**Examen : Sécurité Informatique**

Amel Meddeb Makhlouf

Durée : 1h15 et 15mn pour le chargement sur la plateforme ou l’envoi par email

NOM et Prénom : Mohamedou Bouk

Matricule : 23083

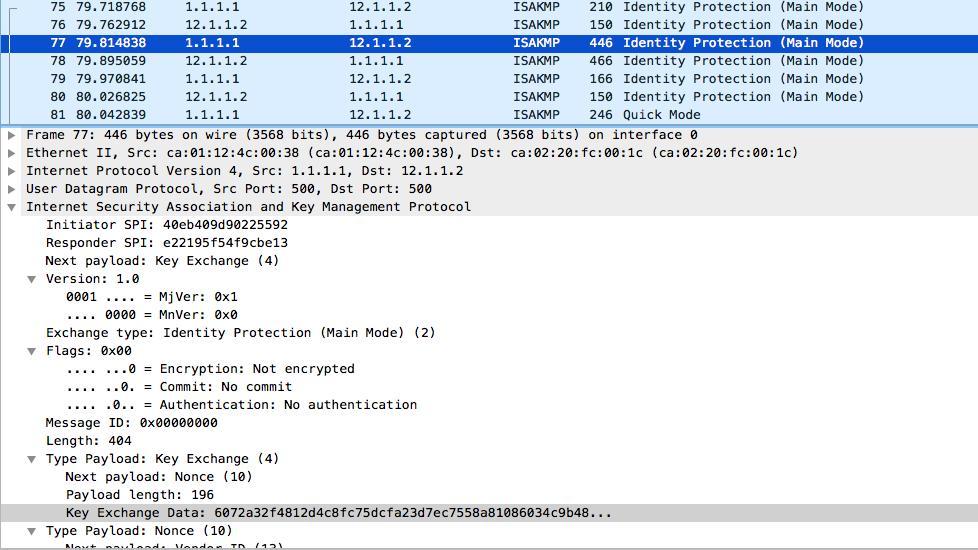
Nombre de pages soumises 8

**NB. Insérer de l’espace pour répondre aux questions sans les supprimer.**

**Veuillez envoyer une version word et une version pdf**

**Exercice 1 : VPN/IPsec (11.5 pts)**

Soit la capture suivante :



1. Donner le protocole utilisé dans ce cas. Expliquer **(1pt)**

Réponse : Le protocole utilisé ici est ISAKMP (Internet Security Association and Key Management Protocol)

Explication : ISAKMP est utilisé pour négocier, établir, modifier et supprimer des associations de sécurité (SA). Il ne transporte pas les clés lui-même, mais fournit un cadre pour les protocoles de gestion de clés comme IKE. Dans cette capture, on voit clairement que le protocole transporte des messages d’Identity Protection

1. S’il s’agit de IKE, de quelle phase s’agit-il ? Expliquer **(1pt)**

Reponse : Oui, il sagit bien du protocole IKE , plus precisément de la phase 1

Explication : Dans la capture, les message sont tout marqué comme "Identity Protection (Main Mode)", ce qui correspond à la Phase 1 - Main Mode. Le but de cette phase est d’établir un canal sécurisé entre les deux pairs en négociant des paramètres cryptographiques

1. Donner le type de SA utilisée et ses caractéristiques ainsi que ses paramètres **(1 pt)**

Réponse : Le type de SA utilisée est une ISAKMP SA (Phase 1).

