

TP5 : SECURITE - IPTABLES**Conception d'une zone démilitarisée**

(DeMilitarized Zone: DMZ)

Veuillez indiquer les informations suivantes :

Binômes		Nom Station ou PC	

PROLOGUE

Le but de ce TP est de concevoir une zone démilitarisée permettant à une entreprise de rendre accessible un serveur http (web) à partir d'internet. Ce serveur web est placé sur une zone neutre (DMZ), indépendante du réseau local de l'entreprise. En cas d'attaque venant d'Internet, seul le serveur http sera accessible.

Ce TP est composé de trois parties

- Configuration de la plate-forme sans mise en oeuvre de sécurité particulière
- Installation et configuration du serveur Apache
- Mise en oeuvre de la DMZ, configuration des règles de filtrage

Liste du matériel nécessaire:

3 PC avec une carte réseau (LAN, DMZ et INTERNET)

1 PC avec 3 cartes réseaux (FIREWALL)

3 câbles croisés

Systèmes d'exploitation utilisés:

Sur LAN et INTERNET: Linux/Windows

Sur FIREWALL et DMZ : Linux

1. Le contexte

1.1 Généralités sur la sécurité

- Serveur Proxy

Le terme Proxy signifie "faire quelque chose pour quelqu'un d'autre". En termes de réseau, un serveur proxy est un ordinateur qui agit pour plusieurs clients. Supposons qu'une machine A souhaite accéder à une page html située sur une machine B. Un proxy HTTP est un serveur qui reçoit la requête venant de la machine A, récupère pour A la page en question auprès de la machine B et retourne le résultat à la machine A. La machine B reçoit une requête venant du proxy et non de la machine A. Il permet donc de masquer l'adresse de A et donc de rendre invisible A pour le monde extérieur. Le proxy peut avoir un cache contenant les pages déjà demandées, de façon à ce que, si une autre machine demande la même page, la copie du cache soit retournée à la place. Ceci permet de réduire la bande passante utilisée, et d'avoir un temps de réponse plus court. En contrepartie, le proxy HTTP peut être un goulot d'étranglement si toutes les machines d'un réseau passent par le proxy HTTP pour accéder à une page web.

- Firewall

Un Firewall est une interface qui protège un réseau local du reste d'Internet. Il est conçu pour contrôler le flux des paquets en entrée/sortie en se basant sur les caractéristiques source ou destination : du réseau, du port, du type de paquet. Un firewall permet de filtrer tous types de trafic et protocoles. Différentes règles peuvent être implémentées.

- Translation d'adresse (Network Address Translation ou IP-Masquerading)

IP Masquerade est une fonction disponible sur Linux. Elle permet d'utiliser un adressage IP indépendant pour un réseau local. Cette fonction est activée sur le routeur en sortie du réseau local. Toute machine A du réseau local accédant au réseau Internet voit son adresse IP remplacée par l'adresse IP du routeur côté internet. Ainsi, A n'est pas visible d'internet, seule l'interface IP du routeur est visible.

- Reroutage de ports (port forwarding)

Le reroutage de ports permet lorsque l'on reçoit un paquet à destination d'un service (numéro de port) de rediriger la demande vers une autre machine internet. On peut utiliser cette technique par exemple:

