# Correction de l'examen RSS410 - Sécurité des Réseaux

## Exercice 1 (15 pts)

1. 1. Expliquer la différence entre un reverse et un bind shell.

Un reverse shell est initié depuis la machine cible vers l'attaquant. Le bind shell attend les connexions entrantes sur la cible. Reverse shell est plus discret car il traverse souvent les firewalls.

1. 2. Donner deux exemples de protocoles sécurisés au niveau de la couche application.

HTTPS (HTTP sécurisé avec TLS) et SMTPS (SMTP sécurisé avec TLS).

1. 3. Quelle est la différence entre un VPN et un Proxy ?

Un VPN crée un tunnel sécurisé entre l'utilisateur et le réseau, en chiffrant tout le trafic. Un proxy agit comme intermédiaire pour certaines requêtes sans forcément chiffrer.

1. 4. Quel est le rôle d’un reverse proxy ?

Il reçoit les requêtes des clients et les redirige vers les serveurs internes tout en masquant leur identité. Il sert de pare-feu applicatif.

1. 5. Comment assurer la confidentialité du trafic DNS ? Quel protocole utiliser ?

En utilisant DoT (DNS over TLS) ou DoH (DNS over HTTPS) pour chiffrer les requêtes DNS.

1. 6. Comment la sécurité de bout en bout est-elle assurée dans le protocole SMTP ?

Par des solutions comme PGP ou S/MIME, qui permettent le chiffrement et la signature des emails.

1. 7. Dans un réseau câblé, expliquer pourquoi le protocole IEEE 802.1X est utilisé.

Pour contrôler l’accès au réseau via une authentification forte des hôtes avant de leur permettre d’émettre du trafic.

1. 8. Dans un réseau Wi-Fi, pourquoi avons-nous besoin du cryptage ?

Pour éviter que des attaquants interceptent ou modifient les communications transmises par les ondes radio.

1. 9. Quand un réseau WiFi est-il vulnérable aux attaques MITM ?

Lorsque l’authentification n’est pas vérifiée (ex: pas de certificat) ou que les données ne sont pas chiffrées (réseaux ouverts).

1. 10. Dans le contexte de la sécurité des réseaux, quel est le rôle d’un honeypot ?

Attirer les attaquants pour observer leurs techniques et protéger les systèmes réels.

1. 11. Quels sont les avantages de l’authentification multifacteur par rapport à l’authentification par mot de passe ?

Elle ajoute une couche de sécurité supplémentaire : mot de passe + objet (ex : téléphone) + biométrie.

1. 12. Donner trois mécanismes d’authentification des utilisateurs.

Mot de passe, certificat numérique, authentification biométrique.

1. 13. Quelle est la fonction des outils suivants :  
   (a) iptables  
   (b) metasploit  
   (c) zeek

- iptables : outil de filtrage de paquets sous Linux  
- metasploit : cadre de test de pénétration pour exploiter des vulnérabilités  
- zeek : IDS pour l’analyse de trafic réseau

## Exercice 2 (5 pts)

1. 1. Ce firewall bloque-t-il le trafic sortant ? Pourquoi ?

Non. Les lignes iptables -A OUTPUT ... -j ACCEPT permettent explicitement le trafic sortant vers certaines IP et états de connexions.

1. 2. Pouvez-vous vous connecter au serveur Web sur l’hôte ?

Oui, si votre IP est dans 192.168.100.1/16, le port 80 est autorisé.

1. 3. Pouvez-vous pinger le serveur à l’aide de la commande ping ?

Non. ICMP n’est pas autorisé par la politique iptables, seulement TCP et UDP sont filtrés.

1. 4. Que va retourner la commande nmap -p 21,22,80,443 192.168.100.4 ?

Ports 22 et 80 : ouverts. Ports 21 et 443 : fermés (car non écoutés par le serveur selon l’énoncé).