**TP 3 - Analyse de flux TCP/IP**

*On se sert d’un poste de travail à l’Efrei, sur une VM Debian.*

1. **Analyse de trames**
	* 1. **Capture de flux associés à la commande ping**
		2. **Capture de flux associés à la commande ping**



* + 1. **Capture de flux associés à la commande tcptraceroute**
	1. Analyse flux ARP et ICMP

Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées?

ICMP

Quelles sont les longueurs des messages échangés par les différents protocoles ?

ICMP : longueur 98

1.3.1 Etude du paquet IP correspondant au premier message ARP Request

Caractéristiques Ethernet :

- Que transporte la trame Ethernet ?

Elle encapsule tout : de l’IP, qui encapsule de l’UDP (ou du TCP), qui encapsule du DNS (dans le cas d’une requête ping serveur.com)

- Quelle est l'adresse MAC source de la trame Ethernet ?

Source : CadmusCo\_c0 :ec :59 d’adresse 08:00:27:c0:ec:

 - Quelle est l'adresse MAC destination trame Ethernet ?

Destination : 59Realtek\_U12 :35 :02 d’adresse 52:54:00:12:35:02

- Quelle est la signification de cette valeur ?

*L’adresse physique de l’hôte de réception.*

*Caractéristiques ARP :*

*- Quelle est la taille l’en-tete ?*

Taille de l’en-tête : 42 bytes (336 bits)

*- Quelle est la valeur du champ Protocol Type contenu dans le message ARP?*

Protocol Type : IP (0x0800)

*- Quelle est l'adresse IP Source du paquet ARP?*

10.0.2.15

*- Quelle est l'adresse IP destination du paquet ?*

10.0.2.2

*- Quelle est l'adresse MAC Source incluse dans le message ARP ?*

Source : CadmusCo\_c0 :ec :59 d’adresse 08:00:27:c0:ec:59

*- Quelle est l'adresse MAC destination incluse dans le message ARP ?*

Destination : 00 :00 :00\_00 :00 :00

**1.3.2. Étude du paquet IP correspondant au second message ARP Reply**

*Caractéristiques Ethernet :*

*- Quelle est l'adresse MAC source de la trame Ethernet ?*

Source : 59Realtek\_U12 :35 :02 d’adresse 52:54:00:12:35:02

*- Quelle est l'adresse MAC destination trame Ethernet ?*

Destination : CadmusCo\_c0 :ec :59 d’adresse 08:00:27:c0:ec:59

*Caractéristiques ARP :*

*- Quelle est la taille l’en-tête ?*

60 bytes

*- Quelle est la valeur du champ Protocol Type contenu dans le message ARP?*

Protocol Type : IP (0x0800)

*- Quelle est l'adresse IP Source du paquet ARP?*

10.0.2.2

*- Quelle est l'adresse IP destination du paquet ?*

10.0.2.15

*- Quelle est l'adresse MAC Source incluse dans le message ARP ?*

Source : 59Realtek\_U12 :35 :02 d’adresse 52:54:00:12:35:02

*- Quelle est l'adresse MAC destination incluse dans le message ARP ?*

Destination : CadmusCo\_c0 :ec :59 d’adresse 08:00:27:c0:ec:59

*- Quelle action effectue la station émettrice après réception du message ARP reply ?*

Elle peut effectuer la suite de ses requêtes. Par exemple, elle peut se synchroniser (paquet NTP)

* 1. **Analyse du message ICMP**

**1.4.1. Message ICMP «Echo Request»**

*- Quelle est la taille l’en-tete ?*

20 bytes

*- Quel est le type de message ICMP ?*

Type : 8 (Echo (ping) request)

*- Quel est son identificateur ?*

Identifier (BE) : 2421 (0x0975)

Identifier (LE) : 29961 (0x7509)

*- Quel est le numéro de séquence ?*

Sequence number (BE) : 1 (0x0001)

Sequence number (LE) : 256(0x0100)

*- Quelle est l'adresse IP destination du paquet ?*

192.102.224.41

*- Quelle est la valeur du champ Protocol Type ?*

IP

*- Quelle est la valeur du champ Time to Live ?*

64

**1.4.2.Message ICMP «Echo Reply»**

*- Quel est le type de message ICMP ?*

Type : 0 (Echo (ping) reply)

*- Quel est son identificateur ? (A comparer à la requête question)*

Identifier (BE) : 2421 (0x0975)

Identifier (LE) : 29961 (0x7509)

C’est le même que précédemment.

