Master 2 SeCReTS

Module "Sécurité Applicative"

Sécurité des Protocoles Internet

Les supports et notes de cours sont autorisés.

Chaque question est notée sur un ou deux points, et seule une réponse complète avec des explications claires et suffisament détaillées se verra accorder la totalité des points. Il est inutile de recopier le cours si on ne sait pas répondre.

1 La sécurité du DNS

1.1 A propos des zones DNS

Une entreprise spécialisée dans le développement d'outils de sécurité dépose son nom de domaine "`sectools.com`". Elle choisit également de déposer "`sectools.net`" (ce dernier étant aussi disponible). Plusieurs sous-domaines sont également créés (rattachés au nom en `.com`) :

- "`www`" et "`mail`" pour les services publics ;
- "`intranet`" pour le nommage des stations de travail appartenant à l'intranet de l'entreprise ;
- "`partners`" pour les infrastructures partagées avec les différents partenaires ;
- "`clients`" pour la relation avec les clients.

L'entreprise a pour le moment deux partenaires commerciaux et décide de déléguer à chacun d'entre-eux un nom de domaine spécifique :

- "`p1.partners.sectools.com`"
- "`p2.partners.sectools.com`"

Enfin, on considère qu'il n'y a que deux stations dans l'intranet : "`station1`" et "`station2`".

▷ *(1 point)* Représenter l'espace de nommage du DNS depuis la racine avec toutes les informations données ci-dessus.

▷ *(1 point)* Délimiter **toutes les zones DNS** présentes dans votre figure.

▷ *(3 points)* Proposer une architecture DNS et donner un schéma détaillé.

1.2 Le mécanisme de résolution

▷ *(4 points)* Expliquez ce qui se passe lorsque vous saisissez une URL dans la barre d'adresse de votre navigateur ?

Soyez très précis : indiquez ce qui se passe au niveau système et au niveau réseau en précisant à chaque stade les différentes erreurs qui peuvent survenir.

1.5 AU

1.3 A propos du contrôle d'accès basé sur le DNS

Certains serveurs web permettent de restreindre un site ou une partie d'un site web en fonction de l'adresse IP source du client. Par exemple, il existe une directive "`allow from`" dans le serveur web *Apache* fonctionnant de la manière suivante :

```
Allow from 10.1.0.0/16     # Autoriser les accès depuis un réseau de classe B
Allow from 82.68.200.19    # Autoriser les accès uniquement depuis cette IP
...
```

On peut également restreindre les accès en se basant sur le nom DNS, par exemple :

```
Allow from prism.uvsq.fr  # Autoriser les accès depuis les machines de l'UVSQ
```

Voici un extrait de la documentation pour cette fonctionnalité :

A (partial) domain-name
Example : Allow from apache.org
Hosts whose names match, or end in, this string are allowed access. Only complete components are matched, so the above example will match foo.apache.org but it will not match fooapache.org. This configuration will cause the server to perform a double reverse DNS lookup on the client IP address, regardless of the setting of the HostnameLookups directive. It will do a reverse DNS lookup on the IP address to find the associated hostname, and then do a forward lookup on the hostname to assure that it matches the original IP address. Only if the forward and reverse DNS are consistent and the hostname matches will access be allowed.

▷ *(1 point)* Comme il est précisé ci-dessus, le serveur doit effectuer **une double requête DNS** pour vérifier que le client a bien le droit d'accéder au site. Expliquez.

1.4 La notion de *Glue Record*

▷ *(2 points)* Qu'est-ce qu'un *glue record* ? Expliquez.

2 Les protocoles web

2.1 Généralités sur HTTP

▷ *(1 point)* Expliquez la différence entre l'hébergement *"basé sur l'adresse IP"* et l'hébergement *"basé sur le nom"*. Quel est l'intérêt de ce dernier ?

2.2 Etude du protocole

Etudier l'échange HTTP ci-dessous :

```
GET / HTTP/1.1
Host: www.google.com

HTTP/1.1 302 Found
Location: http://www.google.fr/
Cache-Control: private
Set-Cookie: PREF=ID=b35e4cfe9ec39d82:TM=1169466816:LM=1169466816:S=NmSN1n16PaBJZ_9v;
    expires=Sun, 17-Jan-2038 19:14:07 GMT; path=/; domain=.google.com
Content-Type: text/html
Server: GWS/2.1
Content-Length: 218
Date: Mon, 22 Jan 2007 11:53:36 GMT

<HTML><HEAD><meta http-equiv="content-type"
content="text/html;charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.fr/">here</A>.
</BODY></HTML>
```

▷ *(1 point)* Indiquer la version du protocole HTTP utilisé par le client et par le serveur
▷ *(1 point)* Quelle devrait être la prochaine requête du client ?

2.3 Le protocole SMTP

2.3.1 Les RBL-DNS

Les RBL-DNS (*Real Time Black-lists DNS*) permettent de maintenir en ligne une base de données des adresses IP sources utilisées par les spammeurs (et connues).

▷ *(2 points)* Sur quelle(s) information(s) se base le MTA pour interroger les RBLs ? Justifier votre réponse.