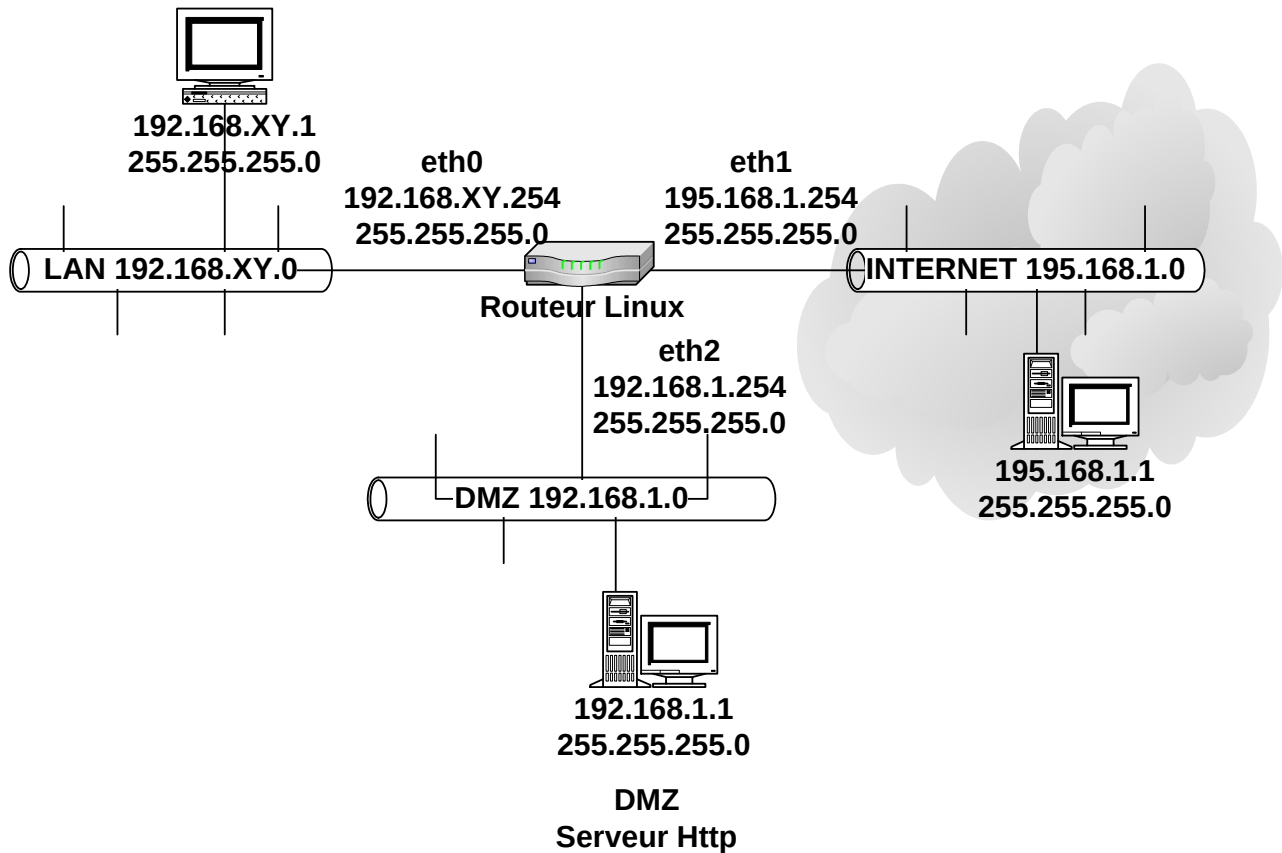
- Pour équilibrer la charge soumise à un serveur http. Il suffit de dupliquer le serveur http sur plusieurs machines et de rediriger les demandes de connexion au serveur http à tour de rôle sur les serveurs http dupliqués.
- Pour masquer la localisation d'un serveur interne. Il faut pour cela activer la translation d'adresse sur le routeur, la machine à l'origine de la demande du service aura l'impression que la réponse provient du routeur.

1.2 Plate-forme de sécurité étudiée

Cahier des charges:

Une entreprise dispose d'un réseau local (machine LAN) et souhaite rendre accessible à partir d'Internet (machine INTERNET) son serveur http (machine DMZ). L'accès entre les différentes machines est géré par le (ROUTEUR).

Le schéma suivant présente l'architecture du réseau avec le plan d'adressage:



Le réseau (LAN) contient les machines de réseau local.

Il doit permettre l'accès à Internet des utilisateurs (vers un serveur http).

Il doit permettre le **ping** d'une machine vers une machine d'Internet (message echo request)

Il doit accepter en retour la réponse du ping (echo request)

Il ne doit pas autoriser une demande de connexion à partir d'une machine venant d'Internet

Les machines du réseau LAN ne doivent pas être visible d'Internet

Les machines du réseau LAN doivent pouvoir accéder au serveur http (serveur web) de l'entreprise (sur la DMZ)

Le Réseau coté DMZ contient les machines accessibles à la fois d'Internet et du réseau LAN.

