Examen de NFA083

Réseaux et Administration Web

22 juin 2017

3 heures

Aucun document autorisé.
Calculatrice, ordinateur et téléphone portable interdits.

Exercice 1: Protocoles Réseau *(4 points)*

On considère un réseau utilisant les protocoles suivant : IP, TCP, UDP, Ethernet.

1. Rappelez le rôle de chacun de ces protocoles ;
2. Donnez un schéma faisant apparaître à quelle couche de la pile réseau interviennent ces protocoles ;
3. Y a-t-il parmi ces protocoles des protocoles appartenant à la même couche ? Si oui, lesquels ? Pourquoi dispose-t-on de plusieurs protocoles de même niveau ?
4. La taille d'une en-tête Ethernet est de 18 octets, celle d'un paquet IP est de 20 et celle d'un datagramme UDP de 8. Si une application souhaite envoyez 1800 octets quels seront le nombre et les tailles des trames transmises sur le réseau ? (Rappel : la MTU sur un réseau Ethernet et de 1500 octets).

Exercice 2: Requête HTTP *(2 points)*

Vous souhaitez récupérer l'énoncé de l'examen de février 2014 de l'UE NFA083 sur le site Internet du département informatique du CNAM. Ce document se trouve à l'URL `http://deptinfo.cnam.fr/~taktaks/NFA083/exam-fev2014.pdf`. Cependant, le seul ordinateur dont vous disposez ne possède pas de navigateur Internet. Par contre, l'outil `telnet` y est installé. Vous décidez donc d'utiliser `telnet` pour récupérer l'énoncé.

1. Donnez la ligne de commande permettant de se connecter au site Internet du département informatique avec `telnet` ;
2. Donnez la requête HTTP qui permet de récupérer ce fichier.

Exercice 3: Système de fichiers UNIX *(4 points)*

1. À quel répertoire correspond le répertoire `~/` ?
2. Quelle est la commande permettant de renommer un fichier ? Donnez un exemple ;
3. Quelle commande doit-on écrire pour déplacer le fichier `~/fichier1.txt` vers le fichier `/tmp/fich-tmp.txt` ?
4. On veut maintenant rendre le fichier `/tmp/fich-tmp.txt` accessible en lecture et écriture à son propriétaire et à son groupe propriétaire, et en lecture à tout le monde. Quelle commande doit-on écrire ?

Exercice 4: Configuration du serveur Apache *(10 points)*

La configuration d'un hôte virtuel est la suivante :

```
<VirtualHost *:80>
 ServerName www.exemple.com
 ServerAlias exemple.com
 DocumentRoot /var/www/

 <Directory /var/www/>
  Options FollowSymlinks
  AllowOverride Options Limit
  Order allow,deny
  Allow from all
 </Directory>
</VirtualHost>
```

On cherche à comprendre la configuration de cet hôte virtuel :

1. Quelles URL permettent d'accéder à cet hôte virtuel ?
2. Où est stocké le contenu du site web ?
3. Quelle méthode de contrôle d'accès est utilisée ?
4. Quelles différences y a-t-il entre les directives `Order Allow,deny` et `Order Deny,allow` ?
5. Dans quel cas doit-on utiliser les directives `Directory`, `Files` et `Location` ? Quand doit-on préférer certaines de ces directives ?

On veut maintenant configurer l'hôte virtuel pour que lors de l'accès à `http://www.exemple.com/public`, le contenu du répertoire `public` soit listé.

6. Donnez les directives permettant d'activer cette fonctionnalité ;

On veut maintenant ajouter un répertoire `/var/www/prive` dont l'accès est protégé par mot de passe.

7. Donnez la commande UNIX permettant de créer ce répertoire ;
8. Donnez les commandes permettant de créer le fichier `/var/www/pwd/htpasswd` contenant le mot de passe `ecila` de l'utilisateur `alice` et le mot de passe `pop` de l'utilisateur `bob` ;
9. Donnez les différentes directives permettant d'activer l'authentification par *login / mot de passe* pour le répertoire `/var/www/prive` en utilisant un fichier .htaccess. Les couples *login / mot de passe* étant enregistrés dans le fichier `/var/www/pwd/htpasswd`.

