Master 2 SeCReTS 2010-2011
Module "Concepts de sécurité & réseaux"
Examen - Partie 1

Sécurité des couches TCP/IP

Les supports et notes de cours sont autorisés.

Chaque question est notée sur un ou deux points, et seule une réponse complète avec des explications claires et suffisament détaillées se verra accorder la totalité des points. Il est inutile de recopier le cours si on ne sait pas répondre.

1 La couche de niveau 2

(1 point) Rappelez le principe des attaques sur le protocole ARP. Comment feriez-vous pour mettre en évidence les attaques de ce type contre votre machine ?

2 La couche de niveau 3 / IP

2.1 Format des datagrammes IP

(1 point) Quelle est la taille maximale (en octets) de la PCI ("*Protocol Control Information*" dans le vocabulaire OSI) contenue dans un datagramme IP ?

2.2 Découpage CIDR

Une grande entreprise décide de louer un bloc d'adresses IP publiques auprès d'un opérateur. Ce dernier leur affecte le bloc `213.20.0.0/22`. L'entreprise en question possède six filiales et souhaite découper son ensemble d'adresses en sept sous-réseaux.

▷ *(2 points)* Proposer une découpage possible et donner pour chaque sous-réseau l'adresse et le masque. Il ne doit pas y avoir de gaspillage (*i.e.* toutes les adresses IP doivent être utilisées).

2.3 Les paquets ICMP

Etudier la capture réseau ci-dessous :

```
13:58:47.619 IP 132.165.66.54 > 132.165.66.55: ICMP echo request, id 0, seq 0, length 12
        0x0000:  4500 0020 0001 0000 4001 ed24 84a5 4236  E.......@..$..B6
        0x0010:  84a5 4237 0800 9399 0000 0000 3132 3334  ..B7........1234
13:58:47.620 IP 132.165.66.55 > 132.165.66.54: ICMP echo reply, id 0, seq 0, length 12
        0x0000:  4500 0020 3150 0000 8001 7bd5 84a5 4237  E...1P....{...B7
        0x0010:  84a5 4236 0000 9b99 0000 0000 3132 3334  ..B6........1234
        0x0020:  3a61 646d 3b20 7061 7373 3a20 237b 0000  :adm; pass: #{..
```

▷ *(1 point)* Remarquez-vous quelque chose de particulier ? Expliquer.

▷ *(1 point)* Selon vous, sur quelle machine la commande `tcpdump` permettant de réaliser cette capture a-t-elle été exécutée ?

3 UDP et TCP

3.1 Décodage de paquets

La capture ci-dessous représente un datagramme IP :

```
4500 003c ad0e 4000 4006 5eca 0aadf 030f  E..<..@.@.^.....
58ab c84a 804e 0016 49db 4177 0000 0000  X..J.N..I.Aw....
a002 16d0 0a11 0000 0204 05b4 0402 080a  ................
000b ec79 0000 0000 0103 0307
```

▷ *(1 point)* Quelles sont les adresses IP source et destination ?

▷ *(1 point)* Le *payload* est-t-il un paquet TCP ? Si oui, donnez le port destination.

3.2 A propos d'IP *spoofing*

*"**L'usurpation d'adresse IP** (en anglais : IP spoofing ou IP address spoofing) est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auquel il a accès."*

▷ *(1 point)* Pourquoi cette technique est généralement beaucoup plus facile à mettre en oeuvre en UDP qu'en TCP ? Expliquez.

▷ *(1 point)* L'adresse IP usurpee doit-elle remplir des conditions particulières ?

Master 2 SeCReTS 2010-2011
Module ``Concepts de sécurité & réseaux''
Examen – Partie 2

Architecture réseau

Consignes :

- 1h maximum ;
- tout document autorisé ;
- aucune communication ;
- aucun accès à un ordinateur, une station de travail, un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Architecture réseau (10 points)

Les questions portent sur le schéma joint. On peut y observer 2 zones publiques, la DMZ (serveurs WWW, DNS et SMTP) et le Proxy, ainsi que 3 zones internes (Administrateurs, Utilisateurs et Serveurs intranet).

Sur le routeur et le pare-feu, le routage entre les interfaces est activé. Sur le pare-feu, tous les types de trafic sont interdits par défaut.

Dans le reste du sujet, lorsqu'on vous demande des règles de routage, vous les exprimerez sous la forme suivante (mot-clé any pour désigner toutes les adresses IP) :

```
permit ip <ip source> <masque source> <ip destination> <masque destination>
```

Pour exprimer des règles de filtrage, vous utiliserez la syntaxe de iptables.

1. Les administrateurs doivent pouvoir accéder au port 22 (SSH) des machines de la DMZ. Décrivez les règles de routage et de filtrage à mettre en place pour autoriser ces accès.
2. On souhaite donner un accès vers Internet aux utilisateurs, en passant par le Proxy présent dans l'architecture.
   - Donnez les règles de routage et de filtrage autorisant respectivement l'accès des utilisateurs vers le proxy et l'accès du proxy vers Internet.
3. Les serveurs de la DMZ doivent être accessibles pour les clients en provenance d'Internet. Donnez les règles de filtrage correspondantes.