Le serveur http de l'entreprise se trouve sur ce réseau.

Il doit répondre aux requêtes du LAN et d'Internet

La machine INTERNET doit pouvoir accéder au serveur http de l'entreprise se trouvant dans la DMZ. Pour des raisons de sécurité, on ne souhaite pas que la machine INTERNET accède au serveur Web directement, avec l'adresse IP du serveur web. Pour cela, il faut mettre en place un reroutage de port pour que toute connexion arrivant sur l'interface externe de la machine ROUTEUR, vers le port standard du serveur http soit redirigée vers le serveur http interne de l'entreprise (sur DMZ). (dans la partie III)
Dans le sens (DMZ) vers (INTERNET) et (LAN) vers (DMZ), une translation d'adresse sera réalisée (dans la partie III).

2. Routage classique**2.1 Mise en oeuvre du routage classique**

Connectez-vous sur les 4 PC.

Sur les machines sous Linux, connectez vous en tant que **root** (password : **efreitr**)

Le but de cette partie est de réaliser l'interconnexion des 4 PC en configurant leurs interfaces Ethernet, en activant le routage IP sur la machine (ROUTEUR) et en configurant les tables de routage des PC sans contrôler les accès (pas de règle de filtrage particulière).

Sur le routeur (firewall)

- Vérifiez sur le routeur que les trois interfaces Ethernet sont actives.

#man **ifconfig** ou **ifstatus** ou **mii-tool**.

- Pour des raisons de sécurités, l'option routage est désactivée par défaut.

L'option **FORWARD_IPV4=no** doit être présente dans le fichier **/etc/network/options**.

Activez, dynamiquement, le routage sur la machine à l'aide de la commande :

echo "1" > /proc/sys/net/ipv4/ip_forward.

Cette commande doit être réexécutée à chaque démarrage du routeur ou après avoir relancé les services réseaux.

Q1 : Déterminez les services actifs sur la machine FIREWALL (#man **netstat** ou **nmap**).

Configurez la passerelle par défaut des pc LAN, DMZ et INTERNET. Cette adresse de passerelle correspond à l'adresse IP du ROUTEUR respectivement coté LAN, DMZ et INTERNET.

Cas d'une station Windows:

- Dans Panneau de configuration/ Réseau/ TCP-IP, vérifiez que l'adresse IP et le masque des stations sont corrects.

- Dans Panneau de configuration/ Réseau/ TCP-IP/Passerelle, indiquez la passerelle par défaut (adresse du routeur)

Cas d'une station sous Linux:

- Vérifiez la configuration de l'interface Ethernet eth0 (#man **ifconfig**).

- Consultez la table de routage du Routeur (firewall) (#man **netstat -r**). Cette table de routage est incomplète.

- Ajoutez la route par défaut à l'aide de la commande route (#man **route**).

- Puis vérifiez à l'aide de la commande **netstat** que la table de routage contient une nouvelle ligne indiquant la route par défaut.

Q2 : Quel est le contenu de la table de routage du pc ROUTEUR ?

Vérifiez à l'aide de la commande **ping** sur les pc LAN, DMZ et INTERNET que vous pouvez accéder à toutes les machines (**ping @IP**).

2.2 Configuration du serveur http

Le but de cette partie est de configurer et de lancer le serveur https de l'entreprise se trouvant sur la machine DMZ.

Q3: Quel est le port TCP d'écoute standard d'un serveur web sécurisé ? (#more /etc/services)

- Editez les fichiers
`#/etc/apache2/ports.conf` (options **Listen**) et
`#/etc/apache2/sites-available/default`,

puis modifiez le port d'écoute du serveur web pour qu'il écoute sur le **port 8080**.