Annexe

1) Commandes Apache

— `a2enmod` et `a2dismod` : commandes permettant d'activer ou de désactiver un module

— `a2ensite` et `a2dissite` : commandes permettant d'activer ou de désactiver un module

— `apache2ctl [start|stop|restart|status|fullstatus]`

— `htpasswd [-c] nom_fichier login` : ajout d'un nouveau couple login/mot de passe dans le fichier `nom_fichier`.

2) Directives Apache

2.1) Configuration d'Hôtes Virtuels

— `<VirtualHost>` : directive permettant de définir la configuration d'un hôte virtuel

— `ServerName` : indique le nom du serveur web virtuel

— `DocumentRoot` : indique le chemin où se trouvent les fichiers pour cet hôte

— `ServerAlias` : permet d'indiquer d'autre noms pour cet hôte

2.2) Conteneurs

— `<Directory /un/chemin/>` et `</Directory>` : définit des directives s'appliquant uniquement à ce répertoire et aux fichiers et sous-répertoires qu'il contient ;

— `<Files nom_de_fichier>` : définit un ensemble de directives s'appliquant uniquement aux fichiers désignés ;

— `<Location URL>` et `</Location>` : définit un ensemble de directives s'appliquant uniquement aux URLs désignés.

2.3) Directive `Options`

`None`	Désactive toutes les options
`All`	Active toutes les options SAUF `Multiviews`
`Indexes`	Permet aux utilisateurs d'avoir des index générés par le serveur si fichier index manquant (ex. `index.html`)
`FollowSymLinks`	Autorise a suivre les liens symboliques
`ExecCGI`	Autorise à exécuter des scripts CGI à partir de ce répertoire
`Includes`	Permet d'ajouter dynamiquement du contenu aux pages HTML (ex. date du jour)
`IncludesNOEXEC`	Permet d'ajouter dynamiquement du contenu mais empêche la commande `exec`
`MultiViews`	Autorise les vue multiples suivant un contexte
`SymLinksIfOwnerMatch`	Autorise a suivre les liens seulement si l'user ID du fichier (ou répertoire) sur lequel le lien pointe est le même que celui du lien

2.4) Directive `AllowOverride`

All	Gère tout ce qui est dans `.htaccess`
AuthConfig	Active les directives d'autorisations
FileInfo	Active les directives contrôlant les documents (`ErrorDocument`, `mod_mime`, `mod_alias`, etc.)
Limit	Active les directives permettant de limiter l'usage de certaines commandes HTTP
None	Ignore les fichiers `.htaccess`
Options	Active la directive `Options`

2.5) Directives `Order`, `Allow`, `Deny`

- `Order` : Définie l'ordre d'évaluation des directives
- `Allow` : Autorise les requêtes depuis les adresses spécifiées
- `Deny` : Refuse les requêtes depuis les adresses spécifiées

2.6) Directives d'Authentification

- `AuthType basic` : type d'authentification classique.
- `AuthName "Message d'information"` : affichera le texte comme invite dans la boîte de dialogue ;
- `AuthUserFile /chemin/vers/passwd` : indique où se trouvent les mots de passe ;
- `Require user userid [userid] ...` : uniquement les utilisateurs nommé ont accès à la ressource ;
- `Require group group-name [group-name] ...` : uniquement les utilisateurs appartement à un groupe nommé peuvent accéder à la ressource ;
- `Require valid-user` : tout utilisateur valide peut accéder à la ressource ;
- `Satisfy All` : la politique d'authentification et celle d'autorisation suivant les adresses sources doivent être satisfaites
- `Satisfy Any` : la politique d'authentification ou celle d'autorisation suivant les adresses sources doit être satisfaite