2.3.2 A propos des listes de diffusion

Les gestionnaires de liste de diffusion utilisent souvent un système appelé VERP (*Variable Enveloppe Return-Path*). Ce système permet, lorsqu'on envoie un message à une liste de diffusion, de positionner le champ `MAIL FROM` de l'enveloppe SMTP à une valeur différente pour chaque adresse de la liste.

▷ *(2 points)* Quel intérêt voyez-vous à cela ?

2.4 Le protocole FTP

2.4.1 Les modes passif et actif

Une session FTP a été capturée avec `tcpdump` :

```
12:56:39.859958 82.67.209.70.32587 > 204.152.191.37.21: S 4066640816:4066640816(0) win 163 ...
12:56:40.049632 204.152.191.37.21 > 82.67.209.70.32587: S 3494014340:3494014340(0) ack 406 ...
12:56:40.049694 82.67.209.70.32587 > 204.152.191.37.21: . ack 1 win 16384 <nop,nop,timesta ...
12:56:40.242135 204.152.191.37.21 > 82.67.209.70.32587: P 1:33(32) ack 1 win 46 <nop,nop,t ...
12:56:40.442035 82.67.209.70.32587 > 204.152.191.37.21: . ack 33 win 16384 <nop,nop,timest ...
12:56:41.500109 82.67.209.70.32587 > 204.152.191.37.21: P 1:11(10) ack 33 win 16384 <nop,n ...
12:56:41.688595 204.152.191.37.21 > 82.67.209.70.32587: . ack 11 win 46 <nop,nop,timestamp ...
12:56:41.688778 204.152.191.37.21 > 82.67.209.70.32587: P 33:67(34) ack 11 win 46 <nop,nop ...
12:56:41.882029 82.67.209.70.32587 > 204.152.191.37.21: . ack 67 win 16384 <nop,nop,timest ...
12:56:42.391939 82.67.209.70.32587 > 204.152.191.37.21: P 11:18(7) ack 67 win 16384 <nop,n ...
12:56:42.580841 204.152.191.37.21 > 82.67.209.70.32587: P 67:94(27) ack 18 win 46 <nop,nop ...
12:56:42.581140 204.152.191.37.21 > 82.67.209.70.32587: P 94:100(6) ack 18 win 46 <nop,nop ...
12:56:42.581145 204.152.191.37.21 > 82.67.209.70.32587: P 100:130(30) ack 18 win 46 <nop,n ...
12:56:42.581215 82.67.209.70.32587 > 204.152.191.37.21: . ack 100 win 16378 <nop,nop,times ...
12:56:42.772030 82.67.209.70.32587 > 204.152.191.37.21: . ack 130 win 16384 <nop,nop,times ...
12:56:42.772131 204.152.191.37.21 > 82.67.209.70.32587: . 130:1578(1448) ack 18 win 46 <no ...
12:56:42.772864 204.152.191.37.21 > 82.67.209.70.32587: P 1578:2149(571) ack 18 win 46 <no ...
12:56:42.772914 82.67.209.70.32587 > 204.152.191.37.21: . ack 2149 win 15813 <nop,nop,time ...
12:56:42.774570 82.67.209.70.32587 > 204.152.191.37.21: P 18:24(6) ack 2149 win 16384 <nop ...
12:56:42.978623 204.152.191.37.21 > 82.67.209.70.32587: P 2149:2168(19) ack 24 win 46 <nop ...
12:56:43.172029 82.67.209.70.32587 > 204.152.191.37.21: . ack 2168 win 16384 <nop,nop,time ...
12:56:44.235549 82.67.209.70.32587 > 204.152.191.37.21: P 24:30(6) ack 2168 win 16384 <nop ...
12:56:44.423795 204.152.191.37.21 > 82.67.209.70.32587: P 2168:2216(48) ack 30 win 46 <nop ...
12:56:44.424360 82.67.209.70.27003 > 204.152.191.37.10003: S 3986369710:3986369710(0) win  ...
12:56:44.614090 204.152.191.37.10003 > 82.67.209.70.27003: S 3504699485:3504699485(0) ack  ...
12:56:44.614165 82.67.209.70.27003 > 204.152.191.37.10003: . ack 1 win 16384 <nop,nop,time ...
12:56:44.614266 82.67.209.70.32587 > 204.152.191.37.21: P 30:36(6) ack 2216 win 16384 <nop ...
12:56:44.803690 204.152.191.37.21 > 82.67.209.70.32587: P 2216:2255(39) ack 36 win 46 <nop ...
12:56:44.803840 204.152.191.37.10003 > 82.67.209.70.27003: F 353:353(0) ack 1 win 46 <nop,  ...
12:56:44.803893 82.67.209.70.27003 > 204.152.191.37.10003: . ack 1 win 16384 <nop,nop,time ...
12:56:44.804356 204.152.191.37.10003 > 82.67.209.70.27003: P 1:353(352) ack 1 win 46 <nop,  ...
12:56:44.804428 82.67.209.70.27003 > 204.152.191.37.10003: . ack 354 win 16032 <nop,nop,ti ...
12:56:44.804643 82.67.209.70.27003 > 204.152.191.37.10003: F 1:1(0) ack 354 win 16384 <nop ...
12:56:44.994779 204.152.191.37.21 > 82.67.209.70.32587: P 2255:2279(24) ack 36 win 46 <nop ...
```

▷ *(1 point)* Indiquer si le client utilise le mode passif ou le mode actif. Justifier.