Lancez le serveur web: `#/etc/init.d/apache2 reload` ou `#/etc/init.d/apache2 restart`

Remarques relatives à apache sécurisé{

*`#cd /etc/apache2/sites-available`
`# cp default ssl`*

*Editez une nouvelle fois les fichiers `#/etc/apache2/ports.conf` et `#/etc/apache2/sites-available/ssl`, puis modifiez le port d'écoute du serveur web sécurisé !
activez le site à l'aide `# a2ensite ssl` }*

Puis vérifiez qu'il est effectivement lancé: (`#man ps`). Le serveur **apache** doit être affiché.
Examiner les processus en exécution en mémoire (`#ps aux | grep apache` et `#pstree`).

Q4 : Pourquoi observez-vous plusieurs fois le serveur apache ?

A partir de la machine LAN, ouvrez un navigateur Internet et connectez-vous au serveur web.

(`http://&IPserveur:port-du-serveur`).

Q5 : Quelle page web est ouverte lorsque vous ne précisez pas de nom de page ?

(Voir le fichier `/etc/apache2/sites-available/default` sur DMZ).

Quelques Paramètres	Commentaires
DocumentRoot	Répertoire racine du site contenant les pages html
LogLevel	Caractériser le niveau d'exigence des événements à surveiller (debug, info, notice, warn, error, crit, alert, emerg)

Sur le serveur DMZ,

- Allez dans le répertoire `/var/www/index.html`;
- Copiez le fichier `index.html` en `test.html` ;
- Editez le fichier et ajoutez une ligne de texte ;
- Vérifiez ensuite que la page est bien accessible à partir dur LAN (`http://&IPserveur:port-du-serveur/test.html`).

2.3 Test de la sécurité de la configuration

A partir du pc INTERNET effectuez un ssh sur l'adresse IP de la DMZ.

La version du système d'exploitation est-elle affichée ?

Q6 : Quelle est cette version ? (`#man uname`)

L'utilitaire **nmap** est un scanner de ports qui permet de déterminer les services actifs sur une machine à distance.

Q7 : À partir du Firewall, déterminez la liste des services actifs du serveur web (`#man nmap`).

3. Mise en oeuvre de la plate-forme sécurisée

La sécurisation de la plate-forme passe par la mise en place d'un firewall sur le pc ROUTEUR et l'implémentation de règles de filtrage. Les règles de filtrage permettent de sécuriser les flux traversant le firewall en fonction de l'adresse du réseau, du port tcp source ou destination.

Pour écrire les règles, vous utiliserez la commande: **iptables**

La commande **iptables** permet de définir les règles de filtrage des flux en entrée/sortie sur le routeur. Iptables se base sur des règles, des options et des protocoles (`#man iptables`).

iptables s'appuie sur deux tables

- **La table FILTER** : est la table par défaut si aucune n'est spécifiée.
Cette table contient toutes les règles de filtrage, il existe 3 types de règles :

- **FORWARD** pour les paquets passant par le firewall ;
- **INPUT** pour les paquets entrant ;
- **OUTPUT** pour les paquets sortants.

Pour chacune de ces règles, 3 options de comportement (ou "policy") :
ACCEPT, DROP, REJECT .

policy **ACCEPT** : Pour accepter un paquet si la règle est vérifiée.
policy **DROP** : Pour rejeter un paquet sans message d'erreur si la règle est vérifiée.
policy **REJECT** : Pour rejeter un paquet en avertissant l'expéditeur (non utilisé dans le TP).

- **La table NAT** (Network Address Translation) : Elle est utilisée pour la translation d'adresse ou la translation de port.

Dans ces tables il existe deux types de règles :

- **PREROUTING** : Pour spécifier "à l'arrivée du firewall"
- **POSTROUTING** : Pour spécifier "à la sortie du firewall".

Il existe 3 targets (ou cibles) : **DNAT, SNAT ; MASQUERADE**.

Les **protocoles** supportés sont ; **tcp, udp, icmp**

Résumé de la commande:

Pour afficher l'état courant du firewall; **iptables -L**

Pour supprimer toutes les règles du firewall (sauf les règles par défaut) : **iptables -F**

Pour définir la politique par défaut; **iptables -P règle option -i interface**

Exemple : **iptables -P INPUT DROP** pour interdire par défaut tout flux en entrée.

