

Février-Mars 2023

# RAPPORT TP SÉCURITÉ RÉSEAUX

**Réalisé par :**  
MOUNOUAR Abderrahim

**Encadrée par :**  
Mme.BOUHADOUR

# Objectif du TP

**Ces TPs ont pour objectif de nous permettre de mettre en pratique les connaissances théoriques acquises pendant les cours. Le but de ces TPs, , est de développer des compétences techniques concrètes, de se familiariser avec des outils et des technologies de sécurité, et d'acquérir une expérience pratique dans la gestion de la sécurité des réseaux et des systèmes. Ils nous permettent également de mieux comprendre les enjeux de la sécurité informatique, en confrontant les aspects théoriques à la réalité des situations concrètes.**

**Le TP de Telnet, SSH, Snort et vsftpd et chiffrement avec ECB et CBC a pour objectif de :**

- Comprendre les protocoles de communication à distance entre ordinateurs (Telnet et SSH).**
- Savoir configurer un serveur de transfert de fichiers sécurisé (vsftpd).**
- Apprendre à détecter les intrusions sur un réseau informatique (Snort).**
- Acquérir des compétences pratiques dans l'utilisation de ces outils pour la sécurité réseau.**
- Comprendre les bonnes pratiques de sécurité associées à l'utilisation de ces protocoles et outils.**
- Comprendre les principes de base du chiffrement avec ECB et CBC.**

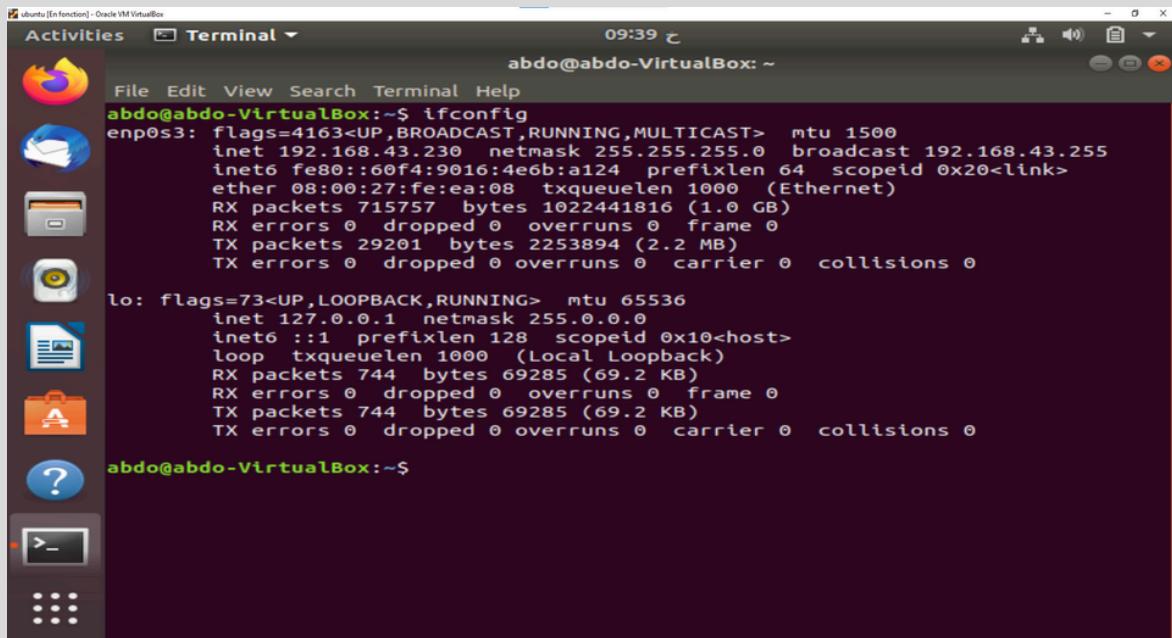
# TELNET & SSH

---

# Test Sniffing sur le protocole Telnet en utilisant l'outils Wireshark

Configuration des adresses IP des machines :

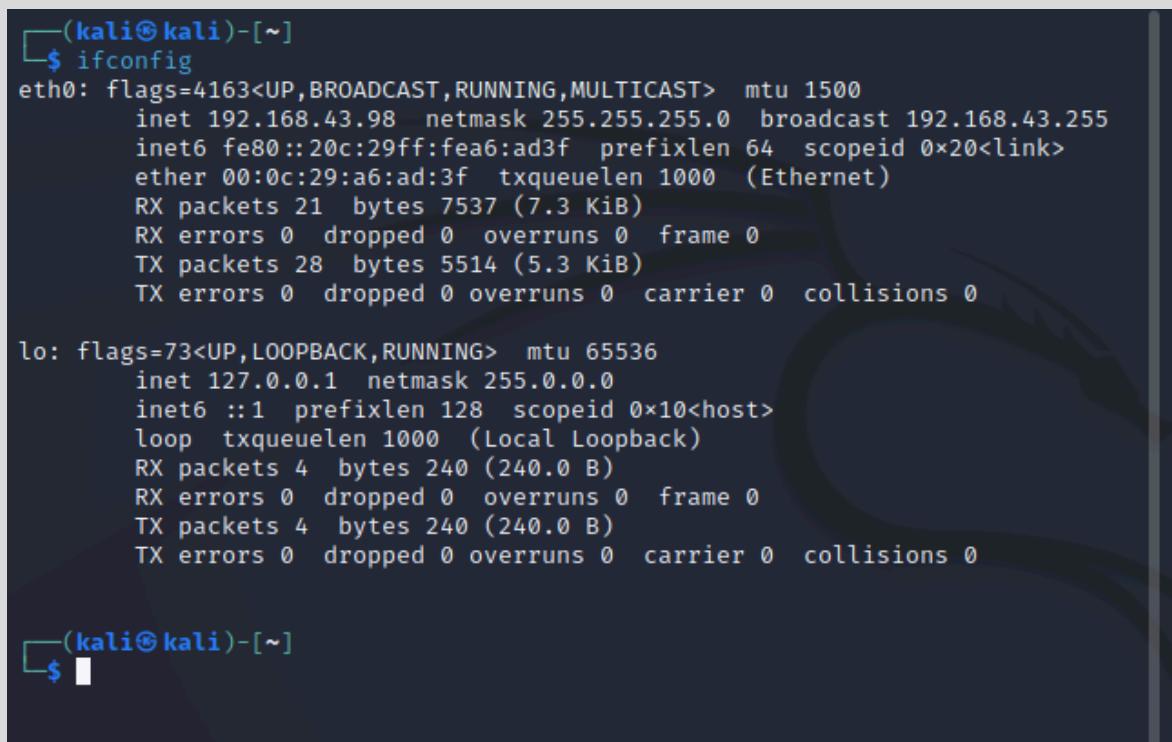
## Machine1 (ubuntu) :



```
ubuntu [En fonction] - Oracle VM VirtualBox
Activities Terminal 09:39 abdo@abdo-VirtualBox: ~
File Edit View Search Terminal Help
abdo@abdo-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.43.230 netmask 255.255.255.0 broadcast 192.168.43.255
        inet6 fe80::60f4:9016:4e6b:a124 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:fe:ea:08 txqueuelen 1000 (Ethernet)
            RX packets 715757 bytes 1022441816 (1.0 GB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 29201 bytes 2253894 (2.2 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 744 bytes 69285 (69.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 744 bytes 69285 (69.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
abdo@abdo-VirtualBox:~$
```

## Machine 2 (kali) :



```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.43.98 netmask 255.255.255.0 broadcast 192.168.43.255
        inet6 fe80::20c:29ff:fea6:ad3f prefixlen 64 scopeid 0x20<link>
          ether 00:0c:29:a6:ad:3f txqueuelen 1000 (Ethernet)
            RX packets 21 bytes 7537 (7.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 28 bytes 5514 (5.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 4 bytes 240 (240.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4 bytes 240 (240.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$
```

