

TP Sécurité de la Messagerie Electronique d'Entreprise

Noms et Prénoms : **Abdel-Malik FOFANA**

Noms et Prénoms : **Ivan KRIVOKUCA**

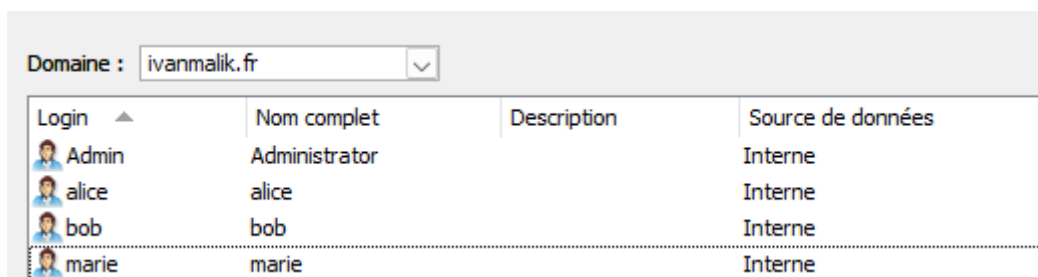
Objectif du TP : installer, analyser et sécuriser un système de messagerie électronique d'entreprise.

Veuillez répondre aux questions suivantes en utilisant **une couleur de police de caractères BLEUE**, et si possible veuillez illustrer vos réponses avec des captures d'écrans (wireshark, tcpview, serveur, client, ...).





1. INSTALLATION D'UN SYSTEME DE MESSAGERIE ELECTRONIQUE D'ENTREPRISE

1.1 – installer et configurer sur votre poste, le serveur Mail fournit avec ce TP. Choisissez un nom de domaine pour votre entreprise comme par exemple « mondomaine.fr ». Vous nommerez alors votre serveur email : « mailhost.mondomaine.fr ». Aidez vous du guide d'administration du serveur si besoin.

1.2 – Sur le serveur, créer 3 comptes utilisateurs au format suivant : login : **alice@mondomaine.fr** et mot de passe : **user1** ; login : **bob@mondomaine.fr** et mot de passe : **user2** ; **marie@mondomaine.fr** et mot de passe : **user3**.



Domaine : ivanmalik.fr

Login	Nom complet	Description	Source de données
 Admin	Administrator		Interne
 alice	alice		Interne
 bob	bob		Interne
 marie	marie		Interne

2. WEBMAIL

Vous allez maintenant tester et accéder à vos comptes email à partir d'un client web (navigateur web).

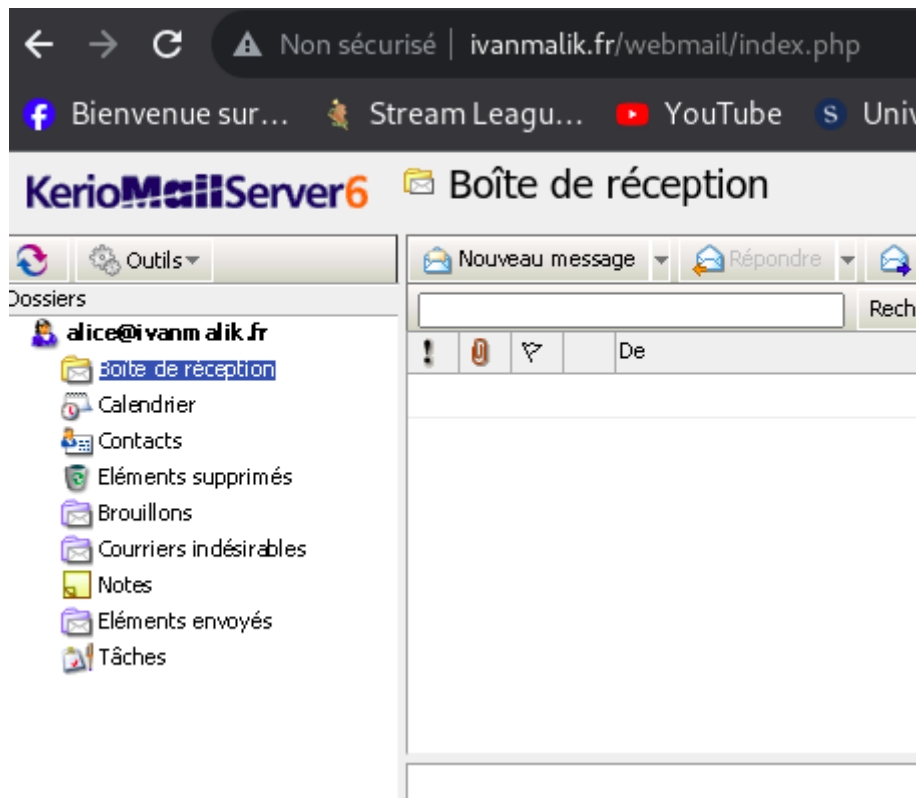
1 - Dans le fichier hosts » du client, ajouter l'alias « www.mondomaine.fr » pour identifier le serveur WebMail. Configurer votre navigateur web pour accéder aux courriels de « **alice** » par le protocole http et le port 80. Rédiger un message à destination de « **bob** ».

