr/kb/differences-imap-pop3>

<https://www.kreativmedia.ch/fr/difference-pop3-imap>

Postfix

<https://www.formatux.fr/formatux-services/module-070-postfix/index.html>

<https://www.linuxpedia.fr/doku.php/serveurs/postfix>

https://www.postfix.org/BASIC_CONFIGURATION_README.html

<https://help.ubuntu.com/community/Postfix>

https://irp.nain-t.net/doku.php/200messagerie:010postfix1:010_anatomie

Dovecot

<https://fr.linuxfromscratch.org/view/blfs-12.1-fr/server/dovecot.html>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-a-postfix-email-server-with-dovecot>

https://doc.dovecot.org/installation_guide/compiling_source/

Historique

<https://www.dolist.com/blog/strategie-email-digitale/histoire-de-email-evolution-et-dates-cles/>

➤ Chapitre 2 :

Partie 1 :

<https://www.altospam.com/glossaire/spam/>

<https://www.cakemail.fr/blog/post/guide-eviter-etre-considere-spam#spam--d%C3%A9finition-et-signalement>

<https://www.cloudflare.com/fr-fr/learning/access-management/phishing-attack/>

<https://www.proofpoint.com/fr/threat-reference/phishing>

<https://fr.mailpro.com/blog/les-virus-par-lemail-ce-quil-faut-savoir#:~:text=Les%20virus%20peuvent%20vous%20attaquer,de%20comprendre%2C%20un%20fichier%20corrompu.>

Partie 2 :

<https://caniphish.com/phishing-resources/blog/compromising-australian-supply-chains-at-scale>

- Email security : attack and defence, Jeffrey Bencteux

<https://blog.improsec.com/tech-blog/arebelongtous>

<https://caniphish.com/phishing-resources/blog/scanning-spf-records>

- “Johnny, you are fired!” – Spoofing OpenPGP and S/MIME Signatures in Emails, Jens Müller, Marcus Brinkmann, Damian Poddebniak, Hanno Böck, Sebastian Schinzel, Juraj Somorovsky, and Jörg Schwenk

➤ Chapitre 3 :

Partie 1 :

<https://www.hostinger.fr/tutoriels/enregistrement-dkim>

https://www.domain.com/help/article/what-are-dkim-and-dmarc?utm_campaign=dynamic_PPC&utm_source=googleads&utm_medium=genericsearch&channelid=P13C46098636S570N0B5578A30D4499E0000V111&gad_source=1&gclid=CjwKCAjw-O6zBhASEiwAOHeGxTu-owxtrlU_yZI9cIyDGgEE7d9RGPXR3E5VLfNah7aJUqflyPU6rBoCd-QQAvD_BwE&gclsrc=aw.ds

<https://www.proofpoint.com/fr/threat-reference/dkim>

<https://www.proofpoint.com/fr/threat-reference/spf>

<https://www.proofpoint.com/fr/threat-reference/dmarc>

[https://www.fortinet.com/fr/resources/cyberglossary/dmarc#:~:text=Le%20DMARC%20\(Message%20Authentication%20Reporting,SPF%20\(%20Sender%20Policy%20Framework\).](https://www.fortinet.com/fr/resources/cyberglossary/dmarc#:~:text=Le%20DMARC%20(Message%20Authentication%20Reporting,SPF%20(%20Sender%20Policy%20Framework).)

<https://www.proofpoint.com/fr/threat-reference/dmarc>

<https://spamassassin.apache.org/doc.html>

<https://faq.o2switch.fr/hebergement-mutualise/tutoriels-cpanel/spam-assassin>

Partie 2 :

<https://mxtoolbox.com/>

https://en.wikipedia.org/wiki/The_Spamhaus_Project

<https://medium.com/@webyildiz/what-is-the-mxtoolbox-9397fd9f5901>

<https://blog.didierstevens.com/2017/08/24/quickpost-using-clamav-on-windows/>

<https://en.wikipedia.org/wiki/ClamAV>

<https://en.wikipedia.org/wiki/VirusTotal>

<https://virustotal.readme.io/docs/how-it-works>