**TRAVAUX PRATIQUES**

|  |  |  |
| --- | --- | --- |
| |  | | --- | | **TP2**  **Analyse des protocoles TCP-IP**  Analyse de la commande ping.   * Quel protocole de niveau réseau est utilisé par la commande Ping ? * Quel est le rôle de la commande ping ? * Effectuez un ping vers votre passerelle. Utilisez un filtre d’affichage permettant de visualiser uniquement les trames correspondant à une commande ping. Analysez les trames visualisées. Combien trouvez-vous de trames ? A quoi correspondent-elles. Quels sont les protocoles présents dans une trame ping ? * Quelles sont les deux éléments qui peuvent être déterminés par la commande ping ? * Quels sont les codes ICMP permettant de déterminer la nature du message ICMP (*Echo Request* ou *Echo Reply*). * A quoi correspondent les données (« Data ») ICMP ? * Pourquoi ICMP n’a pas de ports ?   Analyse de la commande Tracert   * Lancez une capture. Effectuez une commande **tracert** sur un serveur web de votre choix.  Quel protocole de niveau réseau est utilisé par la commande tracert ? Utilisez un filtre d’affichage permettant de visualiser uniquement les trames correspondant à une commande tracert. * Observez les champs TTL des trames émises par votre machine et le champ Type des trames reçues. A partir de ces observations, expliquez le fonctionnement de la commande tracert.   Analyse du protocole IP   * Lancez une capture dans laquelle le protocole IP est présent (vous pouvez utiliser un filtre d’affichage pour isoler certaines trames). * Quelles sont les couches OSI présentes dans les trames relevées ? * Quelle est la version de IP ? * Quelle est la taille l’en-tête IP ? * Le paquet IP est –il fragmenté ? Justifiez votre réponse. * Quelle est la valeur du champ TTL de l’en-tête IP ? Justifiez votre réponse. * Quel est le protocole de niveau supérieur ? Par quelle valeur est-il identifié ? * Pouvez-vous retrouver les valeurs hexadécimales des adresses IP source et destination ?   Analyse d’une connexion TCP.   * Lancez une capture. Connectez-vous à un site web quelconque, puis déconnectez-vous. Analysez la connexion TCP à l’aide de filtres d’affichage. * Combien y-a-t-il de segments d’ouverture et de fermeture de la connexion ? Quelles sont les valeurs des « flags » pour ces segments ? Quels sont les numéros de port utilisés. Justifiez votre réponse. * Vérifiez l’évolution des numéros de séquence et des numéros d’acquittements pour deux trames successives en réponse l’une à l’autre. Vous pouvez pour cela vous aider d’un schéma. * Wireshark possède un outil nommé, *Follow TCP stream* (menu Statistics/Flow Graph/TCP Flow). Vous pouvez ainsi visualiser l’enchainement des segments avec les du numéro de séquence et d’acquittement pour toute la session TCP. | |  | |
| |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif | | | | | | | | | | | | | | | | | | | http://prive.iutenligne.net/11jsG5Kljum6LIB5/informatique/reseaux/lohier/reseaux_fondamentaux/styles/images/pixel-trans.gif |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |