

25/11/2023

TP - Analyse forensic réseau

Cyber management school



Réalisé par : Abdellah

Niveau 0 : Echange Telnet :

1.Qu'est-ce que Telnet ?

Telnet est un protocole de communication qui permet à un utilisateur d'accéder à un autre ordinateur à distance sur un réseau, comme l'Internet. Il fonctionne sur le modèle client-serveur, où l'utilisateur (client) se connecte à un serveur distant à l'aide du protocole Telnet

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

Bien que Telnet ait été largement utilisé par le passé, son utilisation a diminué considérablement de nos jours, principalement en raison de ses vulnérabilités en matière de sécurité. Telnet ne chiffre pas les données pendant la transmission, ce qui expose les informations sensibles à des risques de sécurité élevés.

3. Identifier le rôle de chaque machine dans la communication

Dans une communication Telnet, deux machines sont généralement impliquées : le client Telnet et le serveur Telnet.

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 ?

L'utilisateur (192.168.0.2) envoie une requête à l'adresse suivante 192.168.0.1 qui héberge le site yahoo.com. L'utilisateur veut accéder à l'internet.

De plus, le port de l'utilisateur est 1254 et le port destinataire est 23 (Telnet)

```
on 4, Src: 192.168.0.2, Dst: 192.168.0.1
4
```

On peut aussi voir le contenu des paquets : voici des exemples :

| | |
|---|---|
| <pre>...;...E =Z...@...X ...@...f.S.A C.E-...Kv ...Passwo rd:</pre> | <pre>...;...E 5...@... ...S.A...o }x}...T Kvu</pre> |
|---|---|

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

Dans la barre de recherche, on entre "Telnet" pour filtrer les logs afin d'obtenir uniquement les échanges du protocole Telnet. En vérifiant chaque échange, on aperçoit que le mot de de passe et le login sont découpés, et chaque lettre s'affiche une par une.

```
▼ Telnet  
Data: u
```

```
▼ Telnet  
Data: Password:
```

```
▼ Telnet  
Data: s
```

Avec cette methode , on a obtenu les informations suivantes :

Password : user

Login :fake

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.

-On peut accéder aux informations du paquet en cliquant sur « follow » et puis « TCP stream »

```
.....'.....#..&..$..&..$..#.....  
..bam.zing.org:0.0.....DISPLAY.bam.zing.org:0.0.....xterm-color....  
OpenBSD/i386 (oof) (tty1)  
login: .."....."ffaakkee  
Password:user  
Last login: Thu Dec  2 21:32:59 on tty1 from bam.zing.org  
Warning: no Kerberos tickets issued.  
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999
```

-On peut aller sur « expert information » pour structure le paquet

| Severity | Summary | Group | Protocol | Count |
|----------|---|--------------------|----------|-------|
| Error | Malformed Packet (Exception occurred) | Malformed Protocol | TELNET | 1 |
| Error | Bogus IP length | Protocol | IPv4 | 25 |
| Note | This frame undergoes the connection closing | Sequence | TCP | 1 |
| Note | This frame initiates the connection closing | Sequence | TCP | 1 |
| Note | TCP keep-alive segment | Sequence | TCP | 22 |
| Chat | Connection finish (FIN) | Sequence | TCP | 2 |
| Chat | Connection establish acknowledge (SYN+ACK) | Sequence | TCP | 1 |
| Chat | Connection establish request (SYN) | Sequence | TCP | 1 |

