

25/11/2023

TP - Analyse forensic réseau

Cyber management school



Fait par: Alula Willy-Julien

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 (00F) #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	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 ?

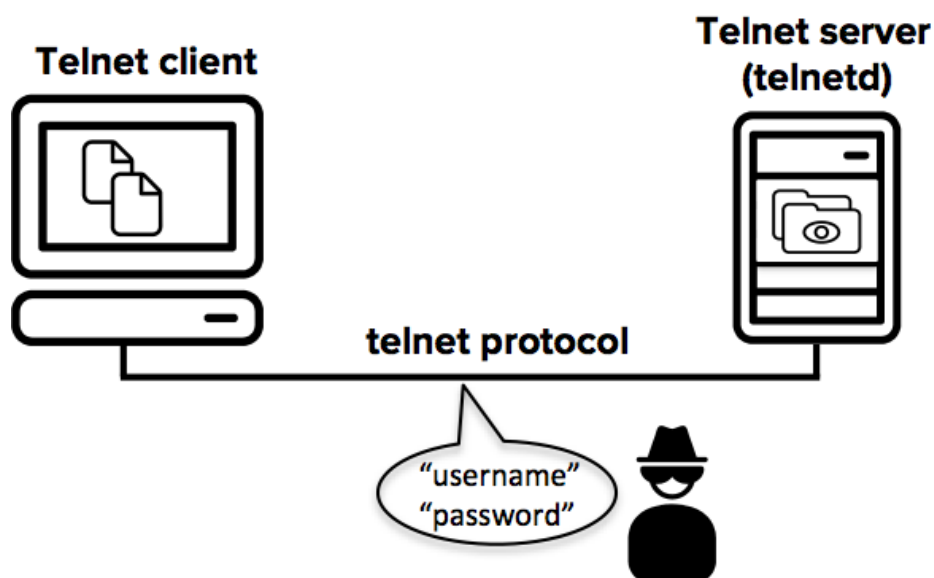
```
$ llss  
$ llss --aa  
..csbrc login mailrc profile .rhosts  
$ //ssbbiinn//ppiinnngg wwwwww..yyaahhoooo..ccoomm  
PING www.yahoo.com (204.71.200.74): 56 data bytes  
64 bytes from 204.71.200.74: icmp_seq=0 ttl=239 time=73.569 ms  
Packet 74. 58 client pkt(s), 78 server pkt(s), 106 turn(s). Click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

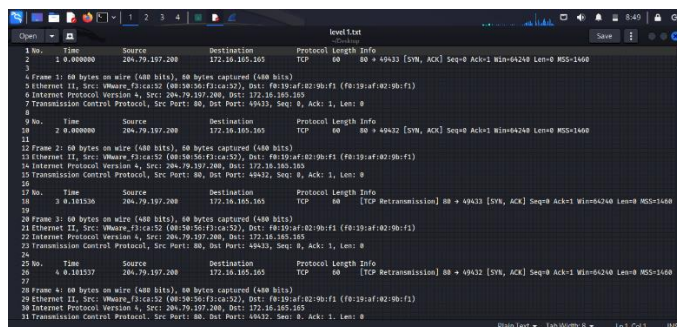
SYN (Synchronise) : Le client envoie un paquet SYN au serveur pour établir une connexion.

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.

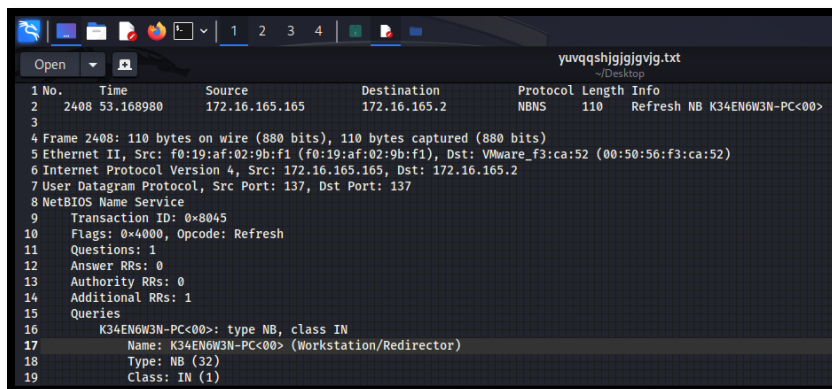
4. Trouvez la commande permettant de faire un filtrage sur les ports dans la barre de recherche Wireshark.

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** »

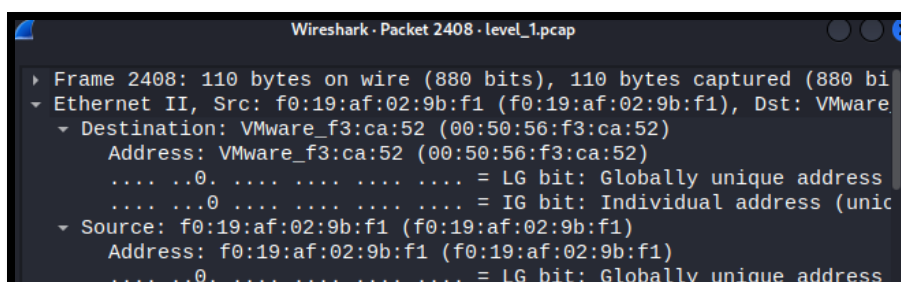


