Université UMBB

Licence L3 : SI

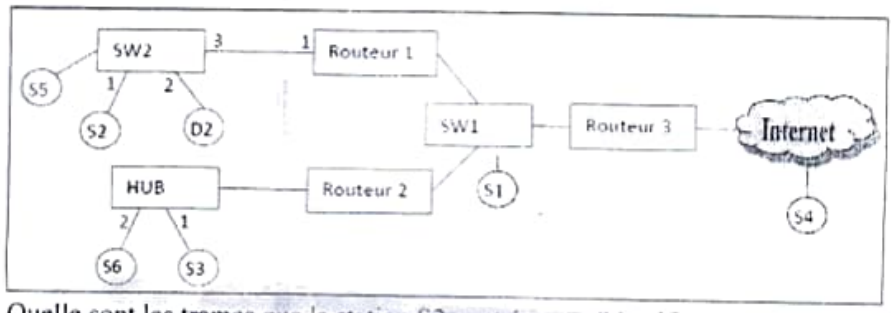
2016/2017

Test de td : Sécurité informatique

Exercice 1 : 7 pts

Répondez aux questions suivantes

1. On souhaite obtenir une double fonctionnalité de confidentialité et l'authenticité/intégrité. Pour cela, il est utile de regrouper la signature et le chiffrement. ALICE et BOB possèdent chacun un couple de clés publiques/privées, et ils ont à leur disposition deux schémas : un crypto système (E,D) et un schéma de signature (S,V). On suppose qu'Alice veut envoyer à Bob un message M à la fois signé et chiffré. Alice chiffre M avec la clé publique de Bob et génère le chiffré « c » ; puis signe « c » et génère la signature « s ». finalement, Alice envoie à BOB le couple (c,s).
   a. Quel est le danger potentiel de ce genre de méthode ? Améliorer le protocole de communication pour obtenir les mêmes fonctionnalités. **(2 pts)**
2. Soit l'architecture réseau suivante :



   a. Quelle sont les trames que la station S2 peut écouter ? justifier votre réponse. **(1 pt)**
   b. Quelles sont les stations qui peuvent être victimes de l'attaque smurf générée par le nœud S2 ? justifier votre réponse. **(1 pt)**
3. Vous examinez votre ordinateur, vous trouvez un module noyau entrain de modifier les fonctions de votre système d'exploitation. De quoi s'agit-il ? justifier votre réponse. **(1 pt)**
4. Citez et expliquez deux méthodes de détection utilisées par les anti-virus. **(2 pts)**

Exercice 2 : 13 pts

Afin de protéger les informations échangées dans le réseau, une autorité « A » décide d'installer un firewall sans-état. L'autorité ayant l'adresse IP 112.98.0.0/24 comporte trois départements : IRS, santé, et IT. Chaque département occupe un sous réseau différent comme suit : IRS occupe le sous-réseau 112.98.1.0/24, santé occupe le sous-réseau 112.98.2.0/24 et IT occupe le sous-réseau 112.98.3.0/24.

Chaque département possède un serveur web tel que : IRS possède le serveur web IRS-WEB hébergé sur @IP 112.98.5.1, Santé possède le serveur web SANTE-WEB hébergé sur @IP 112.98.5.2 et département IT possède le serveur web WEB hébergé sur @IP 112.98.5.3. L'Autorité « A » possède aussi un serveur de messagerie MESSAGE hébergé sur @IP 112.98.5.4.

Les règles d'accès aux ressources du réseau sont définies comme suit :

- Le serveur WEB doit être accessible par les utilisateurs internes et externes de l'entreprise en HTTP.
- Le serveur IRS-WEB est accessible par les utilisateurs des départements IRS et IT en HTTPS.
- Le serveur SANTE-WEB est accessible aux utilisateurs du département SANTE en SSH.
- Le serveur MESSAGE doit être accessible aux utilisateurs internes et externes de l'entreprise.

Université UMBB

Licence L3 : SI 2016/2017

Test de td : Sécurité informatique

- Le département IT peut communiquer avec le serveur WEB via une connexion TELNET.
- Le département IRS peut surfer sur n'importe quel serveur web en dehors de l'autorité.
- L'autorité « A » offre aux utilisateurs externes une application en ligne qui leurs permettre d'envoyer leurs rapports à distance. L'application connecte l'utilisateur au serveur IRS-WEB en HTTPS. Après avoir appuyer sur le bouton « submit », le serveur IRS-WEB se connecte, à l'aide d'un protocole spécial exécuté sur le port 9811, à un serveur spécial appelé IRS-DATA (avec IP 112.98. 1.2) pour transférer les informations au département IRS.

Toute communication non présentée au-dessus doit être bloquée.

Partie A : 9 pts

1. Concevez la structure du réseau de l'autorité « A », en tenant compte du fait que les utilisateurs de l'IRS ne veulent pas que le département IT puisse accéder facilement à leurs ordinateurs. Marquez exactement l'emplacement des quatre serveurs (IRS-WEB, Health-WEB, WEB et MESSAGE), ainsi que l'emplacement du (s) pare-feu (s) que vous utilisez.
2. Remplissez la table de filtrage (voir figure 1) du firewall installé à l'entrée du l'autorité « A ».
3. Remplissez la table de filtrage du firewall installé à l'entrée du sous-réseau IRS.

Name du serveur	Direction du flux	Source Address	Destination Address	Protocol	Source Port	Destination Port	Ack	Action

Figure 1 : table de filtrage

Partie B : 4pts

Un utilisateur du réseau IRS veut se connecter au site web www.example.com qui se trouve en dehors de l'entreprise. Le site web demande à ces utilisateurs de saisir leurs « NOM » dans un formulaire afin de leurs renvoyer une page personnalisée avec le nom entrée en utilisation un script PHP.

On suppose que la page renvoyée est : script langage=

```
<html>
  <head><title>Bonjour</title></head>
  <body><p>Bonjour [nom]</p></body>
</html>
```

1. Expliquer ce qui se passe dans l'exemple précèdent si l'utilisateur fait entrer le nom suivant : **(0.5pt)**

```
Berenice</p><script language="Javascript">alert("Haha")</script>
```

2. Le site est vulnérable à quelle attaque ? quel est son impact sur les utilisateurs du site web ? **(1,5 pts)**
3. Décrivez ce qui se passe lorsque « Bérénice », qui ne doute de rien, clique sur un lien envoyé par « Abélard » pointant vers l'url : **0,5pt)**

```
http://sitevulnerable.fr/index.html?nom=Berenice%3C/p%3D%3Cscript%20
language%3D%22Javascript%22%3Dalert(%22Haha%22)%3C/script%3D
```

Rappel : le caractère spécial % permet d'encoder des caractères dans des URL. %20 est un espace, %22 est un guillemet, %3C et %3D sont les symboles inférieur et supérieur.

4. Sachant qu'il n'est pas possible de transmettre un URL de plus de 256 caractères ce qui limite la taille du script inséré. Proposer une solution de détourner cette restriction. **0,5pt)**

5. Comment peut-on se protéger contre cette attaque ? (1pt)

Bon courage