Caractéristiques :

* Mode : Main Mode
* But : Authentification et etablissement d’un canal sécurisé

Paramètres :

* Algorithme de chiffrement : (ex. AES)
* Hachage : (ex. SHA-1)
* Groupe DH
* SPI : 4be04bd4090225592 / e2219f549fc2b1c8

1. Donner l’utilité du « Main mode » cité sur la figure **(0.5 pt)**

Le Main Mode est utilisé pour établir une ISAKMP SA de manière securisé, en protégant l’identitée de pairs et en negocient les paramètrs cryptographique

1. Donner les deux méthodes d’authentification utilisées par VPN/IPsec **(1pt)**

* Clé pre partagée (PSK)
* Certificat numériques (X.509)

1. Donner trois différences entre le protocole AH en mode transport et le protocole ESP en mode tunnel **(1 pt)**

AH (Transport) ESP (Tunnel)

* Authentifie mais ne chiffre pas
* Ne cache pas en-tête IP
* pas de confidentialité

ESP (Tunnel)

* Chiffre les donnés ,confidentialité.
* Cache en-tête IP d'origine
* Fournit confidentialité + intégrité

1. Préciser les opérations suivies par un routeur (bout du tunnel) qui utilise IPSEC/ESP en mode tunnel pour les paquets reçus **(1.5 pts)**

* Déchiffrement du paquet ESP reçu
* Vérification de l’intégrité
* Décapsulation du paquet IP interne
* Routage du paquet IP décapsulé vers sa destination

1. Voici trois lignes d’une table SPD (Security Policy Database) :

1. src 192.168.0.1 dst 192.168.100.1 protocol icmp → discard

2. src 192.168.2.5 dst 172.16.1.10 protocol udp → apply ESP transport

3. src 192.168.2.0/24 dst 172.16.0.0/16 protocol any → apply ESP tunnel 10.1.1.1 → 10.1.1.2

Et la SA suivante est disponible :

SPI : 0x12345678

Source : 192.168.2.5

Destination : 172.16.1.10

Protocole : ESP

Chiffrement : AES-CBC-128

Authentification : HMAC-SHA1

Lign 1 : Trafic ICMP entre 192.168.0.1 → 192.168.100.1 → bloqué (discard)

Lign 2 : Trafic UDP entre 192.168.2.5 → 172.16.1.10 → ESP en transport, et SA disponible correspondante peut être utilisée

Lign 3 : Trafic entre 192.168.2.0/24 → 172.16.0.0/16 → ESP en tunnel via 10.1.1.1 → 10.1.1.2, utile pour tous protocoles sauf ceux deja explicitement listé.

1. De quel type de configuration s’agit-il ? et quel est le mode IPSec utilisé ? **(1pt)**

* Configuration site-to-site
* Mode IPsec : Transport (car la SA est liée à des adresses précises, sans encapsulation d’un paquet IP complet)

1. À quelle ligne de la table SPD cette SA correspond-elle ? **(0.5 pt)**

Elle correspond à la ligne 2 : src 192.168.2.5 dst 172.16.1.10 protocol udp → apply ESP transport

1. Quel est le mode IPsec utilisé dans cette SA : tunnel ou transport ? **(0.5 pt)**

Transport mode (indiqué explicitement dans la ligne SPD n°2)

1. Que se passe-t-il si l’hôte 192.168.0.1 tente d’envoyer un ping (ICMP) vers 192.168.100.1 ? **(1pt)**

Le paquet sera bloqué

Raison : ligne 1 de la SPD → règle icmp → discard

1. Et si cet hôte tente d’envoyer une requête HTTP (protocole TCP) vers 192.168.100.1 ? **(1pt)**

Le paquet ne match aucune règle SPD

Par défaut : trafic rejeté ou traité sans IPsec .

1. Cette SA permet-elle de sécuriser un trafic HTTP entre les réseaux 172.16.0.0/16 et 192.168.0.0/16 ? **(0.5pt)**

Reponse : Non

Elle ne couvre qu’un flux précis (192.168.2.5 ↔ 172.16.1.10 en UDP), pas un trafic HTTP global entre deux réseaux.

