Université du Québec à Rimouski

Campus de Lévis

TP3 — ANALYSE D’UN INCIDENT DE SÉCURITÉ   
& EXERCICE SUR LE DHCP SNOOPING

Par

Boutin, Frédérik

Pouliot, Mariane

St-Onge, Nathan

Travail présenté à ARSENAULT Martin

Dans le cadre du cours de sécurité informatique

INF36207-MS

4 avril 2023

[Partie 1 : Analyse d’un incident de sécurité (Wireshark) 3](#_Toc131717522)

[Que s’est-il passé sur le poste du dirigeant à son insu ? 4](#_Toc131717523)

[Qu’est-ce que le dirigeant a fait sur le site forum.radioamateur.ca ? 4](#_Toc131717524)

[Pouvez-vous d’écrire la séquence des évènements qui se sont produits ? 4](#_Toc131717525)

[Est-ce qu’il y a eu des attaques et dans la positive, d’où provenait les attaques? 4](#_Toc131717526)

[Est-ce que de l’information a fuité à partir du poste du dirigeant ? 7](#_Toc131717527)

[Quelles sont vos conclusions finales sur cet incident et quel serait le plan d'action à adopter? 7](#_Toc131717528)

[Partie 2 : Exercice sur le DHCP Snooping (Packet Tracer) 8](#_Toc131717529)

[Question 1 8](#_Toc131717530)

[Question 3 10](#_Toc131717531)

[Question 4 12](#_Toc131717532)

[Question 5 14](#_Toc131717533)

[Question 6 16](#_Toc131717534)

[Question 7 17](#_Toc131717535)

[Question 8 18](#_Toc131717536)

[Conclusion 18](#_Toc131717537)

[Bibliographie 20](#_Toc131717538)

# Partie 1 : Analyse d’un incident de sécurité (Wireshark)

### Que s’est-il passé sur le poste du dirigeant à son insu ?

À l’aide de l’outil **NetworkMiner** combiné à **Wireshark**, nous sommes en mesure de détecter que plusieurs sessions de connexion TCP ont été établies d’une manière malicieuse entre un hôte inconnu (**172.25.16.1**) et le poste du dirigeant (**172.25.18.135**). En effet, il y a eu 13 sessions établies entre les deux postes et celles-ci semblent être motivées par de multiples attaques en provenance de l’hôte **172.25.16.1** (se référer à la réponse de la question #4). La figure 1 montre une capture des 13 sessions de connexion entrantes sur le poste du dirigeant. Il est à noter que précédent les sessions, il y a eu un scanne des ports du dirigeant par l’hôte inconnu ainsi que plusieurs cas de redirection de requêtes TCP et de réutilisation de port. De plus, l’hôte malicieux a utilisé différents protocoles avec le poste du dirigeant (SMB, DCERPC, NBSS) qui ont tous été refusés ainsi que SSDP et ICMP. Il est à noter que 8 paquets UDP ont été transmis au dirigeant par l’hôte **172.25.16.1.** Finalement, il est à noter que puisque le dirigeant a utilisé à certaines reprises le protocole http pour l’accès et la connexion au site, il y a de fortes chances que l’hôte inconnu ai capturer ces informations de connexion et les ai utilisées par la suite.

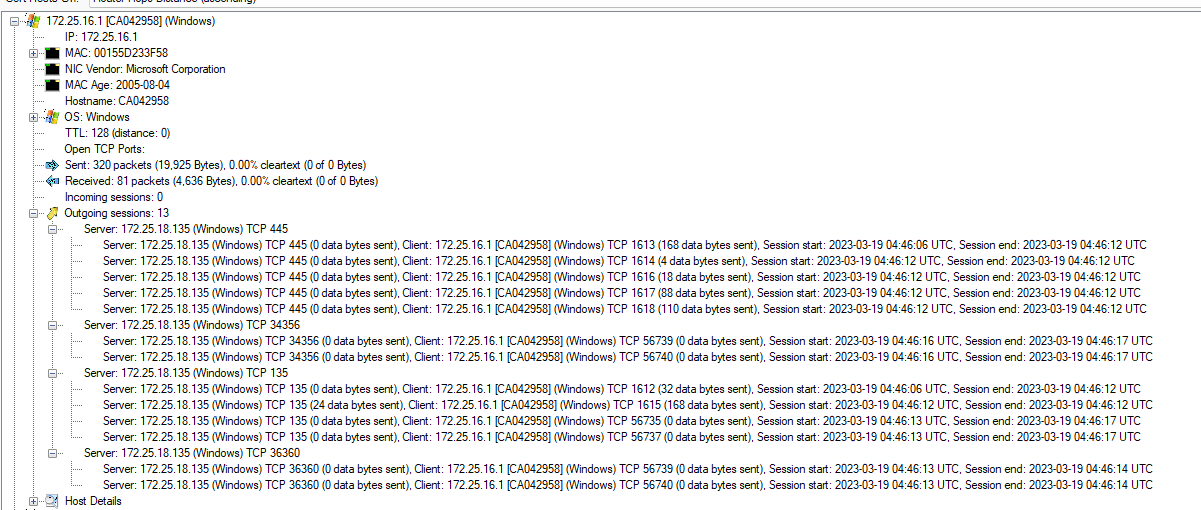


Figure - 13 sessions entre 172.25.16.1 et 172.25.18.135

### Qu’est-ce que le dirigeant a fait sur le site forum.radioamateur.ca ?

Le dirigeant a tout d’abord accéder à la page d’accueil ( ***/index.php*** ), suivit de la page board ( ***?board=2.0*** ), puis il a utilisé la page de connexion dans le but de se connecter à l’aide de son nom d’utilisateur (« ***tata*** ») et de son mot de passe. Par la suite, il a exploré diverses sections du forum dont la page d’accueil, la page help ( ***/action=help*** ) ainsi que plusieurs pages board ( ***?board=69.0, 52.0, 64.0, 65.0*** ), l’accès à une image GIF du site (***veryhot\_post\_sticky.gif***), une page topic (***?topic=7476.0***), suivit de 3 requêtes de connexion (***/index.php?action=login2***), toujours avec l’identifiant « ***tata*** ».

### Pouvez-vous d’écrire la séquence des évènements qui se sont produits ?

\*\*CHRONOLIGIE :