## Machine 3 (windows) :

## **Machine 4 (windows) :**

```
Administrator: Command Prompt

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::551:a4cb:4403:5872%11
IPv4 Address. . . . . : 192.168.193.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::160c:6468:e151:e52f%15
IPv4 Address. . . . . : 192.168.237.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5163:8dc5:dc41:f8a1%6
IPv4 Address. . . . . : 192.168.43.99
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.43.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Windows\system32>
```

**N.B: Toutes les machines appartiennent au même réseau**

## Connection au serveur telnet :

### Sous machine 2 (kali) :

```
abdo@abdo-VirtualBox:~$ telnet 192.168.43.230
Trying 192.168.43.230 ...
Connected to 192.168.43.2301. Connection Telnet
Escape character is '^]'.
Ubuntu 18.04.6 LTS
abdo-VirtualBox login: abdo
Password:
Login incorrect2 Mot de passe
abdo-VirtualBox login: abdo
Password:
Last login: Thu Jan 19 10:06:39 +01 2023 from abdo-VirtualBox on pts/1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

276 updates can be applied immediately.
253 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

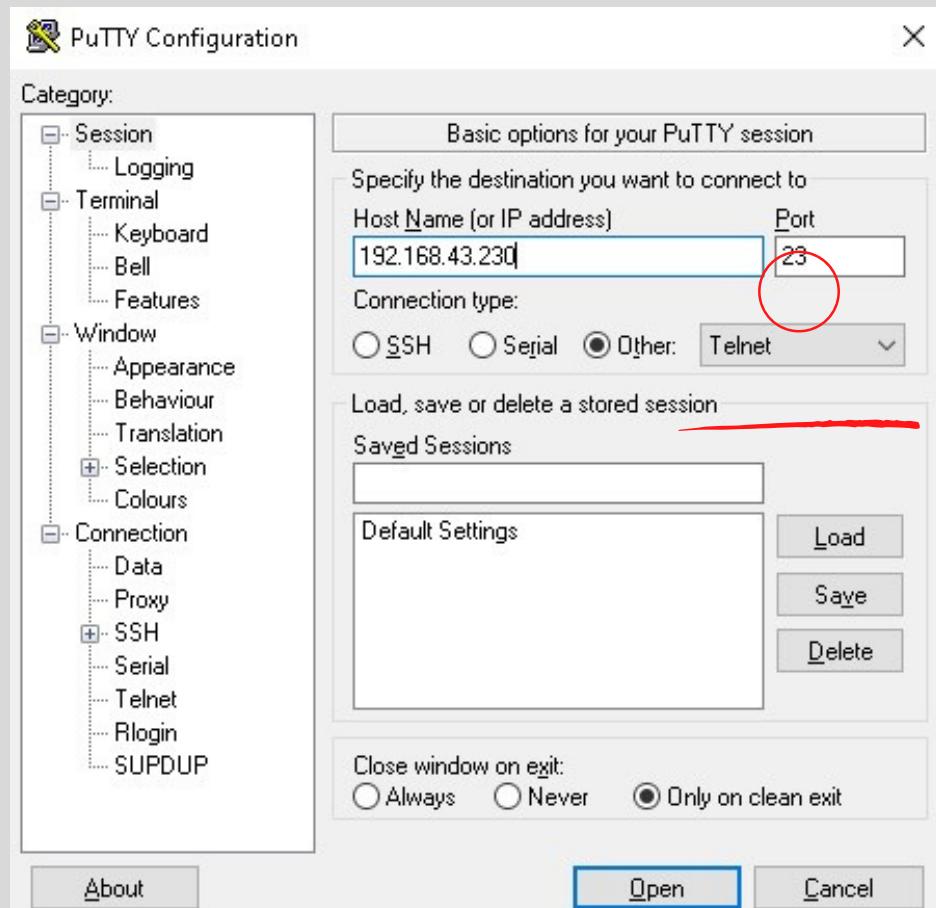
New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

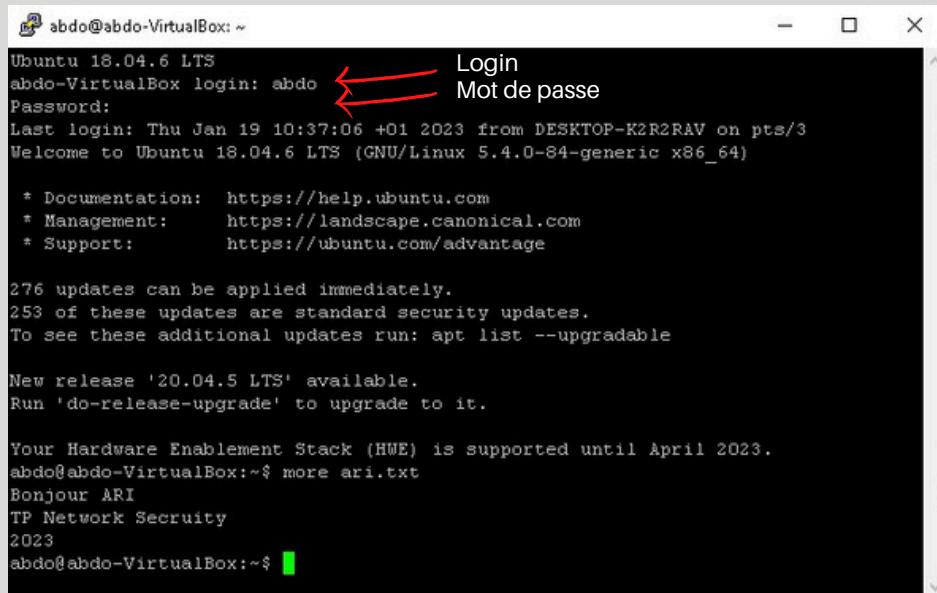
Your Hardware Enablement Stack (HWE) is supported until April 2023.
abdo@abdo-VirtualBox:~$ nano ari.txt
abdo@abdo-VirtualBox:~$ more ari.txt
Bonjour ARI
TP Network Security
2023
abdo@abdo-VirtualBox:~$
```

Annotations:

- Annotation 1: Points to the line "Connected to 192.168.43.230".
- Annotation 2: Points to the line "Login incorrect".
- Annotation 3: Points to the line "Mot de passe".

### Sous machine 4 (Windows) :





```

Ubuntu 18.04.6 LTS
abdo-VirtualBox login: abdo
Password: Mot de passe
Last login: Thu Jan 19 10:37:06 +01 2023 from DESKTOP-K2R2RAV on pts/3
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

276 updates can be applied immediately.
253 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

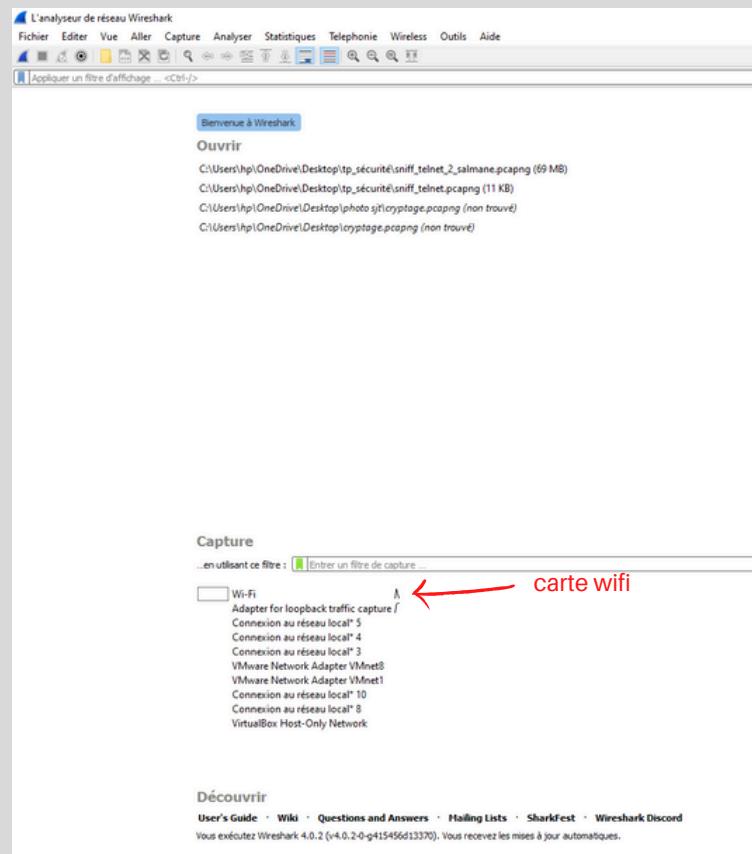
New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
abdo@abdo-VirtualBox:~$ more ari.txt
Bonjour ARI
TP Network Security
2023
abdo@abdo-VirtualBox:~$ 
```

