

Compte-rendu projet YDAYS

Lors de ce premier jour des projets YDAYS, je devais découvrir beaucoup de notions réseau pour avoir des bases dans ce projet, je me suis donc entraîné avec des exercices sur www.rootme.org, dans la catégorie « réseau »

Exercice 1

Énoncé

Un échange authentifié de fichier réalisé grâce au protocole FTP. Retrouvez le mot de passe utilisé par l'utilisateur.

The image shows a Wireshark network traffic capture of an FTP session. The packet list pane on the left shows several packets, with packet 11 selected. The packet details pane on the right shows the structure of packet 11, which is an FTP 'Request' packet. The 'Request' field is expanded, showing the command 'PASS' followed by the password 'cdts3500'. The packet bytes pane at the bottom shows the raw data of the packet, with the password 'cdts3500' visible in the hex and ASCII representation.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.276140	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [ACK] Seq=1 Ack=93 Win=32648 Len=0 TSval=1657560500 TSecr=1657390000
8	4.216600	10.20.144.150	10.20.144.151	FTP	81	Request: USER cdts3500
9	4.217350	10.20.144.151	10.20.144.150	FTP	91	Response: 331 Enter password.
10	4.217630	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [PSH, ACK] Seq=16 Ack=114 Win=32648 Len=0 TSval=1657564500 TSecr=1657394000
11	7.639420	10.20.144.150	10.20.144.151	FTP	81	Request: PASS cdts3500
12	7.843260	10.20.144.151	10.20.144.150	TCP	70	21 → 35974 [PSH, ACK] Seq=114 Ack=31 Win=16384 Len=0 TSval=1657397500 TSecr=1657568000
13	8.184000	10.20.144.151	10.20.144.150	FTP	95	Response: 230 CDTS3500 logged on.
14	8.184360	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [PSH, ACK] Seq=31 Ack=139 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000
15	8.185040	10.20.144.150	10.20.144.151	FTP	72	Request: SYST
16	8.185260	10.20.144.151	10.20.144.150	TCP	70	21 → 35974 [PSH, ACK] Seq=139 Ack=37 Win=16384 Len=0 TSval=1657398000 TSecr=1657568500
17	8.192750	10.20.144.151	10.20.144.150	FTP	147	Response: 215 05/400 is the remote operating system. The TCP/IP version is "V5R2M0".
18	8.193000	10.20.144.150	10.20.144.151	TCP	66	35974 → 21 [PSH, ACK] Seq=37 Ack=216 Win=32648 Len=0 TSval=1657568500 TSecr=1657398000