Master 2 SeCReTS 2010-2011
Module ``Concepts de sécurité & réseaux''
Examen – Partie 2

Architecture réseau

Consignes :

- 1h maximum ;
- tout document autorisé ;
- aucune communication ;
- aucun accès à un ordinateur, une station de travail, un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Architecture réseau (10 points)

Les questions portent sur le schéma joint. On peut y observer 2 zones publiques, la DMZ (serveurs WWW, DNS et SMTP) et le Proxy, ainsi que 3 zones internes (Administrateurs, Utilisateurs et Serveurs intranet).

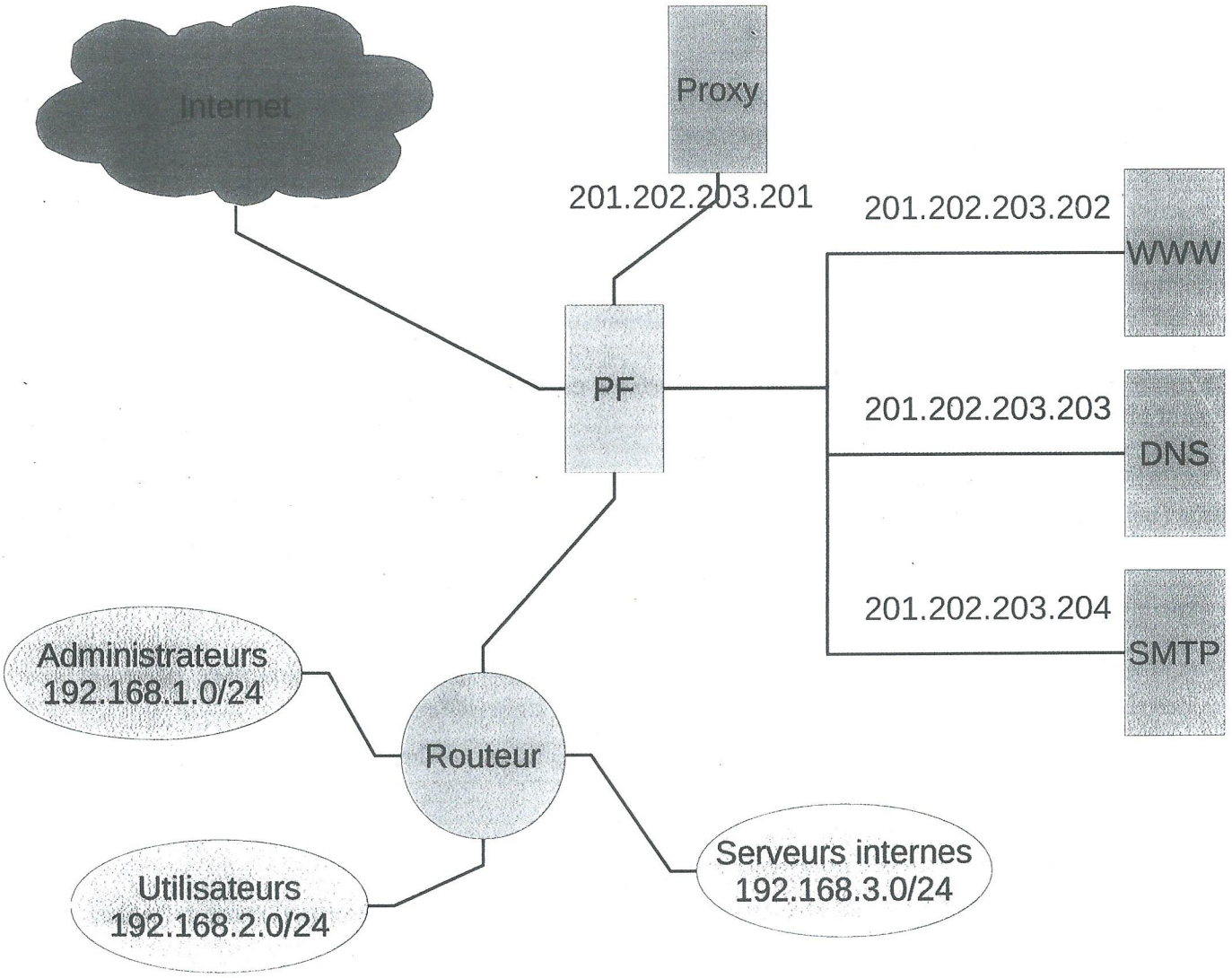
Sur le routeur et le pare-feu, le routage entre les interfaces est activé. Sur le pare-feu, tous les types de trafic sont interdits par défaut.

