Sécurité des réseaux

28 mars 2014

Notes de cours autorisées
Durée de l'épreuve : 2h

Exercice 1. Questions de cours (réponses précises et concises de 5 lignes maximum) :

(a) Quel est le rôle du protocole *spanning-tree* (STP) ? Comment un utilisateur malintentionné peut-il tirer partie de l'activation du protocole sur un port ?

(b) Quel avantage apporte un pare-feu *stateful* ? Comment un tel pare-feu interagit-il avec des paquets IP fragmentés ?

(c) Quel est le rôle du protocole IKE ?

(d) Quel est l'objectif d'une attaque par déni de service ? Quel est l'intérêt d'une telle attaque par réflexion ?

Exercice 2. Quel est le rôle d'un NIDS ? *Snort* est un NIDS qui repose sur un catalogue de règles. En quoi ces règles sont-elles identiques à des règles de pare-feu ? En quoi sont-elles différentes ? Expliquer et interpréter les règles *Snort* suivantes :

```
alert ip $EXTERNAL_NET any -> $HOME_NET any \
(msg:"INDICATOR-SHELLCODE Linux shellcode"; \
content:"|90 90 90 E8 C0 FF FF FF|/bin/sh"; \
fast_pattern:only; metadata:ruleset community; \
classtype:shellcode-detect; sid:652; rev:15;)

alert udp any 19 <> any 7 \
(msg:"SERVER-OTHER UDP echo+chargen bomb"; \
flow:to_server; metadata:ruleset community; \
reference:cve,1999-0103; reference:cve,1999-0635; \
classtype:attempted-dos; sid:271; rev:11;)
```

Exercice 3. Vous êtes chargé de la mise en place du réseau du bureau français de la société VMold spécialisée dans la simulation numérique de moulage industriel. Le bureau français est chargé de la vente, de la formation et du support technique pour la France en lien avec la maison-mère située à New-York. Les locaux loués par la société sont précâblés et une armoire de brassage est prévue pour accueillir les équipements réseau et réaliser le brassage des prises. L'équipement réseau est déjà acheté et est composé de :

— un modem/routeur SDSL mis à disposition par le fournisseur d'accès internet (FAI) connecté d'un côté au réseau du FAI avec une adresse IPv4 fixe `13.37.13.37` et fournissant de l'autre côté des services DHCP et NAT configurables ;

— un commutateur réseau (*switch*) à 24 ports configurables avec gestion des VLAN ;

— un routeur/pare-feu/VPN muni de deux interfaces réseau (interne/externe).

Les locaux de la société accueillent trois types de machines :

— des postes de travail et imprimantes qui peuvent accéder à la fois à l'intranet de la société et à l'internet ;

— des serveurs à placer en DMZ : serveur web des pages http://www.vmold.fr/ (HTTP et HTTPS), serveur mail du domaine `vmold.fr` (SMTP et IMAP) ;

— des postes de formation avec un accès à l'internet uniquement.

Afin de permettre une meilleure communication interne, la société VMold a mis en place un accès VPN pour chacun de ses bureaux depuis ses serveurs situés à New-York. Le VPN permet d'accéder au sous-réseau `10.0.0.0/16`. Le bureau français se voit attribuer le sous-réseau `10.54.0.0/16`. La configuration du serveur VPN Cisco côté new-yorkais, d'adresse IPv4 `2.4.6.8` est la suivante :

```
sysopt connection permit-ipsec
isakmp enable outside
isakmp key mold2dlom address 13.37.13.37 netmask 255.255.255.255
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption 3des
crypto ipsec transform-set strong esp-3des esp-sha-hmac
crypto map french 10 ipsec-isakmp
crypto map french 10 match address 80
crypto map french 10 set peer 13.37.13.37
crypto map french 10 set transform-set strong
crypto map french interface outside
access-list 80 permit ip 10.0.0.0 255.255.0.0 10.54.0.0 255.255.0.0
```

(a) Dessiner un plan d'adressage logique en y précisant les adresses IP et masques des différents sous-réseaux ainsi que les adresses attribuées à chaque interface.

(b) Expliquer comment les VLANs permettent un câblage simple qui met en œuvre le plan d'adressage logique proposé.

(c) Préciser pour chacun des équipements la configuration à réaliser, en particulier :

— la configuration des VLANs sur les ports du commutateur et du routeur ;

— la configuration du VPN ;

— la configuration du pare-feu ;

— la table de routage du routeur ;

— la configuration du NAT entrant au niveau du modem SDSL ;

— la configuration du serveur DHCP au niveau du routeur ;

— la configuration de la zone DNS `vmold.fr`.