7. Quelles commandes ont été utilisées suite à l'authentification ?

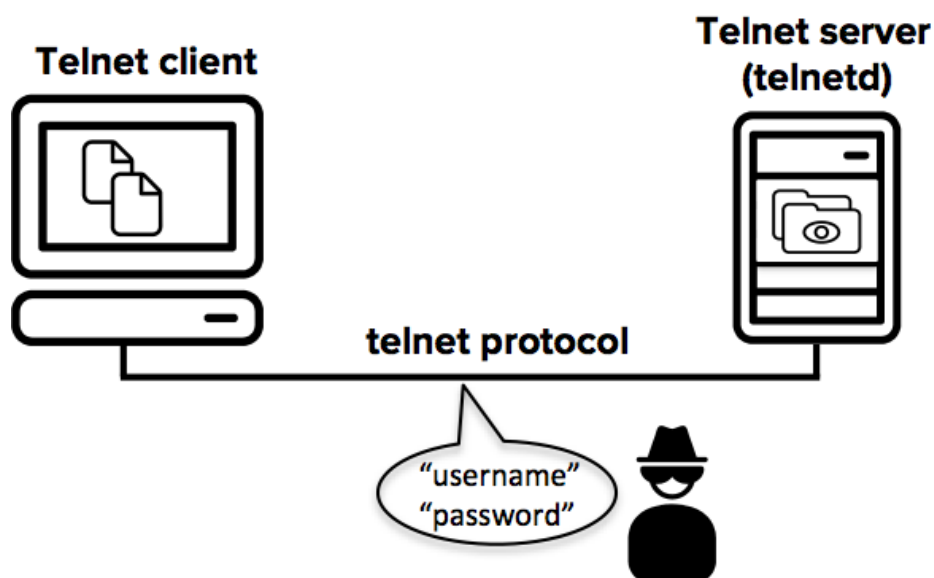
```
$ llss  
$ llss --aa  
..csbrc login mailrc profile .rhosts  
$ //ssbbiinn//ppiinnngg wwwwww..yyaahhoooo..ccoomm  
PING www.yahoo.com (204.71.200.74): 56 data bytes  
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms  
Packet 74. 58 client pkt(s), 78 server pkt(s), 106 turn(s). Click to select.
```

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

Yahoo c'est le nom de domaine sollicité dans les échanges

Conclusion :

Cet exercice nous sensibilise aux vulnérabilités du protocole Telnet, une méthode de communication au travers de laquelle nos informations, telles que les identifiants de connexion et les mots de passe, peuvent être exploitées. Les questions nous guident pour extraire des informations sur un utilisateur fictif. Par conséquent, nous avons pu extraire des informations confidentielles.



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 ?

Ils sont en train d'effectuer un « 3 way handshake » :

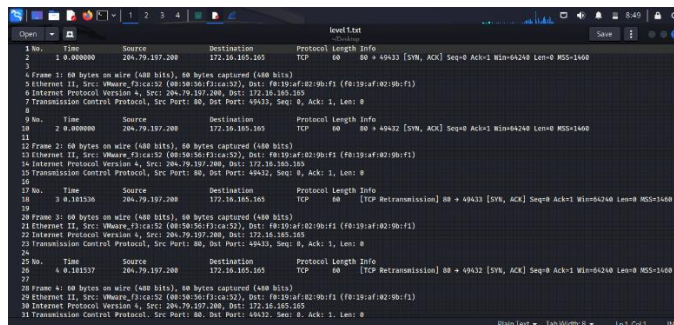
SYN (Synchronise) : Le client envoie un paquet SYN au serveur pour établir une connexion.

SYN-ACK (Synchronize-Acknowledge) : Le serveur répond avec un paquet SYN-ACK, indiquant qu'il est prêt à accepter la connexion.

ACK (Acknowledge) : Le client envoie un paquet ACK pour confirmer la réception du paquet SYN-ACK, établissant ainsi la connexion.

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

Pour rendre plus lisible, on a converti le fichier pcap en texte. Le format texte structure les contenus et rend facile la recherche des informations



| | |
|------------------|----------------|
| IP source | 204.79.197.200 |
| Port source | 80 |
| IP destination | 172.16.165.165 |
| Port destination | 49433 |

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

Le protocole NetBIOS peut utiliser à la fois TCP (port :139) et UDP (port :137), en fonction des besoins spécifiques.

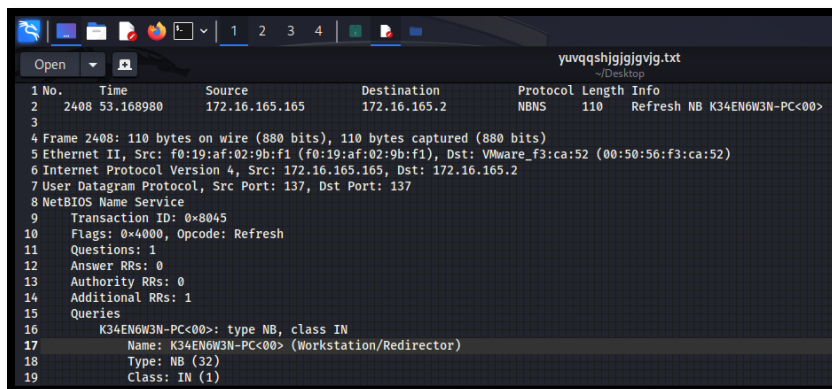
4. Trouvez la commande permettant de faire un filtrage sur les ports dans la barre de recherche Wireshark.