Sniffing des paquets en utilisant l'outil Wireshark :

### Sous machine 3 (Windows) :

**Sniffing des paquets passants de la machine 2 (kali) vers la machine 1 (ubuntu) :**



**Choix du réseau qu'on veut sniffer**

No.	Time	Source	Destination	Protocol	Length	Info
67	30.319557	192.168.43.99	192.168.43.230	TELNET	71	Telnet Data ...
68	30.319557	192.168.43.99	192.168.43.230	TELNET	60	Telnet Data ...
69	30.320292	192.168.43.99	192.168.43.230	TELNET	65	Telnet Data ...
70	30.325457	192.168.43.230	192.168.43.99	TELNET	63	Telnet Data ...
72	30.335259	192.168.43.99	192.168.43.230	TELNET	57	Telnet Data ...
73	30.337209	192.168.43.230	192.168.43.99	TELNET	74	Telnet Data ...
74	30.338298	192.168.43.99	192.168.43.230	TELNET	57	Telnet Data ...
75	30.338802	192.168.43.99	192.168.43.230	TELNET	57	Telnet Data ...
78	30.390332	192.168.43.230	192.168.43.99	TELNET	77	Telnet Data ...
80	31.686794	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
81	31.687000	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
83	31.692194	192.168.43.230	192.168.43.99	TELNET	60	Telnet Data ...
85	31.815099	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
86	31.817497	192.168.43.230	192.168.43.99	TELNET	60	Telnet Data ...
88	31.974408	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
89	31.979182	192.168.43.230	192.168.43.99	TELNET	60	Telnet Data ...
91	32.295660	192.168.43.99	192.168.43.230	TELNET	56	Telnet Data ...
92	32.299551	192.168.43.230	192.168.43.99	TELNET	66	Telnet Data ...
102	36.396375	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
104	36.904813	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
106	36.934485	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
109	37.210950	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
111	37.310703	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
113	37.620785	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
115	37.658699	192.168.43.99	192.168.43.230	TELNET	55	Telnet Data ...
117	38.137820	192.168.43.99	192.168.43.230	TELNET	56	Telnet Data ...
119	38.147377	192.168.43.230	192.168.43.99	TELNET	60	Telnet Data ...
121	38.193866	192.168.43.230	192.168.43.99	TELNET	126	Telnet Data ...
124	38.527214	192.168.43.230	192.168.43.99	TELNET	119	Telnet Data ...

```

0000  4c 34 88 24 30 92 88 b1 11 a2 4f 68 4c 34 88 24 30 92 08 00 45 10 L4 $0...-$0h-$E-
0010  01 f4 81 f9 40 00 40 06 0e 60 c9 a8 2b e6 c9 a8 @...@...-$E-
0020  2b d3 00 17 f4 bd a6 4f 59 ff fc 49 94 76 50 18 +c...0 Y- I-{P-
0030  01 f6 c8 25 00 00 0d 0a 0d 0a 20 20 44 6f 63 ...%...* Doc
0040  75 6d 66 6e 74 61 74 69 6f 6e 3a 20 20 68 74 74 ugmentati on: htt
0050  70 73 3a 2f 2f 68 65 6c 70 2e 75 62 75 6e 74 75 ps://hel p.ubuntu
0060  2e 63 6f 6d 0d 0a 28 2a 2d 61 6e 61 67 65 6d .com...* Managem
0070  65 6e 74 3a 20 20 20 28 68 74 74 70 73 3a 2f ent: https://
0080  2f 6c 61 6e 64 73 63 61 78 65 2e 63 61 6e 6f 6e /landsc pe.canon
0090  69 63 61 6c 2e 63 6f 6d 0d 0a 20 2a 20 53 75 70 ical.com...* Sup
00a0  70 6f 72 74 3a 20 20 20 20 20 20 68 74 74 port: htt
00b0  70 73 3a 2f 2f 75 62 75 6e 74 75 6e 63 6f 6d 2f ps://ubu ntu.com/
00c0  61 64 76 61 6e 74 61 67 65 0d 0d 0a 32 37 36 advantag e...* 276
00d0  20 75 70 64 61 74 65 73 28 63 61 6e 20 62 65 20 updates can be
00e0  61 70 70 6c 69 65 64 20 69 6d 6d 65 64 69 61 74 applied immediat
00f0  65 6c 79 2e 0d 0a 32 35 33 20 6f 66 20 74 68 65 ely...* 25 3 of the
0100  73 65 20 75 70 64 61 74 65 73 20 61 72 65 20 73 se updat es are s
0110  74 61 6e 64 61 72 64 20 73 65 63 75 72 69 74 79 standard security
0120  20 75 70 64 61 74 65 73 2e 0d 0a 54 6f 20 73 65 updates ... To se
0130  65 20 74 68 65 65 20 61 64 64 69 74 69 6f 6e e these addition
0140  61 6c 20 75 70 64 61 74 65 73 20 72 75 6e 3a 20 al updat es run:
0150  61 70 74 28 6c 69 73 74 28 2d 2d 75 70 67 72 61 apt lista...* upgra
0160  64 61 62 6c 65 0d 0a 0d 0a 4e 65 77 20 72 65 6c dable...* New rel
0170  65 61 73 65 20 27 32 30 2e 30 34 2e 35 20 4c 54 ease '20 .04.5 LT
0180  53 27 20 61 76 61 69 6c 61 62 6c 65 2e 0d 0a 52 S' avail able...* R

```

## Filtrage des paquets du protocole TELNET, après les avoir analysés par Wireshark

1

2

3

4

No.	Time	Source	Destination	Protocol	Length	Info
121	3.867392	192.168.43.98	192.168.43.230	TELNET	99	Telnet Data ...
125	3.876709	192.168.43.230	192.168.43.98	TELNET	78	Telnet Data ...
127	3.887799	192.168.43.230	192.168.43.98	TELNET	111	Telnet Data ...
129	3.894814	192.168.43.98	192.168.43.230	TELNET	149	Telnet Data ...
131	3.896358	192.168.43.230	192.168.43.98	TELNET	69	Telnet Data ...
132	3.902355	192.168.43.98	192.168.43.230	TELNET	69	Telnet Data ...
134	3.903647	192.168.43.230	192.168.43.98	TELNET	69	Telnet Data ...
135	3.9108025	192.168.43.98	192.168.43.230	TELNET	69	Telnet Data ...
136	3.911083	192.168.43.230	192.168.43.98	TELNET	109	Telnet Data ...
142	5.296157	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
143	5.296789	192.168.43.230	192.168.43.98	TELNET	67	Telnet Data ...
147	5.526783	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
148	5.527476	192.168.43.230	192.168.43.98	TELNET	67	Telnet Data ...
151	5.620767	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
152	5.621614	192.168.43.230	192.168.43.98	TELNET	67	Telnet Data ...
154	5.835352	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
155	5.836157	192.168.43.230	192.168.43.98	TELNET	67	Telnet Data ...
158	6.115522	192.168.43.98	192.168.43.230	TELNET	68	Telnet Data ...
159	6.117057	192.168.43.230	192.168.43.98	TELNET	78	Telnet Data ...
370	7.794851	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
407	8.394016	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
410	8.454736	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
431	9.420804	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
436	9.456290	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
438	9.727514	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
440	9.757392	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
443	10.444384	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
445	10.4456079	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
448	11.673319	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
450	11.681864	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
452	11.980832	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...
455	12.389713	192.168.43.98	192.168.43.230	TELNET	67	Telnet Data ...