De: alice <alice@malikivan.fr>
A: bob@malikivan.fr
Date: 11/15/2023 02:41 PM
Objet: Test mail http

ça marche !

2 - Quelle est l'URL que doit utiliser le client « alice » ?

En modifiant bien le fichier hosts avec l'adresse IP du serveur, on peut y accéder avec l'adresse: <http://www.ivanmalik.fr/webmail/index.php>

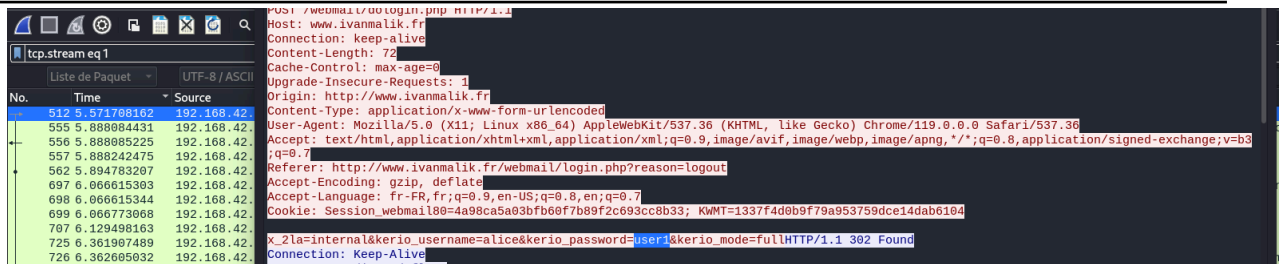


De: alice <alice@ivanmalik.fr>
A: bob@ivanmalik.fr
Date: 11/15/2023 03:26 PM
Objet: test http

test réussi

3 - Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?

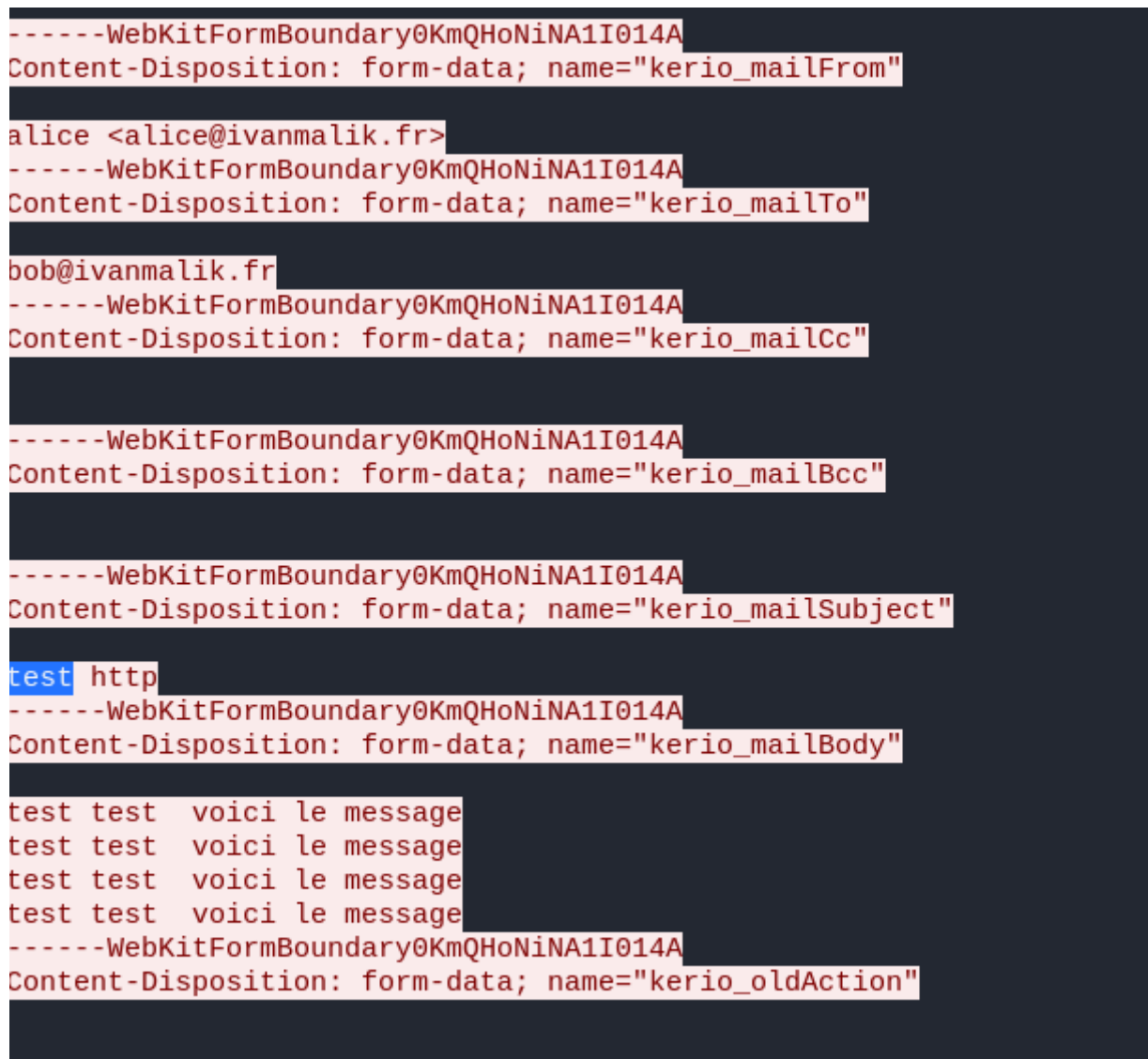
Oui c'est possible, avec Wireshark on a obtenu les résultats suivants