La commande permettant de faire un filtrage sur le port 80 est : « **tcp. Port ==80** ». On a trouvé 2993 paquets. On peut aussi utiliser la commande : http pour avoir les paquets.

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 ?

On connaît l'adresse IP et on veut trouver le nom associé à cette adresse. Pour ce faire, nous allons utiliser le protocole Netbios qui permet de convertir les noms d'ordinateurs en adresses IP et vice versa.

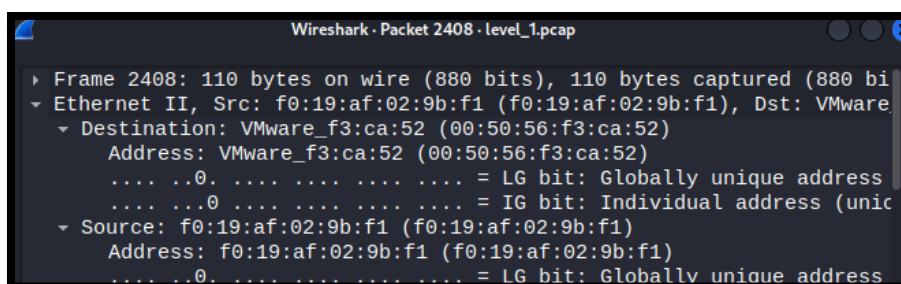
Notre objectif est de trouver les services Netbios en lien avec l'adresse IP en question. Voici la commande utilisée pour atteindre notre objectif : « **ip.addr == 172.16.165.165 and udp.port == 137** »



```
1 No.    Time           Source            Destination      Protocol Length Info
2 2408 53.168980    172.16.165.165    172.16.165.2     NBNS           110    Refresh NB K34EN6W3N-PC<00>
3
4 Frame 2408: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
5 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)
6 Internet Protocol Version 4, Src: 172.16.165.165, Dst: 172.16.165.2
7 User Datagram Protocol, Src Port: 137, Dst Port: 137
8 NetBIOS Name Service
9   Transaction ID: 0x8045
10  Flags: 0x4000, Opcode: Refresh
11  Questions: 1
12  Answer RRs: 0
13  Authority RRs: 0
14  Additional RRs: 1
15  Queries
16    K34EN6W3N-PC<00>: type NB, class IN
17      Name: K34EN6W3N-PC<00> (Workstation/Redirector)
18      Type: NB (32)
19      Class: IN (1)
```

On peut voir que le nom de la machine hôte est : K34EN6W3N-PC<00>

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



```
Wireshark - Packet 2408 - level_1.pcap
> Frame 2408: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
- 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
      .... ..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
```

L'adresse MAC de la machine hôte est : **f0 :19 :af :02 :9b :f1**

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 ?

| Topic / Item | Count | Average | Min Val. | Max Val. | Rate (ms) | Percent | Burst Rate | Burst Start |
|-------------------------|-------|---------|----------|----------|-----------|---------|------------|-------------|
| - Total HTTP Packets | 78 | | | | 0.0009 | 100% | 0.0700 | 8.247 |
| Other HTTP Packets | 0 | | | | 0.0000 | 0.00% | - | - |
| - HTTP Response Packets | 39 | | | | 0.0005 | 50.00% | 0.0400 | 8.247 |
| ???: broken | 0 | | | | 0.0000 | 0.00% | - | - |
| 3xx Server Error | 0 | | | | 0.0000 | 0.00% | - | - |
| 4xx Client Error | 0 | | | | 0.0000 | 0.00% | - | - |
| - 3xx Redirection | 1 | | | | 0.0000 | 2.56% | 0.0100 | 13.139 |
| 301 Moved Permanently 1 | 1 | | | | 0.0000 | 100.00% | 0.0100 | 13.139 |
| - 2xx Success | 38 | | | | 0.0005 | 97.44% | 0.0400 | 8.247 |
| 204 No Content | 1 | | | | 0.0000 | 2.63% | 0.0100 | 3.513 |
| 200 OK | 37 | | | | 0.0004 | 97.37% | 0.0400 | 8.247 |
| 1xx Informational | 0 | | | | 0.0000 | 0.00% | - | - |
| - HTTP Request Packets | 39 | | | | 0.0005 | 50.00% | 0.0600 | 10.598 |
| POST | 1 | | | | 0.0000 | 2.56% | 0.0100 | 2.021 |
| GET | 38 | | | | 0.0005 | 97.44% | 0.0600 | 10.598 |