Flux TCP 4 Ctrl+Alt+ Maj+T

Flux UDP Ctrl+Alt+ Maj+U

Flux DCCP Ctrl+Alt+ Maj+E

Flux TLS Ctrl+Alt+ Maj+S

Flux HTTP Ctrl+Alt+ Maj+H

Flux HTTP/2

Flux RAPIDE

Appel SIP

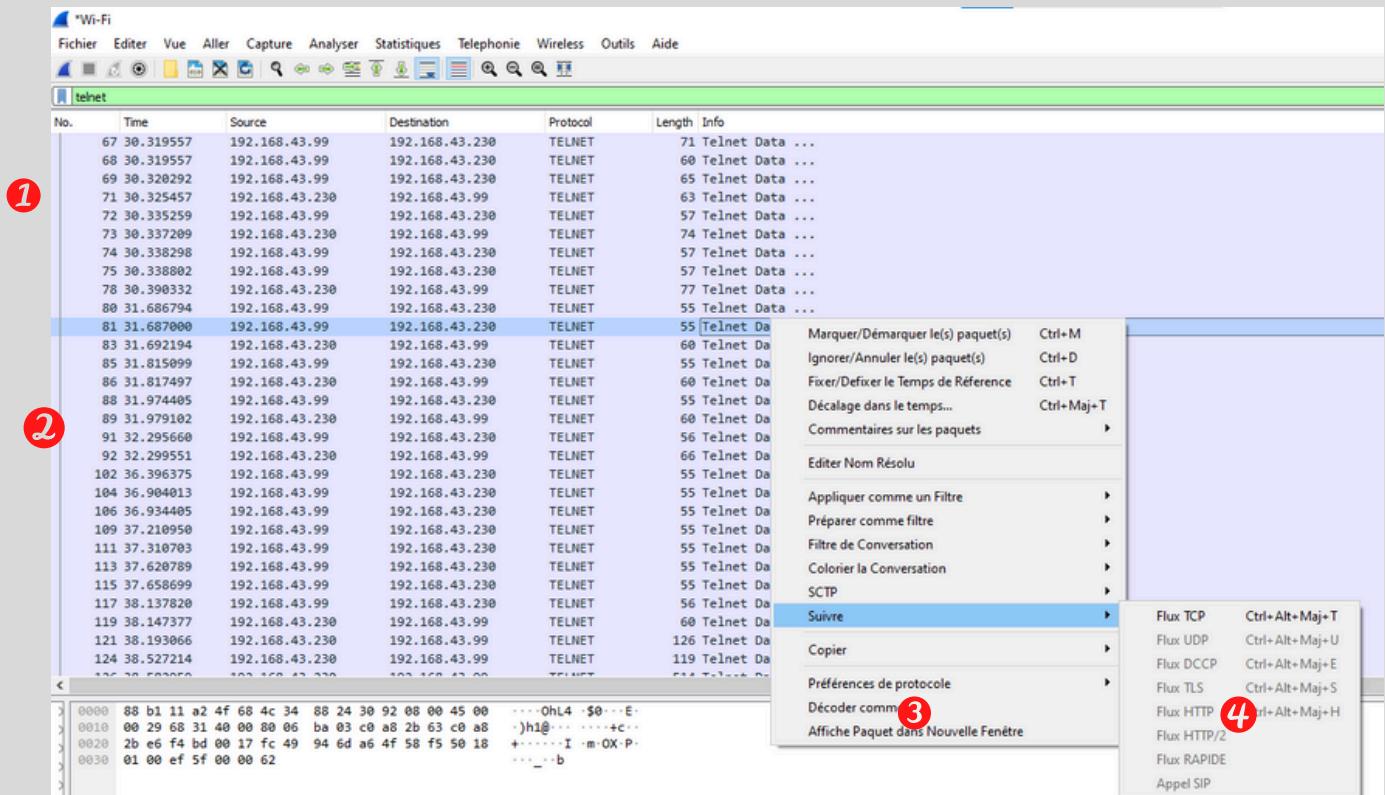
Après, on va suivre le flux TCP pour afficher les données transférées par le protocole TELNET

#### Affichage des données transférées sur le réseau à travers le protocole TELNET

**Remarque : les données transférées par le protocole TELNET ne sont pas chiffrées**

## Sniffing des paquets passants de la machine 4 (windows) vers la machine 1 (ubuntu) :

**Après avoir choisi la carte réseau à sniffer, on filtre les paquets réseau sniffés par protocole (telnet dans notre cas)**



**On va suivre le flux TCP pour afficher les données transférées par le protocole TELNET**

```

Wireshark - Suivre le flux TCP (tcp.stream eq 4) - Wi-Fi

abdo-VirtualBox login: ababddoo
Password: A011003

Last login: Thu Jan 19 10:46:53 +01 2023 from DESKTOP-K2R2RAV on pts/3
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-84-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

276 updates can be applied immediately.
253 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
.J@abdo@abdo-VirtualBox: ~.abdo@abdo-VirtualBox:~$ .[Aexit.[A...more ari.txt

Bonjour ARI
TP Network Security
2023
.J@abdo@abdo-VirtualBox: ~.abdo@abdo-VirtualBox:~$
```

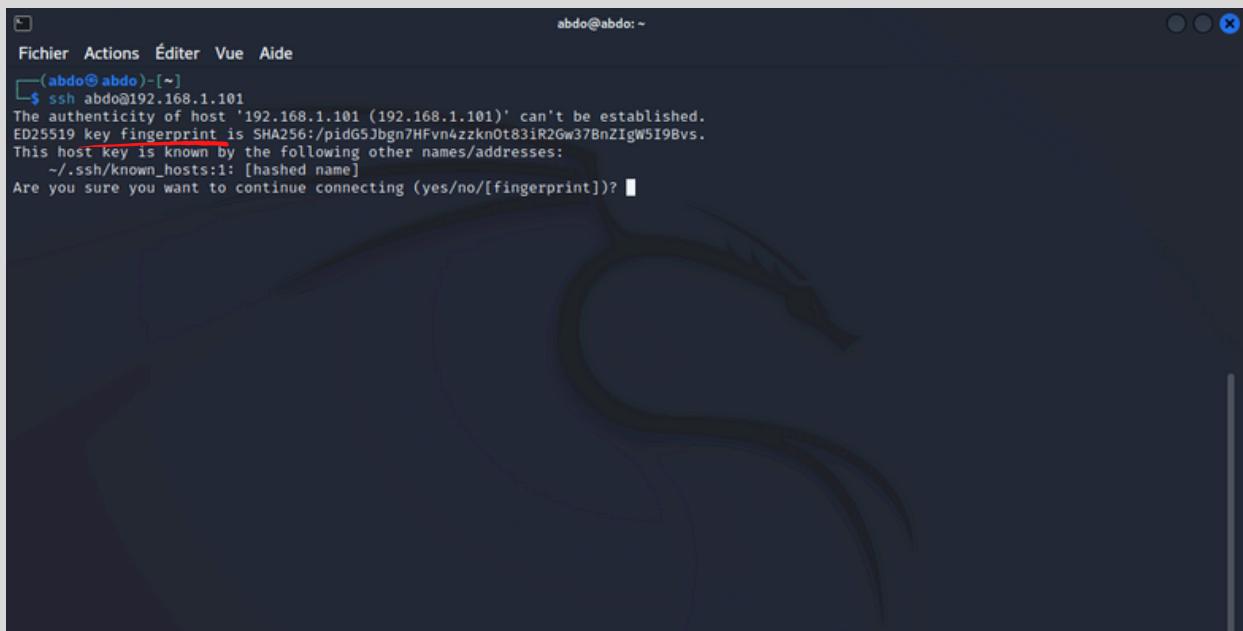
**Affichage des données transférées sur le réseau à travers le protocole TELNET**

# Test Sniffing sur le protocole Telnet en utilisant l'outils Wireshark

Configuration des adresses IP des machines :

