Note WireShark : Mooc.

Commande terminal et utilité :

ifconfig -a (Linux) ou ipconfig /all (Windows) : cette commande donne les informations de configuration réseau sur toutes les interfaces connectées, qu'elles soient actives ou nan.

ifconfig [nom de l'interface] : cette commande donne les informations de configuration réseau sur l'interfaces spécifie uniquement, qu'elles soient actives ou nan.

arp -a : permet d'avoir les @MAC et @IP des hôtes avec lequel vous avez échangez des trames.

Ping -> Protocoles ICMP permet de tester l'accessibilité d'une autre machine placée sur un réseau IP. Et test le temp avant d'avoir reçu la réponse de l'autre machine (round trip-time).

nslookup -> permet d'avoir l'@IP d'un cote spécifique ou le nom de domaine d'une @IP spécifique.
nslookup moodle.u-paris.fr:

```
Server:      192.168.0.254
Address: 192.168.0.254#53

Non-authoritative answer:
Name:   moodle.u-paris.fr
Address: 195.220.128.198
```

Netstat -r : elle permet d'avoir la table de routage sous windows et Linux.

Traceroute nom_de_domaine -> pour connaitre le chemin qu'emprunte ton routeur pour arrive à la passerelle du domaine.
Tracert nom_du_domaine (Windows).

Ifconfig eth0 172.24.0.2 netmask 255.255.0.0 -> modifie l'adresse IP et le masque de réseau de votre serveur linux fedora avec les valeurs 255.255.0.0.

Pour specifier une adresse IP à supprimer de ma table ARP faire ARP -d 192.168.0.0.

Positionner Wireshark en fonction des parquets souhaité : sur le serveur ou la machine cliente. (Capture active).

Commutateur permet de commuter avec l'adresse Mac des différentes stations.

4 méthodes :
- Hub(finit) : équipement physique qui permet de diffuser les trames d'un réseau donnée à toute les machines de ce réseau, permet seulement de connecter mon ordi dessus.

- Port Mirroring : Sur commutateur, (SPAN) on configure un port spécifique afin que tout ce qui transite sur un autre port ou sur plusieurs autre port soit lié sur ce port mirroring, et on se placeras sur ce port et on pourra suiffer.

- TAP : une sonde adaptée à la capture de trame (chère) et limite l'utilisation mais a l'avantage d'avoir la capacité de supporter des vitesses très élevé et capable de faire de la capture sur des médias différent comme la fibre optique.

- ARP Poisoning (déconseillé) : Il s'agit d'une attaque man and the middle de niveau, le principe est de se faire passer vis à vis du serveur pour le poste de travail et inversement et manipuler ARP et ainsi faire penser à nos machines qu'on est leurs interlocuteurs et ainsi intercepte toutes les trames. Mais il y a un problème car il s'agit en réalité d'une attaque.

Les captures de trames avec Wireshark :

click droit -> Exécuter en tant qu'administrateurs.
Le lancer et génère du trafic : Ping par exemple -> protocole ICMP.
Ping google.com -> resolution DNS.
Ping 192.168.0.1 -> réseau local.
Lancer une recherche par exemple.

Il y a alors 3 panneaux :
1) Liste des trames récoltés.
2) Les informations d'une trame lorsqu'elle est sélectionnés.
3) Caractère de la trame capturée en hexadécimal soit à l'état décimal.

Dans le 1e panneaux on a différentes colonnes :
- N° : numero de la trame.
- Time : c'est le temp écoulés depuis la première trame capturée.
- Source : @IP source.
- Destination : @IP Destination.
- Protocole : le protocole applicatif qui a été détectée.
- Info : résumer de tout ce qu'il a analyser.

Dans le 2e panneaux : on a les différents protocoles applicatifs utilisé par cette trame.
- ligne 1 : statistiques sur la trame elle-même.

- ligne 2 : début des infos sur le contenu, et niveau 1 du modèle TCP/IP.

Modèle TCP/IP :
APPLICATION : DNS, HTTP. -> les données brutes.
TRANSPORT : TCP, UDP. -> lien entre l'applicative et le système d'ex.
RESEAU/INTERNET : IP, ICMP. -> IPv4 avec champs source et destination.
ACCÈS AU RÈSEAU : ETHERNET. -> acheminement des messages et aussi contrôles d'erreurs.

Classer les protocoles selon leurs natures.

Option de Wireshark :

Menu capture -> options :
1e fenêtre : paramètres l'interface sur laquelle on capture.
2e fenêtre : sortie : sauvegarder automatiquement un fichier (format, durée du fichiers, cycle...) et le chemin de sauvegarde du fichier. (pcapng -> on peut stocker statistiques, des infos, des commentaires ...).
3e fenêtre : options :
- Option d'affichage : les deux premiers de voir les trames en temp réel et les plus récentes en priorités.
- Résolution de noms :
- Arrêter la capture automatiquement après permet de couper la trame en plusieurs petite trame et ainsi avoir une meilleure efficacité et un meilleur regard.
On peut capturés sur plusieurs interfaces en même temp.

Créer des colonnes :

Je vais dans le paquet en question -> sur le champ qui m'intéresse -> click droit -> appliquer en colonne et ensuite je peux spécifier ce champ avec les préférences.

Pour trier par colonne -> cliquer sur la colonne.