**Exercice 2 : Certificats et PKI (3.5 pts)**

1. **Quels éléments sont généralement inclus dans un certificat X.509 ?**  
   a) La clé publique du sujet  
   b) La clé privée de l'AC  
   c) Le nom du sujet (ex : domaine ou individu)  
   d) La date d'expiration  
   e) L'adresse MAC du serveur

Réponse(s) : a , c , d

1. **Quels mécanismes permettent de vérifier la validité d'un certificat ?**a) La liste de révocation de certificats (CRL)  
   b) Le protocole DHCP  
   c) Le serveur DNS  
   d) Timestamping

Réponse(s) : a , d

1. **Quels sont les utilisations des certificats numériques ?**  
   a) Authentification des sites web (HTTPS)  
   b) Chiffrement des e-mails (S/MIME)  
   c) Génération de nombres aléatoires  
   d) Signature numérique de documents  
   e) Stockage de fichiers cloud

Réponse(s) : a , b , d

1. Donner deux raisons de révocation de certificats **(1 pt)**

* Compromission de la clé privée du titulaire
* Changement d’état ou d’identité du titulaire (ex : employé qui quitte une organisation)

1. Donner deux différences entre une AC (Autorité de certification) et une AE (Autorité d’enregistrement). Expliquer ces différences. **(1 pt)**

Autorité de Certification (AC)

* Signe les certificats (acte cryptographique)
* Entité principale dans la hiérarchie de confiance

Autorité d’Enregistrement (AE)

* Vérifie l’identité des demandeurs
* Joue un rôle délégué et intermédiaire pour la CA

Explication :

* L’AC est responsable de la création et de la signature des certificats.
* L’AE est un intermédiaire qui authentifie les identités avant de transmettre les requêtes à l’AC.

**Exercice 3 : Firewall et IDS (5pts)**

En supposant que la table de filtrage suivante est utilisée au niveau du routeur internet

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| @IP source | @IP dest | Port source | Port dest | Protocole | Action |
| 172.16.0.0 | 172.17.0.1 | > 1024 | 80 | IP | Accept |
| 172.17.0.1 | 172.16.0.0 | > 1024 | 80 | TCP | Deny |
| 172.16.0.0 | 172.17.0.2 | > 1024 | 53 | UDP | Deny |
| 172.17.0.2 | 172.16.0.0 | 53 | > 1024 | UDP | Accept |
| \* | 172.17.0.1 | 80 | > 1024 | TCP | Accept |
| 172.17.0.1 | \* | > 1024 | 80 | TCP | Accept |
| 172.16.0.0 | \* | > 1024 | 80 | TCP | Accept |
| \* | 172.16.0.0 | 80 | > 1024 | TCP | Accept |
| \* | \* | \* | \* | IP | Deny |

1. Corriger cette table de filtrage. Expliquer chaque changement **(1.5 pts)**

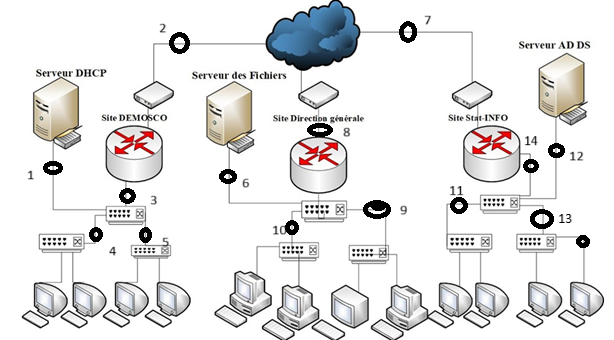
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | @IP source | @IP dest | Port source | Port dest | Protocole | Action | Explication |
| 1 | 172.16.0.0 | 172.17.0.1 | > 1024 | 80 | TCP | Accept | Ajout du protocole TCP au lieu de IP donc plus précis |
| 2 | 172.17.0.1 | 172.16.0.0 | > 1024 | 80 | TCP | Accept | Inversion de la règle 1, acceptée pour la symétrie |
| 3 | 172.16.0.0 | 172.17.0.2 | > 1024 | 53 | UDP | Accept | Correction : DNS en UDP doit être autorisé, pas refusé |
| 4 | 172.17.0.2 | 172.16.0.0 | 53 | > 1024 | UDP | Accept | Réponse DNS depuis le serveur doit être autorisée |
| 5 | \* | 172.17.0.1 | 80 | > 1024 | TCP | Deny | Refuser connexions entrantes vers port HTTP depuis n’importe qui |
| 6 | 172.17.0.1 | \* | > 1024 | 80 | TCP | Accept | Laisser passer les connexions sortantes HTTP |
| 7 | 172.16.0.0 | \* | > 1024 | 80 |  | Accept | Connexions HTTP autorisées aussi depuis ce réseau |
| 8 | \* | 172.16.0.0 | 80 | > 1024 |  | Deny | Interdire connexions entrantes HTTP |
| 9 | \* | \* | \* | \* |  | Deny | Politique de sécurité par défaut : tout ce qui n’est pas explicitement autorisé |