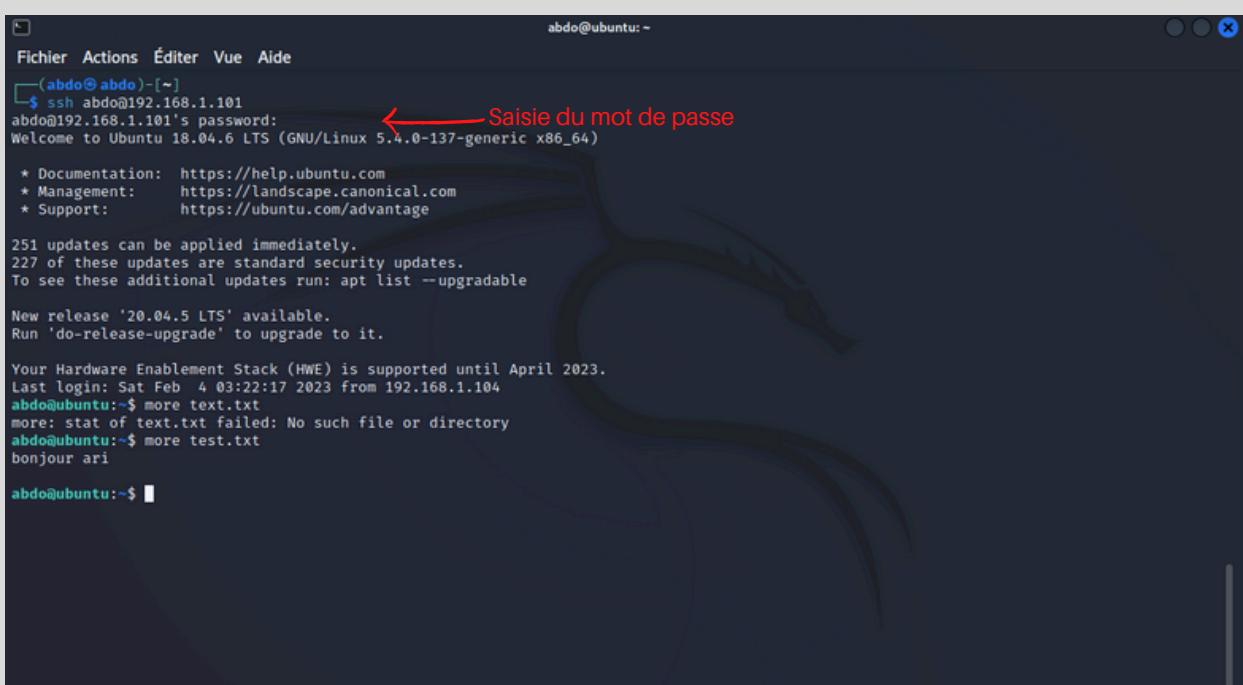
- **Machine serveur ubuntu : 192.168.1.101**
- **Machine kali : 192.168.104**
- **Machine windows : 192.168.1.106**

Connection au serveur SSH:



```
Fichier Actions Éditer Vue Aide
(abdo@abdo)-[~]
$ ssh abdo@192.168.1.101
The authenticity of host '192.168.1.101 (192.168.1.101)' can't be established.
ED25519 key fingerprint is SHA256:/pidG5Jbgn7HFvn4zzkn0t83iR2Gw37BnZigW5I9Bvs.
This host key is known by the following other names/addresses:
  -> /ssh/known_hosts:: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? ■
```

**Lors de la première connexion, une empreinte digitale SSH v2 est générée à partir de la clé publique d'une paire de clés SSH v2.**



```
Fichier Actions Éditer Vue Aide
(abdo@abdo)-[~]
$ ssh abdo@192.168.1.101
abdo@192.168.1.101's password: ← Saisie du mot de passe
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-137-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

251 updates can be applied immediately.
227 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

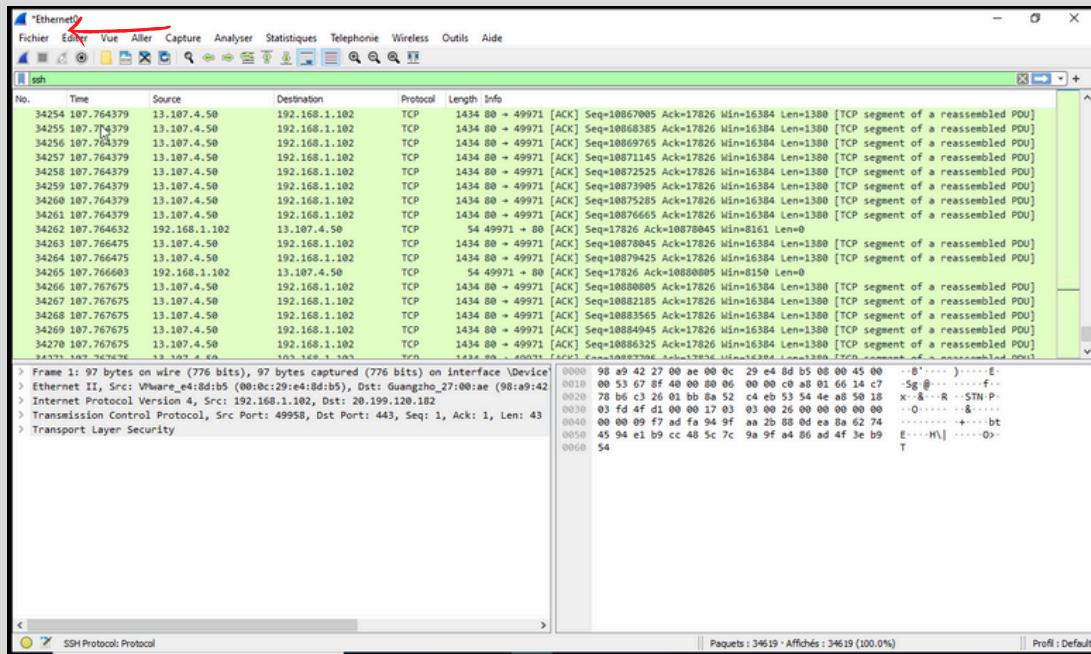
New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Sat Feb  4 03:22:17 2023 from 192.168.1.104
abdo@ubuntu:~$ more text.txt
more: stat of text.txt failed: No such file or directory
abdo@ubuntu:~$ more test.txt
bonjour ari
abdo@ubuntu:~$ ■
```

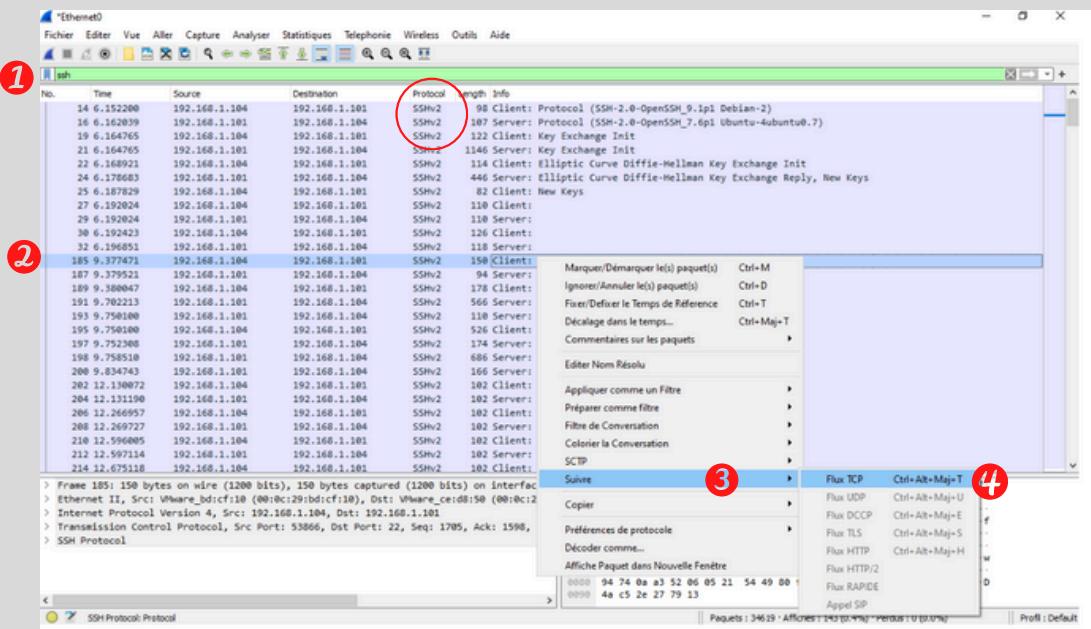
**Après la saisie du mot de passe, la connexion est établie via SSH v2**