1. Établir la connexion avec le site web 72.18.137.100 (3 way hand-shake)
2. Get index du site web [no.24]
3. Get board=2.0 du site web [no.94]
4. Échange SYN-ACK entre 34.120.208.123 et le dirigeant
5. Login au compte tata sur le site web [no.146]
6. Get index du site web [no.195]
7. Broadcast ARP par l’hôte inconnu (Who as 172.25.18.135?, tell : 172.25.16.1) [no.226, 227]
8. Scan SYN (envoie de plus de 200 SYN vers le dirigeant) de la part de 172.25.16.1 [no.228 à 434]
9. Échange SYN-ACK entre 34.120.5.21 et le dirigeant
10. Échange SYN-ACK entre 184.73.218.151 et le dirigeant (échange de certification)
11. SMB par l’hôte inconnu sur le dirigeant [no.527]
12. NBSS par l’hôte inconnu sur le dirigeant [no.539, 550, 555, 560]
13. Protocol DCERPC du dirigeant, refus de requête [no.542]
14. Plusieurs tentative (6) de connexion TCP de la part de 172.25.16.1 sur le port 135 du dirigeant [no.562 à 574]
15. ICMP de hôte inconnu au dirigeant [no.575 à 578 et 631 à 634]
16. Échange UDP + TCP retransmission [no.579, 588-630, 635-638, 641, 644-666, 677-690]
17. Get index board=69 du site web [no.691]
18. Échange SYN-ACK entre 34.120.208.123 et le dirigeant
19. Get help du site web rpécédé par 2 requêtes TCP reset par le dirigeant sur l’hôte inconnu [no.803]
20. Get index du site web [no.830]
21. RTS envers 172.25.16.1 du dirigeant [no.847-854]
22. Get board=52 du site web [no.855]
23. Get board=64 du site web [no.909]
24. Get index du site web [no.925]
25. 2e Broadcast ARP par l’hôte inconnu (Who as 172.25.18.135?, tell : 172.25.16.1) [no.926-927]
26. Get index du site web [no.925]
27. Get board=69 du site web [no.925]
28. SSDP de la part de 172.25.16.1 [no.946-948, 956-958, 960, 962]
29. Get index du site web [no.963]
30. 3e Broadcast ARP par l’hôte inconnu (Who as 172.25.18.135?, tell : 172.25.16.1) [no.926-927]
31. 172.25.16.1 fait un Host Announcement BROWSER [no.1084]
32. Get board=65 du site web [no.1093]
33. Get veryhot\_post\_sticky.gif (GIF89a) [no.1099]
34. Get topic 7476.0 [no.1148]
35. Get index [no.1154]
36. Post Login (tata) [no.1213]
37. Post Login (tata) [no.1266]
38. Post Login (tata) [no.1333]

### Est-ce qu’il y a eu des attaques et dans la positive, d’où provenait les attaques?

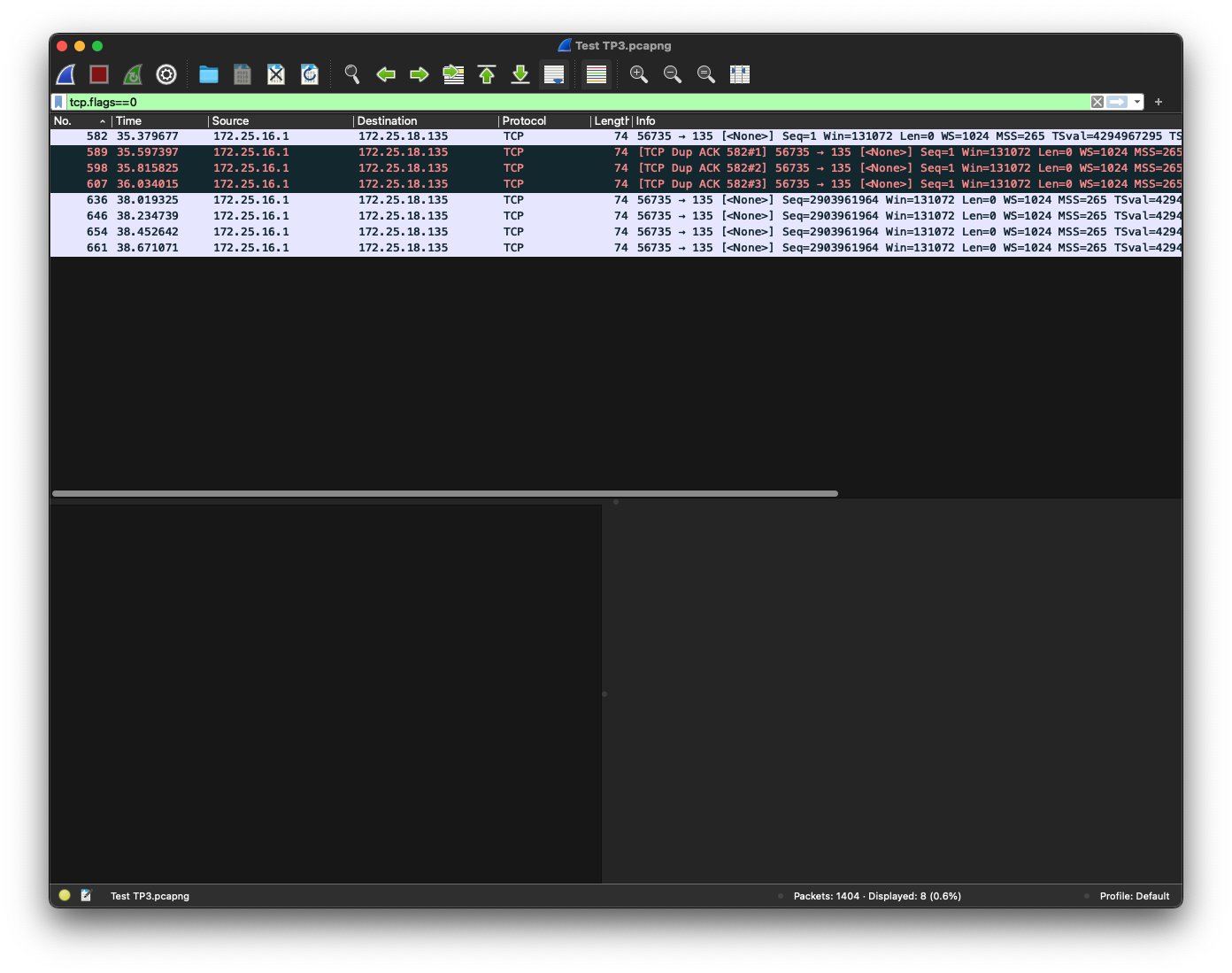
##### (Adresses IP, Adresses MAC, Hostname, etc.)

