Université M'Hamed Bougara Boumerdes / Faculté des Sciences / Département d'Informatique

Module : Sécurité informatique **Examen :** ETLD	**Niveau :** L3 ISIL / SI / ING 3 (S6) **Documents :** non autorisés	**Date :** 17.05.2025 **Durée :** 1h30 min	**Nbr de pages :** 2

Matricule :	**Nom :**	**Prénom :**	**Groupe :**

Exercice 01 (10 points) : Sélectionnez la ou les bonnes réponses.

1. Un actif est :

□Un utilisateur du système □Une attaque potentielle

□Un élément ayant de la valeur pour l'organisation □Aucune réponse 1

2. La combinaison de la probabilité d'occurrence et de l'impact d'un incident définit :

□Une menace □Une politique □Un risque □Aucune réponse 1

3. Quel est l'élément principal du carré de Polybe ?

□La permutation des colonnes □Les coordonnées ligne-colonne

□Le décalage alphabétique □Aucune réponse 1

4. Le principe de Kerckhoffs affirme que :

□La sécurité dépend du secret de l'algorithme □L'algorithme doit être confidentiel

□La sécurité dépend uniquement de la clé □Aucune réponse 1

5. L'indice de coïncidence permet de :

□Déterminer une substitution □Déterminer la probabilité d'une répétition 1

□Calculer le PGCD des distances □Identifier la clé secrète

6. L'effet d'avalanche fait référence à :

□La diffusion des clés □La substitution directe □La substitution □Aucune réponse 1

7. La confusion est assurée par :

□Transposition □Hachage □Compression □Aucune réponse 1

8. Le mode CBC utilise :

□Un vecteur d'insertion □Une signature électronique

□Un vecteur d'initialisation □Un hachage SHA 1

9. Le rejeu consiste à :

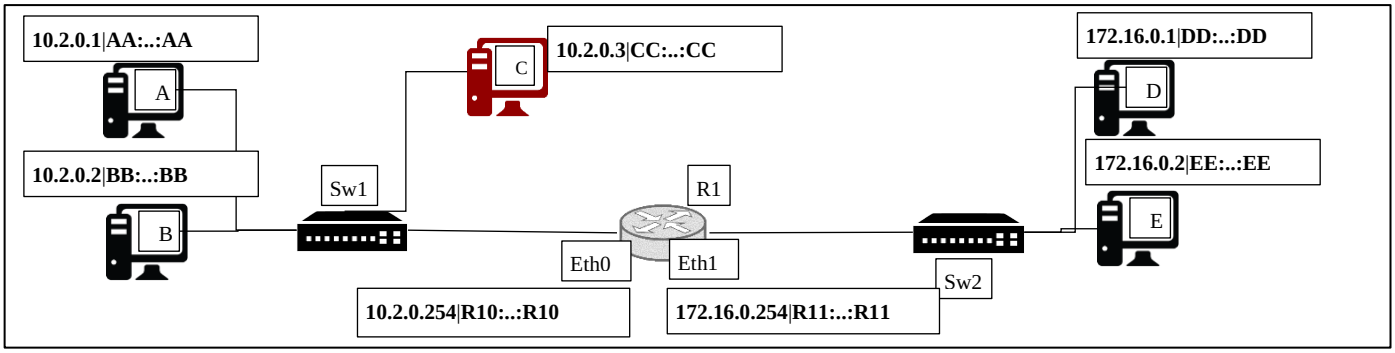
□Capturer et renvoyer un message légitime □Réinitialiser un système cible

□Répéter un mot de passe jusqu'au succès □Répliquer une base de données 1

10.Une attaque de mascarade est liée à :

□L'analyse du trafic □L'usurpation d'identité □L'effacement des traces □La destruction de disques

Exercice 02 (5.5 points) : Soit le réseau câblé suivant : 1



Apres installation du réseau, les machines A, B et D ont échangé des communications respectives.

1) Donner les tables ARP des machines A, B ,D et R1 après ces échanges.

Table ARP « A »		Table ARP « B »		Table ARP « D »		Table ARP « R1 »	
IP	**MAC** 0.25	**IP**	**MAC**	**IP**	**MAC**	**IP**	**MAC**
10.2.0.2	BB :..... :BB	10.2.0.1	AA :... :AA	172.16.0.254	R11 :... :R11	10.2.0.1	AA :... :AA
10.2.0.254	R10 :... :R10	10.2.0.254	R10 :... :R10	.....	.....	10.2.0.2	BB :..... :BB
.....	.....	.....	.....	.....	.....	172.16.0.1	DD :... :DD

La machine C souhaite intercepter l'ensemble du trafic circulant sur le réseau connecté à l'interface eth0, en réalisant une attaque de type ARP spoofing à l'aide de paquets ARP Reply.

