Examen

Concepts de base de la sécurité

Classes: 1ère année SSICE
Session principale
Documents autorisés

N. B :

- Les réponses doivent être reportées sur les pages 5 et 6.

Exercice 1 [2.5pts]:

1) Soit le bout de code BC1 suivant implémenté au niveau d'un serveur. Ce code est vulnérable à quel type d'attaque ? Donner deux conséquences possibles.

BC1 :

```
Void mycopy (char * input) {
char buffer[20];
strcpy(buffer,input);
}
int main(int argc, char * argv[]) {
    mycopy(argv[1]) ;
}
```

2) Soit le bout de code BC2 suivant implémenté au niveau d'un serveur. Ce code est vulnérable à quel type d'attaque ? Comment peut-on alors l'améliorer pour le rendre sécurisé?

BC2 :

```
$login = Request.Form("login")
$password = Request.Form("password")
SELECT * FROM users WHERE Login=$login AND Password=$password
```

Exercice 2 [2.5pts]:

1) Peut-on faire du filtrage au niveau de la couche liaison ? Expliquer?
2) Lequel est le plus gourmant en temps CPU, le filtrage niveau réseau ou le filtrage niveau application ? Expliquer ?
3) Expliquer comment un firewall « statefull » peut filtrer certains paquets sans consulter les règles de filtrage qu'il implémente ?
4) Soit une entreprise possédant un très grand parc informatique. Expliquer pourquoi il est inadéquat d'implémenter la politique de filtrage de cette entreprise dans son routeur par défaut ? proposer une solution ?

Exercice 3 [5pts]:

La chaine de télévision CHTV décide de diffuser, en plus des bulletins quotidiens destinés au grand public, des bulletins d'informations personnalisés qui ne doivent être joué que par les abonnés. Vu que la diffusion hertzienne permet à des attaquants d'écouter librement les émissions de CHTV ou d'émettre sur son canal, les journalistes de CHTV sont préoccupés par la possibilité que la chaine «Pirate TV» diffuse de fausses informations sur le canal de leur chaine.

1. Pour se protéger contre la diffusion de fausses informations «Pirate TV», «CHTV» applique la clé privée kpriv1 à tous ses bulletins d'informations. C'est à dire qu'elle émet le message {bulletin}_kpriv1 (bulletin chiffré avec kpriv1). La technique de chiffrement utilisée est asymétrique ce qui permet de distribuer la clé publique kpub1 à certains intervenants. Tous les récepteurs doivent pouvoir vérifier que le bulletin a bien été émis par «CHTV». Nous supposons que les intervenants appartiennent aux 4 ensembles disjoints : «Maman FM», Abonnés, «Pirate FM», Non- abonnés. A quels intervenants faut-il distribuer la clé kpriv1 ? à quels intervenants faut-il distribuer kpub1 ? justifier votre réponse ?

2. Pour assurer que seuls les abonnés peuvent recevoir les bulletins personnalisés, CHTV, utilise la clé symétrique ksym2, c'est à dire qu'elle émet le message {bulletin spécialisé}_ksym2 (le <bulletin spécialisé chiffré avec la clé ksym2). A quels intervenants faut-il distribuer la clé ksym2? Expliquer ?

3. Chaque mois, CHTV souhaite distribuer la clé ksym2 aux abonnés par le canal hertzien. elle propose d'envoyer à chaque abonné ayant payé son abonnement le message suivant {ksym2}_kpriv1 (ksym2 chiffré avec kpriv1). Pourquoi ce protocole est incorrect ? proposer une correction?

4. Les techniques de protection préconisées précédemment ne sont valides que si l'on fait l'hypothèse que les intervenants ne peuvent pas deviner la valeur des clés utilisées. Dans cette partie, nous supposons que des intervenants malveillants tentent de deviner les clés en essayant toutes les valeurs possibles. Pour une clé codée sur N bits, il y a 2^N valeurs possibles à essayer. Nous supposons qu'un attaquant peut essayer jusqu'à 2^20 clés par seconde (a peu près un million de clés par seconde). En pratique, les attaquants trouvent la bonne clé en essayant seulement la moitié de toutes les valeurs possibles. CHTV souhaite changer la valeur de sa clé kpriv1 tous les 2 ans (2^26 secondes). Déterminer la taille minimale de la clé kpriv1 pour qu'elle ne soit pas découverte par un attaquant durant deux années ?

Exercice 4 [10pts]:

La figure suivante décrit l'architecture d'un réseau local d'une entreprise. Les serveurs www (tcp/80), ftp (tcp 20 et 21) dns (udp/53) et smtp (tcp/25) sont publics. Le routeur interne se charge de translater les adresses privées des utilisateurs internes vers l'adresse 200.1.1.10

Soient les trois politiques suivantes :

P1 : permettre aux utilisateurs sur Internet de communiquer avec les quatre serveurs locaux.