Display filter:

78 requêtes http ont été émises dans ce fichier pcap et parmi ces requêtes il y a 39 réponses et 39 requêtes

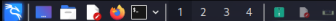
8. En gardant le même filtre que pour la question précédente, donnez le nombre d'adresses IP communiquant sur ce port. (Utiliser pour cela une fonction de Wireshark)


The screenshot displays the Wireshark network protocol analyzer interface. The top status bar indicates a capture on the 'level_1 pcap' file. The main window is divided into three panes: the packet list, packet details, and packet bytes. The packet list shows a list of captured packets, with packet 2 selected. The packet details pane shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the selected packet.



| Address | Packets | Bytes | Total Packets | Percent Filtered | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City | AS |
|----------------|---------|------------|---------------|------------------|------------|------------|------------|------------|---------|------|----|
| 37.200.69.143 | 24 | 13,929 KiB | 1531 | 1.57% | 12 | 7,910 KiB | 12 | 6,019 KiB | | | |
| 74.125.233.96 | 2 | 1,476 KiB | 555 | 0.36% | 1 | 909 bytes | 1 | 602 bytes | | | |
| 82.150.140.30 | 40 | 25,972 KiB | 400 | 10.00% | 20 | 17,143 KiB | 20 | 8,829 KiB | | | |
| 172.16.165.165 | 78 | 49,306 KiB | 3012 | 2.59% | 39 | 19,198 KiB | 39 | 30,107 KiB | | | |
| 185.53.178.9 | 2 | 467 bytes | 17 | 11.76% | 1 | 60 bytes | 1 | 407 bytes | | | |
| 188.225.73.100 | 6 | 4,887 KiB | 95 | 6.32% | 3 | 3,341 KiB | 3 | 1,546 KiB | | | |
| 204.79.197.200 | 4 | 2,587 KiB | 318 | 1.26% | 2 | 786 bytes | 2 | 1,819 KiB | | | |

Grace à cette capture d'écran, on peut affirmer que 7 adresse IP ont communiqué sur ce port.

- Pour les questions 9 et 10 nous allons nous servir du capture d'écran ci-dessous pour répondre à ces questions :


