TP5

Sommaire

4.1Capture de trame ARP et ICMP

```
Microsoft Windows [version 10.0.22631.5335]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>ping 172.17.254.5

Envoi d'une requête 'Ping'  172.17.254.5 avec 32 octets de données :
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64
Réponse de 172.17.254.5 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.17.254.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

J'ouvre l'invite de commande et je ping le serveur aviateur (172.17.254.5)

	295 48.267424	VMware_22:87:6d	Broadcast	ARP	60 Who has 172.17.244.15? Tell 172.17.243.11
→	296 48.373628	172.17.2.2	172.17.254.5	ICMP	74 Echo (ping) request id=0x0001, seq=2/512,
←	297 48.374115	172.17.254.5	172.17.2.2	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512,

j'ai mit un filtre sur wireshark qui esy arp or icmp

-Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

0806

-Quelle est la fonction de la trame ARP Request ?

Elle permet de connaître l'adresse m ac du destinataire

-Quelle signification ont les octets de position 0×04 et 0×05 ligne 0010 ?

trame ARP REQUEST et la trame ARP REPLY

-Quelle est la longueur d'un message ARP contenu dans la trame ?

28 octet

AXEL SANTIN
BTS SIO1

TP5

-Quelle est la longueur de la trame ARP Request ?

14 octet

-Quelle est la longueur de la trame ARP Reply ?

42 octet

-Combien d’octets sont utilisés pour le padding ?

0 octet

Trame ARP request
@Mac destination=FF:FF:FF:FF:FF:FF @Mac source=74:56:3C:2F:96:EC Ethernet Type=0806 Opcode(hexa)=0001 @MAC de la cible=00:00:00:00:00:00 @IP de la cible=172.17.254.5

-Quelle signification ont les octets de position 0×0C et 0×0D ligne 0000 ?

c’est le champ Ether Type (0800)

-Quelle signification a l’octet de position 0×07 ligne 0010 ?

c’est le champ protocole

-Quelle est la longueur de la trame ?

74 octet

-Quelle est la longueur du paquet IP ?

60 octet

-Quelle est la longueur du message ICMP ?

8 octet

-Quelle signification a l’octet de position 0×02 ligne 00020 ?

08 , ca signifie un echo request

-A quoi correspondent les octets à partir de l’octet 0×0A, ligne 00020 ?

c’est les donne ICMP

AXEL SANTIN
BTS SIO1

TP5

-Sélectionnez une trame ICMP Echo Reply. Quelle est le nom et la valeur de l’octet de position 0×02 ligne 00020 ?

0000

4.2Capture de trame ARP,DNS et ICMP

```
C:\Windows\System32>ping www.ac-nice.fr

Envoi d’une requête 'ping' sur www.ac-nice.fr.cdn.cloudflare.net [141.101.90.105] avec 32 octets de données :
Réponse de 141.101.90.105 : octets=32 temps=20 ms TTL=53
Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53
Réponse de 141.101.90.105 : octets=32 temps=16 ms TTL=53

Statistiques Ping pour 141.101.90.105:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 16ms, Maximum = 20ms, Moyenne = 17ms
```

636	222.945888	Giga-Byt_2f:9c:c6	Broadcast	ARP	60	Who has 172.17.5.19? Tell 172.17.2.12
637	223.112169	172.17.2.2	172.17.254.1	DNS	74	Standard query 0x162e A www.ac-nice.fr
638	223.145302	172.17.2.2	172.17.254.1	DNS	74	Standard query 0x162e A www.ac-nice.fr
639	223.169596	172.17.254.1	172.17.2.2	DNS	185	Standard query response 0x162e A www.ac-nice.fr CNAME www.ac-nice.fr.cdn.cloudflare.net A 141.101.90.105 A…
640	223.174491	172.17.2.2	141.101.90.105	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 641)
641	223.194642	141.101.90.105	172.17.2.2	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=53 (request in 640)

J’ai mit un filtre arp or dns or icmp sur wireshark

-La liste des trames commence par une requête et une réponse ARP. Quelle est la machine dont l’adresse MAC est recherchée ?

L’adresse mac sont :

roi (serveur)

stormshield(routeur)

Trame ARP request
@MAC destination=FF:FF:FF:FF:FF:FF
@MAC source=74:56:3C:2F:9C:C6
Ethernet Type=0806
Opcode(hexa)=01
@MAC de la cible=00:00:00:00:00:00
@IP de la cible=172.17.5.19

AXEL SANTIN
BTS SIO1

TP5

-Pour quelle raison trouve-t-on ensuite une requête DNS avant l'échange de trames ICMP suite à l'exécution de la commande ping proprement dite ?

Car on connaît pas l'adresse ip et la requet dns permet de changer le nom de domaine en adresse ip

