

DUVAL Aurélien
NI : 111163937
ip : 192.168.1.163

TP 2 : Scan et footprinting

Question 5 : a)



```
root@kali Aurelien DUVAL :~#ping 192.168.1.110
PING 192.168.1.110 (192.168.1.110) 56(84) bytes of data.
64 bytes from 192.168.1.110: icmp_seq=1 ttl=64 time=0.288 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=64 time=0.273 ms
^C
--- 192.168.1.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.273/0.280/0.288/0.018 ms
root@kali Aurelien DUVAL :~#
```

b)



```
root@kali Aurelien DUVAL :~#nmap -sT 192.168.1.110
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 14:31 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00047s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 00:0C:29:37:A3:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
root@kali Aurelien DUVAL :~#
```

c)

Applications ▾ Places ▾ Terminal ▾ Fri 14:36 root@kali: ~

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap -sS --source-port 25 192.168.1.110
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 14:34 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00014s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 00:0C:29:37:A3:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
root@kali Aurelien DUVAL :~#
```

Places

- Trash
- VMware Tools
- + Other Locations

d)

Applications ▾ Places ▾ Terminal ▾ Fri 14:43 root@kali: ~

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap -sS --exclude 192.168.1.163 192.168.1.0-255
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 14:42 EDT
Nmap scan report for 192.168.1.1
Host is up (0.000060s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
443/tcp   open  https
902/tcp   open  iss-realsecure
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 192.168.1.110
Host is up (0.00018s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 00:0C:29:37:A3:6C (VMware)

Nmap done: 255 IP addresses (2 hosts up) scanned in 14.91 seconds
root@kali Aurelien DUVAL :~#
```

e)

File Edit View Search Terminal Help

```
root@kali Aurelien DUVAL :~#nmap -sU --top-ports 10 192.168.1.110
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 14:56 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00034s latency).
PORT      STATE    SERVICE
53/udp    closed   domain
67/udp    closed   dhcps
123/udp   closed   ntp
135/udp   closed   msrpc
137/udp   closed   netbios-ns
138/udp   closed   netbios-dgm
161/udp   closed   snmp
445/udp   closed   microsoft-ds
631/udp   open|filtered ipp
1434/udp  closed   ms-sql-m
MAC Address: 00:0C:29:37:A3:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.68 seconds
```

root@kali Aurelien DUVAL :~#

+ Other Locations

f)

File Edit View Search Terminal Help

```
root@kali Aurelien DUVAL :~#nmap -sV 192.168.1.110 -p 21
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:11 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00032s latency).
PORT      STATE    SERVICE VERSION
21/tcp    open     ftp      vsftpd 2.0.4
MAC Address: 00:0C:29:37:A3:6C (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.09 seconds
```

root@kali Aurelien DUVAL :~#

Videos
Trash
VMware Tools
+ Other Locations

"5_e.png" selected (102.5 kB)

g)

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap -O 192.168.1.110
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:14 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
631/tcp   open  ipp
MAC Address: 00:0C:29:37:A3:6C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds
root@kali Aurelien DUVAL :~#
```

h)

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap --script ftp-anon.nse 192.168.1.110 -p 21
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:18 EDT
Nmap scan report for 192.168.1.110
Host is up (0.00030s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x  7 1000      513   160 Mar 15  2007 download
|_ drwxrwxrwx  2 0         0     60 Feb 26  2007 incoming [NSE: writeable]
MAC Address: 00:0C:29:37:A3:6C (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
root@kali Aurelien DUVAL :~#
```

Videos
Trash
VMware Tools
+ Other Locations

"5_g.png" selected (105.5 kB)

j)

The screenshot shows a Kali Linux desktop environment. In the top right corner, there is a system tray with icons for battery, signal strength, and network. The main window is a terminal window titled 'Terminal' with the command 'root@kali Aurelien DUVAL :~#'. The terminal output shows the results of an Nmap scan for port 22 on 192.168.1.110. It identifies an open SSH service and notes that the server supports SSHv1. The MAC address is listed as 00:0C:29:37:A3:6C (VMware). The scan took 44.49 seconds. Below the terminal is a file browser window showing a directory structure with 'Pictures', 'Videos', 'Trash', 'VMware Tools', and 'Other Locations'.