Wireshark - Follow TCP Stream (tcp.stream eq 3) - level1_tcpac


10:32

```

POST /fd/lsp.aspx HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://www.bing.com/search?q=ciniholland.nl&q&s=ds&form=QBLM
Content-Type: text/html
Content-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: www.bing.com
Content-Length: 946
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: _HOP; _EDGE_S=1&SID=142DA63B92026172245CA6CF93E5607F; _EDGE_V=1; MUID=3A80A34CF5D6EF70E435B88EBA6F23; MUIDB=3A80A34CF5D6EF70E435B88EBA6F23; _SS=SID=A0908FC80BD4413AE1D031EE7596518; SRCHD=AF=NOFORM; SRCHUSR=AUTOREDIR=&GEQVAR=&DOB=20141116; SRCHPGUSR=CN=666&CH=278; _UR=D=1; WLS=TS=63551706072; SRCHUID=8567E92131124052AD39C36C431082EA

ClientInRequest->Events<E><T>Event_ClientInst</T><IG>ae5990ea2d64991aa8b8996f170a75c</IG><TS>1416103911349</TS><D><T>".CI.BoxModel", "FID": "CI", "Name": "Perf", "Text": "%S3A0X0660X278X3BB0D.%20%3A0X09X90X499X38D1V.b.scopeAK3A08X80X437X30%3BH1.b.log%3A17X19X73X29X38D1V.b.searchboxFor%3A1190X196X49X30X3BD1V%231d_h%3A05X80X126X30X3BD1V%23b.tween%3A106X135X89X0X3%3BSPAN.sb_count%3A120X135X105X30X3B0L%23b.results%3A106X165X560X1188X3BL1.b.algo%3A106X165X560X9X3BL1.b.algo%3A106X260X560X9X3BL1.b.algo%3A106X358X560X9X3BL1.b.algo%3A106X455X560X9X11K3BL1.b.algo%3A106X60X60X9X3BL1.b.algo%3A106X76X340X60X9X3BL1.b.algo%3A106X80X60X60X9X3BL1.b.algo%3A106X95X60X60X9X3BL1.b.algo%3A106X105X60X60X9X3BL1.b.pap%3A106X115X350X60X9X3BL1.b.pap%3A106X126X350X60X9X3BL1.b.pap%3A106X135X350X60X9X3BL1.b.pap%3A106X145X350X60X9X3BL1.b.pap%3A106X155X350X60X9X3BL1.b.pap%3A106X165X350X60X9X3BL1.b.pap%3A106X175X350X60X9X3BL1.b.pap%3A106X185X350X60X9X3BL1.b.pap%3A106X195X350X60X9X3BL1.b.pap%3A106X205X350X60X9X3BL1.b.pap%3A106X215X350X60X9X3BL1.b.pap%3A106X225X350X60X9X3BL1.b.pap%3A106X235X350X60X9X3BL1.b.pap%3A106X245X350X60X9X3BL1.b.pap%3A106X255X350X60X9X3BL1.b.pap%3A106X265X350X60X9X3BL1.b.pap%3A106X275X350X60X9X3BL1.b.pap%3A106X285X350X60X9X3BL1.b.pap%3A106X295X350X60X9X3BL1.b.pap%3A106X305X350X60X9X3BL1.b.pap%3A106X315X350X60X9X3BL1.b.pap%3A106X325X350X60X9X3BL1.b.pap%3A106X335X350X60X9X3BL1.b.pap%3A106X345X350X60X9X3BL1.b.pap%3A106X355X350X60X9X3BL1.b.pap%3A106X365X350X60X9X3BL1.b.pap%3A106X375X350X60X9X3BL1.b.pap%3A106X385X350X60X9X3BL1.b.pap%3A106X395X350X60X9X3BL1.b.pap%3A106X405X350X60X9X3BL1.b.pap%3A106X415X350X60X9X3BL1.b.pap