TP2-1 : DNS et communication
M1-DNR2I

Gaétan Richard

11 janvier 2012

1 DNS

1.1 Champs A, AAAA et PTR

Dans toute la suite, nous utiliserons principalement la commande **host** qui permet de faire des requêtes DNS.

Dans un premier temps, trouvez à quelle(s) adresse(s) correspondent les machines suivantes :

- mike.info.unicaen.fr ;
- mail.info.unicaen.fr ;
- mail.gdr-im.fr ;
- smtp.info.unicaen.fr ;
- www.info.unicaen.fr ;
- www.unicaen.fr ;
- www.renater.fr ;
- www.google.fr.

Pour chacune des addresses IPv4, dites s'il s'agit d'une addresse publique ou privé.

À partir des ips obtenues, retrouver les noms de machines associées. Que dire de la correspondance ?

En utilisant l'option `-l`, trouver toutes les machines de la zone `etu.info.unicaen.fr` et compter leur nombre.

1.2 Champs NS

À l'aide du champ NS, trouver la suite des DNS utilisés pour trouver l'adresse de la machine `rio.etu.unicaen.fr`.

Combien de serveurs DNS possède chaque zone ?

Pour certaines réponses, à qui devrait-on s'adresser pour trouver l'adresse IP du serveur de nom de domaine ? Commenter.

Depuis l'extérieur de l'université, on obtient le résultat suivant :

```
% host www.info.unicaen.fr
```

```
www.info.unicaen.fr is an alias for panoramix.info.unicaen.fr.
panoramix.info.unicaen.fr has address 193.55.128.20
panoramix.info.unicaen.fr has IPv6 address 2001:660:7101::20
```

Commenter.

1.3 Champs CNAME

En combinant des options vues précédemment, essayer de trouver tous les alias de la machine `mail.info.unicaen.fr`.

1.4 Champs MX

Trouver quels serveurs de mails servent à envoyer des mails aux domaines :
- `unicaen.fr` ;
- `info.unicaen.fr`.

Commenter ce résultat obtenu depuis l'extérieur :

```
$ host info.unicaen.fr
info.unicaen.fr mail is handled by 10 mx.unicaen.fr.
```

Consulter le champ `TXT` de `microsoft.com`. Essayer de comprendre à quoi correspond ce champ.

1.5 Propriétaire du domaine

Trouver à l'aide de la commande **whois** le propriétaire du domaine `unicaen.fr`.
Faire de même avec `info.unicaen.fr`.
Qui est alors responsable de ce domaine.

2 Autres services

Dans la suite, on contactera directement différents services en utilisant l'utilitaire **netcat**.

2.1 Découverte de services

À l'aide de la commande **nmap**, trouver tous les services disponibles sur `mike`.
Se connecter aux service *daytime* et comprendre leur fonctionnement.

2.2 Création de service

En utilisant l'option `-l` de **netcat**, ouvrir une connexion à l'écoute sur un port bien choisi. Essayer ensuite de se connecter sur ce port à l'aide d'un autre **netcat**.

Faire de même entre deux machines distantes puis avec deux utilisateurs différents.

2.3 Un premier serveur

En utilisant la variante **nc.traditional** présente sur la machine et en utilisant l'option `-c` qui permet d'exécuter un script, lancer un premier serveur qui répond la ligne entrée en ajoutant la ligne "Echo : " avant (par rapport à **netcat**, il faut ajouter une option `-p` avant d'indiquer le numéro de port).

Écrire ensuite un serveur qui connaît les commandes suivantes :

- `QUIT` pour quitter ;
- `LIST` pour afficher la liste des fichiers dans le répertoire ;
- `HEAD` <*fichier*> pour afficher les premières lignes du fichier donné en argument.

2.4 HTTP

Créer à l'aide de netcat, un serveur "manuel" sur le port *8945* ; regarder ensuite ce qui se passe si on essaie de se connecter en demandant une page web (avec une adresse du type : `http://localhost:8945`. Écrire du html avant de fermer le serveur, que se passe-t-il ?

Essayer maintenant de créer un client "manuel" pour demander la page web du département info.

Écrire un serveur qui sur la requête (unique)

`GET` <*toto.html*> `HTTP/1.1`

renvoie le contenu du fichier <*toto.html*>.

Faites en sorte que ce serveur soit relancé lorsqu'il termine.

Essayer dans votre navigateur d'accéder à une page du type `http://localhost:` <*port*> `/` <*toto.html*> où port est la port sur lequel écoute votre serveur.

Commenter le résultat.