1. Donner la politique de filtrage utilisée par défaut. Expliquer **(0.5 pt)**

Ce firewall est implémenté sur le firewall du site de la direction générale.

Politique par défaut : Deny , Explication : Toute communication non explicitement autorisée dans la table est bloquée par sécurité. Cela évite l’accès non prévu ou mal configuré.

1. Donner les composants existants sur l’interface DMZ. Expliquer  **(1 pt)**



Composants présents dans la DMZ (Zone Démilitarisée) :

L’interface DMZ se trouve entre le réseau interne (réseaux des sites) et Internet, généralement connectée au pare-feu du site principal (ici, le routeur numéro 8 : Site Direction générale). D'après le schéma, les composants accessibles depuis la DMZ sont :

Serveur des Fichiers (repère 6)

* Placé en DMZ pour permettre l’accès aux fichiers depuis l’extérieur sans exposer le réseau interne.

Routeur de la Direction Générale (repère 8)

* Interface principale de la DMZ, connectée à Internet (repère 7), aux autres sites et aux serveurs.

Accès Internet (repère 7)

* Connecté directement à la DMZ pour autoriser/filtrer les connexions extérieures.

Partie du Serveur AD DS (repère 14)

* Peut exposer une interface en DMZ pour fournir l’authentification à des utilisateurs distants (mais la base AD reste sur le réseau interne).

Explication :

La DMZ est une zone réseau intermédiaire qui héberge des services devant être accessibles depuis l’extérieur (Internet), comme :

* les serveurs de fichiers,
* les serveurs web ou FTP,
* parfois une interface d’un contrôleur de domaine (AD DS), tout en protégeant le réseau interne contre les attaques potentielles.

1. Donner l’emplacement possible des différents types d’IDS, en spécifiant pour chaque IDS les composants supervisés. Les numéros sur la figure peuvent vous aider à localiser les IDS. **(2 pts)**

1. NIDS (Network-based IDS)

- Entre Internet (7) et le routeur principal (8) : Supervise tout le trafic entrant/sortant de l’organisation pour détecter les attaques externes (DoS, scans, intrusions).

- Entre le routeur DEMOSCO (3) et le commutateur (4) : Surveille le trafic local du site DEMOSCO, y compris les échanges entre le serveur DHCP (1) et les postes clients.

Entre le routeur Stat-INFO (14) et les commutateurs (11 et 13) : Supervise l’activité réseau des utilisateurs du site Stat-INFO et les échanges avec le serveur AD DS.

2. HIDS (Host-based IDS)

- Sur le serveur DHCP (1) : Contrôle les fichiers système, les journaux, les connexions, pour détecter toute activité malveillante locale.

- Sur le serveur des fichiers (6) : Analyse les accès, les fichiers modifiés et les comportements suspects. Ce serveur est exposé en DMZ, donc critique.

- Sur le serveur AD DS (14) : Surveille les connexions, les journaux d’authentification, les accès à l’annuaire. Cible sensible à protéger contre des attaques internes.

**Je vous remercie vivement pour votre encadrement, votre patience et la clarté de vos explications tout au long de cette matière.**