Sur le premier paquet on a fait “suivre flux tcp” puis on est tombé sur le user= alice et mdp=user1

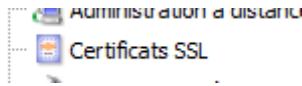
4 - Est-il possible de lire le contenu du message ?

En effet lorsque l’on envoie un message et que l’on écoute avec wireshark on peut voir sur le paquet avec l’option “suivre flux http” les message envoyé en clair



5 - Proposer et décrire une solution pour sécuriser votre accès au courriel par le web.

En utilisant le protocole HTTPS on peut sécuriser cet accès au courriel web. On aura besoin d'un certificat SSL/TLS implémenté sur notre domaine (on peut le faire via Let's Encrypt par ex). Sur Kerio, on peut en créer un directement dans "Configuration/ Certificat SSL"



6 - Quel est l'intérêt d'utiliser le WebMail en lieu et place d'un client natif de courriel (exemples : Apple Mail, MS Outlook, thunderbird) ?.

On a aucune configuration à faire, de plus les emails ne seront pas stockés localement à contrario des clients natifs dans lesquels une sauvegarde est effectuée sur la machine (en plus potentiellement leurs serveurs)

3. ACCÈS AUX EMAILS VIA UN CLIENT NATIF MAIL ET LE PROTOCOLE POP3

1 – Sur les postes clients Installer le client Mail fournit, et configurer les comptes clients « **bob** » ou « **alice** » pour accéder au serveur « mailhost.mondomaine.fr » avec les protocoles **POP3** et **SMTP**.

2. éditer le fichier système suivant pour associer le nom du serveur mail avec l'adresse IPv4 correspondante du serveur.

Windows\system32\drivers\etc\hosts

3. rédiger un premier email par le client **alice** et l'envoyer au client **bob** avec le contenu suivant « bonjour Bob, ceci est un test POP3 de Alice ». Avec Wireshark et TCPview analyser les échanges et répondre aux questions suivantes :

- Quel est le protocole applicatif utilisé par « **alice** » pour l'envoi du message ?
- Quel est le protocole de transport (UDP ou TCP) utilisé par « **alice** » pour l'envoi du message ?
- Quel est le port du client ?
- Quel est le port du serveur ?
- Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?
- Est-il possible de lire le contenu du message ?

4. récupérer le message précédent dans la boîte email de « **bob** » :

- Quel est le protocole de transport (UDP ou TCP) utilisé pour la réception du message ?
- Quel est le port du client ?
- Quel est le port du serveur ?
- Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?
- Est-il possible de lire le contenu du message ?

