

Activité Wireshark

Un analyseur de réseau indispensable

L'objectif de cette activité est de comprendre l'importance d'utiliser des logiciels sécurisés.

1 – Wireshark, c'est quoi ?

Wireshark est un logiciel libre et open source pour l'analyse et le dépannage des réseaux informatiques. Il permet aux utilisateurs de capturer et d'inspecter les données qui circulent sur un réseau informatique en temps réel. Les filtres d'affichage et de capture permettent de se concentrer sur des paquets spécifiques en fonction de critères précis :

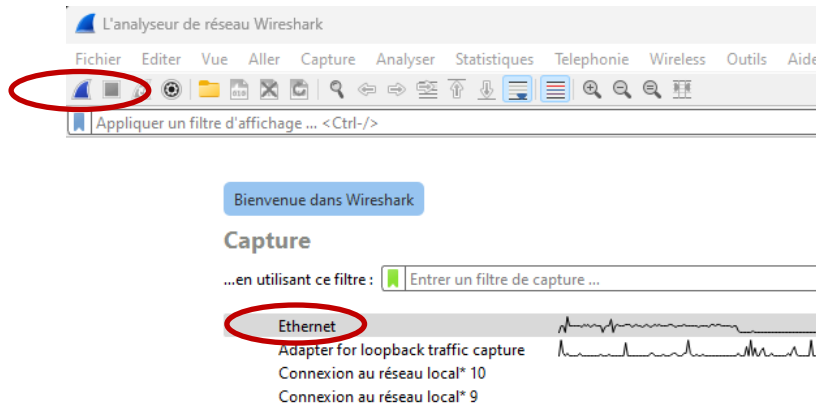
- Adresse IP
- Protocole
- Port
- Etc

Lors de cette activité vous allez voir que l'utilisation d'un logiciel mal sécurisé peut permettre la récupération d'un mot de passe.

2 – Analyse avec Wireshark

1 – Démarrer le logiciel Wireshark. Vous devez sélectionner la carte Ethernet que vous allez analyser. Dans mon cas : "Ethernet".

Pour démarrer la capture, cliquez sur l'aileron de requin et sur le carré rouge pour la stoppée.

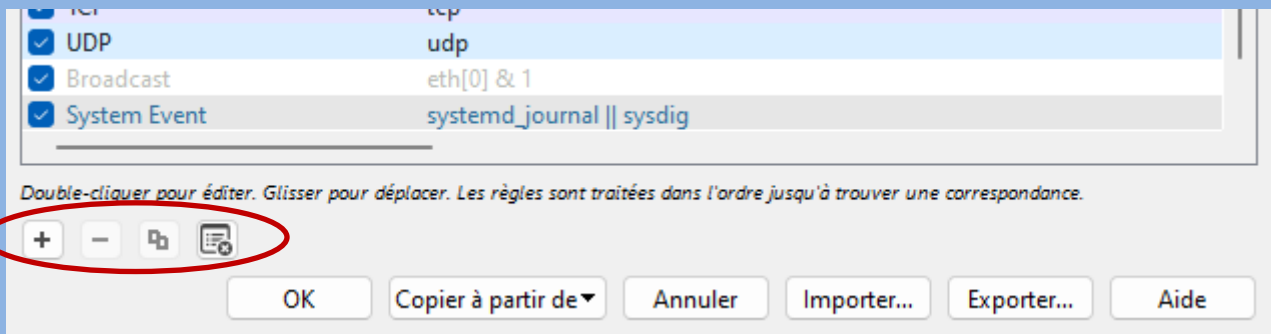


2 – Wireshark utilise un code couleur pour classer les paquets en fonction du protocole, de l'adresse IP, de la fonction, ...

Nom	Filtre
☒ Bad TCP	<code>tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis</code>
☒ HSRP State Change	<code>hsrp.state != 8 && hsrp.state != 16</code>
☒ Spanning Tree Topology Change	<code>stp.type == 0x80</code>
☒ OSPF State Change	<code>ospf.msg != 1</code>
☒ ICMP errors	<code>icmp.type in { 3..5, 11 } icmpv6.type in { 1..4 }</code>
☒ ARP	<code>arp</code>
☒ ICMP	<code>icmp icmpv6</code>
☒ TCP RST	<code>tcp.flags.reset eq 1</code>
☒ SCTP ABORT	<code>sctp.chunk_type eq ABORT</code>
☒ IPv4 TTL low or unexpected	<code>(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim ospf eigrp bgp tc</code>
☒ IPv6 hop limit low or unexpected	<code>(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf bgp tcp.port==</code>
☒ Checksum Errors	<code>eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum</code>
☒ SMB	<code>smb nbss nbns netbios</code>
☒ HTTP	<code>http tcp.port == 80 http2</code>
☒ DCERPC	<code>dcerpc</code>
☒ Routing	<code>hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp</code>
☒ TCP SYN/FIN	<code>tcp.flags & 0x02 tcp.flags.fin == 1</code>
☒ TCP	<code>tcp</code>
☒ UDP	<code>udp</code>
☒ Broadcast	<code>eth[0] & 1</code>
☒ System Event	<code>systemd_journal sysdig</code>

✍ 3 – Effectuez une capture de 2 secondes environ et vérifiez le code couleur. Suivant le résultat de votre capture, relevez trois couleurs et le protocole associé.