*- Quel est le numéro de séquence ?*

Sequence number (BE) : 1 (0x0001)

Sequence number (LE) : 256(0x0100)

*- Quelle est l'adresse IP destination du paquet ?*

10.0.2.15

*- Quelle est la valeur du champ Protocol Type ?*

IP

*- Quelle est la valeur du champ Time to Live ?*

62

**1.4.3. Étude du message ICMP – Compléments**

*- Comparer ces données avec celles affichées dans le message de requête avec celles affichées dans le message de requête.*

Elles sont semblables à l’exception du TTL et l’IP de destination

*- Comment les champs d'identification et numéro de séquence évoluent dans le temps ?*

Ils restent identiques.

*- Est-ce que les séquences de données des requêtes et des réponses changent ?*

Non

*- Calculer l'écart de temps entre l'émission de chaque message Echo Request et la réception de chaque message Echo Reply.*

Il se passe environ 0.002 secondes. Cohérent avec une moyenne de ping à 150ms.

1. **Analyse des flux web**
	1. **Protocoles capturés**
* *Quels sont les protocoles indiqués dans la colonne Protocol de la fenêtre de liste des trames capturées ?*

TCP, HTTP, TLSv1.2

* *Quelle est l'utilité de la requête N°1 ?*

Elle permet d’établir la connexion avec le proxy Efrei

**2.4. Trame Ethernet, paquet IP et datagramme UDP**

**2.4.1. Analyser la trame correspondant au premier message DNS émis par le client Web.**

*- Quelles sont les adresses (MAC|Ethernet) et IP du client ?*

MAC : CadmusCo\_c0 :ec :59 d’adresse 08:00:27:c0:ec:59

Ethernet :

IP : 10.0.2.15

* *Quel est le contenu du champ type de la trame Ethernet ?*

Type : IP

*- Quelles sont les adresses destination (MAC|Ethernet) et IP ?*

MAC : 59Realtek\_U12 :35 :02 d’adresse 52:54:00:12:35:02

Ethernet :

IP : 192.102.224.14

*- À quelles machines correspondent ces adresses ?*

Il s’agit du proxy de l’Efrei, permettant la connexion au web

**2.4.2. Analyser l'en-tête IP du premier message DNS émis par le client Web.**

*- Quelle est la taille de l'en-tête ? Quelle est la longueur totale du paquet ?*

Taille en tête : 20, longueur totale 60

* *Repérer le champ « type de protocole » dans l'en-tête. Quel est le numéro et le type de protocole présent dans les données du paquet ?*

Protocole en-tête : IP

Protocole dans le paquet : UDP (17)

**2.4.3. Analyser l'en-tête UDP du premier message DNS émis par le client Web.**

*- Quels sont les numéros de ports du client et du serveur ?*

Client : 56856

Serveur : 53

*- Quelles sont les particularités de ces valeurs ?*

53 est le port utilisé classiquement par DNS alors que le port client est généré à la volée

*- Quel est le protocole de couche application présent dans les données du message ?*

IP

*- Quelle est la valeur indiquée dans le champ longueur de l'en-tête UDP ?*

Longueur 40

*- Est-ce qu'elle correspond à l'information donnée dans l'en-tête du paquet IP ?*

Oui, elle correspond à la longueur totale – l’en-tête

**2.5. Service DNS**

**2.5.1. Analyser le message de requête DNS émis par le client Web.**

*- Quel est le champ qui indique si le message est une requête ou une réponse ?*

Champ Info de Wireshark : « Standard query **response** », et « Flags » dans le détail du paquet

*- Quelle est l'information transportée dans le corps de la requête ? Identifier le type et la classe de la requête.*