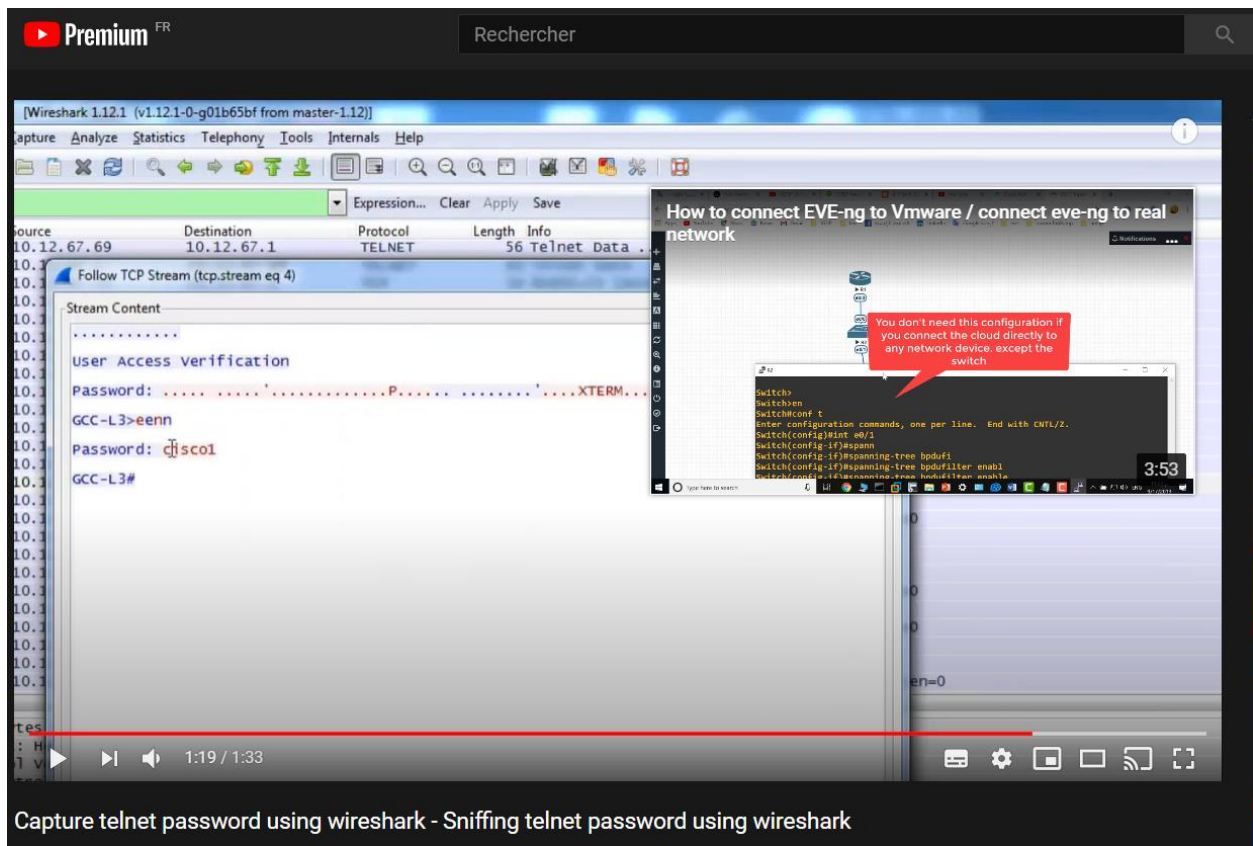
> Frame 11: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Ethernet II, Src: IbmRisc6_9c:14:fe (00:06:29:9c:14:fe), Dst: IbmRisc6_9c:14:ae (00:06:29:9c:14:ae)
> Internet Protocol Version 4, Src: 10.20.144.150, Dst: 10.20.144.151
> Transmission Control Protocol, Src Port: 35974, Dst Port: 21, Seq: 16, Ack: 114, Len: 15
> File Transfer Protocol (FTP)
[Current working directory:]

```
0000  00 06 29 9c 14 ae 00 06 29 9c 14 fe 08 00 45 00  ..).....).....E-
0010  00 43 2d 76 40 00 40 06 d7 e9 0a 14 90 96 0a 14  .C-v@.@.....
0020  90 97 8c 86 00 15 01 c1 b9 c6 60 b5 3f 16 80 18  .....-?....
0030  7f 88 bb 15 00 00 01 01 08 0a 62 cc 7b 00 62 c9  .....-b-{-b-
0040  d3 50 50 41 53 53 20 63 64 74 73 33 35 30 30 0d  .PPASS c dts3500-
0050  0a
```

Lors de cet exercice, il fallait retrouver le mot de passer de l'utilisateur parmi la liste FTP, je l'ai retrouvé grâce au mot « PASS »

Énoncé

Retrouvez le mot de passe de l'utilisateur dans cette capture réseau de session TELNET.



Dans cet exercice, j'ai eu du mal à retrouver le mot de passe, je me suis donc aidé de YouTube afin d'avoir une explication. J'ai ensuite compris qu'en ouvrant l'onglet « Analyze », « Follow » et « TCP Stream » une page s'ouvre et nous affiche toutes les informations de l'utilisateur ainsi que le mot de passe.

ch2 (1).pcap
File Edit View Go Capture Analyze

No.	Time	Source
45	9.122102	192.168.0.2
46	9.123415	192.168.0.1
47	9.143053	192.168.0.2
48	9.217653	192.168.0.2
49	9.218919	192.168.0.2
50	9.220307	192.168.0.1
51	9.233053	192.168.0.2
52	9.433115	192.168.0.2
53	9.434404	192.168.0.1
54	9.446537	192.168.0.1
55	9.463059	192.168.0.2
56	9.464208	192.168.0.1

Frame 56: 75 bytes on wire (600)
Ethernet II, Src: WesternD_9f:a0
Internet Protocol Version 4, Src
Transmission Control Protocol, S
Telnet
Data: Password:

Wireshark - Follow TCP Stream (tcp.stream eq 0) - ch2 (1).pcap

```

.....!..".'.#..%..!..".P.....b.....b....B.
.....".'.#..&..$..&..$.#.....9600,9600....#.bam.zing.org:
0.0.....'.DISPLAY.bam.zing.org:0.0.....xterm-color.....!.....
OpenBSD/i386 (oof) (ttty1)

login: .."....."ffaakkee
.
Password:user
.
Last login: Thu Dec  2 21:32:59 on ttty1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

$ llss
.
$ llss --aa
.
..      .cshrc      .login      .mailrc      .profile      .rhosts
$ //ssbbiinn//ppiinn gg  wwwwww..yyaahhooooo..cccoomm

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
64 bytes from 204.71.200.74: icmp_seq=1 ttl=239 time=71.099 ms
64 bytes from 204.71.200.74: icmp_seq=2 ttl=239 time=68.728 ms
64 bytes from 204.71.200.74: icmp_seq=3 ttl=239 time=73.122 ms
64 bytes from 204.71.200.74: icmp_seq=4 ttl=239 time=71.276 ms
64 bytes from 204.71.200.74: icmp_seq=5 ttl=239 time=75.831 ms
64 bytes from 204.71.200.74: icmp_seq=6 ttl=239 time=70.101 ms
64 bytes from 204.71.200.74: icmp_seq=7 ttl=239 time=74.528 ms
64 bytes from 204.71.200.74: icmp_seq=8 ttl=239 time=74.514 ms
64 bytes from 204.71.200.74: icmp_seq=9 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=10 ttl=239 time=75.188 ms
64 bytes from 204.71.200.74: icmp_seq=11 ttl=239 time=72.925 ms
...^C