%3A106X425X350X60X9X3BL1.b.pap%3A106X435X350X60X9X3BL1.b.pap%3A106X445X350X60X9X3BL1.b.pap%3A106X455X350X60X9X3BL1.b.pap%3A106X465X350X60X9X3BL1.b.pap%3A106X475X350X60X9X3BL1.b.pap%3A106X485X350X60X9X3BL1.b.pap%3A106X495X350X60X9X3BL1.b.pap%3A106X505X350X60X9X3BL1.b.pap%3A106X515X350X60X9X3BL1.b.pap%3A106X525X350X60X9X3BL1.b.pap%3A106X535X350X60X9X3BL1.b.pap%3A106X545X350X60X9X3BL1.b.pap%3A106X555X350X60X9X3BL1.b.pap%3A106X565X350X60X9X3BL1.b.pap%3A106X575X350X60X9X3BL1.b.pap%3A106X585X350X60X9X3BL1.b.pap%3A106X595X350X60X9X3BL1.b.pap%3A106X605X350X60X9X3BL1.b.pap%3A106X615X350X60X9X3BL1.b.pap%3A106X625X350X60X9X3BL1.b.pap%3A106X635X350X60X9X3BL1.b.pap%3A106X645X350X60X9X3BL1.b.pap%3A106X655X350X60X9X3BL1.b.pap%3A106X665X350X60X9X3BL1.b.pap%3A106X675X350X60X9X3BL1.b.pap%3A106X685X350X60X9X3BL1.b.pap%3A106X695X350X60X9X3BL1.b.pap%3A106X705X350X60X9X3BL1.b.pap%3A106X715X350X60X9X3BL1.b.pap%3A106X725X350X60X9X3BL1.b.pap%3A106X735X350X60X9X3BL1.b.pap%3A106X745X350X60X9X3BL1.b.pap%3A106X755X350X60X9X3BL1.b.pap%3A106X765X350X60X9X3BL1.b.pap%3A106X775X350X60X9X3BL1.b.pap%3A106X785X350X60X9X3BL1.b.pap%3A106X795X350X60X9X3BL1.b.pap%3A106X805X350X60X9X3BL1.b.pap%3A106X815X350X60X9X3BL1.b.pap%3A106X825X350X60X9X3BL1.b.pap%3A106X835X350X60X9X3BL1.b.pap%3A106X845X350X60X9X3BL1.b.pap%3A106X855X350X60X9X3BL1.b.pap%3A106X865X350X60X9X3BL1.b.pap%3A106X875X350X60X9X3BL1.b.pap%3A106X885X350X60X9X3BL1.b.pap%3A106X895X350X60X9X3BL1.b.pap%3A106X905X350X60X9X3BL1.b.pap%3A106X915X350X60X9X3BL1.b.pap%3A106X925X350X60X9X3BL1.b.pap%3A106X935X350X60X9X3BL1.b.pap%3A106X945X350X60X9X3BL1.b.pap%3A106X955X350X60X9X3BL1.b.pap%3A106X965X350X60X9X3BL1.b.pap%3A106X975X350X60X9X3BL1.b.pap%3A106X985X350X60X9X3BL1.b.pap%3A106X995X350X60X9X3BL1.b.pap%3A106X1005X350X60X9X3BL1.b.pap%3A106X1015X350X60X9X3BL1.b.pap%3A106X1025X350X60X9X3BL1.b.pap%3A106X1035X350X60X9X3BL1.b.pap%3A106X1045X350X60X9X3BL1.b.pap%3A106X1055X350X60X9X3BL1.b.pap%3A106X1065X350X60X9X3BL1.b.pap%3A106X1075X350X60X9X3BL1.b.pap%3A106X1085X350X60X9X3BL1.b.pap%3A106X1095X350X60X9X3BL1.b.pap%3A106X1105X350X60X9X3BL1.b.pap%3A106X1115X350X60X9X3BL1.b.pap%3A106X1125X350X60X9X3BL1.b.pap%3A106X1135X350X60X9X3BL1.b.pap%3A106X1145X350X60X9X3BL1.b.pap%3A106X1155X350X60X9X3BL1.b.pap%3A106X1165X350X60X9X3BL1.b.pap%3A106X1175X350X60X9X3BL1.b.pap%3A106X1185X350X60X9X3BL1.b.pap%3A106X1195X
```