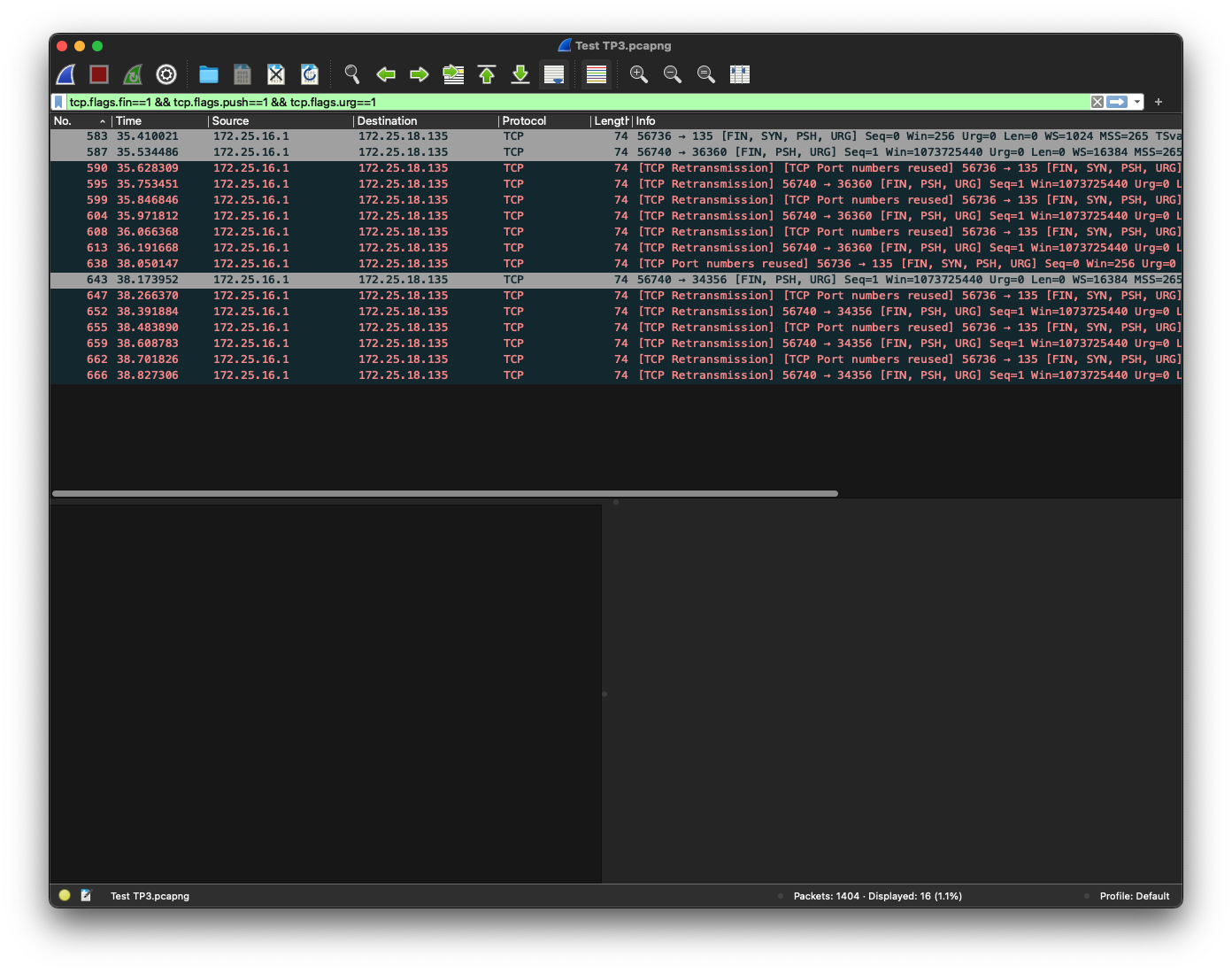
Nous avons pu remarquer quelques attaques.

D’abord, aux lignes 228-434 du fichier Wireshark, nous suspectons que l’hôte inconnu tente de scanner les ports du dirigeant afin de savoir lesquels sont ouvert. Ceci se traduit par l’envoi de paquets SYN en destination du dirigeant (172.25.18.135), il est possible de voir que les ports 135 et 445 sont ouvert par un retour SYN ACT.

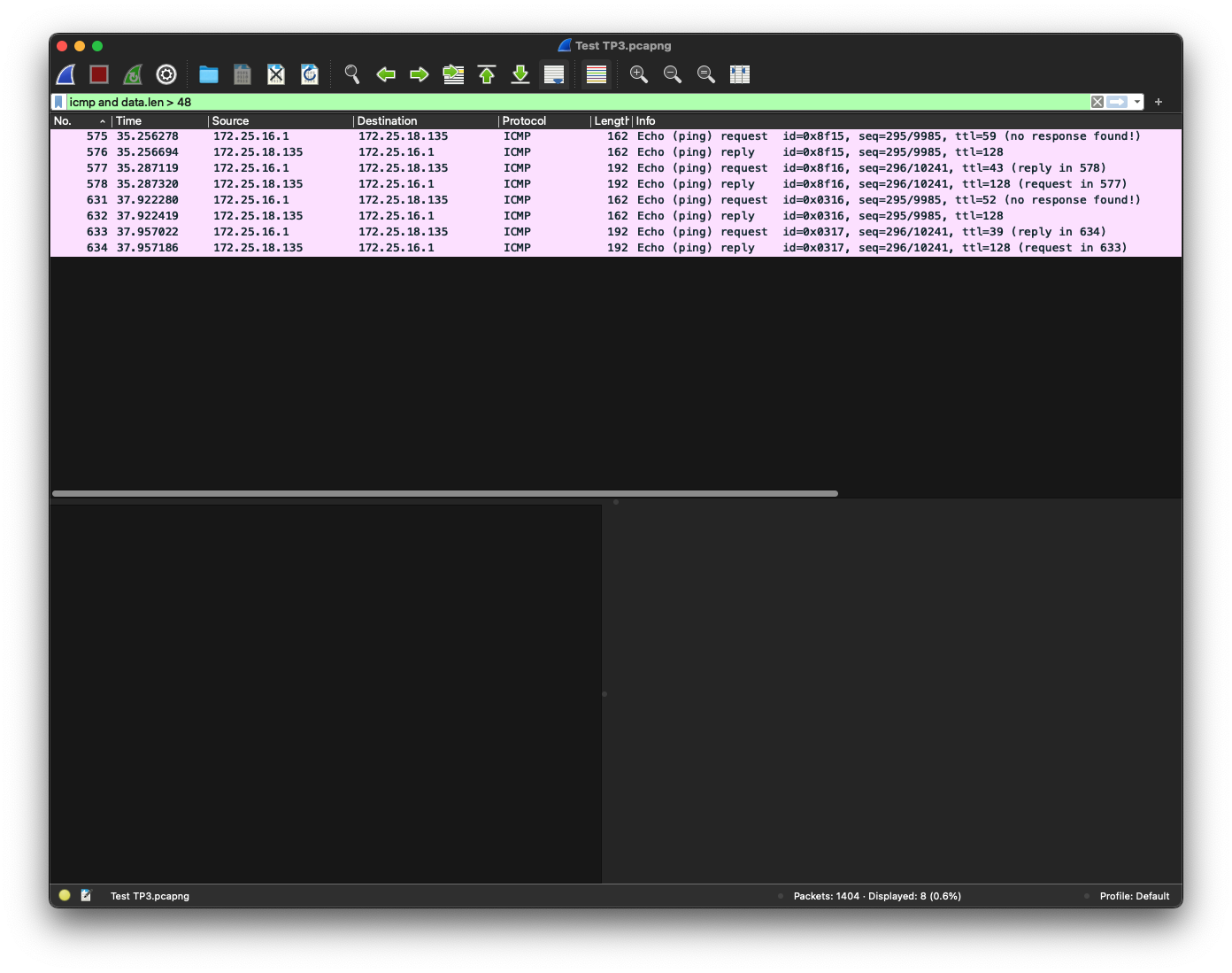
Ensuite, nous pouvons remarquer des connexions bloquées par un pare-feu. En effet, à quelques reprises, nous avons pu observer quelques envois des paquets [RST, ACK] ou [RST], ceux-ci permettant entre autres la réinitialisation forcée de la connexion entre deux appareils. Par exemple, à la ligne 528, l’appareil du dirigeant (172.25.18.135) interrompt brutalement la connexion avec l’hôte ayant l’adresse IP 172.25.16.1. D’ailleurs, une telle interruption entre ces deux hôtes se reproduit aux lignes 540, 551, 556, 561, etc.