2) Donnez les paquets ARP Reply que la machine C doit envoyer pour intercepter le trafic échangé entre les machines A et R1, en précisant tous les champs ?

ARP	IP Src : 10.2.0.1 MAC src:CC:…:CC IP dst :10.2.0.254 MAC dst :R10:…:R10
ETH	MAC src:CC:…:CC MAC dst :R10:…:R10

0.25 0.25 0.25

ARP	IP Src : 10.2.0.254 MAC src: CC:…:CC IP dst : 10.2.0.1 MAC dst :AA:…:AA
ETH	MAC src:CC:…:CC MAC dst :AA:…:AA

3) Citez deux contremesures pouvant être mises en œuvre pour se protéger contre cette attaque ?

a) Utiliser des entrées ARP statiques 1

b) Activer les Port Security sur les switches. 1

Exercice 03 (4.5 points)

Un site web propose un moteur de recherche permettant de trouver les différentes entreprises qui offrent des emplois. Lors de l'utilisation de ce formulaire de recherche, l'URL affichée dans le navigateur est la suivante : ***emploisjeunes.com/rechercher.php?search=numidex.*** La page de résultats reproduit l'affichage du nom de l'entreprise recherchée ainsi qu'une liste des offres d'emploi correspondantes.

1. Comment un attaquant doit procéder pour vérifier si le site web est vulnérable à une attaque XSS ? Justifiez.

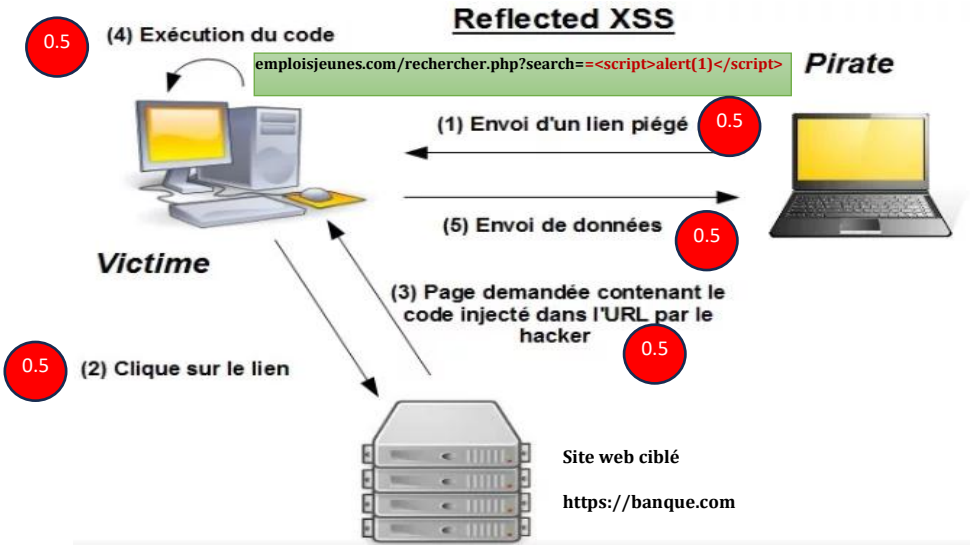
I 'attaquant commence par écrire dans le champ de recherche (ou dans l'url dans le paramètre ***search***) un script javascript de type <script> alert(1)</script>.
emploisjeunes.com/rechercher.php?search=<script> alert(1)</script> 1

Si à l'affichage de la page le navigateur exécute le code javascript et une alerte 1 est affichée alors le site est vulnérable. 0.5

2. Si le site est vulnérable, quel est le type de cette attaque XSS ?

XSS réfléchi. 0.5

3. Donnez le schéma global qui représente les étapes de cette attaque. (Numérotez les étapes)



0.5 0.5 0.5 0.5 0.5

Question bonus :

Le pirate lance un ARPSpoof comme suit: [root@pirate -> ~]$ arpspoof -t 10.15.2.171 10.0.0.1
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f
0:0:86:35:c9:3f 0:60:8:de:64:f0 0806 42: arp reply 10.0.0.1 is-at 0:0:86:35:c9:3f

Analysez les lignes ci-dessus et associez chaque IP/MAC à l'une des machines suivantes : la machine pirate, la machine cible, la machine usurpée

IP machine cible : *10.15.2.171* 0.25	Mac cible : *0:60:8:de:64:f0* 0.25
Mac machine pirate : *0:0:86:35:c9:3f* 0.25	Ip machine usurpée : *10.0.0.1* 0.25

Bon courage.