Pour ajouter une nouvelle règle au firewall:

#iptables -A règle -i interface
-s &res/nb-bit-masque-reseau
-d &res/nb-bit-masque-reseau
-p protocole -j option

exemples :

#iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT

#iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.3.0/24 -p icmp --icmp-type echo-request -j ACCEPT

Cette commande accepte de forwarder le flux venant du réseau IP 192.168.1.0 avec le masque 255.255.255.0 (24 bits à "1") vers le réseau destination 192.168.3.0 pour le protocole icmp uniquement les paquets contenant un echo-request (il est possible d'être plus au moins laxiste en ajoutant les interfaces ou en omettant le type de paquets)

Les règles **PREROUTING** et **POSTROUTING** accompagnées des options **-t nat** permettent de faire de la translation d'adresse. Le masquage de destination (**-j DNAT**) associé au **PREROUTING** permet de masquer le destinataire du paquet alors que le masquage de la source (**-j SNAT**) associé à **POSTROUTING** permet de masquer l'émetteur du paquet.

exemple :

#iptables -t nat -A PREROUTING -i eth1 -d 195.168.1.254/24 -p tcp -m multiport --dports 80,443 -j DNAT --to-destination 192.168.1.1:3128

Cette commande permet de faire un masquage de destination (**-j DNAT**): toutes les requêtes venant de eth0 à destination de 195.168.1.254 (le routeur ici) et à destination des ports 80 et 443 sont redirigées de façon masquée vers la machine 192.168.1.1 sur le port 3128.

Attention il faut aussi ajouter une règle qui acceptera de forwarder les requêtes entre le routeur et la machine 192.168.1.1 et pour les mêmes ports et le même protocole.

Exemple :

```
#iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -j SNAT -to-source 192.168.1.254
```

permet de masquer la source des paquets provenant du réseau 192.168.3.0 en remplaçant le champs source dans l'entête IP par l'adresse 192.168.1.254

Vous allez maintenant construire un script firewall dans le répertoire /root. Le script firewall doit être exécutable (#chmod +x /root/firewall).

Editer le fichier (#vi /root/firewall)

La première ligne du fichier doit être : iptables -F

Ceci permet de vider les règles de filtrage sauf celles par défaut.

Q8: Réalisez une configuration par défaut du firewall qui rejette tout flux dans le règles input, output et forward. Donnez la syntaxe des trois lignes obtenues dans le fichier. Vérifiez maintenant que les 3 PC ne se ping plus (pc LAN vers INTERNET et DMZ)

Q9 : Quel est l'état d' iptables (iptables -L) ?

3.1 Filtrage entre LAN et DMZ

Le but de cette partie est de réaliser une translation d'adresse pour toute adresse venant du PC LAN vers le réseau de la DMZ.

Q10 : Ajouter les filtres permettant d'accepter sur l'interface du firewall coté LAN un ping venant du réseau (LAN). (Règles iptables -A sur input et output).

- Donnez les règles ajoutées.
- Exécutez votre script.
- Faites un ping entre sur le PC LAN vers l'interface 192.16.1.254 ;
- Quel résultat obtenez-vous ?

Q11 : Même question pour la liaison PC DMZ et interface du routeur coté DMZ.

Q12 : Ajoutez une règle sur le firewall permettant de faire de la translation d'adresse entre le pc LAN et DMZ (règle forward).

- Donnez la règle ajoutée.
- Exécutez votre script.

Sur le PC DMZ, lancez **wireshark** et sur le PC LAN, tapez: ping 192.168.1.1

Q13 : Donnez la séquence des trames obtenue sur le PC DMZ. Interprétez les résultats obtenus.

On souhaite maintenant permettre l'accès au serveur http pour les machines du (LAN).

Proposez les règles de filtrage **INPUT**, **OUTPUT** et **FORWARD** adaptées pour une connexion (LAN) à destination du serveur http, sur le port d'écoute sur serveur http.