Regles de coloration :

Le bouton a cote du zoom permet de retirer tous les couleurs qui ont été prédéfinies par Wireshark, pour paramétrer une couleur je vais aller dans vue -> coloring rules ->là j'ai tout.

Pour ajouter une couleur : vue -> coloring rules -> + -> remplir les champs -> ok (coché la règles bien sûr).

(Temporaire):

Pour retrouver une coloration -> allé sur le paquet et click droit sur le l'@IP et appliquée une couleur. (Marche aussi pour une communication Web).

Ou clicker sur la trame de la conversation -> click droit -> colorier la conversation -> protocole intéresser -> choix de la couleur.

Informations d'une trames : second panneau.

On observe les différentes informations dans l'ordre des protocoles applicative TCP/IP.

1ere ligne : Frame ... :
1 : Interface ID: Interface sur laque notre trame a été capturée.
2 : Encapsulation Type: type de la trame Ethernet ...
3 : l'heure a laquelle elle a été capturée.
4 : time shift -> en general a 0 c le fuseau horaires.
5 : Epoch time : le temp au format Unix.
6 - 8 : temp pour calculer le temp de latence.
9 : Frame Length : la taille et frame Frame Number le numéro de la trame.
10 : si il est marqué ou ignoré.
11 : Protocole in frame -> tt les protocoles présent dans cette trame.

Les filtres :

creer un filtre : si un bug pendant exam alle sur Expression a cote de la barre de recherche et tt les filtres sont présent.
barre de recherche - > nom protocole (icmp (ping), http, dns...).
ip.src adresse ip source.
ip.addr = dest ou source.
opérateur logique : && ou

https.hots contains trameo pour spécifier une recherche sur un site particulier.
frame contains Linkedin -> si je veux rechercher des trames qui comportes le site Linkedin.

pour sauvegarder un filtre : le taper dans la barre de recherche et cliquer sur le marque page a gauche de la barre de recherche et je l'enregistre.

dans un DNS le flan permet de savoir si il s'agit d'une requête ou d'une question(0x0100).

Pour cherche dans une requête une chaine de caractère, un filtre d'affichage, une valeur hexa, Regular Expression -> cliquer sur la

loupe.
option : chercher dans le paquet, dans les infos, taille du paquets. @.

On peut lancer une capture avec un filtre déjà assigné : avant de lancer cliquer sur option et entrer les filtres de captures : web = port 80 / host trame.net. / net 192.168.0.0/24.

Partie 2 : Analyse de protocole.

Analyse du protocole ARP : niveau 2.

Basé sur le broadcast, Correspondance @MAC/IP.

peu de couche car niveau 2 :
ligne 1 deja analyser.
ligne 3 :
Hardware Type : Ethernet.
Protocoles : IPv4.
Harware size et protocole size.
Opcode : requête(1) ou réponses (2).
Sender Mac adresse , Sender IP , Target Mac, Target IP.

Gratuitous Arp -> révèle les doublons, ils apparaissent dans le champs Info du premier panneaux.

Analyse du protocole DNS : niveau 4.

DNS permet d'effectuer une résolution nom de machine -> @IP et inversement.

N°	TYPE	DESCRIPTION
1	A	Obtenir IPv4 a partir d'un nom.
2	NS	Serveur de nom pour la résolution.
5	CNAME	Alias d'un nom.
6	SOA	Autorité sur la zone.
12	PTR	Résolution Inverse.
15	MX	Redirection des e-mails vers un serveur SMTP.
28	AAAA	Obtenir une IPv6 a partir d'un nom.
255	ANY	Requête sur tous les enregistrements de la zone.

DNS :
Transaction ID : l'ID de la requête pour retrouver la réponse.
Flags :
Queries : Reprends l'information relative a la question comme l'@IP d'un site … en fonction du type de la requête.

Analyse du protocole DHCP : niveau 3.

DHCP permet d'allouer des adresses IP à des machines d'un réseau de manière dynamique.

Au début il n'a pas d'adresse IP (discover) d'où le 0.0.0.0 en @IP, il sera envoyé au broadcast général.
Transaction ID : identifie la demande et sera réutiliser pour les réponses.
Bootstrap Protocol:
Bootp flags :
- @IP client.
- @MAC présente.

Puis il y à différente option, il s'agit des différentes requêtes que l'utilisateur de la machine fait, comme demander d'avoir une ancienne @IP qu'il possédait, le nom de la machine, et tout ce qui est nécessaire au paramétrage de la machine option (55).

Dans la réponse : au même endroit on revoit les nouvelles informations proposer alors par le serveur DHCP. (offer)
Il y a ensuite la confirmation dans Request.

S'il y a ensuite des DHCP Discover sans réponses c'est que la machine ne fait pas parti du réseau.

Analyse du protocole HTTP : niveau 4.

Utiliser le filtre http pour afficher du trafic web.
Click droit -> suivre -> le flux TCP.
On vat observer la connexion et ce qui s'est passer durant la session comme SYN – SYN ACK – ACK.
Statistiques -> trafic des flux on a les différentes séquences avec les réponses et toute la conversation qui a été réaliser.

Pour retrouver une requête émise comme la connexion à un site, cherche la requête de type POST :
On va dans l'onglet http :
Et le formulaire avec le username, password, Login de ce qu'on a taper.

Analyse du protocole SSL - TLS : niveau 4.
Analyse du protocole HTTPS : niveau 4.