

Durée : 20 minutes

Documents autorisés : tous

## Examen de réseau et éléments de correction

Supposons qu'un utilisateur saisisse les commandes suivantes :

```
user$ telnet www.hotmail.com 80 > trace.txt
GET / HTTP/1.0
Host: www.hotmail.com

user$
```

L'utilisateur obtient un fichier `trace.txt` qui contient les informations suivantes :

```
Trying 157.55.43.16...
Connected to dispatch.kahuna.glbdns.microsoft.com.
Escape character is '^]'.
HTTP/1.1 302 Found
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Location: https://login.live.com/login.srf?
wa=wsignin1.0&rpsnv=11&ct=1329082185&rver=6.1.6206.0&wp=MBI&wreply=http:%2F
%2Fmail.live.com%2Fdefault.aspx&lc=1033&id=64855&mkt=en-US&cbcxt=mai&snc=1
Server: Microsoft-IIS/7.5
xxn: 65
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
Set-Cookie: KSC=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: kr=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: bsc=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: rru=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: prc=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: mt=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
Set-Cookie: DWN=; domain=.mail.live.com; expires=Thu, 01-Jan-1970 12:00:01 GMT; path=/
MSNSERVER: H: DUB111-W65 V: 16.2.3026.119 D: 2012-01-20T02:16:11
Date: Sun, 12 Feb 2012 21:29:44 GMT
Connection: close
Content-Length: 340

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="https://login.live.com/login.srf?
wa=wsignin1.0&amp;rpsnv=11&amp;ct=1329082185&amp;rver=6.1.6206.0&amp;wp=MBI&amp;wreply=htt
p:%2F%2Fmail.live.com%2Fdefault.aspx&amp;lc=1033&amp;id=64855&amp;mkt=en-
US&amp;cbcxt=mai&amp;snc=1">here</a>.</h2>
</body></html>
```

**Question 1 :** À quoi sert ce qu'a tapé l'utilisateur ?

**Réponse :** L'utilisateur a tapé une commande permettant se connecter sur le port 80 (HTTP) de

[www.hotmail.com](http://www.hotmail.com), et de sauvegarder le résultat dans un fichier nommé « trace.txt ». Ensuite, l'utilisateur a envoyé une commande HTTP pour obtenir le fichier racine (nommé « / »), en indiquant qu'il s'adressait à l'hôte [www.hotmail.com](http://www.hotmail.com).

**Remarque :** Le serveur de hotmail refuse de répondre si l'hôte n'est pas précisé, alors que cet hôte pourrait (en théorie) être connu, puisqu'il s'agit du serveur sur lequel on se connecte. Toutefois, les serveurs web peuvent héberger plusieurs sites portant des noms différents : il est alors impératif de savoir à quel site (parmi ceux hébergés) la requête s'adresse.