P2 : permettre aux utilisateurs locaux (réseaux 10.10.0.0/24 et 200.1.1.0/28) d'accéder aux serveurs web, smtp et dns sur Internet

P3 : permettre aux utilisateurs locaux (réseaux 10.10.0.0/24) d'accéder aux serveurs locaux

1) Donner le nombre total de règles à implémenter pour chaque politique en précisant dans quel routeur doit-on implémenter ces règles?
2) Donner les règles de filtrages (répondants aux trois politiques P1, P2 et P3) à appliquer aux paquets entrant par l'interface E1 du routeur périphérique en se limitant aux critères suivants:

Adr IP Source	Adr IP destination	Protocole	Port source	Port dest	Action

3) Déterminer et corriger les deux anomalies existantes dans les règles de filtrage suivantes implémentées au niveau du routeur périphérique

N°	@IP source	@IP dest	Port source	port dest	protocole	ACK=1	Action
1	200.1.1.14/28	toutes	>1023	~~80~~ tous	TCP	*	Autoriser
~~2~~	~~200.1.1.0/28~~	~~toutes~~	~~>1023~~	~~80~~	~~TCP~~	~~*~~	~~Autoriser~~
3	200.1.1.11/28	toutes	>1023	80	TCP	*	Bloquer

4) Soient les règles de filtrage suivantes implémentées au niveau du routeur périphérique
   a. Donner la politique correspondante aux règles {1,2} et aux règles {3,4}
   b. Traduire ces règles en utilisant des ACL Cisco et les affecter aux interfaces adéquates

N°	Interface Entrée	Interface sortie	Adr IP source	Adr IP destination	Protocole	Port Source	Port dest	Action
1	E0	E1	200.1.1.0	toutes	TCP	> 1023	80	Accepter
2	E1	E0	toutes	200.1.1.0	TCP	80	> 1023	Accepter
3	E1	E0	toutes	200.1.1.14	TCP	80	>1023	Accepter
4	E0	E1	200.1.1.14	toutes	TCP	>1023	80	Accepter

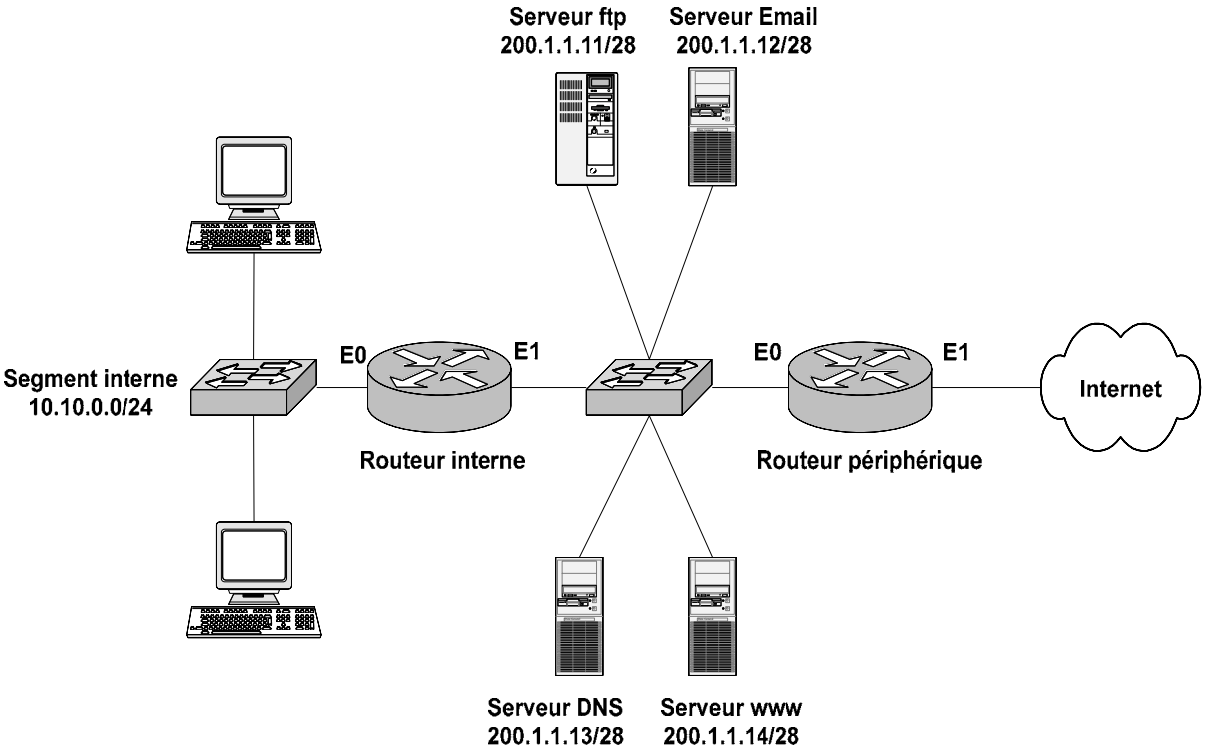

Figure 1 : architecture d'un réseau local

Université de Tunis Elmanar — Section : — A.U. : 2011/2012

ISI

Module : **Concepts de base de la sécurité**

Classe : 1SSICE

Session : **Principale**

Signatures des Surveillants

Nom : …… Prénom :……..