# Sniffing des paquets passants de la machine kali vers la machine ubuntu :

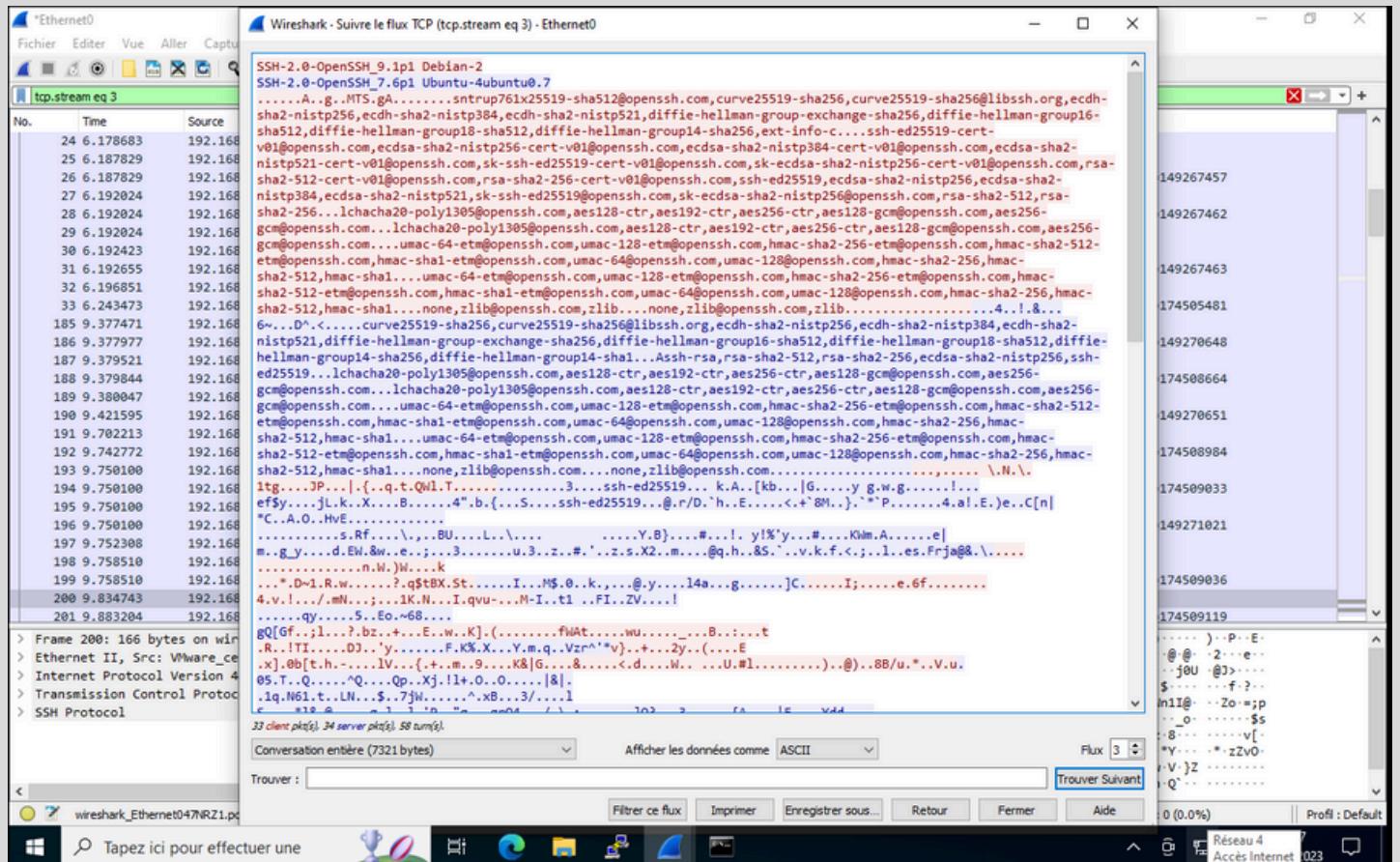
Après avoir choisi la carte réseau à sniffer, on filtre les paquets réseau sniffés par protocole (SSH dans notre cas)



Filtrage des paquets par protocole (SSH), après les avoir sniffés par Wireshark



Après, on va suivre le flux TCP pour afficher les données transférées par le protocole SSH



## Affichage des données transférées sur le réseau à travers le protocole SSH

**Remarque : les données transférées par le protocole SSH sont chiffrés**

**SNORT**

---

#### **La vérification de la bonne installation et la version de Snort**

**La configuration de l'adresse du réseau sur lequel snort surveillera le trafic et tous les réseaux externes comme étant potentiellement dangereux dans le fichier /etc/snort/snort.conf**

## Définition de l'emplacement des règles de détection

```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules

#####
# Step #9: Customize your Shared Object Snort Rules
# For more information, see http://vrt-blog.snort.org/2009/01/using-vrt-certified-shared-object-rules.html
#####

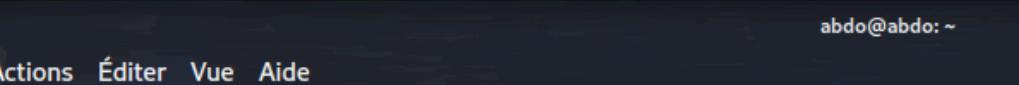
# dynamic library rules
# include $SO_RULE_PATH/bad-traffic.rules
# include $SO_RULE_PATH/chat.rules
# include $SO_RULE_PATH/dos.rules
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/icmp.rules
# include $SO_RULE_PATH/imap.rules
# include $SO_RULE_PATH/misc.rules
# include $SO_RULE_PATH/multimedia.rules
# include $SO_RULE_PATH/netbios.rules
# include $SO_RULE_PATH/nntp.rules
# include $SO_RULE_PATH/p2p.rules
# include $SO_RULE_PATH/smtp.rules
# include $SO_RULE_PATH/snmp.rules
# include $SO_RULE_PATH/specIFIC-threats.rules
# include $SO_RULE_PATH/web-activex.rules
# include $SO_RULE_PATH/web-client.rules
# include $SO_RULE_PATH/web-iis.rules
# include $SO_RULE_PATH/web-misc.rules

# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
include $RULE_PATH/local.rules
```

fichier des règles

## **Inclusion du fichier de règles de détection dans la configuration du snort**

## Activation de détection des paquets ICMP



```
Fichier Actions Éditer Vue Aide
└── (abdo@abdo)-[~]
    $ sudo nano /etc/snort/snort.conf
[sudo] Mot de passe de abdo :
└── (abdo@abdo)-[~]
    $ sudo touch /etc/snort/rules/local.rules
```

A red arrow points from the text "fichier des règles" to the command `sudo touch /etc/snort/rules/local.rules`.

