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.

1.2 Le mécanisme de résolution

Soit la situation suivante :

- vous disposez d'une station sous Linux connectée à Internet ;
- le serveur DNS actuellement paramétré dans `/etc/resolv.conf` ne fonctionne pas (ou bien n'est pas accessible) ;
- vous connaissez les adresses IP de quelques serveurs DNS racines :
  - `198.41.0.4`
  - `192.228.79.201`
  - `192.33.4.12`
  - ...

Enfin, le fichier `/etc/hosts` contient juste les lignes suivantes :

```
127.0.0.1       localhost.localdomain   localhost

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
```

Votre objectif est de parvenir à consulter la page web `http://www.sectools.com/index.html` avec le navigateur de cette station de travail.

▷ *(1 point)* Lorsque vous saisissez une URL dans la barre d'adresse du navigateur, quel type d'information ce dernier doit-il récupérer dans le DNS ?

▷ *(1 point)* Que se passe-t-il si vous essayez d'accéder à l'URL indiquée ci-dessus dans l'état actuel de la configuration ? Expliquer **très clairement** en donnant les détails techniques (notamment les échanges réseaux).

▷ *(1 point)* Est-il possible de prendre l'adresse IP d'un des serveurs racines et de la paramétrer comme serveur dans le fichier `/etc/resolv.conf` ? Expliquer.

▷ *(2 points)* Expliquer **clairement** comment vous pouvez, avec le programme `host`, retrouvez l'information dont a besoin votre navigateur pour consulter la page web demandée. Expliquer chaque étape et donner les détails techniques qui vous semblent pertinents.

▷ *(1 point)* A partir de l'information obtenue lors de la question précédente, que devez-vous modifier dans la configuration pour que la page puisse enfin être ouverte dans le navigateur ?

1.3 A propos des CNAME

Comme vous le savez, les serveurs de messageries responsables de l'acheminement des mails pour un domaine sont généralement listés dans les enregistrements de type `MX` de ce domaine.

Pour vérifier ce comportement, on procède au test suivant sur un serveur de messagerie (MTA) :

- on exécute `tcpdump` pour capturer et afficher le trafic DNS transitant par l'interface réseau ;
- on demande au serveur de traiter un message à destination d'une adresse quelconque, par exemple "`contact@sectools.com`".

De manière surprenante, on se rend compte que la première requête DNS qu'affiche par `tcpdump` est une recherche sur les enregistrements de type `CNAME` pour le domaine "`sectools.com`".

▷ *(1 point)* Expliquer les raisons de cette requête ?

1.4 A propos des "*lame delegation*"

Une *lame delegation* est une erreur de paramétrage relativement fréquente dans l'infrastructure DNS, on peut même trouver une page Wikipedia spécifique pour cette erreur :

"In domain name systems, a lame delegation, also known as a lame response, is a type of error that results when a name server is designated as the authoritative server for a domain name for which it does not have authoritative data"

Concrètement, cela peut se produire lorsqu'un administrateur supprime un des serveurs DNS autoritaires pour son domaine sans en informer le parent, c'est-à-dire le responsable du domaine supérieur qui lui a délégué son nom de domaine.

▷ *(1 point)* Quels sont les problèmes occasionnés par cette erreur ?

1.5 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.

1.6 A propos de *DNS spoofing*

Les employés de la société `sectools.com` consultent leur messagerie au travers d'un webmail accessible en SSL à l'adresse `https://webmail.sectools.com/` (adresse IP `88.159.200.17`).

Dans un aéroport, un des ingénieurs de l'entreprise décide de consulter sa messagerie en attendant son vol. Il se connecte au réseau WiFi public de l'aéroport, puis lance son navigateur pour aller sur le webmail. Une boîte de dialogue apparaît, l'informant que le certificat du site n'est pas valide.

Méfiant, il décide de ne pas ignorer cet avertissement et exécute dans un terminal la commande suivante :

```
user@laptop:~$ sudo netstat -atpun
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:47308           0.0.0.0:*               LISTEN      924/rpc.statd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      872/portmap
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1275/cupsd
tcp        0      0 10.221.10.239:34903     209.85.146.102:443      ESTABLISHED 9161/firefox-bin
tcp        0      0 10.221.10.239:49471     209.85.146.102:80       ESTABLISHED 9161/firefox-bin
udp        0      0 0.0.0.0:41981           0.0.0.0:*                           924/rpc.statd
udp        0      0 0.0.0.0:111             0.0.0.0:*                           872/portmap
udp        0      0 0.0.0.0:676             0.0.0.0:*                           924/rpc.statd
```

▷ *(2 points)* Quelle interprétation pouvez-vous donner de la capture d'écran ci-dessus ? Expliquer et donner des détails techniques sur les vulnérabilités du DNS qui pourraient être à l'origine de ce problème.

