TP1

I. Connaître sa machine

Avec la commande **ipconfig /all**, répondez aux questions suivantes :

a) Quel est le nom de votre machine ?

b) Donnez les interfaces réseaux actives sur votre PC. A quoi correspondent-elles ?

c) Quelle est l'adresse Ethernet (MAC) de votre pc ?

d) Quel est le constructeur de votre carte réseau Ethernet ?

II. Observer les trames Ethernet

A) Format de trames Ethernet

a) Donnez le format d'une trame Ethernet (II)

b) Identifier la source, le destinataire et le protocole applicatif encapsulé dans la trame ethernet ci-dessous :

```
ff  ff  ff  ff ff  ff  00 30  48 56 2b c8 08 06 00 01
08 00 06 04 00 01 00 30  48 56 2b c8 86 9d 69 15
00 00 00 00 00 00 86 9d  69 c0 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00
```

B) Wireshark

Wireshark (anciennement *Ethereal*) est un analyseur réseau très populaire. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau. Un manuel utilisateur se trouve ici : http://david.roumanet.free.fr/serendipity/uploads/reseaux/Manuel_WireShark.pdf

e) Téléchargez et installer wireshark (http://www.wireshark.org/download.html)

c) Démarrer **wireshark** (dans les raccourcis ou en ligne de commande). et charger la capture http://webia.lip6.fr/~lepape/ens/isn/tp/TP1/capture_arp.pcap Dans le menu **View>Name Resolution**, décochez les options de résolution de noms si elles sont sont cochées. Que voyez-vous ? Identifiez la fenêtre de résumé, la fenêtre d'arborescence de protocoles et la fenêtre de vue des données.

d) Pour limiter le nombre de données, l'utilisateur peut spécifier un filtre d'affichage (http://openmaniak.com/fr/wireshark_filters.php#display) . Filtrer les paquets en ne gardant que les trames **arp**.

e) Pour cet exercice, il faut savoir qu'une machine n'est connue par son adresse MAC que sur le réseau local. Sur Internet, une machine est connue par une adresse globale, appelée adresse IP**.** Que fait le protocole ARP ?

f) Consulter la table ARP de votre PC avec la commande **arp -a**
Que contient-elle ?

g) Analyser les trames 70 et 71.

h) La table ARP sur pc32 ne contenait pas pc31 et l'utilisateur exécute la commande **ping pc31.** Que fait la commande ? Quelle nouvelle entrée doit être enregistrée dans la table ARP de pc32 ?

III. Sécurité des trames ethernet

i) Ouvrez l'url suivante . http://webia/lip6.fr/~lepape/ens/isn/tp/TP1/coucou.html . Le site demande un login (**test**) et un mot de passe (**soleil**). La capture de cette opération est ici : http://webia.lip6.fr/~lepape/ens/isn/tp/TP1/capture_htaccess.pcap Filtrez les messages HTTP uniquement. Quelle opération HTTP a été effectuée ? Que lui a répondu le serveur ?

j) Dans la fenêtre de protocoles de la trame 679, chercher le champ d'authentification (Authorization). Avec l'outil en ligne http://www.dolcevie.com/js/converter.html, retrouver le codage hexadecimal correspondant à cette information et vérifier la correspondance dans la trame de wireshark.

k) Parmi ces informations de description se trouve les informations d'authentification. Sachant que ces informations sont codée en base 64 et à l'aide de l'outil en ligne http://www.hcidata.info/base64.htm, retrouver le login et le mot de passe.

l) Recommencer la même manipulation cette fois en utilisant un protocole sécurisé (https). https://webia.lip6.fr/~lepape/ens/isn/tp/TP1/coucou.html La capture de cette opération est ici : http://webia.lip6.fr/~lepape/ens/isn/tp/TP1/capture_htaccess_securise.pcap
Attention : le filtre http ne fonctionne plus et le filtre https n'est pas reconnu. Il faut filtrer avec le filtre `tcp.port == 443`. Que constatez-vous ?