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap -script sshv1.nse 192.168.1.110 -p 22
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:19 EDT
Nmap scan report for 192.168.1.110
Host is up (0.0003s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
| sshv1: Server supports SSHv1
MAC Address: 00:0C:29:37:A3:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 44.49 seconds
root@kali Aurelien DUVAL :~#
```

j) (1)

The screenshot shows a Kali Linux desktop environment with a terminal window titled 'Terminal' running a comprehensive Nmap scan (-v option) on 192.168.1.110. The output is very long and includes various NSE scripts like vuln, http-csrf, http-dombased-xss, http-fileupload-exploiter, http-frontpage-login, http-slowloris-check, and http-vuln-cve2012-0225. The scan identifies several open ports: 80/tcp (HTTP), 21/tcp (FTP), 22/tcp (SSH), and 631/tcp (CUPS). It also performs a SYN Stealth Scan and a Parallel DNS resolution. The NSE script vuln finds no vulnerabilities. The NSE script http-vuln-cve2012-0225 finds a Slowloris DOS attack vulnerability. The entire process takes 13.00 seconds.

```
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap -v -script vuln 192.168.1.110
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:38 EDT
NSE: Loaded 86 scripts for scanning
NSE: Script Pre-scanning.
Initiating NSE at 15:38
Completed NSE at 15:38, 0.00s elapsed
Initiating ARP Ping Scan at 15:38
Scanning 192.168.1.110 [1 port]
Completed ARP Ping Scan at 15:38, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:38
Completed Parallel DNS resolution of 1 host. at 15:38, 13.00s elapsed
Initiating SYN Stealth Scan at 15:38
Scanning 192.168.1.110 [1000 ports]
Discovered open port 80/tcp on 192.168.1.110
Discovered open port 21/tcp on 192.168.1.110
Discovered open port 22/tcp on 192.168.1.110
Discovered open port 631/tcp on 192.168.1.110
Completed SYN Stealth Scan at 15:38, 0.10s elapsed (1000 total ports)
NSE: Script scanning 192.168.1.110.
Initiating NSE at 15:38
Completed NSE at 15:43, 313.54s elapsed
Nmap scan report for 192.168.1.110
Host is up (0.0003s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
| sslv2-drown:
|_ http-open:
|_ http-vuln-cve2012-0225:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: ! TKEI Y VIII NFRAPI F
```

(2)

(3)

```
[root@kali ~]# nmap -sS 192.168.1.110 -p3  
[+] Starting Nmap 6.40 ( http://nmap.org ) at 2015-08-15 15:43 CEST  
[+] Scanning 1 host (1 port up)  
[!] Service detection disabled  
[!] Script scanning disabled (try --script=enable)  
[+] Nmap done: 1 IP address (1 host up) scanned in 327.31 seconds  
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.044KB)  
[root@kali ~]#
```

k) (1)

The screenshot shows the Zenmap interface with the target set to 192.168.1.110. The Nmap Output tab is selected, displaying the following scan results:

```
nmap -sS -p [20-440] -T4 -A -v 192.168.1.110
Nmap scan report for 192.168.1.110
Host is up (0.00074s latency).
Not shown: 271 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x  7 1000      513        160 Mar 15  2007 download
| drwxrwxrwx  2  0         0        60 Feb 26  2007 incoming [NSE: writeable]
22/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.2.4 ((Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
| http-server-header: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2
| http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:37:A3:6C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Uptime guess: 0.038 days (since Fri Oct 21 14:33:31 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=195 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix
```

Service Info: OS: Unix

TRACEROUTE

HOP	RTT	ADDRESS
1	0.74 ms	192.168.1.110

A terminal window is open in the background showing the command being run:

