**Réseau**

Black Hats: les méchants

Grey Hats : méchant et gentil

White Hats: les Gentils

Crakers: spécialiste pour cracker des mots de passe

Carder : pirate dans les cartes bancaire

Phreaker : pirate dans les réseau téléphonique

RSSI : le responsable de la sécurité des systèmes d’information

Attaque DoS-DDoS : un ensemble d’ordinateur qui attaque un pc qui sera saturer.

ANSSI : L'Agence nationale de la sécurité des systèmes d'information est un service français créé par décret en juillet 2009.

**Couche Appl\_Partie\_1**

Nom de domaine pleinement qualifier = FQDN

Racine = c’est le big boss par exemple

AAAA = ipv6

CNAME = un Alias, un surnom (ex : web est = à WWW)

NS = Name serveur

MX= messagerie, mail

**Le Protocol http**

Le Protocol http = Sert a transporter la page web

Dns utilise le port 53 , transforme un nom de domaine en IP

http utilise le port 80

HTTPS = port 443

FTP = port 21

Proxy = c’est un serveur qui fait la demande à notre place pour filtrer ( sécuriser les demande)

Erreur 404 veut dire que le client demande une information qui n’existe pas.

SMTP est le Protocol qui sert à envoyer un mail

POP3 et IMAP servent à relever du mail , réception d’email

POP3 = plutôt basique ( internet de l’époque ) efface le mail du serveur et le télécharge en local sur la machine, on pouvait lire nos mails sans connexion.

IMAP = accède au mail sur le serveur mais possibilité de les télécharger en local

SMB = Protocol d’IBM qui permet de partager de fichiers ou des ressources.

FTP = transfert de fichier mais plus loin, de plus longue distance

TFTP = la même que FTP mais pas sécuriser.

**Couche transport**

Il y a deux Protocol UDP et TCP

Le fait de segmenter permet qu’on puisse faire du multiplexage

**Multiplexage** = Le multiplexage est une technique qui permet de transmettre plusieurs signaux ou flux de données à travers un même canal de communication, en les combinant et en les séparant de manière à ce qu'ils puissent être utilisés indépendamment à l'extrémité de la transmission. Cela optimise l'utilisation du canal et permet d'économiser de la bande passante.

Le numéro de port identifie le service de la machine

IP + numéro de port = Socket

**Étape de session TCP**

* ACK → le champ acknowledge number est valide
* SYN → ouverture de session
* FIN → fermeture de session
* Sequence number = le numéro du premier octet de données du

segment → identifie le segment envoyé par la source.

* Acknowledgement number = le numéro du prochain octet

(segment) attendu par le récepteur.

* Segment envoyé → copié dans une file d’attente pendant une

tempo donnée.

* Si pas d’aknowledgement avant la fin de tempo → segment

Renvoyé.

* !!! Full duplex → un périphérique = émetteur et récepteur

**Je dois connaitre cela !**

Les adresses de Classe A commencent par 0xxx en

binaire, ou 0 à 127 en décimal.

• Les adresses de Classe B commencent par 10xx en

binaire, ou 128 à 191 en décimal.

• Les adresses de Classe C commencent par 110x en

binaire, ou 192 à 223 en décimal.

**Les masques par défaut**

• Le masque par défaut des adresses de Classe A

est 255.0.0.0 ou /8

• Le masque par défaut des adresses de Classe B

est 255.255.0.0 ou /16

• Le masque par défaut des adresses de Classe C

est 255.255.255.0 ou /24

**Exemple de l’architecture d’une adresse IP et de son masque**

1

Une image contenant texte, présentation, lecture, intérieur

Description générée automatiquement

2

Une image contenant texte, tableau blanc, écriture manuscrite

Description générée automatiquement

Une image contenant texte, tableau blanc, intérieur, Course

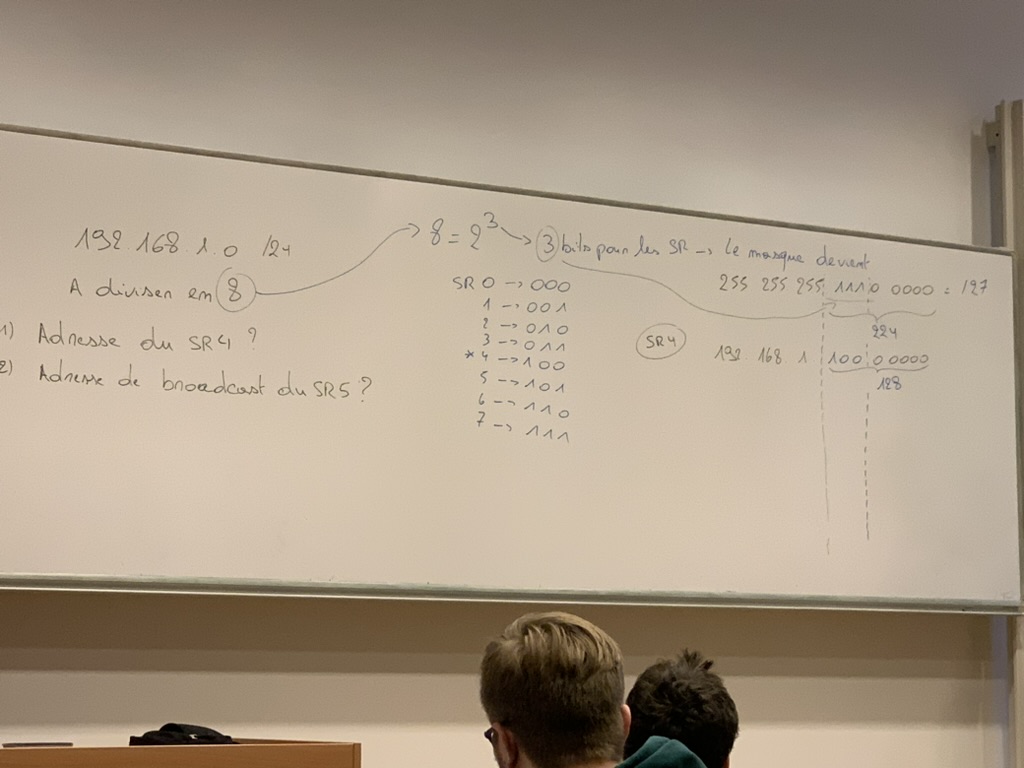
Description générée automatiquementSous Réseaux 0

Une image contenant texte, tableau blanc, intérieur, Course

Description générée automatiquementSous Réseau 2



**Sous Réseau 3**

Exercice :

Une image contenant texte, tableau blanc, écriture manuscrite, intérieur

Description générée automatiquement

