Master 2 SeCReTS

Module "Concepts de sécurité & réseaux"

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

(3 points) Vous êtes connecté sur un réseau non sûr, par exemple un grand réseau WiFi public. Rappelez les différents risques auxquels vous êtes exposés ainsi que les moyens de protection pouvant y faire face.

2 La couche de niveau 3 / IP

2.1 Format des datagrammes IP

(1 point) Quelle est la taille maximale (en octets) des données utilisateur (*User Data* dans le vocabulaire OSI) contenues dans un datagramme IP ?

2.2 Découpage `CIDR`

Une entreprise décide de louer un bloc d'adresses IP publiques auprès d'un opérateur. Ce dernier leur affecte le bloc `203.10.8.128/25`. L'entreprise en question possède quatre filiales et souhaite découper son ensemble d'adresses en cinq 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).

3 UDP et TCP

3.1 Décodage de paquets

La capture ci-dessous représente une capture de datagrammes IP :

```
15:33:15.859680 IP 10.220.61.111.55613 > 213.186.200.1.80: Flags [S], seq 1104053741, win 14600,...
        0x0000:  4500 003c c8b5 4000 4006 8bff 0adc 3d6f E..<..@.@.....=o
        0x0010:  d5ba c801 d93d 0050 41ce 85ed 0000 0000 .....=.PA.......
        0x0020:  a002 3908 e635 0000 0204 05b4 0402 080a ..9..5..........
        0x0030:  0097 4d58 0000 0000 0103 0307            ..MX........
15:33:18.865048 IP 10.220.61.111.55613 > 213.186.200.1.80: Flags [S], seq 1104053741, win 14600,...
        0x0000:  4500 003c c8b6 4000 4006 8bfe 0adc 3d6f E..<..@.@.....=o
        0x0010:  d5ba c801 d93d 0050 41ce 85ed 0000 0000 .....=.PA.......
        0x0020:  a002 3908 e635 0000 0204 05b4 0402 080a ..9..5..........
        0x0030:  0097 4e85 0000 0000 0103 0307            ..N.........
15:33:24.875046 IP 10.220.61.111.55613 > 213.186.200.1.80: Flags [S], seq 1104053741, win 14600,...
        0x0000:  4500 003c c8b7 4000 4006 8bfd 0adc 3d6f E..<..@.@.....=o
        0x0010:  d5ba c801 d93d 0050 41ce 85ed 0000 0000 .....=.PA.......
        0x0020:  a002 3908 e635 0000 0204 05b4 0402 080a ..9..5..........
        0x0030:  0097 50de 0000 0000 0103 0307            ..P.........
```

▷ *(2 points)* Pour chacun de ces datagrammes, le *payload* est-t-il un paquet TCP ? Si oui, comment interprétez-vous cette copie d'écran.

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 usurpée doit-elle remplir des conditions particulières ?