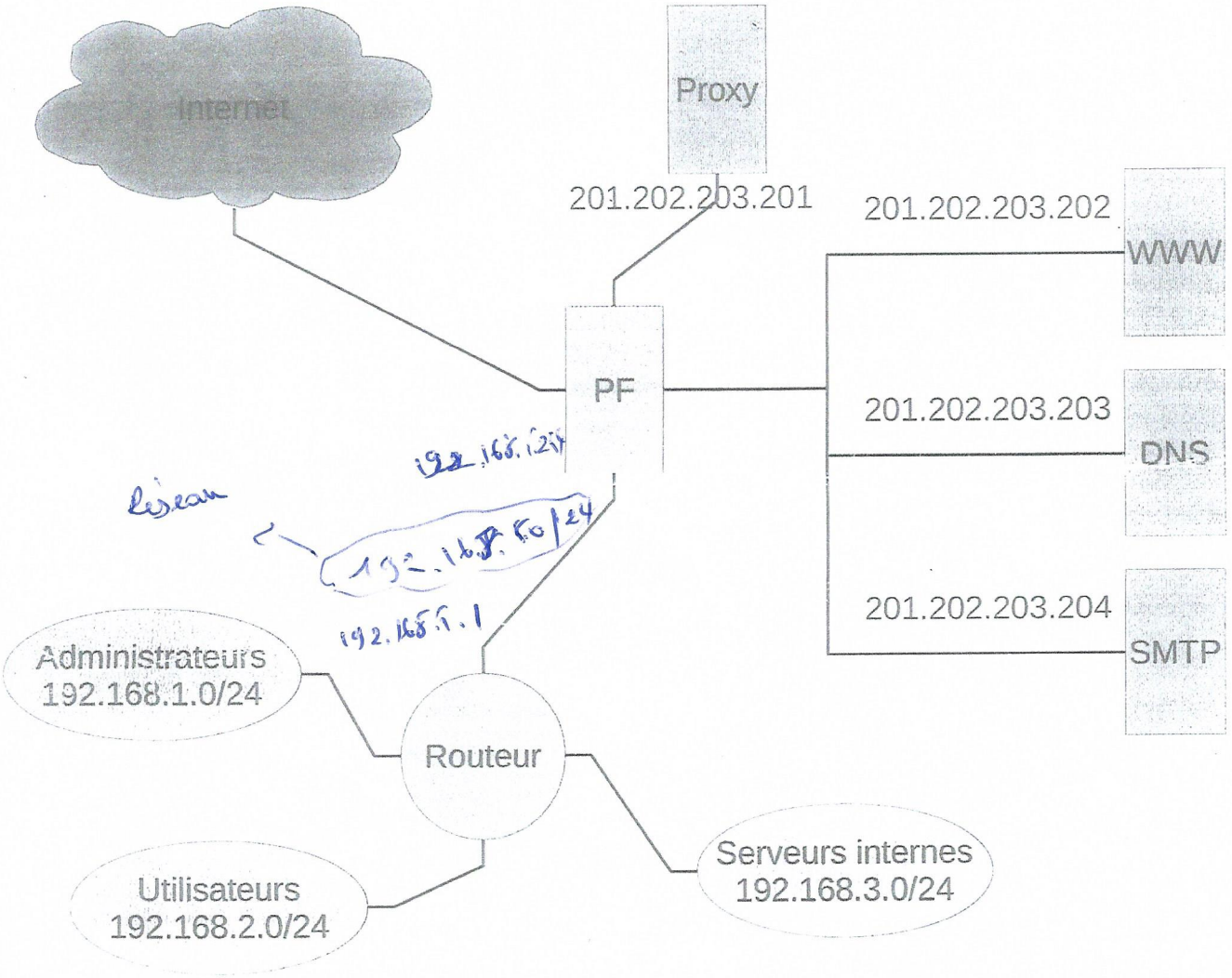
Dans le reste du sujet, lorsqu'on vous demande des règles de routage, vous les exprimerez sous la forme suivante (mot-clé any pour désigner toutes les adresses IP) :

```
permit ip <ip source> <masque source> <ip destination> <masque destination>
```

Pour exprimer des règles de filtrage, vous utiliserez la syntaxe de iptables.

1. Les administrateurs doivent pouvoir accéder au port 22 (SSH) des machines de la DMZ. Décrivez les règles de routage et de filtrage à mettre en place pour autoriser ces accès.
2. On souhaite donner un accès vers Internet aux utilisateurs, en passant par le Proxy présent dans l'architecture.
   - Donnez les règles de routage et de filtrage autorisant respectivement l'accès des utilisateurs vers le proxy et l'accès du proxy vers Internet.
3. Les serveurs de la DMZ doivent être accessibles pour les clients en provenance d'Internet. Donnez les règles de filtrage correspondantes.


Internet
Proxy
201.202.203.201
201.202.203.202
WWW
PF
201.202.203.203
DNS
201.202.203.204
SMTP
Administrateurs
192.168.1.0/24
Routeur
Utilisateurs
192.168.2.0/24
Serveurs internes
192.168.3.0/24


Internet
Proxy
201.202.203.201
201.202.203.202
WWW
PF
201.202.203.203
DNS
201.202.203.204
SMTP
Administrateurs
192.168.1.0/24
Routeur
Utilisateurs
192.168.2.0/24
Serveurs internes
192.168.3.0/24