```
root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:21 EDT
root@kali Aurelien DUVAL :~#
```

(2)

The screenshot shows the Zenmap interface with the target set to 192.168.1.110. The Nmap Output tab is selected, displaying the following scan results:

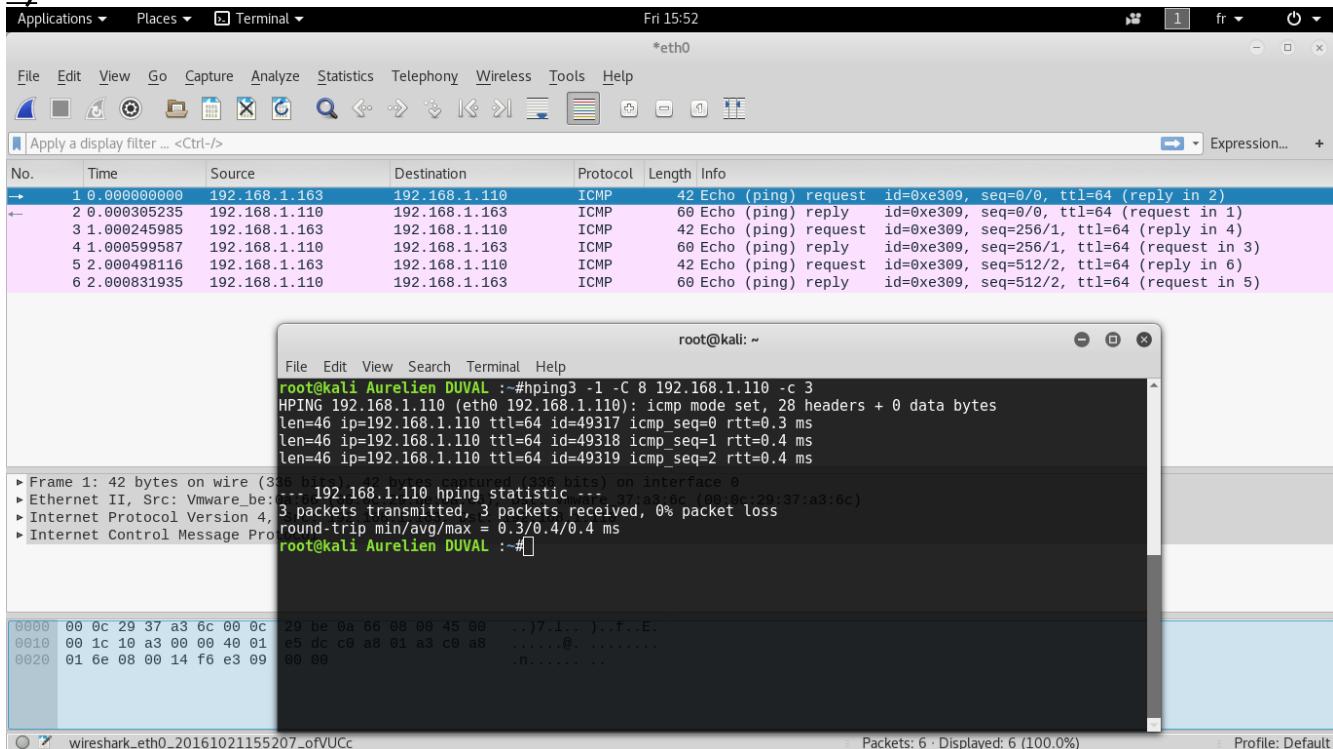
Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 2.0.4
22	tcp	open	tcpwrapped	
80	tcp	open	http	Apache httpd 2.2.4 ((Unix) mod_ssl/2.2.4 OpenSSL/0.9.8b DAV/2)

A terminal window is open in the background showing the command being run:

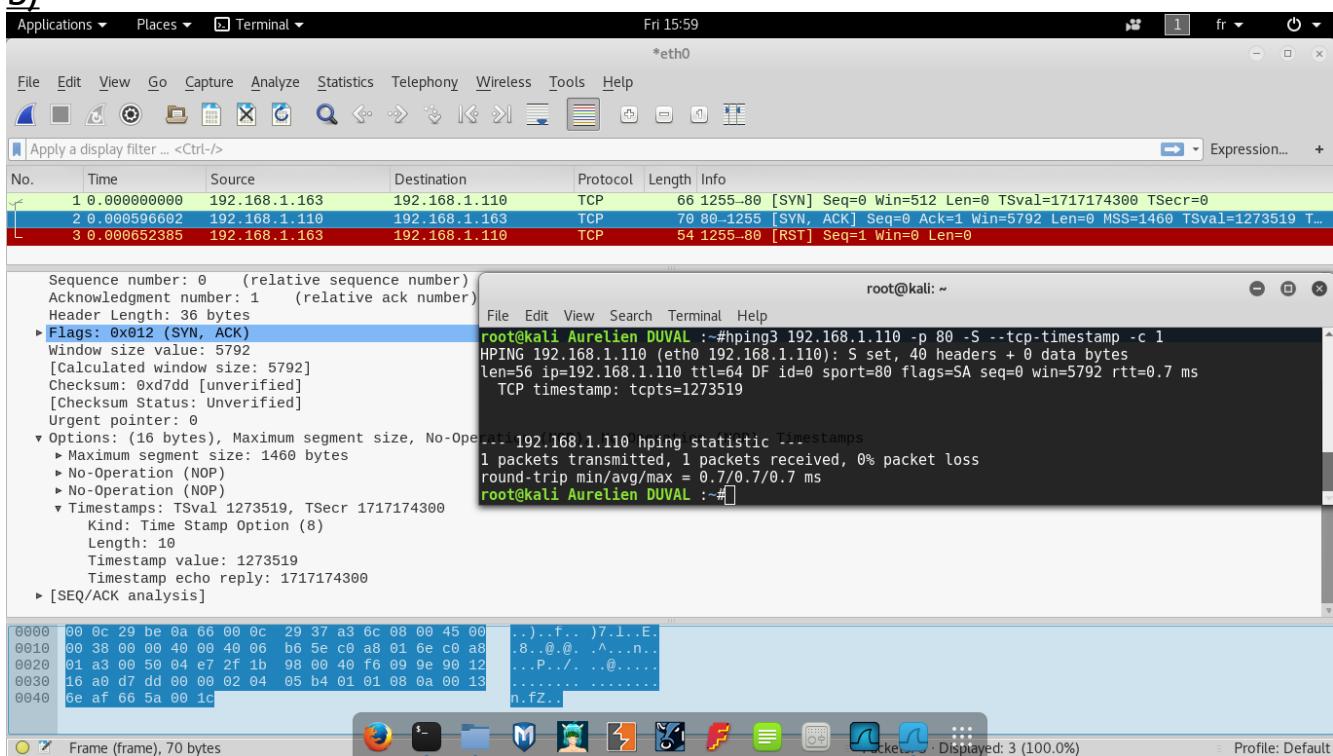
```
root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-21 15:21 EDT
root@kali Aurelien DUVAL :~#
```

Question 6:

a)



b)



c)

Applications ▾ Places ▾ Terminal ▾ Fri 16:07 *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.163	192.168.1.110	TCP	54	1535-80 [FIN, SYN] Seq=0 Win=512 Len=0
3	0.001406037	192.168.1.163	192.168.1.110	TCP	54	1535-80 [RST] Seq=1 Win=0 Len=0
2	0.001369327	192.168.1.110	192.168.1.163	TCP	60	80-1535 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460

File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~# hping3 -S -F -p 80 192.168.1.110 -c 1
HPING 192.168.1.110 (eth0 192.168.1.110): SF set, 40 headers + 0 data bytes
len=46 ip=192.168.1.110 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=1.4 ms
--- 192.168.1.110 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.4/1.4/1.4 ms
root@kali Aurelien DUVAL :~#

000. = Reserved: Not set
.... 0 = Nonce: Not set
.... 0.... = Congestion Window Reduced (CWR): Not set
.... 0.... = ECN-Echo: Not set
.... 0.... = Urgent: Not set
.... 0.... = Acknowledgment: Not set
.... 0.... = Push: Not set
.... 0.... = Reset: Not set
► 0.... 1 = Syn: Set
► 0.... 1 = Fin: Set