L’adresse IP correspondant au nom de domaine demandé, type A et classe IN

*- Quel est l'identificateur de transaction de la requête ?*

Identification : 0x3595

*- Quelles devraient être les adresses (MAC|Ethernet) et IP de ce paquet ? Vérifier que les adresses attendues sont présentes.*

On devrait avoir :

MAC : 59Realtek\_U12 :35 :02 d’adresse 52:54:00:12:35:02

Ethernet :

IP : 10.0.1.1

Ce qu’on a

*- Quelles sont les tailles du paquet IP et du message UDP ? Sont-elles supérieures aux messages requêtes ?*

IP : taille totale 95, header 20 = taille effective de 75

UDP : taille de 75

*- Quel est l'identificateur de transaction de la réponse ? Est-ce qu'il correspond à la requête ?*

Transaction ID : 0x3369, c’est le même que pour la requête

*- Combien de réponses sont disponibles dans le message de réponse ? Comparer les réponses et leurs valeurs TTL (Time-to-live).*

Time to live = 3600 et time to live = 300

**2.6. Connexion TCP**

*- Quelles sont les adresses (MAC|Ethernet) et IP attendues pour cette trame ?*

MAC : CadmusCo\_C0 :ec :59 (d’adresse 08 :00 :27 :c0 :ec :59)

Ethernet :

IP : 10.0.2.15

*- Quelles sont les valeurs des champs type et protocole respectivement attendus pour cette trame et ce paquet ?*

Type : IP (0x0800)

*- Expliquer les valeurs des adresses destination (MAC|Ethernet) et IP ? À quels hôtes correspondent ces adresses ?*

MAC : Realtek\_U12 :35 :02 d’adresse 52 :54 :00 :12 :35 :02

Ethernet :

IP : 192.102.224.14

Il s’agit du proxy de l’Efrei

*- Identifier les numéros de ports utilisés par le client. Pourquoi ces valeurs sont-elles utilisées ?*

Source port : 33544

Destination port : 3128

Le port source est utilisé à la volée, le port de destination est classiquement utilisé pour du TCP

*- Quelle est la longueur du segment TCP ?*

34 (70 – header de 40)

*- Quel est le numéro de séquence initial (Initial Sequence Number ou ISN) émis par le client vers le serveur ?*

0

*- Quelle est la taille de fenêtre initiale ?*

29200

*- Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ?*

1460

*- Trouver la valeur hexadécimale de l'octet qui contient l'indicateur d'état SYN ?*

A0 02

*- Combien de temps s'est écoulé entre la capture du premier et du second segment TCP ?*

Environ 0.0001 seconde

*- Relever les valeurs des champs suivants de cette trame :*

*- Adresses MAC source et destination de la trame Ethernet.*

Source : Realtek\_U12 :35 :02 d’adresse 52 :54 :00 :12 :35 :02

Destination: CadmusCo\_C0 :ec :59 (d’adresse 08 :00 :27 :c0 :ec :59)

*- Adresses source et destination du paquet IP.*

Source : 192.102.224.14

Destination : 10.0.2.15

*- Numéros de séquence et d'acquittement du segment TCP.*

Seq = 0

Ack = 1

*- Valeurs des indicateurs d'état.*

60 12

*- Quelle est la longueur du segment TCP ?*

Longueur totale : 44

*- Quel est le numéro de séquence initial (Initial Sequence Number ou ISN émis par le serveur vers le client ?*

0

*Quelle est la taille de fenêtre initiale ?*

29200

*Quelle est la taille maximale de segment (Maximum Segment Size ou MSS) ?*

1460

*- Combien de temps s'est écoulé entre la capture du second et du troisième segment TCP ?*

Environ 0.00001 seconde

*- Comparer cette valeur avec celle relevée entre le premier et le second segment et expliquer la différence.*

Elle est beaucoup plus faible, du fait que le client sait qui contacter et que le serveur s’attend à une telle requête de la part du client.

*- Relever les valeurs des champs suivants de cette trame :*

*- Numéros de séquence et d'acquittement du segment TCP*

Seq = 1

Ack = 1

*- Valeurs des indicateurs d'état*

50 10

*- Taille de fenêtre*

37376

*- Quelle est la longueur du segment TCP ?*

Longueur totale 54 – header 20 = 34