4. ACCÈS AUX EMAILS VIA UN CLIENT NATIF MAIL ET LE PROTOCOLE POP3

1. – Sur un 2^{ème} poste client, installer également le client natif Mail fournit et créer le compte utilisateur « **marie** » pour utiliser les deux protocoles **IMAP4** et **SMTP**. Utiliser : login : **marie@mondomaine.fr** et mot de passe : **user3**.

2. Installer et lancer les logiciels Wireshark et TCPview sur ce second poste.

3 - rédiger un email par le client **Alice** et l'envoyer au client **Marie** avec le contenu suivant « bonjour Marie, ceci est un test IMAP avec Alice ». Télécharger le message sur la boîte email de **Marie**. Avec Wireshark et TCPview analyser les échanges et répondre aux questions suivantes :

- Quel est le protocole de transport (UDP ou TCP) utilisé pour la réception du message ?
- Quel est le port du client ?
- Quel est le port du serveur ?
- Est-il possible de capturer votre login et votre mot de passe ? Passe-t-il en clair ?
- Est-il possible de lire le contenu du message ?

4. Expliquer dans un tableau comparatif, les principales différences fonctionnelles entre un client email utilisant POP3 et IMAP4.

5. Au moyen de la commande système « nslookup », déterminer les adresses IP et les noms des serveurs SMTP de votre université ainsi que le nom symbolique du serveur DNS (Domain Name Service) utilisées par votre terminal pour naviguer sur l'Internet ? Reportez ces informations ci-dessous.

6. Créer un répertoire « Projet Réseaux » dans la boîte email de « Alice ». Puis configurer un « **Filtre** » des messages appelé « projet Réseaux » qui devra classer automatiquement les messages envoyés à Alice et respectant les règles suivantes :

- Si les mots « projet » OU « réseaux » font partis du sujet du message reçus ET si l'émetteur est « Bob ».

Faire un test d'envoi de messages de **Bob** vers Alice avec comme sujet « **projets** ». Puis un second message de **Bob** vers **Alice** avec comme sujet « **projet** ».

5. SECURITÉ DES COMMUNICATIONS EMAIL AVEC SMTPS (SMTP OVER SSL)

1 – configurer votre client pour que « **Alice** » puisse transmettre un email à « **Bob** » en utilisant le **protocole SMTP over SSL** (SMTPS). Le sujet et le contenu du message seront « test d'envoi de message avec SMTPS »

2 – quel est le numéro de port du serveur SMTPS ?

3 – avec le sniffer de réseau, vérifier si :

- votre login et mot de passe sont transmis en clair ?

- le contenu du message est en clair et peut donc être intercepté ?

4 – quel(s) type(s) de chiffrement et de clé(s) est (sont) utilisé(s) par SMTPS ?

5 - Quels sont les services de sécurité fournis par une connexion SMTP over SSL (SMTPS) ?

6. SECURITÉ DES COMMUNICATIONS EMAIL AVEC IMAPS (IMAP over SSL)
--

1 – configurer votre client pour que « **Marie** » puisse récupérer son email de « **Alice** » en utilisant le **protocole IMAP over SSL (IMAPS)**.

2 – quel est le numéro de port du serveur IMAPS ?

3 – avec le sniffer de réseau, vérifier si :

- votre login et mot de passe sont transmis en clair ?

- le contenu du message est transmis en clair ?

4. Quel est le port du serveur en mode d'accès POP3S (POP3 over SSL) ?

t « **projet** ».

7. SECURITÉ DU COURRIEL DE BOUT EN BOUT AVEC PGP

2.1 – Installer dans l'ordre « GnuPG » puis « Enigmail ».

2.2 – créer une bi-clé et publier (upload) votre clé publique sur le serveur « pool.sks-keyservers.net »

2.3 – Configurer le client Mail (onglet Enigmail) pour envoyer un courriel « signé » avec PGP. Quels sont les services de sécurité assurés par la signature numérique de votre message email ?

2.4 – Configurer le client Mail pour envoyer un courriel « crypté » avec PGP. Quels sont les services de sécurité assurés par le chiffrement de votre message email ?

2.5 – A quel moment et comment est récupéré la clé publique par le récepteur.

2.6 – quelle clé est utilisée pour assurer l'authenticité des courriels ?

2.7 – quelle clé est utilisée pour assurer la confidentialité des courriels ?

2.8 – Quelle est la fonction de hachage utilisée par GnuPG ?

2.9 – Vérifier avec le sniffer de réseau si votre **login** et **votre mot de passe** sont protégés. Expliquer pourquoi.