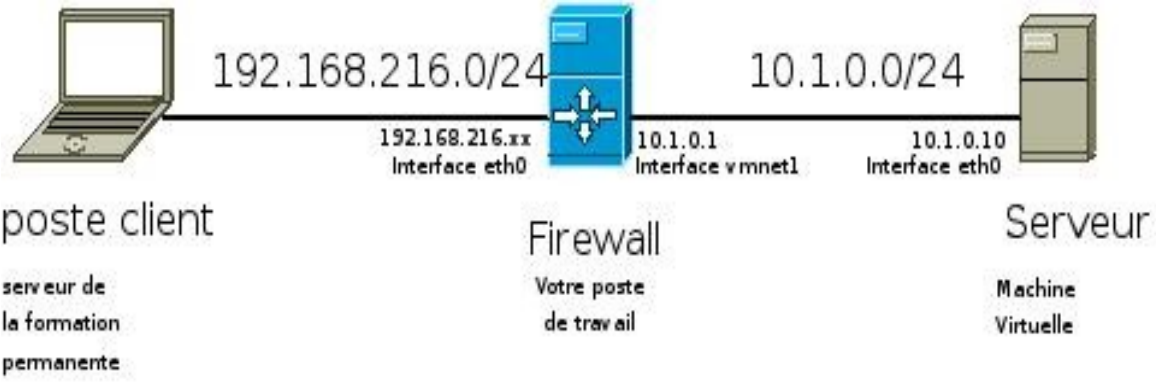
TP SECU FILTRAGE DYNAMIQUE 2006-2007

Présentation du TP

utilisation d'une machine VMWARE sous DEVIL-LINUX comme serveur
le firewall sera votre poste de travail sous Mandriva-2007
le firewall a deux cartes réseaux eth0 (interface externe) et vmnet1 (interface interne)
addresse IP du réseau interne 10.1.0.0/24 le fw en 10.1.0.1 et le serveur en 10.1.0.10



quelques indications:

iptables -D « règle » : supprime une règle
iptables -F : supprime TOUTES LES REGLES
iptables -L : liste les règles en cours

exemples : iptables -t filter -L -nv (n signifie numeric (pas de résolution dns et v verbose))

I Préparation

1 Créer le répertoire /tmp/ « votre login »
dans /tmp/« votre login » éclater le fichier ~weill/vmware-filtrage-dyn.tar.gz en **utilisateur normal**
vérifiez que l'addresse de l'interface vmnet1 est bien 10.1.0.1
vérifiez que l' « IP Forwarding » est actif sur votre firewall
regarder le script /tmp/ « votre login »/tp5/activate-nat-bidir.sh
modifier l'addresse IP_SECONDARY et éventuellement INTERFACE si ce n'est pas eth0
puis l'exécuter sur la mandriva sous ROOT
il est aussi important de vérifier qu'il n'y a pas de messages d'erreurs

2 pour lancer la machine virtuelle la commande se fait en utilisateur (PAS ROOT) est :
cd /tmp/« votre login »/tp5
```
vmplayer linux.vmx
```
elle boote sur une image iso bootcd.iso
elle sauvegarde sa config sur une disquette virtuelle floppy-config

3 configuration de la devil
login root
mot de passe: azerty

Le setup est déjà prédéfini comme dans le TP précédent sur NAT

A partir de là il vous faudra quatre terminaux :
un sur la machine virtuelle (via ssh)
un sur le firewall en root
un sur le firewall simple utilisateur
un sur srvlnx.formation.jussieu.fr pour jouer le rôle de client externe

PORTAIL DE LA FORMATION PROFESSIONNELLE AU MAROC

Télécharger tous les modules de toutes les filières de l'OFPPT sur le site dédié à la formation professionnelle au Maroc : **www.marocetude.com**

Pour cela visiter notre site www.marocetude.com et choisissez la rubrique :

MODULES ISTA

sur le firewall (votre mandriva 2007) éditer le fichier /etc/sysconfig/syslog
ajouter « -r » à la variable SYSLOGD_OPTION
ceci pour accepter les logs distants (UDP port 514)
redémarrer le service syslog :
/etc/init.d/syslog restart