[TCP Flags:SF]
Window size value: 512
[Calculated window size: 512]
Checksum: 0xdaid [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

0000 00 0c 29 37 a3 6c 00 0c 29 be 0a 66 08 00 45 00 ..)7.1...)..f..E.
0010 00 28 2c 30 00 00 40 06 ca 3e c0 a8 01 a3 c0 a8 .(.,0..@. .>....
0020 01 6e 05 ff 00 50 13 20 7a 84 14 49 a7 25 50 03 .n...P. z..I.%P.
0030 02 00 da 1d 00 00

Frame (frame), 54 bytes

d)

Applications ▾ Places ▾ Terminal ▾ Fri 16:13 *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.254	192.168.1.110	UDP	42	2946-53 Len=0
2	0.002763525	Vmware_37:a3:6c	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.110
3	1.002850074	Vmware_37:a3:6c	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.110
4	2.002866358	Vmware_37:a3:6c	Broadcast	ARP	60	Who has 192.168.1.254? Tell 192.168.1.110

File Edit View Search Terminal Help
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali Aurelien DUVAL :~# hping3 -2 -p 53 192.168.1.110 -a 192.168.1.254 -c 1
HPING 192.168.1.110 (eth0 192.168.1.110): udp mode set, 28 headers + 0 data bytes
--- 192.168.1.110 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
► Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
► Ethernet II, Src: Vmware_be:0a:66 (00:0c:29:be:0a:66), Dst: Vmware_37:a3:6c (00:0c:29:be:0a:6c)
► Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.110
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 28
Identification: 0x98cf (39119)
Flags: 0x00
0.... = Reserved bit: Not set
0.... = Don't fragment: Not set
0000 00 0c 29 37 a3 6c 00 0c 29 be 0a 66 08 00 45 00 ..)7.1...)..f..E.
0010 00 1c 98 cf 00 00 40 11 5d 45 c0 a8 01 fe c0 a8@.]E.....
0020 01 6e 0b 82 00 35 00 08 6f 6a .n...5.. oj

wireshark_eth0_20161021161253.WhQ6i6

Question 7 :

a)