```

Exercice 3

Énoncé

Retrouvez les données normalement confidentielles contenues dans cette trame :

(e.g. 45 78 61 6d 70 6c 65 21):

Open File

Paste hex numbers or drop file

69 67 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a

Character encoding

ASCII

Convert

Reset

Swap

s àiøZÿ` @&S `*% PÀP AD B3 t P%ê}
, Áx áĭ
>i~ÓGET / HTTP/1.1
Authorization: Basic Y29uZmk6ZGVudG1hbA==
User-Agent: InsaneBrowser
Host: www.myipv6.org

Copy

Save

Y29uZmk6ZGVudGhhbA==

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for multiple entries).

Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE > Decodes your data into the textarea below.

confi:dential

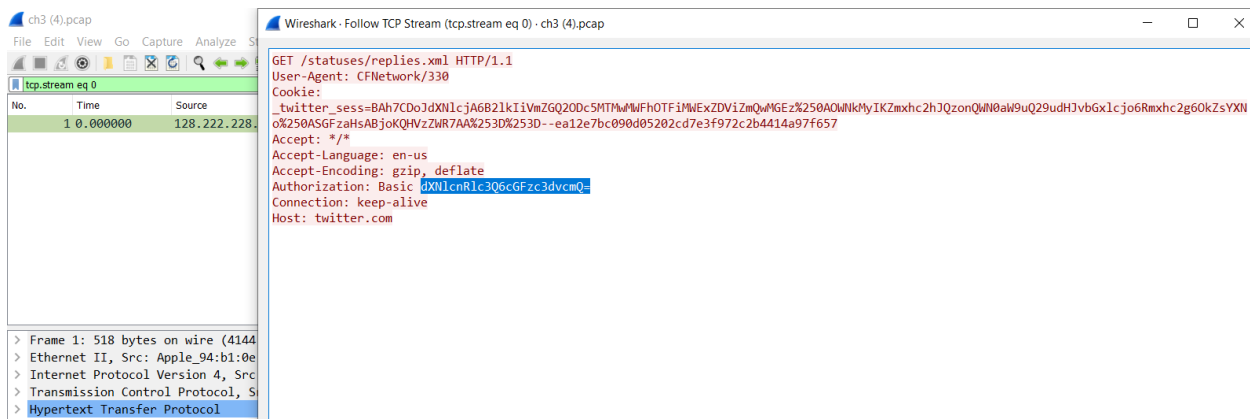
Dans cet exercice, nous avons un tableau constituées de valeurs en hexadécimale, et nous devons y retirer les valeurs confidentielles.

J'ai donc converti tout le tableau en Base64 à l'aide d'un convertisseur sur internet, puis converti la Base64 afin d'obtenir le mot de passe.

Exercice 4

Énoncé

Une session d'authentification twitter a été capturée. Retrouvez le mot de passe de l'utilisateur dans cette capture réseau.



Lors de cet exercice, j'ai utilisé le même procédé que pour l'exercice 2, mais cette fois-ci le mot de passe est en Base64, il m'a donc fallu le décoder à l'aide d'un site internet qui décode la Base64.

A screenshot of a web-based Base64 decoder. The input field at the top contains the Base64 string 'dXNlcnRlc3Q6cGFzc3dvcmQ='. Below the input field is a section with options: 'Source character set' is set to 'UTF-8', 'Decode each line separately' is unchecked, and 'Live mode' is set to 'OFF'. A green button labeled '< DECODE >' is visible. Below the button, the output field displays the decoded text 'usertest:password'.

Le mot de passe est donc : password.

Énoncé

La réponse est le hash SHA1 de la concaténation de l'adresse MAC (en majuscules) et du nom du téléphone.