**Question 2 :** Expliquez le contenu de la trace. Vous pouvez vous aider des indications ci-dessous :

- Quel protocole est utilisé ? Où sont les deux parties de la réponse ? Quel type de fichier est envoyé par le serveur ?
- **Réponse :** Le protocole affiché dans la trace est le protocole HTTP. La première partie de la réponse est située avant la ligne vide (de « HTTP/1.1 » à « Content-Length : 340 ») : il s'agit de l'entête de la réponse. La deuxième partie de la réponse est située après la ligne vide (de « <html> » à « </html> ») : il s'agit du corps de la réponse. Le type de fichier envoyé par le serveur est un fichier HTML (comme l'indique la ligne « Content-Type: text/html », ou encore le fait que le fichier commence par « <html> »).
- Quel est le code de réponse du serveur ? Pourquoi n'est-ce pas le traditionnel « 200 OK » ?
- **Réponse :** Le code de réponse du serveur est 302. Ce code est un code de succès partiel (ce qui est confirmé par l'explication textuelle « Found »). Il ne s'agit pas du code 200, car la page est en fait redirigée automatiquement vers une autre page (cf la ligne commençant par « Location »), et même vers un autre protocole (en l'occurrence, HTTPS). La réponse à la dernière question donne aussi des indications sur le fait que la réponse est une redirection.  
**Remarque :** Lorsque l'on tape <http://www.hotmail.com> dans un navigateur, on peut remarquer que l'adresse tapée dans la zone d'URL change bien pour l'URL indiquée dans la réponse (éventuellement, aux paramètres près).
- Quel est le nom du logiciel serveur et sa version ?
- **Réponse :** Le nom du logiciel serveur est Microsoft-IIS. La version du serveur est 7.5.
- Est-ce que le serveur envoie des cookies ? À quoi sert le « domain » ? Est-ce que ces cookies sont expirés ?
- **Réponse :** Oui, le serveur envoie sept cookies (chacun est identifié par la ligne « Set-Cookie »). Le nom du cookie est le premier paramètre (dans la trace, aucun des cookies n'a de valeur), puis vient le domaine, puis l'expiration, puis le chemin (dans le domaine). Le domaine indique quel site a accès aux informations de ce cookie. Comme le domaine de chaque cookie est .mail.live.com, aucun site externe n'aura accès à ces cookies. La date d'expiration étant antérieure à la date actuelle, tous les cookies sont déjà expirés : ils ne seront pas sauvegardés en mémoire ou sur disque. Il s'agit probablement de cookies anciennement utilisés par le serveur web, mais à présent obsolètes.
- Quel est le lien entre les IP et noms de serveurs présents dans la trace et dans la commande ?
- **Réponse :** L'utilisateur se connecte sur le site [www.hotmail.com](http://www.hotmail.com), qui est traduit en adresse IP 157.55.43.16 (première ligne du fichier « trace.txt »). Après une requête DNS inverse (permettant d'obtenir le nom de domaine à partir de l'adresse IP, alors qu'une requête DNS standard transforme une adresse IP en nom de domaine), on se rend compte que l'adresse IP correspond à un serveur nommé dispatch.kahuna.glb dns.microsoft.com. On peut supposer que [www.hotmail.com](http://www.hotmail.com) est un alias DNS correspondant à plusieurs machines différentes : chaque client est redirigé sur l'une des machines, afin de pouvoir distribuer la charge de répondre aux requêtes HTTP sur plusieurs machines.

**Remarque :** En testant plusieurs fois le « telnet », on se rend compte que le nom du serveur ne change pas : il s'agit toujours du serveur dispatch. L'hypothèse que [www.hotmail.com](http://www.hotmail.com) est un alias DNS est donc fausse. Une deuxième hypothèse est de considérer que le serveur dispatch est un serveur web frontal, c'est-à-dire qu'il n'est pas chargé de répondre lui-même aux requêtes, mais qu'il délègue cette tâche à des serveurs secondaires (parmi une liste). Cette hypothèse est confirmée par le nom du serveur : « dispatch » signifie aussi « répartir », « distribuer ».

- **Suite de la réponse :** Il existe d'autres noms de serveurs présents dans la trace : login.live.com et mail.live.com. Ces noms de serveurs appartiennent au domaine « live.com » (qui n'est pas le même domaine que « hotmail.com » ou que « microsoft.com »). Il est toutefois très probable que ces machines soient administrées par la même entité.
- Si un navigateur web ne comprend pas la réponse « 302 Found », qu'est-ce qui sera affiché ? Est-ce une information affichée sur les navigateurs récents ?
- **Réponse :** Si un navigateur ne comprend pas la réponse « 302 Found », il va afficher le contenu du fichier HTML qui a été reçu. Ce fichier HTML est très simple : il affiche « Object moved to here », avec un lien hypertexte sur le mot « here » renvoyant sur la même adresse que l'adresse de redirection (à l'exception du fait que les caractères spéciaux, comme « & », sont échappés en HTML par « &amp; »).