N° CIN : …….

N° d'inscription : ……

Signature de l'étudiant

Date :…/…/2012 Salle n° :……. Place n° :……..

Examen de : … Concepts de base de la sécurité …

Documents autorisés

Appréciations du correcteur

Exercice 1 :

1)	Attaque :…**buffer overflow**…… Conséquence 1 :…… **arrêt de l'application correspondante**……. Conséquence 2 :…… **injection d'un code malicieux**…….
2)	Attaque :… **SQL injection**…… Amélioration :**tester la présence de caractères spéciaux (#, ', /, *…etc) dans les chaines saisies avant de lancer la requête**

Exercice 2 :

1)	Réponse (cocher la bonne case) : oui ■ non □…… Explication :…**filtrage selon l'adresse physique (adresse MAC) par exemple**……. ……
2)	Réponse (cocher la bonne case) : le filtrage niveau réseau □ le filtrage niveau application ■ …… Explication :…**au niveau application, nous pouvons filtrer les données (images, texte…etc). ce filtrage prend beaucoup plus de temps que le filtrage niveau réseau qui se base seulement sur les entêtes des protocoles** ……
3)	Explication :…**un firewall statefull gère une zone mémoire qui détient les états des connexions en cours. Un paquet appartenant à l'une de ces connexions sera accepté sans lire les règles de filtrage**……. ……
4)	Explication :…**l'implémentation d'ACL dans les routeurs est adapté pour les PME sinon le routeur sera congestionné et ses performances seront médiocre**…… Solution :…**Prévoir un firewall matériel ou logiciel implémenté sur une station de travail**……

Exercice 3 :

1)	Il faut distribuer kpriv1 à : …**CHTV**……car…**se sont les seuls qui vont diffuser des informations (propriétaires de la chaîne)**……. Il faut distribuer kpub1 à : ……**tout le monde**…… car …… **kpub1 est une clé publique utilisé pour déchiffrer les informations destiné à tous**…….
2)	Il faut distribuer ksym2 à : ……**CHTV et abonnés**……car……**les informations personnalisé ne peuvent être déchiffré que par ces deux groupes**…….

NE RIEN ECRIRE ICI

✂- -

3)	Ce protocole est incorrecte car……**n'importe quel entité possède la clé publique et peut donc déchiffrer le message et retrouver ksym2**……. Solution :…chiffrer **la nouvelle clé ksym2 avec l'ancienne clé (le but n'est pas la sécurité de la clé)** ………………………
4)	**En 2 ans, un attaquant peut essayer $2^{20}*2^{26}=2^{46}$ clés. Pour une clé de taille N, le nombre de clés possible est 2^{N}. Il faut que le nombre de clés que l'attaquant peut essayer soit inférieur aux nombre de clés possible (en pratique à la moitié des clés possibles) ➔ $2^{46}<2^{N}$ ou ($2^{46}<2^{N-1}$) ➔ N=47 (ou N=48)**…………………………………………………………………. ……….

Exercice 4 :

	politique	Nombre de règles	routeurs
1)	P1	**10**	**R périphérique**
	P2	**9 ou 12**	**Les deux routeurs**
	P3	**10**	**R interne**

	IPsource	IP destination	Protocole	Port source	Port dest	Action
2)	***	***.12***	***TCP***	***>1023***	***25***	***Accepter***
	***	***.14***	***TCP***	***>1023***	***80***	***Accepter***
	***	***.13***	***UDP***	***>1023***	***53***	***Accepter***
	***	***.11***	***TCP***	***>1023***	***21***	***Accepter***
	***	***.11***	***TCP***	***>1023***	***20 ou >1023***	***Accepter***
	***	***200.1.1.0/28***	***TCP***	***80***	***>1023***	***Accepter***
	***	***200.1.1.0/28***	***TCP***	***25***	***>1023***	***Accepter***
	***	***200.1.1.0/28***	***UDP***	***53***	***>1023***	***Accepter***

3)	Anomalie 1: anomalie de……**masquage**……………entre les règles ………**1 et 3**……………………………………………. Correction :……**mettre « tous sauf 80 » pour le port destination de la règle 1**……………………………………….
	~~Anomalie 2: anomalie de………………………………entre les règles ………………………………………………………~~ ~~Correction :……~~

4) a)	Politique des règles {1,2} :…**permettre aux utilisateurs du réseau 200.1.1.0 d'accéder aux services web sur Internet** … Politique des règles {3,4} :…**permettre au serveur web local d'accéder aux serveurs web externes**……………………
4)b)	**# access list 111 permit tcp 200.1.1.0 0.0.0.15 any eq 80** …………………………………………………………… **#access list 112 permit tcp any 200.1.1.0 0.0.0.15 gt 1023** …………………………………………………………. **#int E0** ……….. **#ip access group 111 in**…………………………………………………………………………………………….. **#int E1**………………………..……………………………………………………………………………….. **#ip access group 112 in**……………………………………………………………………………………………..