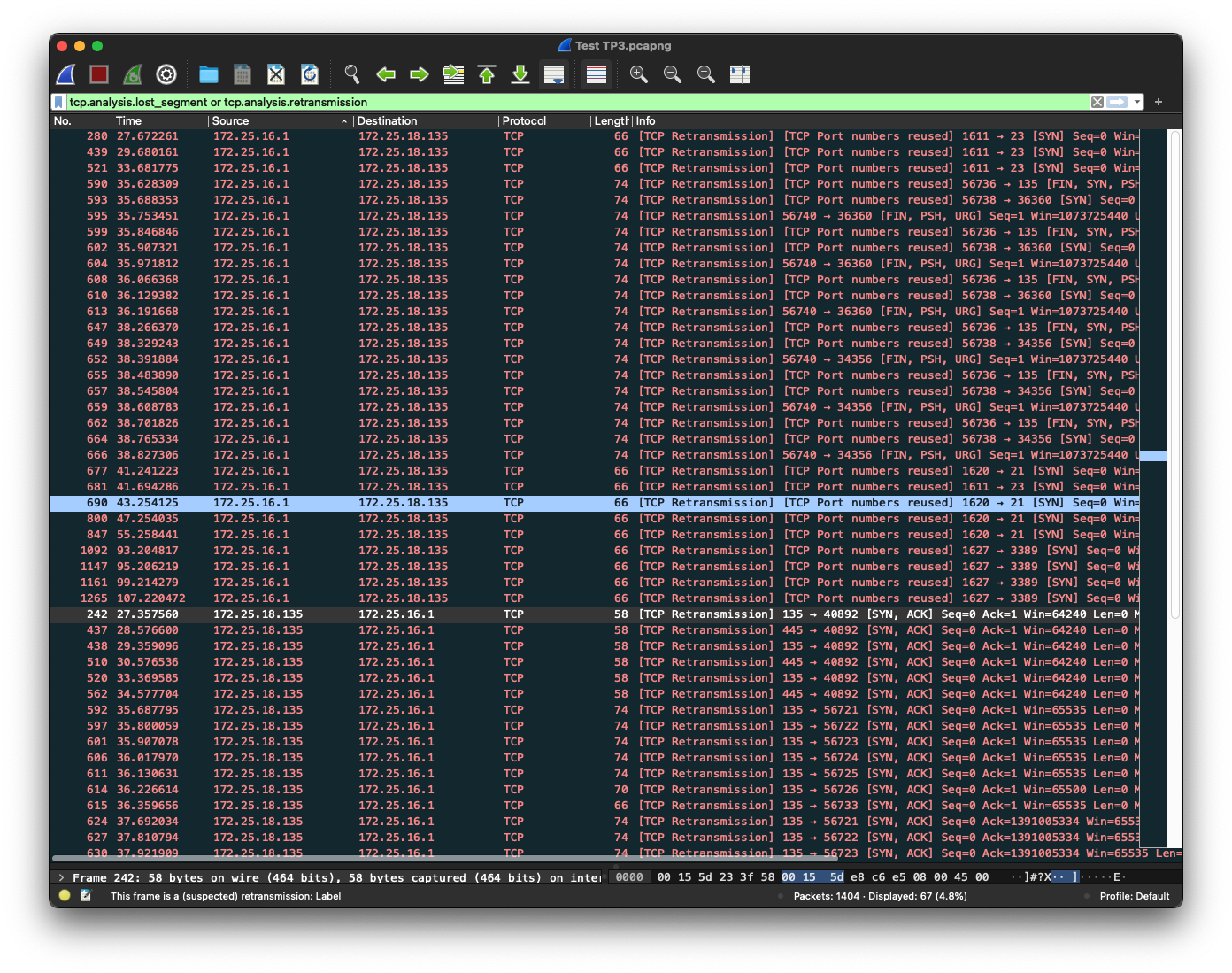
Nous pouvons aussi remarquer qu’à plusieurs reprises, l’hôte 172.25.16.1 tente potentiellement de pénétrer un ou plusieurs pare-feux, tout en essayant de découvrir des ports ouverts (attaque de type *TCP Null scanning*). Ces actions semblent avoir pour objectif de se connecter au poste du dirigeant. Ce constat peut être justifié par l’envoi de paquets sans *flag* en provenance de l’hôte 172.25.16.1 vers le poste du dirigeant ( Detecting Network Attacks with Wireshark, 2023) :



Une autre technique ayant été peut être utilisée est celle nommée TCP Xmas scan. Cette attaque peut être remarqué lorsqu’un hôte tente d’envoyer des paquets avec les *flags* FIN, PUSH et URG. Encore, cette attaque permet de pénétrer des pare-feux pour découvrir des ports ouverts, et donc vulnérables à des attaques ( Detecting Network Attacks with Wireshark, 2023). Dans le cas de la situation à l’étude, nous pouvons remarquer que l’hôte 172.25.16.1 envoie ce genre de requête à l’hôte du poste du dirigeant (172.25.18.135) :

D’autant plus, une attaque de type *ICMP Flood* peut être détecté. En effet, l’hôte 172.25.16.1 semble vouloir congestionner le réseau en envoyant de manière consécutive de lourds paquets (supérieur à 48 octets) au poste du dirigeant (à travers le lancement de plusieurs ping). Ces paquets surpasse la taille normale de paquets envoyés par une commande ping, soit de 32 octets pour les terminaux Window et de 48 octets pour les appareils Linux (Detecting Network Attacks with Wireshark, 2023).

Ces envois se sont déroulés en deux temps. Nous pouvons remarquer que ces deux tentatives se sont déroulées dans les intervalles des numéros de capture 575 à 578 et 631 à 634 :

Nous pouvons aussi remarquer que plusieurs paquets ont été perdus lors de certains échanges entre les hôtes 172.25.16.1 et 172.25.18.35 (dirigeant). En effet, il y a eu retransmission de plusieurs paquets en provenance de l’hôte inconnu 175.25.16.1. Une telle situation peut être causée par une attaque par déni de service (Detecting Network Attacks with Wireshark, 2023). Voici la capture Wireshark montrant un aperçu de ces multiples retransmissions :

En bref, dans la capture WireShark, il a été possible de détecter plusieurs attaques. Dans leur majorité, celles-ci provenaient de l’adresse IP 172.25.16.1 possédant l’adresse MAC suivante 00 : 15 : 5d : 23 : 3f : 58 et le HostName suivant : CA042958. Ce dernier propos est vérifiable grâce au Brodcast effectué par le dirigeant (Who as 172.25.16.1, tell 172.25.18.35) à la ligne #676.

### Est-ce que de l’information a fuité à partir du poste du dirigeant ?

Selon les informations examinées sur Wireshark et NetworkMiner, il semblerait que oui parce que 13 sessions ont été effectuées entre le l'utilisateur inconnu (172.25.16.1) et le dirigent (172.25.18.135). De plus, puisque plusieurs requêtes, dont des requêtes de connexion, ont été effectuées par le dirigeant en protocol http, on peut facilement présumé que l’utilisateur inconnu a pu avoir accès aux informations de login et les utiliser par la suite.

### Quelles sont vos conclusions finales sur cet incident et quel serait le plan d'action à adopter?

Nous pouvons conclure que plusieurs communications entre le client (172.25.18.135) et le serveur hébergeant forum.radioamateur.ca (72.18.137.100) n’ont pas été sécurisés, puisqu’utilisées avec le protocole HTTP. Tel que mentionné précédemment, il s’agit d’une problématique puisque qu’il rend les informations échangées accessible à d’autres utilisateurs utilisant un logiciels d’écoute réseau (Networking sniffing). Ainsi, ces derniers peuvent utiliser, par exemple, les informations de connexion du dirigeant au sein d’une capture Wireshark (i.e. nom d’utilisateur « tata ») pour se connecter au site.