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

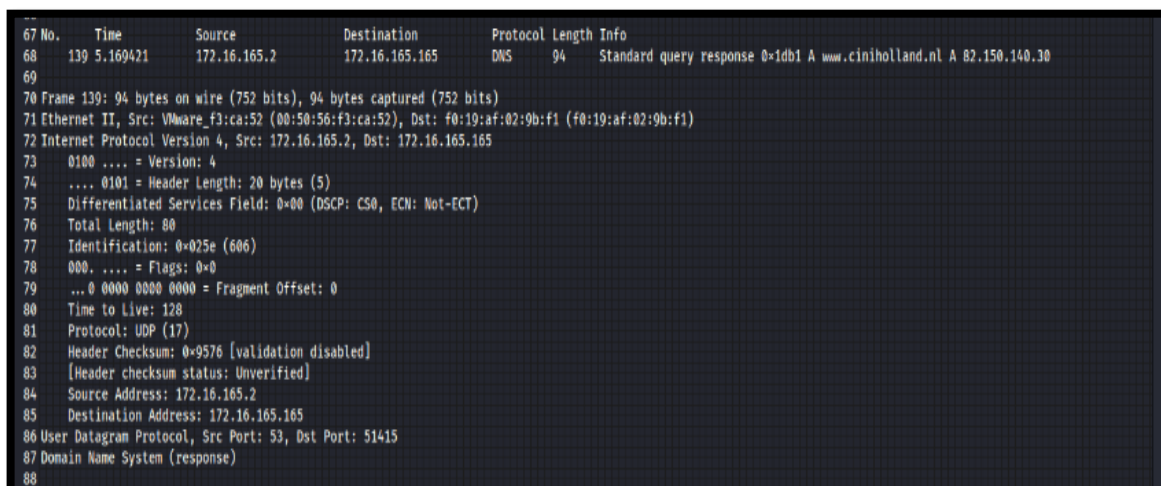
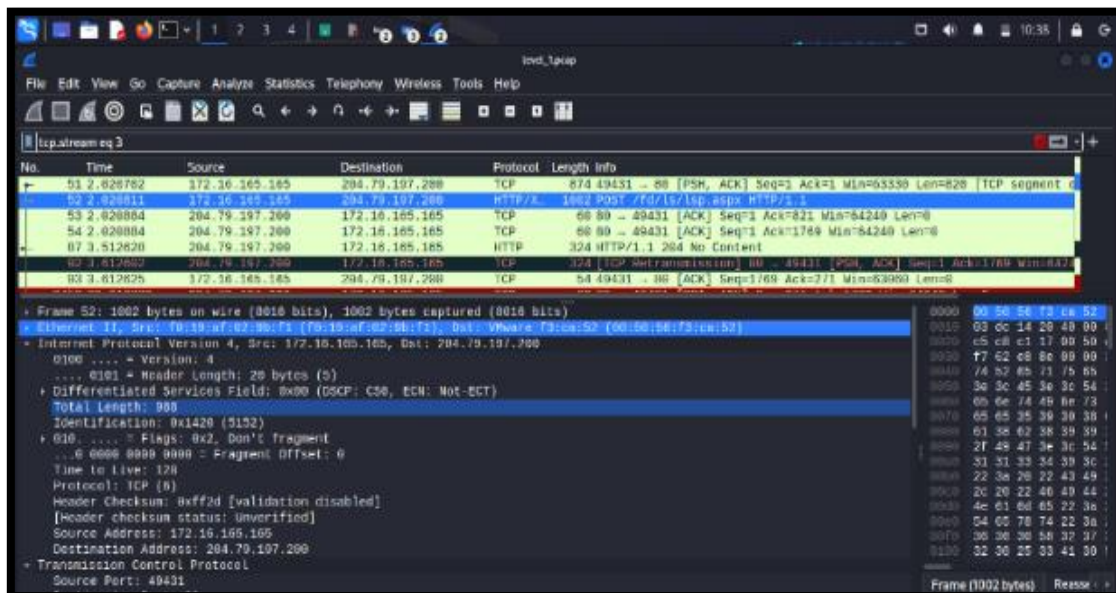
Le navigateur utilisé est Mozilla et sa version est Mozilla/4.0. En ce qui concerne Windows, ils ont utilisé le Windows NT 6.1.

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 ?

Referer: http://www.bing.com/search?q=ciniholland.nl&q=ds&form=QBLH

L'utilisateur a utilisé bing. L'utilisateur a cherché « www.ciniholland.nl »

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 ?

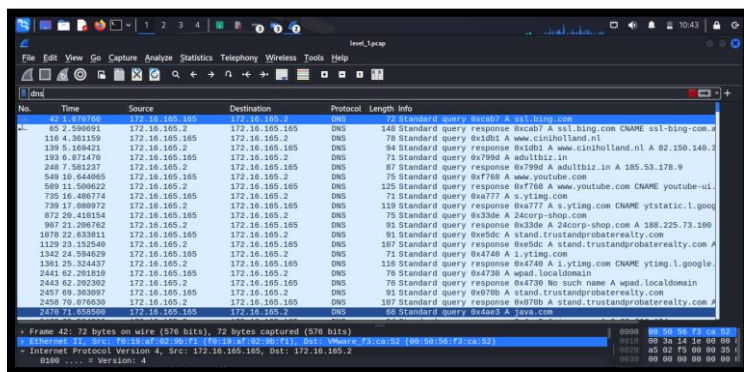


L'adresse MAC et l'adresse IP de la machine hébergeant ce site web est respectivement : 00 :50 :56 :f3 :ca :52 et 82.150.140.30 .C'est une machine virtuelle qui s'intitule VMware

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

Un FQDN (Fully Qualified Domain Name) est un nom de domaine complet qui spécifie son emplacement exact dans la hiérarchie du système de noms de domaine (DNS). Il comprend le nom d'hôte et le domaine, ainsi que le suffixe de domaine.

