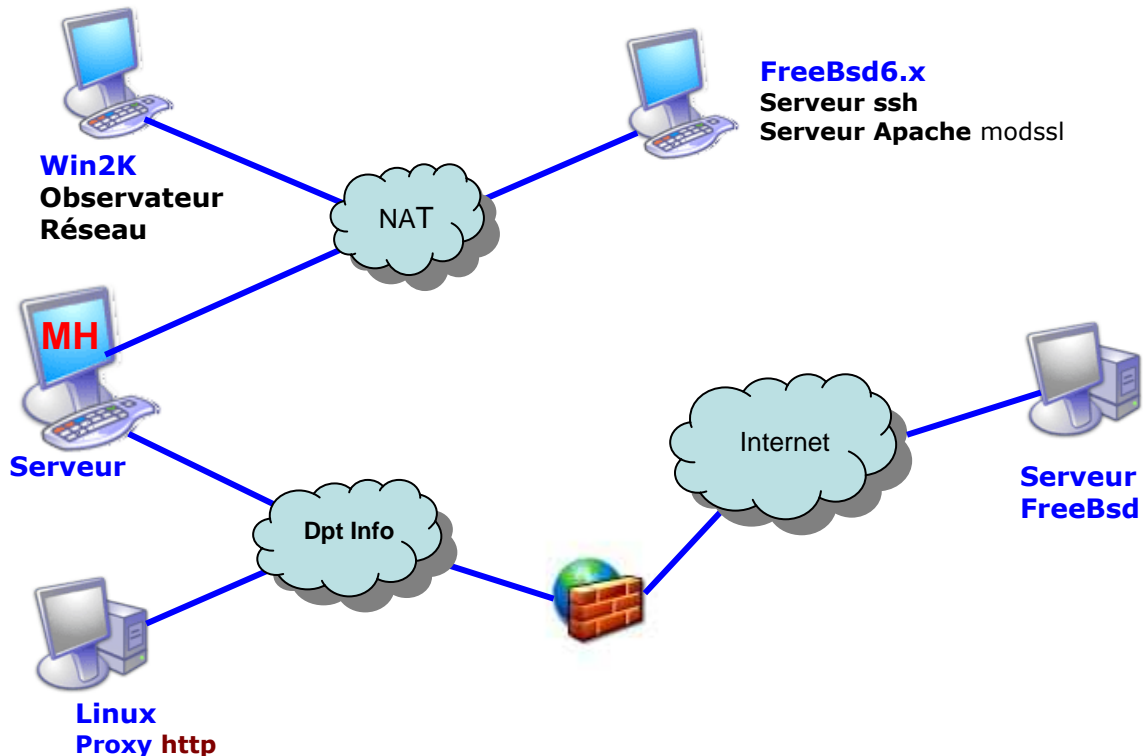


SSL : La couche Transport Sécurisée

But du TP : Mise en œuvre des mécanismes SSL (Secure Socket Layer) : ssh, openssl et https



Etape A : Configuration de ssh sur la machine FreeBSD

- Copier et configurer la machine FreeBSD6.x en mode NAT.
- Lancer la machine FreeBSD (`root/iut`)
- Configurer la machine FreeBSD : IP, DNS, hostname, lancement ssh
- Lancement et configuration de sshd (autoriser connexion root)
- Tester la connexion ssh depuis le client MH ou la MV Win98 (le client ssh peut être installé depuis www.ssh.com) Des copier/coller de texte sont désormais possible depuis le client ssh (éviteront les copies d'écran noir de VMware).

Etape B : Lancement du serveur apache sur la machine FreeBSD

- Installation du package *apache-xxx...*
 - `sysinstall`
 - Configure / Media / Http via proxy / ...
 - Configure / Packages / www → apache* ...
- Voir la configuration du serveur httpd

- rechercher httpd.conf
- consulter les ports utilisés
- rechercher le répertoire racine du serveur et la page d'accueil.
- Lancement du serveur apache (voir /usr/local/etc/rc.d)
- Installation du package *lynx-ssl-xxx...* et tester le serveur apache en local
 - **sysinstall**
 - Configure / Media / Http / ...
 - Configure / Packages / www → lynx...
- Interroger le serveur httpd avec un navigateur sur MH
- Quelle configuration faut-il mettre en place pour interroger votre serveur httpd depuis une autre MH de la salle 17 ?

Etape C : Installation de l'observateur réseau

- Copier la machine Win2K en mode NAT
- Lancer et configurer la machine Win2K
- Installer la sonde depuis www.wireshark.com
- Capturer le flux pour visualiser en clair le contenu des échanges HTTP et HTML (*Follow TCP Sessions*).

Etape D : Redirection de port avec le serveur ssh

- Configurer la redirection de port sur le client ssh de MH, pour pouvoir interroger le serveur httpd depuis MH. Est-il possible de l'interroger depuis une autre MH ?
- Capturer le flux et visualiser le contenu des échanges HTTP et HTML.

Etape E : Installation du serveur apache mod-ssl

- Installation du package *apache+mod_ssl-xxx...* (*désinstallation de la version précédente recommandée*)
- Génération d'un certificat autosigné *X.crt* et de la clé privée *X.key* avec les outils **openssl**.
- Voir la configuration du serveur httpd (mettre à jour les directives **SSLCertificateFile** et **SSLCertificateKeyFile**).
- Lancer le serveur apache sécurisé
- Interroger le en https avec lynx en local, puis avec un navigateur sur MH.
- Quelle configuration faut-il mettre en place pour interroger le serveur httpd modssl depuis un navigateur de l'Internet ?

- Capturer le flux et visualiser le contenu des échanges HTTP et HTML entre MH et MV FreeBSD (*Follow TCP Sessions*).

Dossier à rendre :

Vous rédigerez étape par étape un dossier dans lequel vous indiquerez les résultats obtenus à chaque étape, (copies d'écran, trames, schémas) et les réponses aux éventuelles questions. Le dossier sera nommé *S51_TP2_<Nom>.pdf* (ex : *S51_TP2_Muller.pdf*) et sera envoyé par mail (*S51_TP2_Muller.zip* → *Dominique.Grad@urs.u-strasbg.fr*) pour le **vendredi 11 janvier 08** au plus tard.