Un plan d’action qui pourrait être adopté serait d’utiliser un certificat SSL. Ce principe consiste à chiffrer de manière asymétrique la connexion entre un client et un serveur. Ainsi, lorsqu’un client tenterait d’envoyer des informations au serveur, celles-ci seront chiffrées par une clé publique et pourront seulement être déchiffrées par la clé privé détenue par le serveur (notes de cours séance 7 Yacine, 2023).

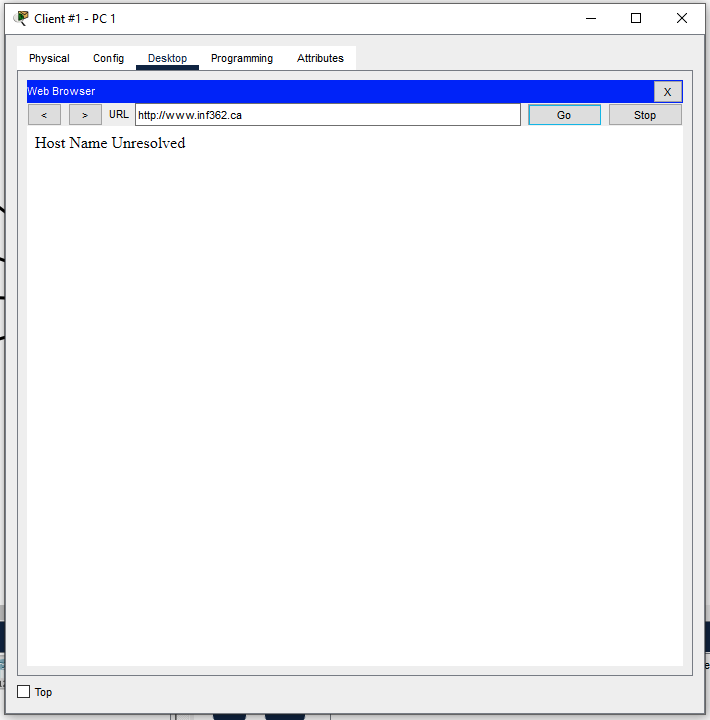
# Partie 2 : Exercice sur le DHCP Snooping (Packet Tracer)

### Question 1

#### Ouvrez le PC #1, à partir du « Web Browser » disponible dans l’onglet « Desktop », rendez-vous sur le site web du cours à partir des adresses spécifiées.

##### Que pouvez-vous constater en visitant le site ?

En visitant le site [www.inf362.ca](http://www.inf362.ca), il est possible de remarquer que le site affiche « Host Name Unrevolved ».



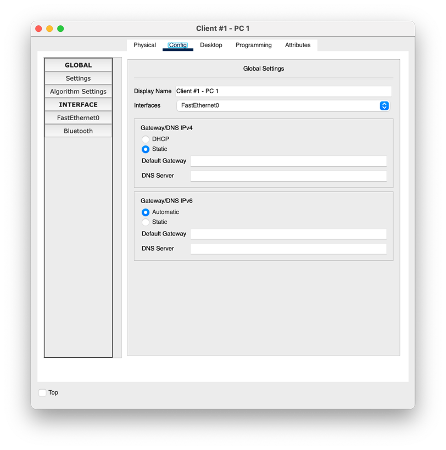
#### *Toujours sur le PC #1, lancez un ping vers le serveur Web avec l’adresse inf362.ca à partir de l’outil « Command Prompt » disponible dans l’onglet Desktop.*

##### Quelle adresse IP est résolue par le ping ?

Aucune adresse IP

##### Que pouvez-vous constater ?

En consultant la configuration du PC #1, nous pouvons remarquer qu’aucune adresse d’un serveur DNS est spécifiée :



Ainsi, le PC #1 ne peut pas avoir accès au site, car il n’a pas accès à un serveur DNS associant les noms de domaine du site et l’adresse IP du serveur hébergeant ce site.

Également, nous pouvons remarquer que l’adresse IP 0.0.0.0 est associée au PC #1 :



Ainsi, en ayant cette adresse, le PC #1 ne peut pas communiquer avec un autre appareil faisant partie du réseau (Mitchell, 2020).

Bref, configuré de cette façon, le PC #1 ne peut pas accéder au site du cours et résoudre l’adresse IP du serveur l’hébergeant en lançant la commande ping. D’ailleurs, le résultat de cette précédente commande nous permet de déduire que le paquet ICMP (ping) a été rejeté en silence sans qu'aucune réponse n'ait été envoyée.

#### Ouvrez le PC #2 et réalisez les mêmes opérations

##### Que pouvez-vous constater en visitant le site ?

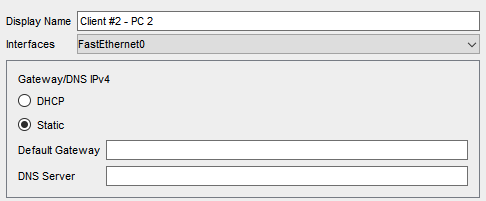
Il est possible de constater que le même message que sur le PC #1 s’affiche, soit « Host Name Unresolved »

##### Quelle adresse IP est résolue par le ping ?

Aucune adresse IP

##### Que pouvez-vous constater ?

Tout comme sur le PC#1, le PC#2 ne possède aucune configuration au niveau du serveur DNS



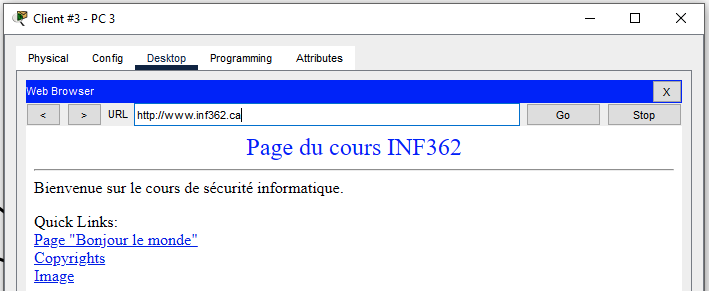
Également, l’adresse IP du PC #2 est 0.0.0.0, ce qui ne lui permet pas de communiquer avec d’autres appareils présents dans le réseau.