## **Creation du fichier des règles "/etc/snort/rules/local.rules"**

```
GNU nano 6.4 /etc/snort/rules/local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
alert icmp any any → $HOME_NET any (msg:"ICMP traffic detected"; sid:10000001; rev:001;)

règle de detection
```

### Ajout de la règle de détection des paquets ICMP

"alert icmp any any -> \$HOME\_NET any (msg:"ICMP traffic detected"; sid:10000001; rev:001;)"

Démarrage du snort abdo@abdo:~

```
$ sudo snort -A console -q -u snort -c /etc/snort/snort.conf -i eth0
[abdo@abdo:~]#
```

paquets ICMP détectés

```
root@abdo:~/home/abdo
# ip link set eth0 promisc on
[root@abdo:~/home/abdo]
```

ping sur notre machine

```
C:\> ping -t 192.168.43.228
```

**Détection des paquets ICMP dans le réseau destinés à notre machine KALI 192.168.43.228/24 et initiés par notre machine Windows 192.168.43.175/24**

**VSFTPD**



```
abdo@abdo: /etc
Fichier Actions Éditer Vue Aide
└──(abdo@abdo)-[~]
$ sudo apt install vsftpd
Lecture des listes de paquets ... Fait
Construction de l'arbre des dépendances ... Fait
Lecture des informations d'état ... Fait
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
  0 mis à jour, 1 nouvellement installés, 0 à enlever et 1425 non mis à jour.
Il est nécessaire de prendre 142 ko dans les archives.
Après cette opération, 351 ko d'espace disque supplémentaires seront utilisés
.
Réception de :1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd6
4 3.0.3-13+b2 [142 kB]
142 ko réceptionnés en 1s (126 ko/s)
Préconfiguration des paquets ...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données ... 415374 fichiers et répertoires déjà install
és.)
Préparation du dépaquetage de ... /vsftpd_3.0.3-13+b2_amd64.deb ...
Dépaquetage de vsftpd (3.0.3-13+b2) ...
Paramétrage de vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Traitement des actions différées (« triggers ») pour man-db (2.11.0-1+b1) ...
Traitement des actions différées (« triggers ») pour kali-menu (2022.4.1) ...
```

### Installation du service vsftpd par la commande sudo apt install vsftpd

```
abdo@abdo: /etc
Fichier Actions Éditer Vue Aide
GNU nano 6.4          /etc/vsftpd.conf *
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES ← enable anonymous
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter
^X Quitter   ^R Lire fich.  ^\ Remplacer   ^U Coller      ^J Justifier
```

On accède au fichier "vsftpd.conf" et on change la configuration afin de sécuriser le bon fonctionnement selon notre besoin

```

GNU nano 6.4          /etc/vsftpd.conf *
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES      ← anonymous upload
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES ← anonymous mkdir write enable
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter
^X Quitter   ^R Lire fich.  ^V Remplacer   ^U Coller      ^J Justifier

```

**La configuration au-dessus donne l'accès aux utilisateurs anonymes, et les autorise de créer les dossiers et d'importer les fichiers**

```

abdo@abdo:/srv/ftp
Fichier Actions Éditer Vue Aide
└── abdo@abdo-[/srv/ftp] ← anonymous directory
    └── ls
        test_ari.txt  test.txt
abdo@abdo:~/chiffrement
abdo@abdo-[/srv/ftp]
$ [ ]
GNU nano 6.4          textdechiffrer.txt
bonjour ari . tp security
avec Mme BOUHADOUR

```

**"/srv/ftp" dossier gérant les fichiers des clients anonymous**

## Connexion par client normal :

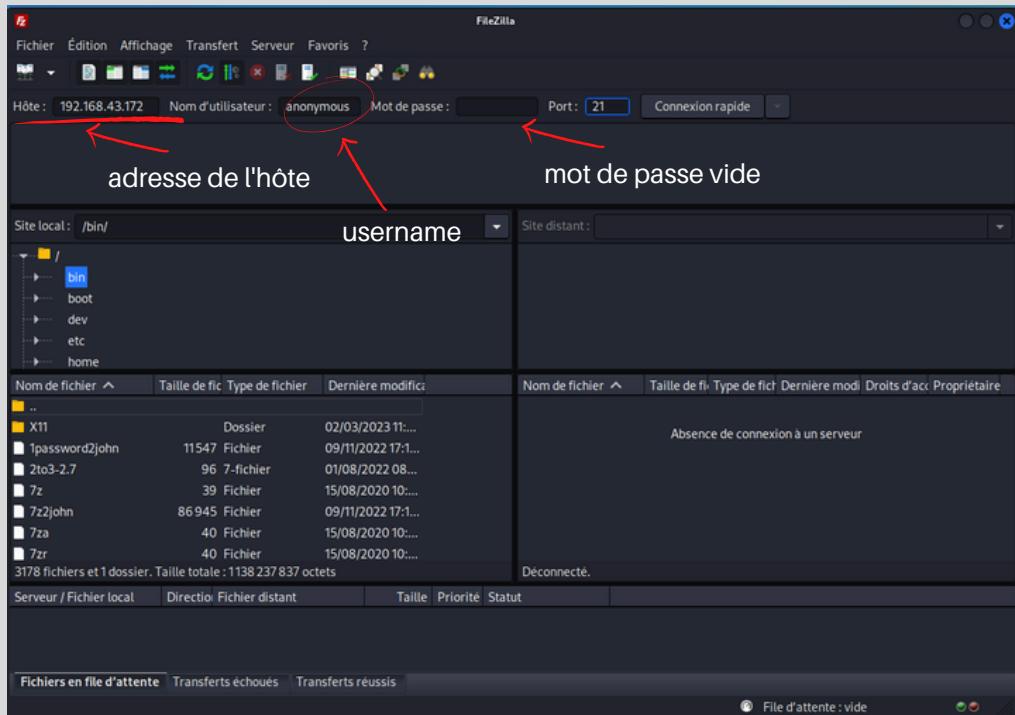
```
abdo@abdo: ~
Fichier Actions Éditer Vue Aide
└$ sudo ftp 192.168.43.172 connexion ftp
Connected to 192.168.43.172.
220 (vsFTPd 3.0.3)
Name (192.168.43.172:abdo): tp_security
331 Please specify the password.
Password: password client
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8914|)
150 Here comes the directory listing.
drwxr-xr-x 2 0 0 4096 Mar 02 10:52 cours les fichiers du
226 Directory send OK.
ftp> cd cours
client
250 Directory successfully changed.
ftp> get security.txt download du fichier
local: security.txt remote: security.txt
229 Entering Extended Passive Mode (|||57928|)
150 Opening BINARY mode data connection for security.txt (0 bytes).
0 0.00 KiB/s
226 Transfer complete.
ftp> put security.txt upload du fichier
local: security.txt remote: security.txt
229 Entering Extended Passive Mode (|||42162|)
550 Permission denied.
ftp> █
```

**Connexion au serveur ftp en utilisant un username et un mot de passe, ensuite execution des commandes : ls, get et put.**

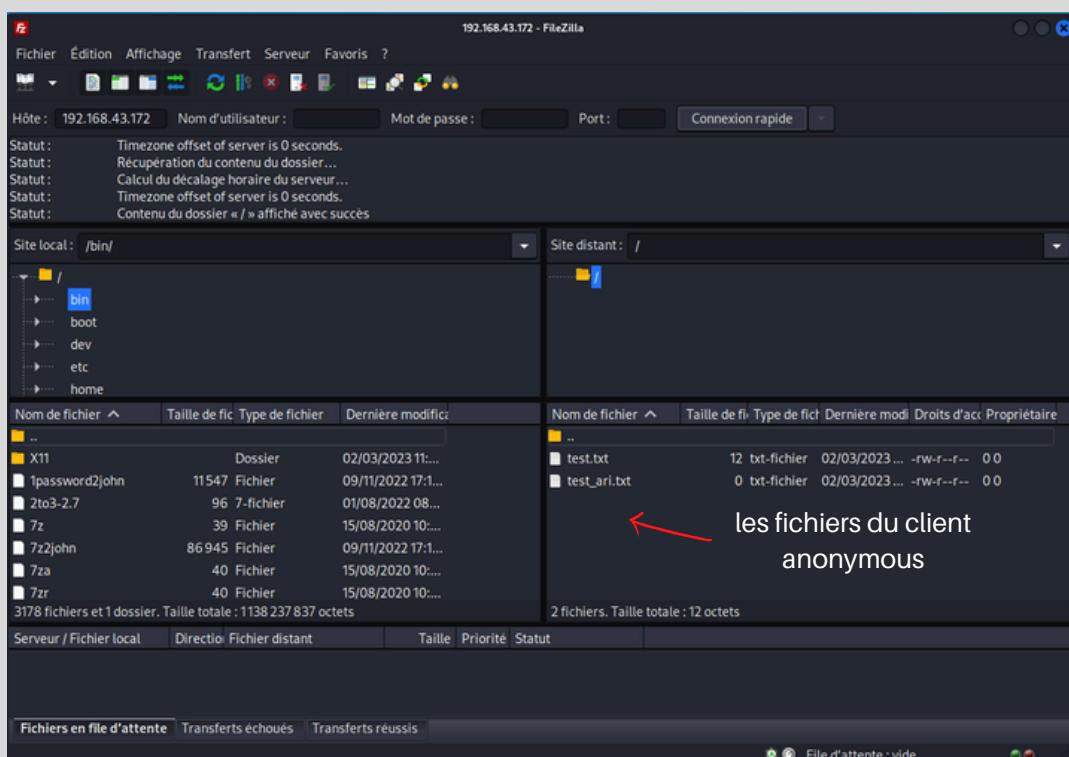
## Connexion par client anonymous :

```
abdo@abdo: ~
Fichier Actions Éditer Vue Aide
└$ ftp 192.168.43.172 connexion ftp
Connected to 192.168.43.172.
220 (vsFTPd 3.0.3)
Name (192.168.43.172:abdo): anonymous username anonymous
331 Please specify the password.
Password: mot de passe vide
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||20658|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 12 Mar 02 12:05 test.txt
-rw-r--r-- 1 0 0 0 Mar 02 12:05 test_ari.txt
226 Directory send OK.
ftp> get test_ari.txt download du fichier
local: test_ari.txt remote: test_ari.txt
229 Entering Extended Passive Mode (|||31213|)
150 Opening BINARY mode data connection for test_ari.txt (0 bytes).
0 0.00 KiB/s
226 Transfer complete.
ftp> █
```