```
Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie  . . . . : 277
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.105


Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie  . . . . : 277
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.106


Nom d'enregistrement. : www.ac-nice.fr.cdn.cloudflare.net
Type d'enregistrement : 1
Durée de vie  . . . . : 277
Longueur de données . : 4
Section . . . . . . . : Réponse
Enregistrement (hôte) : 141.101.90.107
```

je demarre un nouvelle capture wireshark et je vide le cache dns grace a la commande opconfig flushdns

```
C:\Windows\System32>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Windows\System32>
```


AXEL SANTIN
BTS SIO1

TP5

-Quels sont les différents protocoles encapsulés dans une trame DNS ?

Les protocol sont :

ipv4

UDP

Ethernet

-Quelle est la machine destinataire de la requête DNS ? Quelle est son IP (cf. en-tête IP) ?

C’est el serveur roi 172.17.254.1

-Quelle signification ont les octets de position 0×0C, 0×0D ligne 0000 et 0×07 ligne 0010 ?

champ Ether Type 0800 ,IP champ protocol 11 , champ port 53, DNS

-Développez la section Domain Name System (query) et plus précisément la rubrique Queries. Quels sont les valeurs hexadécimales des octets correspondant au nom de domaine internet ac nice.fr ?

Les octet sont de la ligne 0030 et position 0X06 àla ligne 0040 a la position 0X05

-Sélectionnez la trame comportant la réponse à la requête DNS et développez la section Domain Name System (response) et plus particulièrement la rubrique Answers. Recherchez les valeurs hexadécimales et décimales de l’adresse IP du serveur web hébergeant le site de l’académie de Nice.

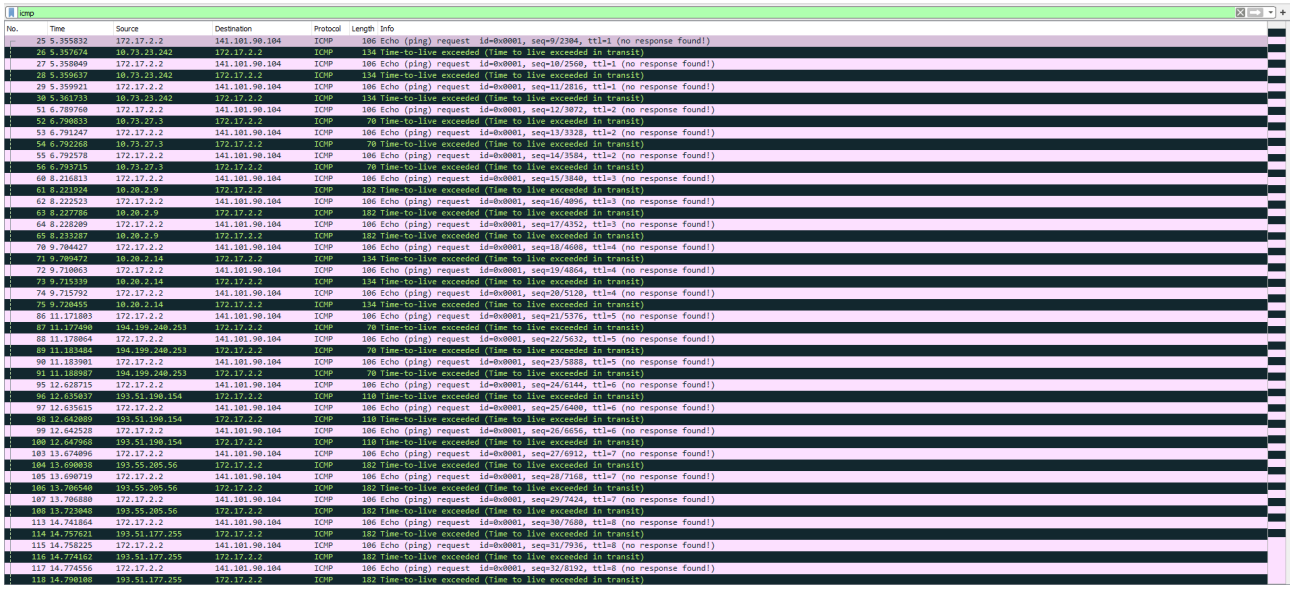
Les valeur sont 0000

4.3Commande Tracert et capture de trames ICMP

Je demarre une capture wireshark

et dans l’invite de commande je met la commande Tracert www.ac-nice.fr

TP5



No.	Time	Source	Destination	Protocol	Length	Info
25	5.355832	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=9/2304, ttl=1 (no response found!)
26	5.357674	10.73.23.242	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
27	5.358049	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=10/2560, ttl=1 (no response found!)
28	5.359637	10.73.23.242	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
29	5.359921	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=1 (no response found!)
30	5.361733	10.73.23.242	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
51	6.789760	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=2 (no response found!)
52	6.790833	10.73.27.3	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
53	6.791247	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=2 (no response found!)
54	6.792268	10.73.27.3	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
55	6.792578	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=2 (no response found!)
56	6.793715	10.73.27.3	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
60	8.216813	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=3 (no response found!)
61	8.221924	10.20.2.9	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
62	8.222523	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=3 (no response found!)
63	8.227706	10.20.2.9	172.17.2.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
64	8.228209	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=3 (no response found!)
65	8.233287	10.20.2.9	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