### Question 3

#### Ouvrez le PC #3 et réalisez les mêmes opérations

##### Que pouvez-vous constater en visitant le site ?

En visitant le site [www.inf362.ca](http://www.inf362.ca), il est possible de remarquer que le site affiche le contenu de la page Web. Ce contenu correspond au suivant :

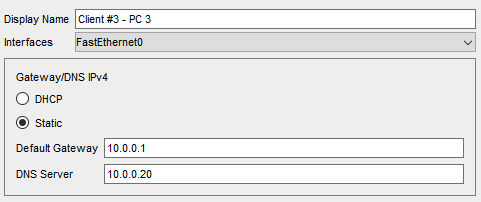


##### Quelle adresse IP est résolue par le ping ?

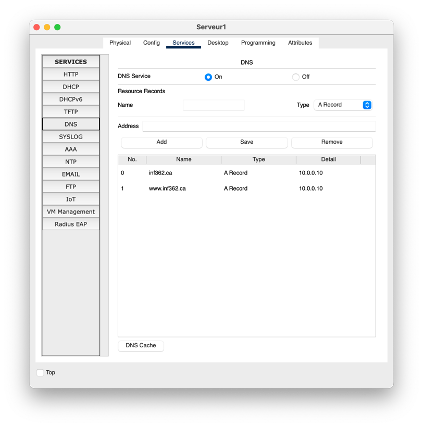
L’adresse 10.0.0.10 est résolu par le ping

##### Que pouvez-vous constater ?

Nous pouvons constater qu’un serveur DNS est configuré au sein du PC #3, ce qui représente une première condition pour accéder potentiellement au site du cours :



En consultant les détails serveur DNS avec l’adresse IP 10.0.0.20 (serveur 1), nous pouvons remarquer que les adresses inf362.ca et [www.inf362.ca](http://www.inf362.ca/) sont associées au serveur ayant l’adresse 10.0.0.10 (serveur 3) :



D’ailleurs, l’adresse 10.0.0.10 est une adresse de Classe A, donc d’une adresse propre au réseau privé utilisé.

Également, nous pouvons remarquer qu’une adresse IP autre que 0.0.0.0 est associée au PC #3 :



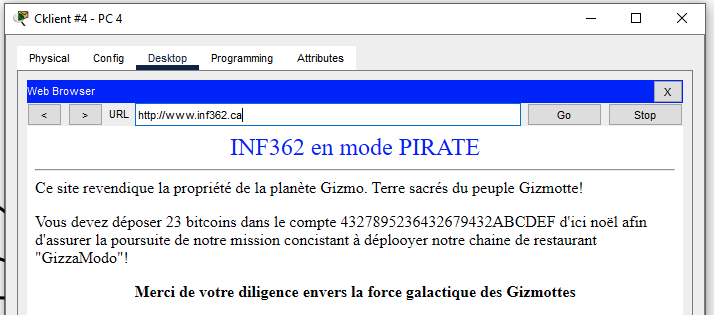
Bref, le PC #3 est en mesure d’accéder au site du cours, car il contient une adresse IP valide. D’autant plus, un serveur DNS est configuré, ce qui lui permet d’accéder au site du cours.

### Question 4

#### Ouvrez le PC #4 et réalisez les mêmes opérations

##### Que pouvez-vous constater en visitant le site ?

En visitant le site [www.inf362.ca](http://www.inf362.ca), il est possible de remarquer que le site affiche le contenu de la page Web. Toutefois, le contenu n’est pas le même que sur le PC#3. En effet, il semble y avoir eu un détournement vers une page en mode « pirate ». Voici le contenu correspondant :



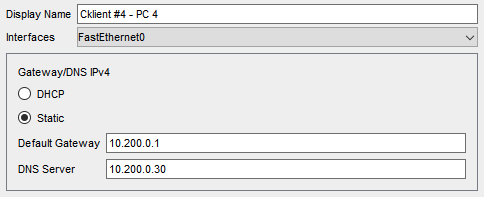
##### Quelle adresse IP est résolue par le ping ?

L’adresse résolue par le ping est la 10.200.0.30:

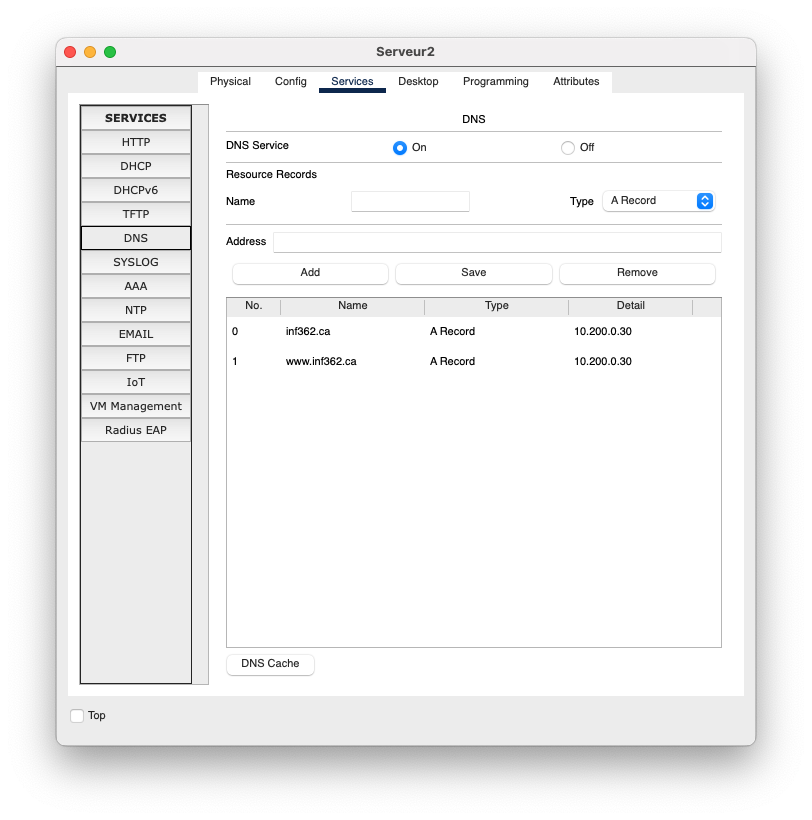


##### Que pouvez-vous constater ?

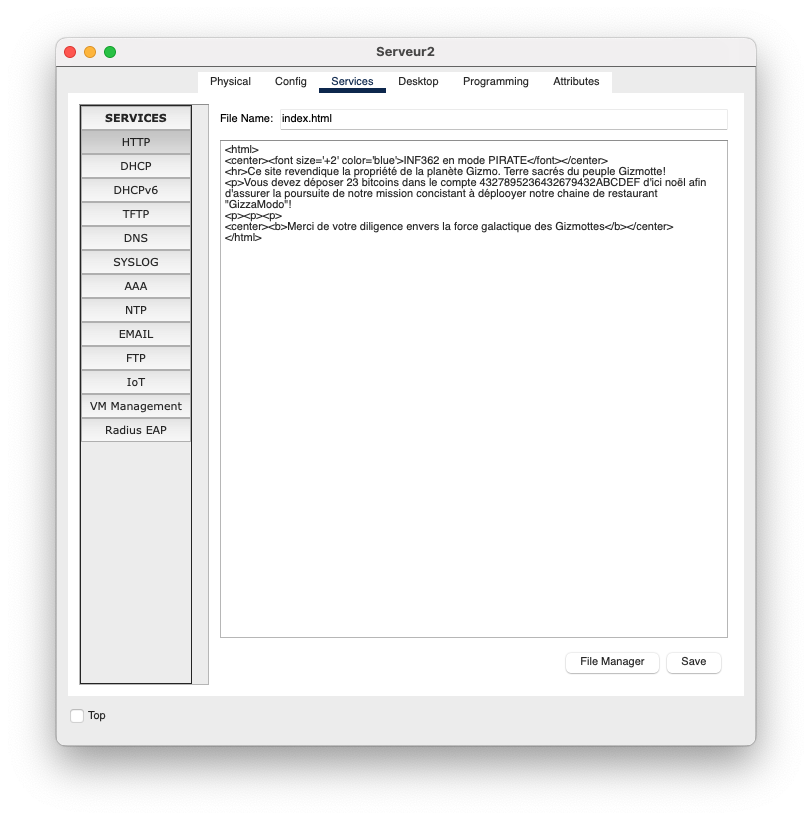
Nous pouvons constater que le PC #4 n’est pas associé au même serveur DNS que le PC #3. En effet, la résolution d’adresse pour le site inf362.ca n’est pas la même. En consultant la configuration du PC #4, nous pouvons confirmer cette hypothèse :