Les logs de la machine virtuelle seront disponibles dans le fichier /var/log/messages de la mandriva 2007

II Filtrage sur la machine virtuelle

Normalement si le setup est bon un ping depuis le client doit fonctionner
vérifier par tcpdump sur le serveur virtuel

tout paquet venant de la machine virtuelle sort avec comme adresse l'adresse secondaire du firewall 192.168.216.1XX (1XX étant l'adresse de votre poste + 100)
tout paquet à destination de l'adresse 192.168.216.1XX est redirigé sur la machine 10.1.0.10

sur la machine virtuelle, dans /etc/init.d vous avez un script appelé « firewall.rules »
c'est ici que vous devrez mettre vos règles en commençant par commenter les 2 lignes suivantes
iptables -A INPUT -i eth0 -j LOG --log-prefix 'FIRST ACCEPT'
iptables -A INPUT -i eth0 -j ACCEPT

lisez le pour le comprendre

pour redémarrer les règles la commandes est :
/etc/init.d/firewall restart
pour supprimer toutes les règles
/etc/init.d/firewall stop

1 expliquer la règle suivante se trouvant dans firewall.rules

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

2 autoriser SSH vers la machine virtuelle uniquement depuis 10.1.0.1

3 autorisez ICMP vers la machine virtuelle de partout sauf le réseau 10.1.0.0/24

4 autoriser le ftp avec suivi de connexions depuis partout

faites des essais **depuis le firewall** en mode actif et passif
qu'en concluez vous

charger le modules de suivi de connexion du protocol ftp
sur le serveur virtuel par la commande suivante :

```
modprobe ip_conntrack_ftp
```

et refaites les tests **depuis le firewall**

Maintenant refaites le test **depuis un client externe**

en fait cela ne marche pas correctement car la partie translation d'adresse sur le firewall doit avoir un module pour pouvoir changer les adresses qui sont transmises dans les données du paquets
sur le firewall il faut charger le modules ip_nat_ftp (modprobe ip_nat_ftp)

III FILTRAGE sur le firewall

IMPORTANT DESACTIVEZ TOUTES LES REGLES DE FILTRAGE SUR LE SERVEUR VIRTUEL

dans /tmp/ « votre login »/tp5 il y a un Shell-Script « `iptables-fw.sh` »

le lire puis l'exécuter sous ROOT

Partie A
Vérifier que la machines virtuelle est bien filtrée dans les 2 sens (via ssh, nmap ou ping par exemple) tout en regardant les logs (rappel de la commande : tail -f /var/log/messages)
Quelle règle a permis ce filtrage total ?

Autoriser une connexion ssh sur la machine virtuelle 10.1.0.10 depuis l'extérieur (client externe) ainsi que sa règle de log associée (en lui donnant un nom clair pour l'identifier)
Aidez vous des logs pour comprendre les problèmes
Que concluez-vous ?

Partie B
1) Création de zone de filtrage
Pour faciliter le travail de filtrage, on va s'aider de la possibilité offerte par iptables de créer des chaînes utilisateurs (iptables -N *chaînes*).

On commence par créer :
- une chaîne INTERNET vers le réseau privé (LAN) qui est nommée : I2L
- une chaîne LAN vers l'extérieur (INTERNET) qui est nommée : L2I
- une chaîne de log pour les accès autorisés qui est nommée : LOGnACCEPT
- une chaîne de log pour les accès refusés qui est nommée: LOGnDROP

On continue par créer :
- les différentes règles de logs associées aux 2 chaînes de logs (LOGnACCEPT et LOGnDROP) précédemment créées (donner toujours un préfixe d'identification simple et clair).
- Créer les règles de forward associées aux chaînes L2I et I2L

2) Autoriser tout trafic (sans logs) du réseau privé vers l'extérieur.

3) Autoriser ssh, puis ping (avec les logs) depuis l'extérieur vers la machine virtuelle 10.1.0.10.

Ne pas oublier de mettre en place une règle de suivi de session. Pourquoi ?

4) Autoriser ftp (avec les logs) depuis l'extérieur vers la machine virtuelle 10.1.0.10.