Activité A9 : Etude de a commande ping et du protocole HTTP (Web) avec l'analyseur de protocoles wireshark

Vous devez connaitre les base dans l'utilisation de l'analyseur de protocoles wireshark.

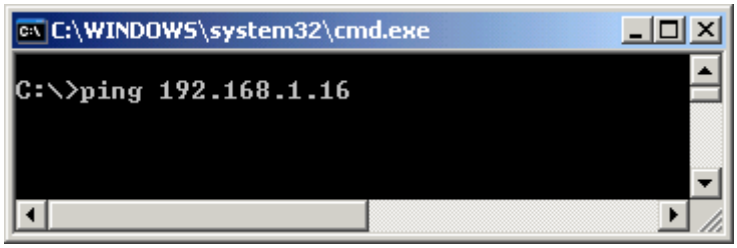
- Tutoriel : découverte de l'analyseur de protocoles Wireshark

Utiliser wireshark pour le protocole ICMP (ping)

Etape 1 : exécuter un ping

- Lancez une capture puis Wireshark.
- Ouvrez une **invite de commandes** et envoyez une commande ping à l'adresse IP d'un poste informatique de la salle ou du serveur DC-BTSSIO.

Remarque : pour ce document et à titre d'illustration, l'adresse IP choisie est 192.168.1.16 **Ce n'est pas l'adresse IP que vous devez utiliser**.



Une fois que vous avez reçu le résultat attendu, arrêtez la capture des paquets.

Étape 2 : observation du volet de la liste des paquets

Le volet supérieur de Wireshark doit ressembler à ce qui suit :

No.	Time	Source	Destination	Protocol	Length	Info
10	1.861971	192.168.1.200	192.168.1.16	ICMP	74	Echo (ping) request id=0x0200,
11	1.864525	192.168.1.16	192.168.1.200	ICMP	74	Echo (ping) reply id=0x0200,
12	1.870497	192.168.1.27	239.255.255.250	SSDP	398	NOTIFY * HTTP/1.1
13	1.912254	192.168.1.27	239.255.255.250	SSDP	342	NOTIFY * HTTP/1.1
14	1.929240	192.168.1.27	239.255.255.250	SSDP	408	NOTIFY * HTTP/1.1
15	1.934814	192.168.1.13	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1e>
16	1.959185	192.168.1.27	239.255.255.250	SSDP	406	NOTIFY * HTTP/1.1
17	1.989348	192.168.1.27	239.255.255.250	SSDP	396	NOTIFY * HTTP/1.1
18	2.685710	192.168.1.13	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1e>
19	2.869414	192.168.1.200	192.168.1.16	ICMP	74	Echo (ping) request id=0x0200,
20	2.872818	192.168.1.16	192.168.1.200	ICMP	74	Echo (ping) reply id=0x0200,
21	3.436773	192.168.1.13	192.168.1.255	NBNS	92	Name query NB WORKGROUP<1e>
22	3.882275	192.168.1.200	192.168.1.16	ICMP	74	Echo (ping) request id=0x0200,
23	3.884493	192.168.1.16	192.168.1.200	ICMP	74	Echo (ping) reply id=0x0200,
24	4.887705	192.168.1.200	192.168.1.16	ICMP	74	Echo (ping) request id=0x0200,
25	4.890464	192.168.1.16	192.168.1.200	ICMP	74	Echo (ping) reply id=0x0200,
26	6.636720	GemtekTe_77:4e:a0	Microsof_01:0f:1c	ARP	60	Who has 192.168.1.200? Tell 192

- Examinez, dans votre propre capture de paquets, les paquets obtenus qui sont semblables aux paquets de la liste ci-dessus : paquets 19, 20, 22, 23, 24 et 25
- Observez la liste des paquets de Wireshark et répondez aux questions suivantes :
  - Quel protocole est utilisé avec la commande ping ? ...
  - Quel est le nom complet du protocole ? ..
  - Quels sont les noms des deux messages ping ? ...
  - Qui envoie les messages ping (précisez qui envoie quel type de message) ? ...

Étape 3 : sélection (mise en surbrillance) du premier paquet de requête d'écho de la liste Regardez le détail des informations obtenues :

Quels sont les protocoles inclus dans la trame Ethernet ? ...

Étape 4 : fermer la capture (sans sauvegarder)

2. Capture des PDU associées à un processus HTTP

Étape 1 : lancement de la capture des paquets

- Lancez une capture puis Wireshark.
- Ouvrez un navigateur Web et saisissez l'URL du site web http://www.reseaucerta.org Une fois la page Web **téléchargée** dans son intégralité, **arrêtez** la capture des paquets dans Wireshark.

Étape 2 : agrandissement du volet de la liste des paquets de Wireshark et passage en revue des PDU répertoriées

- Localisez et identifiez les paquets TCP et HTTP associés au téléchargement de la page Web.
  - Quel est l'adresse IP du serveur web ? ..
  - Identifiez les types de messages échangés. Quels sont-il ? ...

Étape 3 : mise en surbrillance d'un paquet HTTP du volet supérieur portant la mention « (text/html) » au niveau de la colonne Info

- Dans le volet des **détails** de paquet (volet du milieu), cliquez sur le signe « **+** » situé en regard de **Linebased text data: html**
  - Quel type d'informations s'affiche-t-il lorsque vous développez cet élément ? ...
- Examinez la partie mise en surbrillance dans le volet des octets.

Elle indique les **données HTML transportées** par le paquet.

Une fois **terminé**, fermez **Wireshark** en choisissant l'option **Continue without Saving** (Poursuivre sans enregistrer).

Pour terminer, indiquez à quelle **couche** du modèle TCP/IP corresponde les informations d'encapsulation capturées.

Informations	Couche correspondante du modèle TCP/IP
-	-
-	-
-	-
-	-