En consultant la configuration du serveur à l’adresse 10.200.0.30 hébergeant le service DNS, nous pouvons remarquer que les adresses IP associés aux noms de domaines du site du cours ne sont plus les mêmes:



En effet, ces adresses correspondent au serveur 2, hébergeant également un service HTTP. En consultant les fichiers Web contenus au sein de ce service, nous pouvons constater que ceux-ci réfèrent à la version compromise du site. Par exemple, voici le code HTML représentant la page principale de cette version piratée du site:

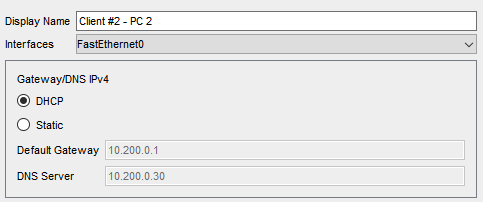


### Question 5

#### Rendez-vous sur le « Serveur4 ». Dans l’onglet « Service », cliquez sur le bouton « DHCP » dans le menu de gauche et désactivez le service via le bouton à droite « Service = OFF ». Attendez une minute que le service cesse de fonctionner. Rendez-vous ensuite sur le PC #2, dans le « Command Prompt » et lancez la commande : **ipconfig /renew**. Le PC devrait obtenir une adresse dans le réseau **10.200.0.x.** Rendez-vous ensuite sur le site inf362.ca dans le « Web Browser ».

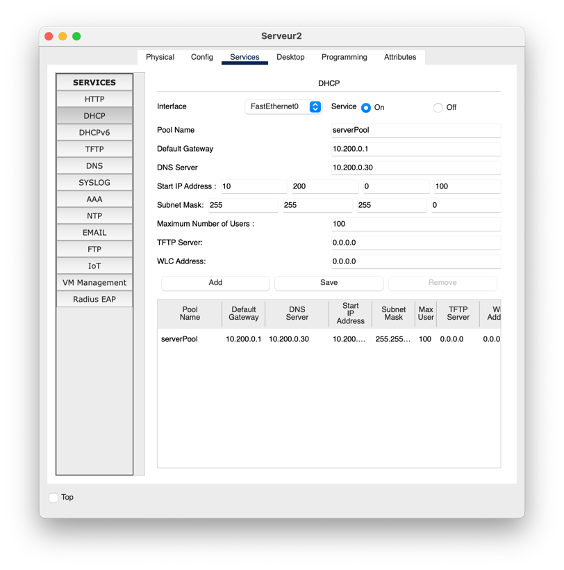
##### Que pouvez-vous conclure à la suite de ces tests ?

À la suite de ces tests, il est possible de constater que le PC#2 peut maintenant accéder au site du cours. En effet, en lançant la commande ipconfig /renew, le PC #2 a renégocié une adresse IP avec le serveur DHCP présent dans le réseau (McDunnigan, s.d.):

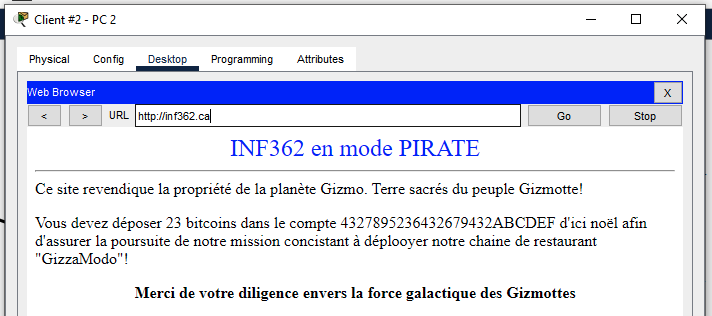


Dans ce cas, c’est le serveur 2 qui a répondu à cette requête, car il est dorénavant le seul serveur offrant ce service.

En consultant la configuration DHCP du serveur 2, nous pouvons remarquer que celui-ci assigne automatiquement à ses hôtes lui faisant appel l’adresse du serveur DNS 10.200.0.30 :



Toutefois, il est important de mentionner, quand ayant cette adresse DNS au sein de sa configuration, le navigateur du PC #2 affiches le contenu de la page web correspondant au contenu du cours en mode « pirate ».



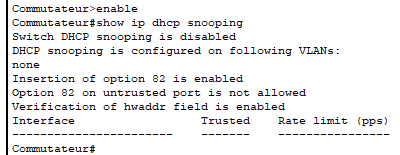
### Question 6

#### Rendez-vous sur le commutateur dans l’onglet « CLI ». Cliquez dans l’écran « IOS Command Line Interface » et donnez quelques coups de « Enter » sur le clavier. Entrez en mode privilégié dans le commutateur en saisissant la commande **enable** suivie d’un coup de « enter ».

#### Vérifiez si le commutateur est protégé contre le DHCP Snooping en lançant la commande : **show ip dhcp snooping.**

##### Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?

Le commutateur n’est pas protégé contre le DHCP Snooping. En effet, en lançant la commande précédente, le message suivant s’affiche : Switch DHCP snooping is disabled:



Plus précisément, le commutateur n’est pas configuré afin de restreindre l’activité de serveurs DHCP non autorisés (Bhanu, 2022). En effet, la configuration actuelle du commutateur ne spécifie pas les ports valables où les communications des serveurs DHCP sont permises. Ainsi, chaque client DHCP n’est pas protégé contre les attaques DHCP possibles. Par exemple, il est possible qu’un client DHCP reçoive des informations réseau erronés provenant d’un serveur DHCP invalide (Huawei, 2021). Nous pouvons d’ailleurs percevoir cette problématique au sein du réseau à l’étude. En effet, précédemment, lorsque le PC #2 a effectué une requête DHCP à l’aide de la commande ipconfig /renew, le serveur 2 a été celui qui a répondu à cette requête et qui a fourni au PC #2 des informations réseau invraisemblablement valides. Lorsque le PC #2 tentait d’accéder au site du cours, une version piratée de ce site s’affichait au sein du navigateur.

##### À l’aide d’une recherche sur internet, que permet l’option 82 du service DHCP ?

L’option 82 du service DHCP permet d’ajouter un niveau de sécurité supplémentaire lors de l’allocation d’adresses IP. Elle peut être appliquée à un réseau local virtuel (VLAN), à un domaine de passerelle (Bridge Domain) ou de manière globale au sein d’un réseau (Juniper Networks, 2022). En effet, cette option permet à un serveur DHCP d’allouer seulement des adresses IP à des appareils reconnus et identifiables sur le réseau (Juniper Networks, 2021). Afin de connaître la validité de ces appareils, le serveur DHCP fait la vérification de certaines informations contenues dans l’entête des paquets formant les requêtes. Lorsque l’option 82 est activée, ces informations sont ajoutées par le commutateur faisant le relais entre les appareils demandant une adresse IP et le serveur DHCP. Ces informations permettent de connaître la localisation d’un client et de lui associer une adresse IP:

* Circuit Id : il s’agit de l’identifiant du VLAN ou du domaine de passerelle par rapport au commutateur où la requête a été reçue;
* Remote Id : il s’agit de l’identifiant de l’appareil faisant appel au service DHCP;
* Vendor Id : il s’agit de l’identifiant du vendeur de l’appareil faisant appel au service DHCP (Juniper Networks, 2021).