AB:CD:EF:12:34:56monTelephone -> 836eca0d42f34291c5fefe91010873008b53c129

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	controller	host	HCI_EVT	13	Rcvd Connect Request
2	0.000995	controller	host	HCI_EVT	7	Rcvd Command Status (Accept Connection Request)
3	0.151001	controller	host	HCI_EVT	14	Rcvd Connect Complete
4	0.151927	controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Supported Features)
5	0.158944	controller	host	HCI_EVT	14	Rcvd Read Remote Supported Features
6	0.160013	controller	host	HCI_EVT	7	Rcvd Command Status (Read Remote Extended Features)
7	0.165028	controller	host	HCI_EVT	16	Rcvd Read Remote Extended Features Complete
8	0.166012	controller	host	HCI_EVT	7	Rcvd Command Status (Remote Name Request)
9	0.184990	controller	host	HCI_EVT	258	Rcvd Remote Name Request Complete
10	0.187930	controller	host	HCI_EVT	13	Rcvd Command Complete (IO Capability Request Reply)
11	3.518018	controller	host	HCI_EVT	13	Rcvd Command Complete (User Confirmation Request Reply)
12	4.557935	controller	host	HCI_EVT	7	Rcvd Encryption Change

> Frame 9: 258 bytes on wire (2064 bits), 258 bytes captured (2064 bits)

> Bluetooth

> Bluetooth HCI H4

▼ Bluetooth HCI Event - Remote Name Request Complete

Event Code: Remote Name Request Complete (0x07)

Parameter Total Length: 255

Status: Success (0x00)

BD_ADDR: SamsungE_b9:4f:c6 (0c:b3:19:b9:4f:c6)

Remote Name: GT-S7390G

[illegible]

SHA1

Convertissez simplement vos fichiers au format Sha1 pour convertir des mots de passe par exemple. Le SHA-1 (Secure Hash Algorithm) est très utile pour la sécurisation du stockage des mots de passe d'un site web. Dans les questions, nous vous expliquerons aussi la différence avec SHA2 et SHA256.




Attention : SHA1 ne devrait aujourd'hui plus être utilisé. Nous vous recommandons bcrypt !

Résultat du hash

Le hash de votre texte est :

c1d0349c153ed96fe2fadf44e880aef9e69c122b

Recommencer



Exercice 6

Énoncé

Trouvez le mot de passe "Enable".

Pour trouver le mot de passe « Enable », j'ai relevé tous les mots de passes de la liste, puis je les ai converti en grâce a un site internet en Hash Cisco 7.

Le point commun de tous ces mots de passes était qu'ils commençaient tous par « 6sK0 » j'ai donc pris ce début et y ai ajouté « 6Sk0_enable » (format des autres mot de passes.

```
.
security passwords min-length 8
no logging console
enable secret 5 $1$p8Y6$MCdRLBzuGlF0s9S.hXOp0.
!
username hub password 7 025017705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
```


1 – Recherche en ligne

HASH Cisco 7 demandé : 025017705b3907344e

Mot de passe correspondant : 6sK0_hub

HASH Cisco 7 (Exemple : 062B0A33)

Exercice 8

Énoncé

Retrouvez le TTL employé pour atteindre l'hôte ciblé par cet échange de paquets ICMP.

Pour retrouver le TTL, j'ai parcouru la liste et vérifié à quel moment il y allait avoir une réponse, cette réponse est finalement arrivée au « ttl=13 », donc la réponse est 13.

No.	Time	Source	Destination	Protocol	Length	Info
65	44.790695	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=9216/36, ttl=12 (no response found!)
66	44.870689	204.2.121.162	24.6.126.218	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
67	44.874186	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=9472/37, ttl=12 (no response found!)
68	44.969505	204.2.121.162	24.6.126.218	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
69	44.973782	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=9728/38, ttl=12 (no response found!)
70	45.077511	204.2.121.162	24.6.126.218	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	49.252888	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=9984/39, ttl=13 (reply in 72)
72	49.345998	198.173.244.32	24.6.126.218	ICMP	106	Echo (ping) reply id=0x0200, seq=9984/39, ttl=51 (request in 71)
73	49.346312	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=10240/40, ttl=13 (reply in 74)
74	49.424540	198.173.244.32	24.6.126.218	ICMP	106	Echo (ping) reply id=0x0200, seq=10240/40, ttl=51 (request in 73)
75	49.425163	24.6.126.218	198.173.244.32	ICMP	106	Echo (ping) request id=0x0200, seq=10496/41, ttl=13 (reply in 76)
76	49.503822	198.173.244.32	24.6.126.218	ICMP	106	Echo (ping) reply id=0x0200, seq=10496/41, ttl=51 (request in 75)

```
> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on 0
> Ethernet II, Src: AmbitMic_aa:af:80 (00:d0:59:aa:af:80), Dst: Cadant_22:89:c2 (00:01:5c:22:89:c2)
> Internet Protocol Version 4, Src: 24.6.126.218, Dst: 198.173.244.32
> Internet Control Message Protocol
```

Lors de cette première journée de YDAYS, j'ai découvert WireShark et appris à me familiariser avec ce logiciel, et ces exercices m'ont beaucoup aidé. J'ai également appris à convertir des valeurs afin d'obtenir un mot de passe.