Vous pouvez également créer votre propre règle de couleur en fonction de critères tels que l'adresse IP source ou de destination, le port, le protocole, la taille du paquet, etc.



Dans l'ensemble, les règles de couleur dans Wireshark sont un outil puissant pour aider les utilisateurs à analyser le trafic réseau et à identifier rapidement les paquets importants ou suspects.

Pour la suite du TP vous utiliserez la capture "capture1.pcapng".

✍ 4 – Ouvrir le fichier "capture1.pcapng" puis relevez la durée de la capture et le nombre de trames. Calculez le nombre de trames par seconde.

✍ 5 – Utilisez la combinaison suivante : Ctrl + Shift + Alt + C. Qu'obtenez-vous ?

👉 6 – Retrouvez la valeur du nombre de trames par seconde (pps) et vérifiez votre calcul de la question 4.

👉 7 – Lorsque vous faites l'analyse d'une capture, vous pouvez ajouter des commentaires en lien avec certaines trames. Par exemple, sélectionnez la trame 5, clic droit puis "commentaire sur les paquets" et "ajouter un nouveau commentaire". Ecrivez : "l'adresse IP 192.168.1.25 est celle du poste de DUPONT".

👉 8 – Utilisez à nouveau la combinaison : Ctrl + Shift + Alt + C. Vérifier la présence du commentaire dans les propriétés du fichier de capture.
Ceci est utile lorsque plusieurs personnes sont amenées à travailler sur le même fichier ou pour mettre en avant une analyse, une méthodologie, ...

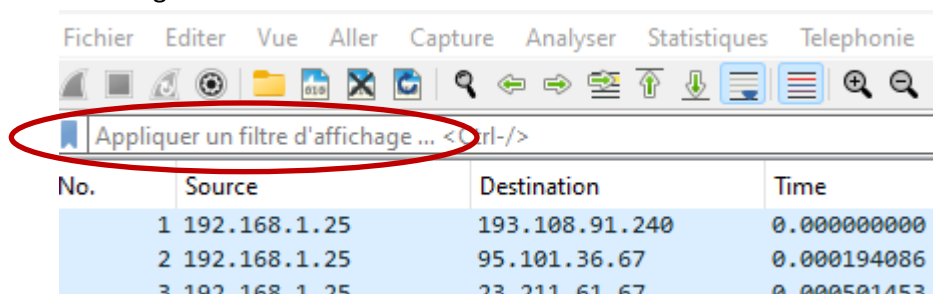
✍ 9 – Quels sont les protocoles utilisés lors de cette capture ?

 10 – Complétez le tableau suivant :

Nom du protocole	La fonction de ce protocole
DNS	DNS (Domain Name System) est un système utilisé pour traduire les noms de domaine en adresses IP. Il permet aux utilisateurs d'accéder à des sites web et à d'autres ressources en ligne en utilisant des noms de domaine faciles à retenir, plutôt que des adresses IP numériques difficiles à mémoriser.
TCP	
http	
TLSv1.2	
TLSv1.3	
IPv4	
OSCP	

3 – Analyse du protocole DNS

11 – Vous allez filtrer les trames. Si l'on souhaite filtrer le protocole DNS il suffit d'écrire "dns" dans la zone de filtrage de WireShark. Faites le test.



Vous consterez que seule les trames qui utilisent le protocole DNS sont affichées. Cela fait encore beaucoup.

12 – Cliquez sur la trame 5. On constate que WireShark vous indique (flèche dans la marge gauche) que la réponse se situe à la trame 11.

The screenshot shows the Wireshark interface with packet 5 selected. A red circle is drawn around the packet list, and another red circle is drawn around the packet details pane. A vertical dashed line with arrows at both ends connects the selected packet to the packet details pane, indicating the response relationship.

No.	Source	Destination	Time	Protocol
5	192.168.1.25	96.7.49.67	0.000933416	DNS
6	192.168.1.25	23.211.133.67	0.001402533	DNS
7	192.168.1.25	95.100.168.67	0.001580626	DNS
8	192.168.1.25	84.53.139.67	0.002143888	DNS
9	192.168.1.25	184.26.160.67	0.002389726	DNS
10	192.168.1.25	84.53.139.64	0.002630466	DNS
11	96.7.49.67	192.168.1.25	0.002906056	DNS

13 – Que pouvez-vous en conclure en analysant ces deux trames ?