Lorsque le serveur DHCP est en mesure de valider les informations de l’entête, il envoie une réponse ACK au commutateur pour que ce dernier relaie cette information au client. Une réponse NACK sera envoyée si la requête n’est pas conforme (Deland-Han, 2023).

### Question 7

#### Dans l’écran de configuration du commutateur en « Command Line », entrez en mode de commande en plaçant la commande **conf T**. Lancez alors la commande : **ip dhcp snooping** et reprenons les précédentes questions.

##### Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?

La protection contre le DHCP Snooping du commutateur est activée, mais elle n’est pas appliquée à un ou à des VLANs précis. Ainsi, la prochaine étape à effectuer afin de configurer la fonctionnalité contre le DHCP Snooping serait d’ajouter un port de confiance associé à un VLAN précis. Ainsi, le serveur DHCP faisant partie de ce réseau local virtuel serait autorisé à allouer des adresses IP aux client DHCP.

#### Retournez dans le « Command Prompt » des PC #1 et #2 et relancez la commande **ipconfig /renew** sur les deux PC.

##### Que pouvez-vous conclure ?

Il n’est plus possible d’effectuer une configuration d’un serveur DHCP sur le PC#1 et le PC#2. La requête DHCP échoue :



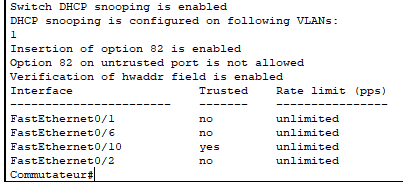
En effet, aucun port de confiance est configuré pour rendre la protection contre le DHCP Snooping fonctionnel.

### Question 8

#### À la suite de la multitude des opérations (voir PDF), vérifiez si le commutateur est protégé contre le DHCP Snooping en lançant la commande : **show ip dhcp snooping**.

##### Est-ce que le commutateur est protégé contre le DHCP Snooping, détaillez votre réponse ?

Le commutateur est dorénavant protégé contre le DHCP Snooping:



En effet, le serveur 4 peut offrir un service DHCP, car il est associé au port de confiance fa0/10 (faisant partie du VLAN 1). Même si le serveur 2 offre aussi techniquement un service DHCP, il n’est plus considéré pour de telles requêtes, puisqu’il n’est pas attaché au port fa0/10.

### Conclusion

##### À la lumière de cet exercice, pouvez-vous identifier quels sont les services malveillants présents sur le réseau ? et où se trouvent-ils ?

Les services DHCP, DNS et HTTP étant exploités au sein du serveur 2 sont malveillants.

##### Décrivez votre démarche qui vous mène à ce constat.

En effet, en réalisant les manipulations demandées au sein de la question #4, nous avons pu constater que le PC #4 a accédé à une version piratée du site du cours. En consultant la configuration du PC #4, nous avons pu remarquer que l’adresse IP du serveur exploitant le serveur DNS était 10.200.0.30, soit celle correspondant au serveur 2. À ce stade, nous avons pu alors déjà déduire que le service DNS de ce serveur était malveillant et menait à un serveur non autorisé. Ensuite, en consultant les paramètres de ce service DNS, nous avons pu conclure que les noms de domaine du site étaient associés à l’adresse IP du serveur 2. En observant la configuration du service HTTP du serveur 2, nous avons pu remarquer que celui-ci contient des fichiers HTML permettant la génération de la version compromise du site du cours. Enfin, tel que mentionné en répondant à la question #5, le service DHCP du serveur 2 est compromis puisqu’il transmet aux client DHCP lui faisant appel des informations compromises, comme celle du serveur DNS à utiliser (celui du serveur 2).

##### Que pouvez-vous conclure de ce type d’attaque ?

Lorsqu’un commutateur ne possède pas de configuration sur le port de confiance du serveur DHCP, un utilisateur malveillant peut simuler qu’il représente le dit serveur DHCP et ainsi contrôler l’attribution des adresse IP, cela peut s’avérer dangereux pour de l’écoute de données (Man in the middle) ou dans le cas d’un détournement de site web comme dans l’exercice présent.

##### \*\*\*\*\*\*Que pouvez-vous conclure sur la protection appliquée et quelles sont les informations que l’administrateur réseau doit détenir afin d’assurer une configuration de la protection adéquate ?

Nous pouvons conclure que la protection contre le DHCP Snooping mise en place permet de définir clairement quel serveur DHCP pourra répondre aux requêtes des clients DHCP. Afin d’assurer une configuration adéquate, l’administrateur doit bien connaître l’infrastructure réseau mise en place afin de pouvoir cerner quels sont les serveurs fiables. Ainsi, un meilleur contrôle pourra être exercé et seuls les services valides pourront être exécutés (i.e. service DHCP). Plus précisément, il doit être en mesure de connaître l’adresses des serveurs hébergeant les services DHCP, DNS et HTTP valides.

# Bibliographie

« Detecting Network Attacks with Wireshark - InfosecMatter ». s. d. Consulté le 6 avril 2023. <https://www.infosecmatter.com/detecting-network-attacks-with-wireshark/?fbclid=IwAR2JfL4cgMBWzCBlEJhR8q795VAs-u0nPi2OsU5oMmIBRcvji-CQ1Czf9NU>.

Bhanu, P. (2022, 21 mars). *What is DHCP snooping*. Repéré à l’adresse <https://www.tutorialspoint.com/what-is-dhcp-snooping>

Deland-Han. (2023, février 23). *DHCP client can’t get a DHCP-assigned IP address—Windows Server*. Repéré à <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/dhcp-client-fail-obtain-valid-ip-address>

Huawei. (2021, 30 mars). *What Is DHCP Snooping ? Why Do We Need DHCP Snooping ?* Repéré à l’adresse <https://info.support.huawei.com/info-finder/encyclopedia/en/DHCP+Snooping.html>

Juniper Networks. (2021). *Understanding DHCP Option 82*. Repéré à [Understanding DHCP Option 82 | Junos OS | Juniper Networks](https://www.juniper.net/documentation/us/en/software/junos/security-services/topics/concept/port-security-dhcp-option-82.html)

Juniper Networks. (2022, 11 mai). *DHCP Relay Agent Information Option (Option 82)*. Repéré à [DHCP Relay Agent Information Option (Option 82) | Junos OS | Juniper Networks](https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcp-relay-agent-information-option82.html)

McDunnigan, M. (s.d). *What Does IPConfig/Renew Accomplish?* Repéré à l’adresse <https://yourbusiness.azcentral.com/ipconfig-renew-accomplish-27621.html>

Mitchell, B. (2020, 7 novembre). *What It Means When You See the 0.0.0.0 IP Address*. Repéré à ﷟HY[ps://www.lifewire.com/four-zero-ip-address-818384](ps://www.lifewire.com/four-zero-ip-address-818384%22ht)