Etude des trames (avec Wireshark)

BTS SiO1 2022-2023 / IZAC Matthieu

-SOMMAIRE

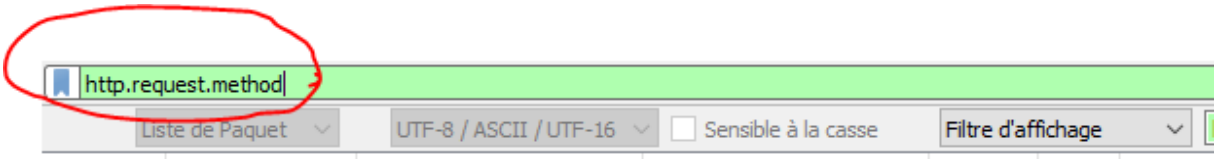
- C’est quoi wireshark ?

Wireshark est un logiciel open source d’analyse des protocoles réseau créé par Gerald Combs en 1998. Un groupe international d’experts réseau et de développeurs gère aujourd’hui cet outil et le met à jour pour assurer sa compatibilité avec les nouvelles technologies réseau et méthodes de chiffrement. Wireshark ne pose absolument aucun risque de sécurité. Il est notamment utilisé par des agences gouvernementales, de grandes entreprises, des organisations à but non lucratif et des établissements pédagogiques pour résoudre des problèmes réseau et assurer des formations. Il n’y a pas de meilleur moyen pour apprendre le fonctionnement des réseaux que d’analyser du trafic sous le microscope de Wireshark. La question de la légalité de Wireshark est souvent posée, car il s’agit d’un puissant outil de capture de paquets. Pour rester du côté lumineux de la Force, il ne faut utiliser Wireshark que sur les réseaux autorisé.

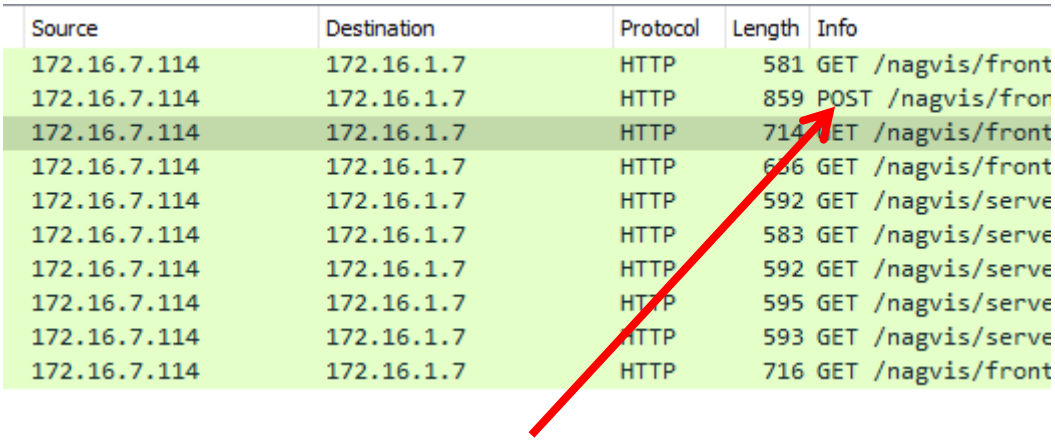
D’après : https://www.varonis.com/fr/blog/comment-utiliser-wireshark

- Trouver divers informations via l'étude des trames.

Pour commencer il faut trouver la méthode post qui suit le protocole http étant donné que c'est un serveur web, pour cela on filtre les trames à l'aide d'un contrôle F et en rentrant « http.request.method == POST »

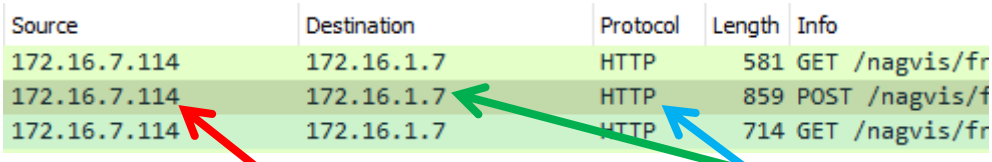


On obtient cela :