```

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 ?

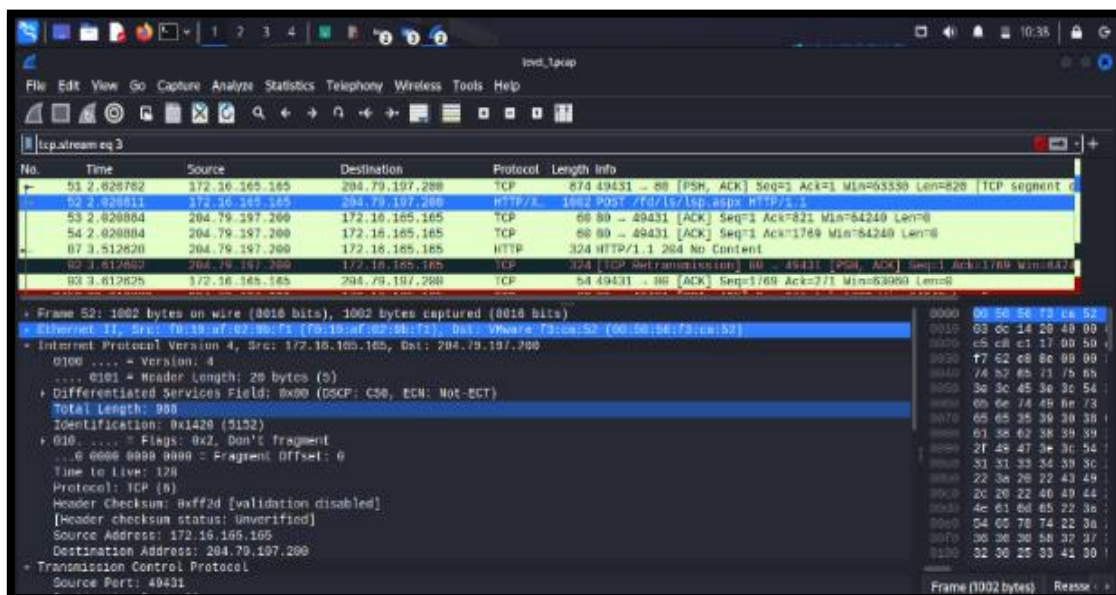
Le navigateur utilisé est Mozilla et sa version est Mozilla/4.0. En ce qui concerne Windows, ils ont utilisé le Windows NT 6.1.

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 ?



