Fiche Exercices pratiques 11 – Pile TCP/IP - Wireshark

Laurent Signac – CC-BY-SA – 08-06-21 1403 63fd3028c39709b23fc0

1 Données sur votre machine

Obtenez l'adresse IP de votre machine et son masque de sous-réseau. Combien de machines peut contenir votre sous-réseau ? Pouvez-vous dire des choses particulières sur ce réseaux (public ou privé, adresse particulière) ?

2 Table de routage

Consultez votre table de routage (`route -n` ou `route print`). Identifiez la passerelle par défaut. Pinguez la machines 194.254.43.242. Observez la route empruntée pour joindre cette machine (`traceroute 194.254.43.242` ou `tracert`) (si disponible sur votre poste).

3 Dissection d'un ping

Exécutez Wireshark, puis faites Capture/Options, sélectionnez l'interface et lancez la capture. Pinguez une autre machine de la salle et arrêtez la capture. Repérez les trames echo Request et echo Reply.

Dans ces trames, identifiez l'entête ICMP. Qu'est ce qui indique que la trame est de type echo Request ? Quelle est la signification des autres champs de l'entête ICMP ?

En descendant d'un cran dans l'encapsulation, observez l'entête IP. Qu'est ce qui permet à Wireshark de savoir que les données encapsulées dans IP sont des données ICMP ?

Repérez dans l'entête IP les adresses source et destination du ping.

En descendant encore dans les couches, identifiez l'entête Ethernet. Quelle est sa longueur ? Relevez les adresses physiques de machines concernées par le ping.

4 Cache ARP

Listez les machines dans votre cache ARP (`arp -n`). Avec Wireshark, capturez un ping vers la machine `194.254.43.242`. Dans Wireshark, pour une trame echo Request, observez l'entête Ethernet, retrouvez l'adresse MAC du destinataire.

Recherchez l'adresse MAC de `194.254.43.242` dans votre cache ARP. Expliquez. (Réponse à faire vérifier, il y a un piège).

5 Protocole HTTP

Lancez une capture Wireshark. Depuis un terminal, à l'aide du programme telnet (ou PuttY sous Windows), connectez vous au serveur Web `deptinfo-ensip.univ-poitiers.fr` en HTTP sur le port 80 et accédez à la page `/demo/page.html`. Vérifiez que vous avez bien réussi à accéder à la page.

Arrêtez la capture, sélectionnez la requêtes HTTP dans Wireshark et allez dans le menu Analyze / Follow TCP Stream : Wireshark reconstruit le dialogue avec le serveur et l'affiche sous forme de Texte.

Quel est le type de serveur Web auquel vous vous êtes connecté (nom du logiciel et numéro de version) ?

6 Connexion TCP

Lancez une capture Wireshark. Ouvrez un navigateurs Web, et affichez la page :

`http://deptinfo-ensip.univ-poitiers.fr/demo/page.html`

Dans la capture, recherchez les trames de connexion Tcp. Identifiez l'échange des numéros de séquence.