70	9.704427	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=18/4608, ttl=4 (no response found!)
71	9.709472	10.20.2.14	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
72	9.710063	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=4 (no response found!)
73	9.715339	10.20.2.14	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
74	9.715792	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=4 (no response found!)
75	9.720455	10.20.2.14	172.17.2.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
86	11.171803	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=5 (no response found!)
87	11.177490	194.199.240.253	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
88	11.178064	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=5 (no response found!)
89	11.183484	194.199.240.253	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
90	11.183901	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=5 (no response found!)
91	11.188987	194.199.240.253	172.17.2.2	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
95	12.628715	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=24/6144, ttl=6 (no response found!)
96	12.635037	193.51.190.154	172.17.2.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
97	12.635615	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=6 (no response found!)
98	12.642089	193.51.190.154	172.17.2.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
99	12.642528	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=6 (no response found!)
100	12.647968	193.51.190.154	172.17.2.2	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
103	13.674096	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=7 (no response found!)
104	13.690038	193.55.205.56	172.17.2.2	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
105	13.690719	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=7 (no response found!)
106	13.706540	193.55.205.56	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
107	13.706880	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=7 (no response found!)
108	13.723048	193.55.205.56	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
113	14.741864	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=8 (no response found!)
114	14.757621	193.51.177.255	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
115	14.758225	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=8 (no response found!)
116	14.774162	193.51.177.255	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
117	14.774556	172.17.2.2	141.101.90.104	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=8 (no response found!)
118	14.790108	193.51.177.255	172.17.2.2	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

-Sélectionnez la première trame ICMP Echo request. Développez l'en-tête IP. Quelle est l'adresse IP Destination (valeurs déci. et hexa.) ?

hexa=8D:65:5A:68

decimale=141.101.90.104

-Sélectionnez le champ TTL. Quelle est la valeur portée par ce champ (valeurs déci. et hexa.) ?

Hexa=01

decimale=1

-Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

Protocole ICMP

hexa=01

decimale=1

-Sélectionnez la trame, comportant un message d'erreur ICMP Time-to-live exceeded, envoyée par le premier routeur rencontré. Développez la section correspondant au message ICMP. Quelle est la valeur portée par le champ Type (valeurs déci. et hexa.) ?

Hexa=40

decimale=64

AXEL SANTIN
BTS SIO1

TP5

AXEL SANTIN
BTS SIO1