**Connexion au serveur ftp en entrant anonymous comme username et sans saisir un mot de passe, puis l'execution des commandes : ls et get.**



### **Connexion au serveur ftp par un client "FILEZILLA" par un client anonymous**



### **Après connexion on a la possibilité de télécharger les fichiers depuis le serveur ftp**

**N.B: Le upload des fichiers vers le serveur, même si cela a été précédemment autorisé dans le fichier de configuration "vsftpd.conf"**

# CHIFFREMENT

---

## Chiffrement par des-ecc :

The screenshot shows a terminal window titled "abdo@abdo: ~/chiffrement". The file "text.txt" is open in nano 6.4. The content of the file is:

```
GNU nano 6.4
bonjour ari . tp security
avec Mme BOUHADOUR
```

The bottom status bar shows keyboard shortcuts for various operations like Help (^G), Quit (^X), Write (^O), Read file (^R), Find (^W), Replace (^R), Cut (^K), Copy (^C), Paste (^V), Execute (^T), and Justify (^J). The message "[ Lecture de 2 lignes ]" indicates the file contains 2 lines.

On crée un fichier "text.txt" contenant de l'infomation en clair

The screenshot shows a terminal window titled "abdo@abdo: ~/chiffrement". The command entered is:

```
$ openssl enc -e -des-ecb -in text.txt -out textchiffre.txt
```

Annotations with red arrows point to specific parts of the command:

- An arrow points to the "-e" option in the command with the label "Chiffrement".
- An arrow points to the password entry field with the label "Mot de passe de chiffrement".

The terminal also displays a warning message about the use of DES-ECB mode:

```
enter DES-ECB encryption password:  
Verifying - enter DES-ECB encryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.
```

On chiffre le fichier "text.txt" on utilisant l'algorithme du chiffrement DES en mode de fonctionnement ECB, le résultat est sauvegardé dans un fichier "textchiffre.txt"

```
GNU nano 6.4          textchiffre.txt
Salted_...]♦♦♦^FPr^0+
H♦wP♦♦^S^NNS)3~♦q♦♦♦^Cv♦@♦♦$♦3♦♦p♦4e♦^X! J+♦$s
```

Text chiffré

**Le contenu du fichier "textchiffre.txt" est le texte crypté  
du fichier "text.txt"**

```
abdo@abdo: ~/chiffrement
Fichier Actions Éditer Vue Aide
(abdo@abdo)-[~/chiffrement]
$ nano text.txt

(abdo@abdo)-[~/chiffrement]
$ openssl enc -e -des-ecb -in text.txt -out textchiffre.txt
enter DES-ECB encryption password:
Verifying - enter DES-ECB encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

(abdo@abdo)-[~/chiffrement]
$ nano textchiffre.txt

(abdo@abdo)-[~/chiffrement]
$ openssl enc -d -des-ecb -in textchiffre.txt -out textdechiffre.txt
```

Déchiffrement

**On déchiffre le fichier "textchiffre.txt", précédemment chiffré on  
utilisant l'algorithme du chiffrement DES en mode de fonctionnement  
ECB, le résultat est sauvegardé dans un fichier "textdechiffre.txt"**

GNU nano 6.4 textdechiffrer.txt

bonjour ari . tp security  
avec Mme BOUHADOUR

[ Lecture de 2 lignes ]

**Text déchiffré**

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter  
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier

**Le contenu du fichier "dechiffrer.txt" est le même que celui du fichier d'origine "text.txt"**

### Chiffrement par des-cbc :

GNU nano 6.4 CBC\_DES\_clear.txt \*

tp cryptage CBC DES ARI 2023

**Text clair**

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

**On crée de nouveau un fichier "CBC\_DES\_clear.txt" contenant de l'infomation en claire**

```
root@kali: /home/kali
File Actions Edit View Help
└─(root㉿kali)-[~/home/kali]
# nano CBC_DES_clear.txt

└─(root㉿kali)-[~/home/kali]
# openssl enc -e -des-cbc -in CBC_DES_clear.txt -out CBC_DES_crypted.txt
enter DES-CBC encryption password:
Verifying - enter DES-CBC encryption password:
** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

└─(root㉿kali)-[~/home/kali]
#
```

A red arrow points from the text "Chiffrement" to the command "openssl enc -e".

**On chiffre le fichier "CBC\_DES\_clear.txt" en utilisant l'algorithme du chiffrement DES en mode de fonctionnement ECB, le résultat est sauvegardé dans un fichier "CBC\_DES\_crypted.txt"**

```
root@kali: /home/kali
File Actions Edit View Help
GNU nano 6.4          CBC_DES_crypted.txt
Salted__x!^A^V^,^2F%^)a@I+z+b4@9^QD^.

└─(root㉿kali)-[~/home/kali]
```

A red arrow points from the text "Text chiffré" to the encrypted text in the terminal window.

**Le contenu du fichier "CBC\_DES\_crypted.txt" est le texte crypté du fichier "CBC\_DES\_clear.txt"**

```
root@kali: /home/kali
File Actions Edit View Help
[(root㉿kali)-[/home/kali]
# nano CBC_DES_clear.txt

[(root㉿kali)-[/home/kali]
# openssl enc -e -des-cbc -in CBC_DES_clear.txt -out CBC_DES_crypted.txt
enter DES-CBC encryption password:
Verifying - enter DES-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

[(root㉿kali)-[/home/kali]
# nano CBC_DES_clear.txt

[(root㉿kali)-[/home/kali]
# nano CBC_DES_crypted.txt
Déchiffrement
[(root㉿kali)-[/home/kali]
# openssl enc -d -des-cbc -in CBC_DES_crypted.txt -out CBC_DES_decrypted.txt
enter DES-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

[(root㉿kali)-[/home/kali]
# ]
```

**On déchiffre le fichier "CBC\_DES\_crypted.txt", précédemment chiffré en utilisant l'algorithme du chiffrement DES en mode de fonctionnement CBC, le résultat est sauvegardé dans un fichier "CBC\_DES\_decrypted.txt"**

The image shows two terminal windows side-by-side. Both windows have a title bar 'root@kali: /home/kali' and a menu bar 'File Actions Edit View Help'. The left window displays the file 'CBC\_DES\_clear.txt' which contains the text 'tp cryptage CBC DES ARI 2023'. The right window displays the file 'CBC\_DES\_decrypted.txt' which also contains the text 'tp cryptage CBC DES ARI 2023'. The nano editor interface is visible at the bottom of both windows, showing various keyboard shortcuts like 'G Help', 'X Exit', 'W Write Out', 'R Read File', etc.

**Le contenu du fichier "CBC\_DES\_decrypted.txt" est le même que celui du fichier d'origine "CBC\_DES\_crypted.txt"**