

TP SECURITE

nmap tcpdump wireshark et filtrage iptables statique

NMAP est un scanner de ports

TCPDUMP et WIRESHARK sont des sniffers

Ce tp se fera directement sur la mandriva

le poste 216-pc01 sera utilisé comme client par tout le monde

A aucun moment du TP il est nécessaire d'être root sur 216-pc1

vérifier la présence sur votre poste des commandes nmap , tcpdump et wireshark (ex
ethereal)

si elle ne sont pas disponibles sur votre poste les installer :

urpmi tcpdump

urpmi nmap

urpmi wireshark

1 NMAP

Depuis la machine 216-pc01 faire un scan tcp de votre poste sur tous les ports tcp

vérifier que vous avez bien au moins les services ftp,ssh et web

2 TCPDUMP et WIRESHARK

lancer sur votre poste de travail la commande (Il faut etre root pour sniffer les paquets):

tcpdump -i eth0 port 21 -w /tmp/"votre login"/ftp-session.log

depuis un terminal sur la machine 216-pc01

faites un ftp vers votre machine

rentrer votre login et votre mot de passe

tapper dir

stopper la commande tcpdump (^C)

lancer : wireshark /tmp/"votre login"/ftp-session.log

clicquer sur analyse

follow tcp stream

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



The screenshot shows the homepage of MarocEtude.Com. At the top, a navigation bar contains links: HOME, LIVRES, MODULES ISTA, ANNUAIRE ECOLES, DOCTORAT, LETTRE DE MOTIVATION, NOUS CONTACTER, and SE CONNECTER. A blue arrow points to the 'MODULES ISTA' link. Below the navigation bar is a large banner with the site's logo 'Maroc Etude.Com' and the tagline 'Connaissance - Métier - Technique'. Underneath the banner are several links: Annonces Google, Emploi Maroc, Messagerie, Télécharger Un Jeu, and Maroc Annonces. The main content area features a central advertisement for MacKeeper with a '-20%' discount. To the left is a 'Connexion' section with fields for 'Identifiant' (containing 'sniper') and 'Mot de passe', a 'Se souvenir de moi' checkbox, and a 'Connexion' button. To the right is a sidebar with 'Annonces Google' and a list of links: Jeu De Jeux, Jeux Sur Internet, Ecole Ingénieur, Dépanner et configurer votre réseau à domicile, (Outil de Diagnostic), WI-FI / Ethernet, Console de jeu, Imprimante, and Messagerie. At the bottom of the page, a quote reads: "On ne jouit bien que de ce qu'on partage" [Madame de Genlis].

que constatez vous ?

3 filtrage statique

Récupérer le fichier ~weill/iptables-statique.sh

le lire

l'exécuter sur votre poste (sous root)

les messages de log se trouvent dans /var/log/messages

faite un ssh vers le poste 216-pc01

fonctionne t'il ?

quelle règles le bloque

rajouter une règle d'autorisation des flux de retour tcp avec log

(message TCP RETOUR)

refaite le ssh vers le poste 216-pc01 en vérifiant les messages de log

lancer maintenant depuis 216-pc01 un scan tcp vers votre poste

quels sont les ports ouverts ?

autoriser les demandes de connexions ssh et www vers votre poste avec log

(message SSHSRV et WWWSRV)

vérifier que cela fonctionne convenablement

autoriser les ftp (passif et actif) depuis la machine 216-pc01

on logguera chacune des règles avec un message différent