14 – Quelle est l'adresse IP du serveur DNS ?

15 – Effectuez une nouvelle recherche, sélectionnez seulement les trames qui utilisent l'adresses ip du serveur DNS.

Commencez à taper "ip" dans la barre de recherche. WireShark vous propose différentes syntaxes. A vous de jouer !

Commande :

16 – Quelles sont les trames que vous avez trouvées ?

17 – Sélectionner la trame 31. Quelle est l'adresse du serveur DNS utilisé et retrouvez l'adresse IP du site demandé ?

Ces données sont aussi accessibles dans les données des trames 31 et 47.

No.	Source	Destination	No.	Source	Destination	Time	Pi
31	192.168.1.25	23.74.25.192	31	192.168.1.25	23.74.25.192	0.018700865	DI
47	23.74.25.192	192.168.1.25	47	23.74.25.192	192.168.1.25	0.022139383	DI

> Frame 31: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0

> Ethernet II, Src: ASUSTekCOMPU_2e:15:90 (bc:ee:12:2e:15:90), Dst: 08:00:27:00:00:00

> Internet Protocol Version 4, Src: 192.168.1.25, Dst: 23.74.25.192

> User Datagram Protocol, Src Port: 57861, Dst Port: 53

Domain Name System (query)

Transaction ID: 0x2e19

> Flags: 0x0010 Standard query query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 1

Queries

> ns1-1.akamaitech.net: type A, class IN

Additional records

> <Root>: type OPT

[Request In: 31]

[Response In: 47]

> Frame 47: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface 0

> Ethernet II, Src: AnovFrance_0c:ed:79 (a4:3e:51:0c:ed:79), Dst: 08:00:27:00:00:00

> Internet Protocol Version 4, Src: 23.74.25.192, Dst: 192.168.1.25

> User Datagram Protocol, Src Port: 53, Dst Port: 57861

Domain Name System (response)

Transaction ID: 0x2e19

> Flags: 0x8400 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 1

Queries

> ns1-1.akamaitech.net: type A, class IN

Answers

> ns1-1.akamaitech.net: type A, class IN, addr 193.108.88.1

Additional records

> <Root>: type OPT

[Request In: 31]

[Time: 0.003438518 seconds]

- 18 – Pouvez vous en déduire le numéro du port utilisé par le service DNS ?
- 19 – Trame 113, nouvelle demande DNS, analysez la réponse et donnez l'adresse IP du site recherché.
- 20 – A partir de quelle trame, ce site est-il consulté ?
- 21 – Pour suivre une requête et consulter toutes les trames en lien avec celle sélectionnée, faire un clic droit puis suivre, puis sélectionné un des protocoles proposés. L'ensemble des trames concernées s'affiche.
- 22 – Pourquoi a-t-on soit du TCP, soit du HTTP comme protocole ?
- 23 – Expliquez l'échange au niveau des trames 115, 116 et 117 ?
- 24 – Que se passe-t-il à la trame 118 ? Expliquez la suite.
- 25 - Expliquez l'échange entre les trames 121 et 135.

 26 – Que se passe-t-il ensuite ?

3 – Analyse du protocole OCSP

Présentation du protocole OCSP

Le protocole OCSP (**O**nline **C**ertificate **S**tatus **P**rotocol) est un protocole de sécurité utilisé pour vérifier l'état d'un certificat numérique. Il permet de déterminer si un certificat est toujours valide ou s'il a été révoqué, c'est-à-dire s'il a été annulé avant sa date d'expiration normale.

Le protocole OCSP fonctionne en permettant à un client de demander l'état d'un certificat à un serveur OCSP. Le serveur OCSP vérifie l'état du certificat auprès de l'autorité de certification (CA) qui a émis le certificat, puis renvoie une réponse au client indiquant si le certificat est **valide** ou **révoqué**.

Le protocole OCSP est utilisé dans de nombreuses applications en ligne, telles que la navigation web sécurisée (HTTPS), la messagerie électronique sécurisée (SMTPS, IMAPS, POP3S), le transfert de fichiers sécurisé (FTPS, SFTP) et les connexions VPN sécurisées.

 27 – Isolez les trames OCSP.

Vous pouvez constater qu'il existe une trentaine de lignes, soit des requêtes, soit des réponses. Il faut utiliser une autre méthode pour isoler une requête et sa réponse.

 28 – Sélectionnez la première trame OCSP (trame 221) et sélectionnez l'option suivre.

 29 – On constate que les échanges ont commencé à la trame 218. Pourquoi ?

Trame 218, 219, 220 :

Trame 221 :

Trame 224 :

Trame 233 :

Trame 223 :

 30 – Analysez en détail la requête OCSP (trame 221)

URL du site contacté :

Type de hashage :

 31 – Analysez en détail la réponse (trame 233)

Statut de la réponse :