Q14 : Donnez les règles de filtrage obtenues et vérifiez sur le pc LAN que cela fonctionne. (Utilisez un navigateur et connectez vous à l'url : <http://192.1681.1:8080>)

3.2 Filtrage (LAN) et (INTERNET)

Le filtrage à effectuer est analogue. Les PC du LAN ne doivent pas être directement visibles. Réalisez la configuration des règles de filtrage **INPUT**, **OUTPUT** et **FORWARD** pour accepter un ping et un accès à un serveur Web situé sur internet.

On réalisera un translation d'adresse pour toute machine ayant comme adresse source le réseau LAN et comme réseau destination le réseau INTERNET.

Q15 : Donnez les filtres obtenus.

3.3 Filtrage (DMZ) et (INTERNET)

Cette dernière partie est consacrée à la configuration entre le PC DMZ et le PC INTERNET.
La configuration est légèrement plus complexe.

Le serveur http de l'entreprise doit être accessible à partir du pc internet mais pas directement.
On ne souhaite pas autoriser les accès directs (avec l'adresse ip 192.168.1.1) depuis internet.
A partir du PC INTERNET, seul une connexion url : <http://195.168.1.254> doit fonctionner.

Pour cela, il faut mettre en place une translation d'adresse du réseau DMZ vers le réseau INTERNET et un forwarding de port pour que toute connexion http venant d'INTERNET vers la machine 195.168.1.254 soit redirigée vers la machine 192.168.1.1, vers le port d'écoute du serveur http (sur DMZ).

Q16 : Quelles sont les règles de filtrage iptables pour réaliser cette translation d'adresse ?
Indiquez les règles nécessaires.

Q17 : Utilisez la commande demandée pour réaliser le forwarding de port. Décrivez cette commande.
Testez la configuration sur le PC Internet en : Lancer Internet explorer et connectez vous au serveur <http://195.168.1.254> Vous devez normalement accéder au serveur de l'entreprise sur la DMZ.

Q18 : Analysez les trames obtenues lors de la connexion http précédente sur le pc DMZ.
Utilisez l'outil **wireshark** sur le pc DMZ.

ANNEXES APACHE2

Conventions typographiques :

signifie que c'est une commande qui doit être écrite dans le shell

Tâches à réaliser au préalable

- Se connecter en tant que root sur le serveur puis effectuer une mise à jour :

Login : **root** passwd = **efreitr**

- Connecter la station concernée par la mise à jour au réseau du laboratoire.
Demander éventuellement aux encadrants de vous assister dans cette tâche.

Avant de procéder à l'installation de tout service sur la station, il est fortement recommandé de vérifier sa configuration, notamment l'adresse IP et le nom de la station.

Procéder à la mise à jour :

```
# apt-get update      puis      # apt-get upgrade
```

Une fois le serveur à jour, l'installation des différents services nécessaires sur la station concernée peut commencer.

Attention, pensez à redémarrer les services après chaque installation ou reconfiguration :

```
# /etc/init.d/service-name restart
```

Installer apache 2

Dans le cadre du TP, il est nécessaire d'installer un serveur HTTP (Apache version 2) sur la station DMZ. Les utilisateurs du réseau Public (Internet) et Privé (LAN) pourront accéder à ce service.

```
# apt-get install apache2
```

Configuration d'apache2.conf

Editer le fichier de configuration principal d'apache2 :

```
# vi /etc/apache2/apache2.conf
```

Quelques Paramètres	Commentaires
DocumentRoot	Répertoire racine du site contenant les pages html
CustomLog	Stocker les logs du virtualhost
LogLevel	Caractériser le niveau d'exigence des événements à surveiller (debug, info, notice, warn, error, crit, alert, emerg)

Après diverses modifications des paramètres, relancez le serveur web:

```
#/etc/init.d/apache2 reload ou      #/etc/init.d/apache2 restart
```

Apache2 écoute sur le port 80 (La modification du port se fait dans le `/etc/apache2/ports.conf`)

Tester l'installation d'apache : <http://AddresselpStation>