2 Les protocoles web

2.1 Généralités sur HTTP

Dans une entreprise, un utilisateur mécontent fait remonter un problème au support technique car il ne parvient pas à se connecter à l'adresse `http://www.jeux-en-ligne.com/index.html`.

Le technicien prenant en charge cet appel décide d'utiliser `netcat` et de se connecter sur le port `TCP/80` du site afin d'en vérifier le bon fonctionnement.

Il procède de la manière suivante :

```
tech@support:~$ nc www.jeux-en-ligne.com 80
GET / HTTP/1.1
```

```
HTTP/1.1 400 Bad Request
Date: Mon, 13 Dec 2010 12:01:27 GMT
Server: Apache/2.0.59 (Unix) mod_ssl/2.0.59 OpenSSL/0.9.8g
Content-Length: 336
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.0.59 (Unix) mod_ssl/2.0.59 OpenSSL/0.9.8g Server at x.ovh.net Port 80</address>
</body></html>
```

▷ *(1 point)* Qu'en pensez-vous ? Est-ce la bonne méthode pour résoudre le problème ?

2.2 Authentification en HTTP

Vous disposez d'un site web hébergé chez un prestataire qui ne vous permet pas d'avoir une version SSL/TLS de votre site. Vous souhaitez restreindre certaines parties de votre site à des utilisateurs bien identifiés (par des logins/mots de passe).

▷ *(1 point)* Indiquez les solutions techniques envisageables.

▷ *(1 point)* Existe-t-il, toujours dans le même cadre, un moyen permettant d'éviter que le mot de passe de l'utilisateur circule en clair sur le réseau ?

2.3 Le protocole FTP

2.3.1 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.

2.3.2 La sécurisation des flux

Il existe un protocole appelé FTPS permettant de rajouter des extensions de sécurité au protocole FTP et notamment le chiffrement des flux avec SSL/TLS (le protocole ne change pas).

▷ *(1 point)* Donner les avantages et les inconvénients de cette solution.

3 Serveurs mandataires

3.1 Proxy HTTP

Observez la conversation HTTP suivante (extraite d'une seule connexion TCP) :

```
GET / HTTP/1.0
If-Modified-Since: Fri, 29 Oct 2010 12:29:59 GMT
If-None-Match: "216605676"
Host: moutane.rstack.org
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.13)
Gecko/20101206 Ubuntu/10.10 (maverick) Firefox/3.6.13
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Via: 1.0 proxy.bruyeres.cea.fr:3128 (squid)
Cache-Control: max-age=0
Connection: keep-alive

HTTP/1.0 304 Not Modified
Content-Type: text/html
Accept-Ranges: bytes
ETag: "216605676"
Last-Modified: Fri, 29 Oct 2010 12:29:59 GMT
Connection: keep-alive
Date: Tue, 14 Dec 2010 17:06:48 GMT
Server: lighttpd/1.4.28

GET /main.css HTTP/1.0
If-Modified-Since: Tue, 23 Mar 2010 13:33:52 GMT
If-None-Match: "3209089464"
Host: moutane.rstack.org
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.13)
Gecko/20101206 Ubuntu/10.10 (maverick) Firefox/3.6.13
Accept: text/css,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Referer: http://moutane.rstack.org/
Via: 1.0 proxy.bruyeres.cea.fr:3128 (squid)
Cache-Control: max-age=0
Connection: keep-alive

HTTP/1.0 304 Not Modified
Content-Type: text/css
Accept-Ranges: bytes
ETag: "3209089464"
Last-Modified: Tue, 23 Mar 2010 13:33:52 GMT
Connection: keep-alive
Date: Tue, 14 Dec 2010 17:06:48 GMT
Server: lighttpd/1.4.28
```

▷ *(1 point)* En observant les requêtes et les réponses, pensez-vous que la requête soit passée par un serveur proxy ? Qu'est-ce que vous pouvez apprendre sur le navigateur Web utilisé ?

▷ *(1 point)* Combien de ressources sont demandées par le navigateur ? Le serveur `HTTP` (`moutane.rstack.org`) a-t-il renvoyé les ressources correspondantes ? Si non, pourquoi ?

3.2 Proxy générique

Dans l'entreprise, un utilisateur souhaite mettre en place un client d'un protocole applicatif qui n'est supporté par aucun serveur proxy. Cependant, l'administrateur sécurité ne veut pas autoriser les connexions directes à Internet. Tous les flux réseau doivent passer par la DMZ.

▷ *(1 point)* Donnez une proposition d'architecture pour que l'utilisateur puisse mettre en place ce nouveau logiciel. En particulier, expliquez quel type de proxy pourrait être utilisé.