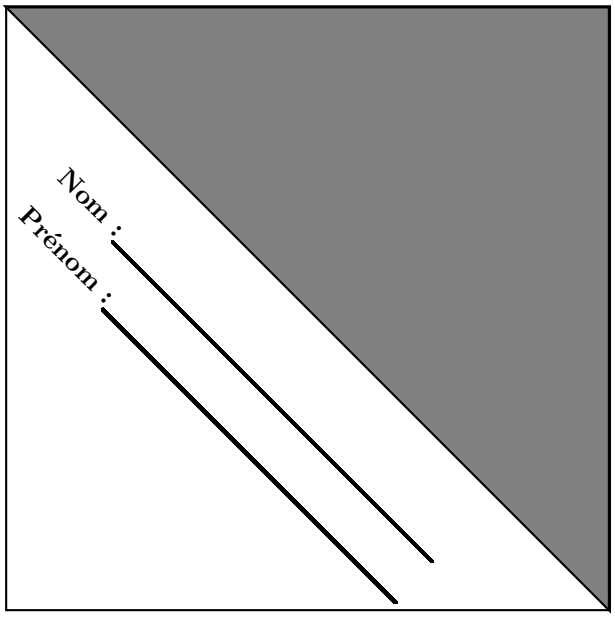
Université Côte d'Azur — SI5, parcours CyberSec
Sécurité des réseaux — 2024–2025

Examen janvier 2025

**Durée :** 1 heure 30

Note :




L'examen comporte 4 parties indépendantes. Répondez sur la copie avec clarté et concision. Documents autorisés.

# 1 En bref [5 points]

**1.** Expliquez le risque potentiel lié à l'utilisation de `STARTTLS` sur le port `imap/143` par rapport à l'utilisation de `SSL/TLS` sur le port `imaps/993`.

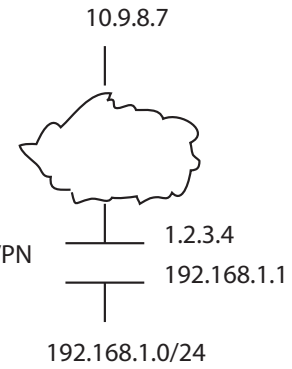
**2.** Expliquez l'intérêt d'utiliser des *aliases* ou des *reverse aliases* pour les adresses de courrier électronique.

**3.** Expliquez l'intérêt du transfert de port par `ssh`.

**4.** Comment peut-on contourner le mécanisme de `dhcp` quand il attribue une adresse IP à partir d'une adresse MAC fixée ?

**5.** Dites à quoi sert le fichier d'extension `.csr` (pour certificate signing request) lors de la création d'un certificat.

## 2 À l'aide ! [4 points]




Vous êtes administrateur de sécurité du site `monsite.com` tel que décrit dans la figure ci-contre. La passerelle de ce réseau héberge un serveur VPN en mode bridge qui établit un tunnel VPN entre l'extérieur (en l'occurrence un client connecté depuis l'adresse `10.9.8.7`) et le réseau `192.168.1.0/24` via le réseau tunnel de service `1.2.3.0`.
Le client se plaint de ne pas pouvoir accéder à Internet lorsqu'il se connecte au VPN. En revanche, il accède sans problème aux machines situées sur le réseau `192.168.1.0/24`.

**1.** Pouvez-vous lui expliquer pourquoi il n'a pas accès à Internet ?

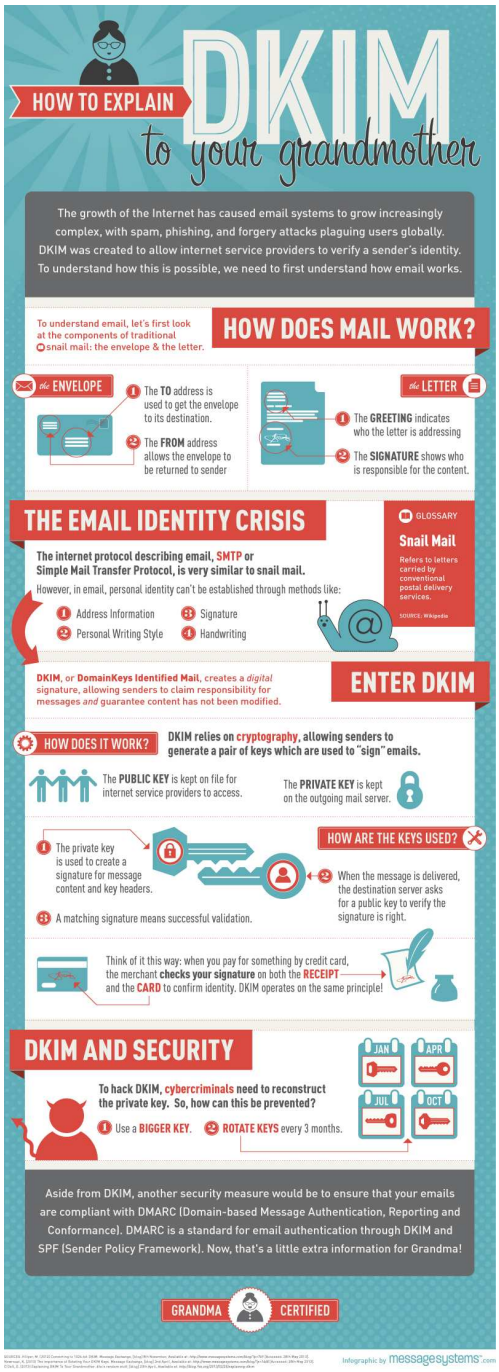
**2.** Que faudrait-il faire pour corriger ce problème ?

## 3 Sécurité du mail [5 points]

L'infographie de la page suivante explique le fonctionnement de DKIM.
**1.** Expliquez brièvement quelles sont les menaces contre lesquelles DKIM peut lutter et son utilité.

**2.** La configuration (`smtp` et `imaps`) du TP permet-elle d'assurer les propriétés de confidentialité, d'intégrité et d'authentification du courrier électronique ? Vous détaillerez votre réponse pour l'envoi ainsi que pour la lecture des mails.

**3.** Au cas où certaines proprétés de sécurité de la question **2.** ne seraient pas satisfaites, dites comment mettre en place une attaque et avec quel outil.




**4.** Selon vous, est-il utile d'utiliser en même temps `DKIM`, `TLS` et `GPG` (ou `s/mime`) pour assurer la sécurité du mail (justifiez votre réponse).

# 4 Analyse d'un scan nmap [6 points]

Voici le scan du réseau des TP par `nmap` :

```
monHote:~ bmartin# nmap 192.168.228.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 16:03 CET
Nmap scan report for Machine1 (192.168.228.1)
Host is up (0.0017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for Machine2 (192.168.228.2)
Host is up (0.0023s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT    STATE           SERVICE
22/tcp  open            ssh
25/tcp  open            smtp
80/tcp  open            http
143/tcp open            imap
443/tcp open            https
993/tcp open            imaps
1194/udp open|filtered  openvpn
```

**1.** Précisez le rôle de `Machine1` et de `Machine2` au sein du réseau scanné (`192.168.228.0`).

**2.** Dites si `Machine1` et `Machine2` possèdent un firewall (en justifiant votre réponse).

**3.** Pouvez-vous donner un aperçu de la politique de sécurité déployée sur ce réseau (en justifiant brièvement).