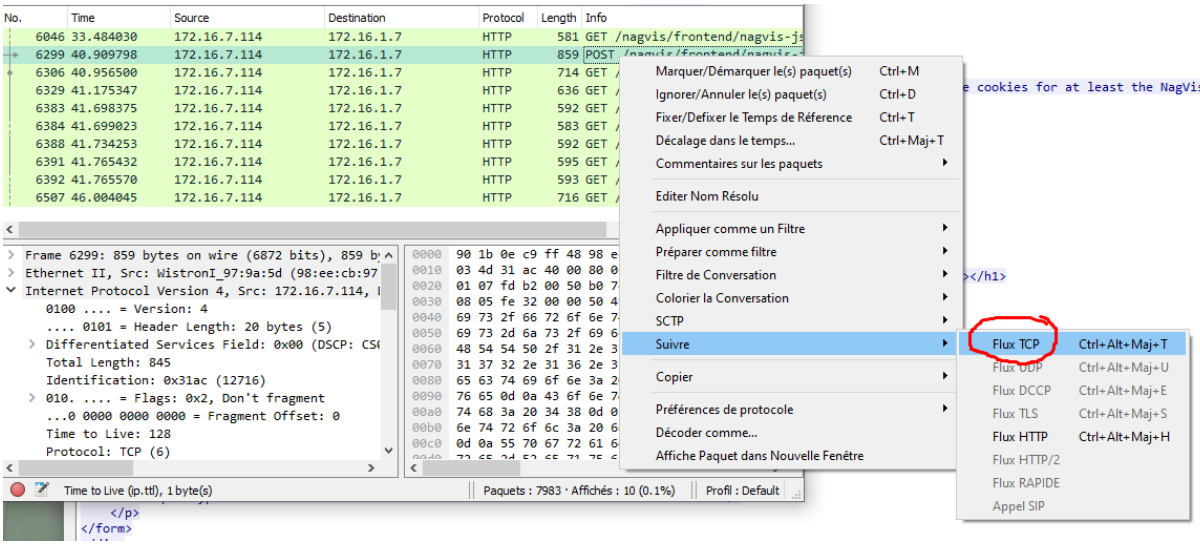
Source	Destination	Protocol	Length	Info
172.16.7.114	172.16.1.7	HTTP	581	GET /nagvis/front
172.16.7.114	172.16.1.7	HTTP	859	POST /nagvis/fron
172.16.7.114	172.16.1.7	HTTP	714	GET /nagvis/front
172.16.7.114	172.16.1.7	HTTP	656	GET /nagvis/front
172.16.7.114	172.16.1.7	HTTP	592	GET /nagvis/serve
172.16.7.114	172.16.1.7	HTTP	583	GET /nagvis/serve
172.16.7.114	172.16.1.7	HTTP	592	GET /nagvis/serve
172.16.7.114	172.16.1.7	HTTP	595	GET /nagvis/serve
172.16.7.114	172.16.1.7	HTTP	593	GET /nagvis/serve
172.16.7.114	172.16.1.7	HTTP	716	GET /nagvis/front

La méthode POST se trouve donc ici c'est celle-là qui nous intéresse.



Source	Destination	Protocol	Length	Info
172.16.7.114	172.16.1.7	HTTP	581	GET /nagvis/fr
172.16.7.114	172.16.1.7	HTTP	859	POST /nagvis/f
172.16.7.114	172.16.1.7	HTTP	714	GET /nagvis/fr

On retrouve donc ici : l'ip de l'ordinateur qui a renseigné les infos, l'ip du serveur non sécurisé qui les a enregistrés ainsi que le protocole utilisé.



On va ensuite dans flux TCP pour trouver le mot de passe ainsi que l'identifiant rentré par l'utilisateur qui a envoyé la trame.

```
POST /nagvis/frontend/nagvis-js/index.php HTTP/1.1
Host: 172.16.1.7
Connection: keep-alive
Content-Length: 48
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://172.16.1.7
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Referer: http://172.16.1.7/nagvis/frontend/nagvis-js/index.php
Accept-Encoding: gzip, deflate
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=7hm8s1e77r28c936s9tf8ut50v; nagvis_session=th0qb2kag97ckilpuvnlqss7m1

_username=admin&_password=admin&submit=ConnexionHTTP/1.1 302 Found
Date: Wed, 08 Mar 2023 14:59:34 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: nagvis_session=th0qb2kag97ckilpuvnlqss7m1; path=/;HttpOnly
Location: /nagvis/frontend/nagvis-js/index.php
X-Frame-Options: sameorigin
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET /nagvis/frontend/nagvis-js/index.php HTTP/1.1
```

On trouve donc bien un nom d'utilisateur ainsi que son mot de passe.

- Comment sécuriser les trames ?

Pour éviter tout problème il faut se passer d'utiliser un protocole http qui lui, n'est pas sécuriser il faut privilégier l'utilisation du protocole https (Hyper Text Transfer Protocol Secure) qui comme son nom l'indique est sécurisé. Les données échangées seront de ce fait chiffrées et évite d'être espionné à l'aide d'un simple renifleur de trame tel que wireshark.