13. 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.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|----------------|----------------|----------|--------|--|
| 62 | 1.981746 | 172.16.165.105 | 172.16.165.2 | DNS | 72 | Standard query 0x1001 A ssl-bing.com |
| 65 | 2.590901 | 172.16.165.2 | 172.16.165.105 | DNS | 148 | Standard query response 0xcab7 A ssl-bing.com CNAME ssl-bing-com.4 |
| 116 | 4.361159 | 172.16.165.105 | 172.16.165.2 | DNS | 78 | Standard query 0x1001 A www.cinoholland.nl |
| 139 | 5.108421 | 172.16.165.2 | 172.16.165.105 | DNS | 94 | Standard query response 0x1db1 A www.cinoholland.nl A 82.150.140.2 |
| 193 | 6.871470 | 172.16.165.105 | 172.16.165.2 | DNS | 71 | Standard query 0x799d A adultbiz.in |
| 248 | 7.581237 | 172.16.165.2 | 172.16.165.105 | DNS | 87 | Standard query response 0x799d A adultbiz.in A 185.53.178.9 |
| 549 | 10.844805 | 172.16.165.105 | 172.16.165.2 | DNS | 75 | Standard query 0x7f88 A www.youtube.com |
| 589 | 11.500422 | 172.16.165.2 | 172.16.165.105 | DNS | 125 | Standard query response 0x7f88 A www.youtube.com CNAME youtube-vi |
| 735 | 16.486774 | 172.16.165.105 | 172.16.165.2 | DNS | 71 | Standard query 0xa777 A s.ytimg.com |
| 739 | 17.080972 | 172.16.165.2 | 172.16.165.105 | DNS | 119 | Standard query response 0xa777 A s.ytimg.com CNAME ytstatic.l.goog |
| 872 | 20.431154 | 172.16.165.105 | 172.16.165.2 | DNS | 75 | Standard query 0x33de A 24corp-shop.com |
| 907 | 21.206762 | 172.16.165.2 | 172.16.165.105 | DNS | 91 | Standard query response 0x33de A 24corp-shop.com A 188.225.73.100 |
| 1070 | 22.033811 | 172.16.165.105 | 172.16.165.2 | DNS | 91 | Standard query 0xe5dc A stand.trustandprobaterality.com |
| 1129 | 23.152540 | 172.16.165.2 | 172.16.165.105 | DNS | 107 | Standard query response 0xe5dc A stand.trustandprobaterality.com A |
| 1342 | 24.504429 | 172.16.165.105 | 172.16.165.2 | DNS | 71 | Standard query 0x4748 A i.ytimg.com |
| 1381 | 25.324437 | 172.16.165.2 | 172.16.165.105 | DNS | 119 | Standard query response 0x4748 A i.ytimg.com CNAME ytimg.l.google |
| 2441 | 62.201810 | 172.16.165.105 | 172.16.165.2 | DNS | 76 | Standard query 0x4730 A wpaad.localdomain |
| 2443 | 62.202302 | 172.16.165.2 | 172.16.165.105 | DNS | 76 | Standard query response 0x4730 No such name A wpaad.localdomain |
| 2457 | 69.303097 | 172.16.165.105 | 172.16.165.2 | DNS | 91 | Standard query 0x070b A stand.trustandprobaterality.com |
| 2458 | 70.076630 | 172.16.165.2 | 172.16.165.105 | DNS | 107 | Standard query response 0x070b A stand.trustandprobaterality.com A |
| 2470 | 78.025500 | 172.16.165.105 | 172.16.165.2 | DNS | 72 | Standard query 0x4730 A wpaad.localdomain |

14. Quelles 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 maximum ?

La taille maximale d'un segment TCP est 1500 octets (46 à 1500 octets).

Si un datagramme TCP dépasse la taille maximale autorisée par la MTU, TCP utilise le processus de fragmentation pour diviser le datagramme en segments plus petits qui peuvent être transmis individuellement sur le réseau sous-jacent. Les fragments sont ensuite réassemblés à la réception.

Conclusion :

Cet exercice nous amène à analyser des requêtes, et on se rend compte qu'il y a de nombreuses requêtes envoyées depuis une même adresse. Cela nous conduit à constater qu'un attaquant tente d'attaquer ce système afin de le rendre dysfonctionnel.