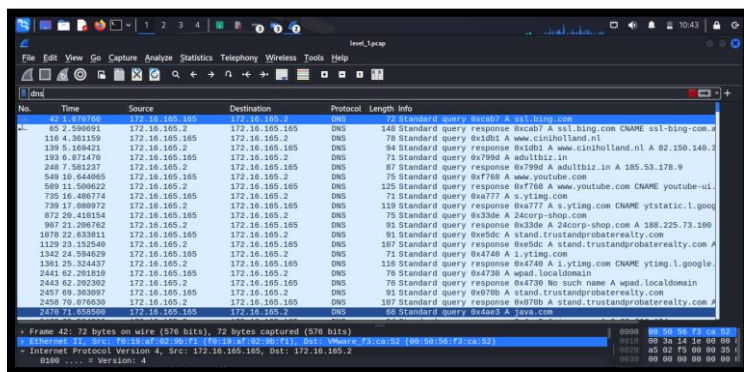
```
67 No.    Time           Source           Destination      Protocol Length Info
68   139  5.169421      172.16.165.2     172.16.165.165  DNS        94      Standard query response 0x1db1 A www.ciniholland.nl A 82.150.140.30
69
70 Frame 139: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
71 Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
72 Internet Protocol Version 4, Src: 172.16.165.2, Dst: 172.16.165.165
73  0100 .... = Version: 4
74  .... 0101 = Header Length: 20 bytes (5)
75  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
76  Total Length: 80
77  Identification: 0x025e (606)
78  000. .... = Flags: 0x0
79  ... 0 0000 0000 0000 = Fragment Offset: 0
80  Time to Live: 128
81  Protocol: UDP (17)
82  Header Checksum: 0x9576 [validation disabled]
83  [Header checksum status: Unverified]
84  Source Address: 172.16.165.2
85  Destination Address: 172.16.165.165
86  User Datagram Protocol, Src Port: 53, Dst Port: 51415
87  Domain Name System (response)
88
```

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	172.16.165.165	172.16.165.2	DNS	72	Standard query 0x1001 A ssl-bing.com
65	2.590901	172.16.165.2	172.16.165.165	DNS	148	Standard query response 0xcab7 A ssl-bing.com CNAME ssl-bing.com
116	4.361159	172.16.165.165	172.16.165.2	DNS	78	Standard query 0x1001 A www.cin.nl
139	5.108421	172.16.165.2	172.16.165.165	DNS	94	Standard query response 0x1001 A www.cin.nl
193	6.871479	172.16.165.165	172.16.165.2	DNS	71	Standard query 0x799d A adu1b1z.in
248	7.581237	172.16.165.2	172.16.165.165	DNS	87	Standard query response 0x799d A adu1b1z.in
549	10.844805	172.16.165.165	172.16.165.2	DNS	75	Standard query 0x7f88 A www.youtube.com
589	11.500422	172.16.165.2	172.16.165.165	DNS	125	Standard query response 0x7f88 A www.youtube.com CNAME youtube-vi
735	16.486774	172.16.165.165	172.16.165.2	DNS	71	Standard query 0xa777 A s.ytimg.com
739	17.080972	172.16.165.2	172.16.165.165	DNS	119	Standard query response 0xa777 A s.ytimg.com CNAME ytstatic.l.google
872	20.431154	172.16.165.165	172.16.165.2	DNS	75	Standard query 0x33de A 24corp-shop.com
907	21.206762	172.16.165.2	172.16.165.165	DNS	91	Standard query response 0x33de A 24corp-shop.com
1070	22.033811	172.16.165.165	172.16.165.2	DNS	91	Standard query 0xe5dc A stand.trustandprobate.com
1129	23.152540	172.16.165.2	172.16.165.165	DNS	107	Standard query response 0xe5dc A stand.trustandprobate.com
1342	24.544629	172.16.165.165	172.16.165.2	DNS	71	Standard query 0x4748 A i.ytimg.com
1381	25.324437	172.16.165.2	172.16.165.165	DNS	119	Standard query response 0x4748 A i.ytimg.com CNAME ytimg.l.google
2441	62.201810	172.16.165.165	172.16.165.2	DNS	76	Standard query 0x4730 A wpa2.localdomain
2443	62.202302	172.16.165.2	172.16.165.165	DNS	76	Standard query response 0x4730 No such name A wpa2.localdomain
2457	69.303097	172.16.165.165	172.16.165.2	DNS	91	Standard query 0x070b A stand.trustandprobate.com
2458	70.076630	172.16.165.2	172.16.165.165	DNS	107	Standard query response 0x070b A stand.trustandprobate.com
2470	78.025500	172.16.165.165	172.16.165.2	DNS	72	Standard query 0x4730 A wpa2.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.