```

File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nc -vzn 192.168.1.110 10-100
(UNKNOWN) [192.168.1.110] 80 (http) open [use twice to be more verbose]
(UNKNOWN) [192.168.1.110] 22 (ssh) open for connects and final net reads
(UNKNOWN) [192.168.1.110] 21 (ftp) openLF as line-ending
root@kali Aurelien DUVAL :~# nc -# zero-I/O mode [used for scanning]
port numbers can be individual or ranges; lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-\data').
root@kali:~# nc -h |grep TCP
[v1.10-4]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [-options] [hostname] [port]
options:
  -c shell commands      as '-e'; use /bin/sh to exec [dangerous!]
  -e filename            program to exec after connect [dangerous!]
  -b                   allow broadcasts
  -g gateway             source-routing hop point[s], up to 8
  -G num                source-routing pointer: 4, 8, 12, ...
  -T traffic             this cruft
  -i secs               delay interval for lines sent, ports scanned
  -V VMware tools        set keepalive option on socket
  -l                   listen mode, for inbound connects
  -n                   numeric-only IP addresses, no DNS
  -f Other-o file        hex dump of traffic
  -p port               local port number
  -r                   randomize local and remote ports
  -q secs               quit after EOF on stdin and delay of secs
  -s addr              local source address
  -T tos               set Type Of Service
  -t                   answer TELNET negotiation
  -U                   UDP mode
  -v                   verbose [use twice to be more verbose]
  -w secs               timeout for connects and final net reads
  -C                  Send CRLF as line-ending
  -z                  zero-I/O mode [used for scanning]
port numbers can be individual or ranges; lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-\data').
root@kali:~#

```

b) (1)

```

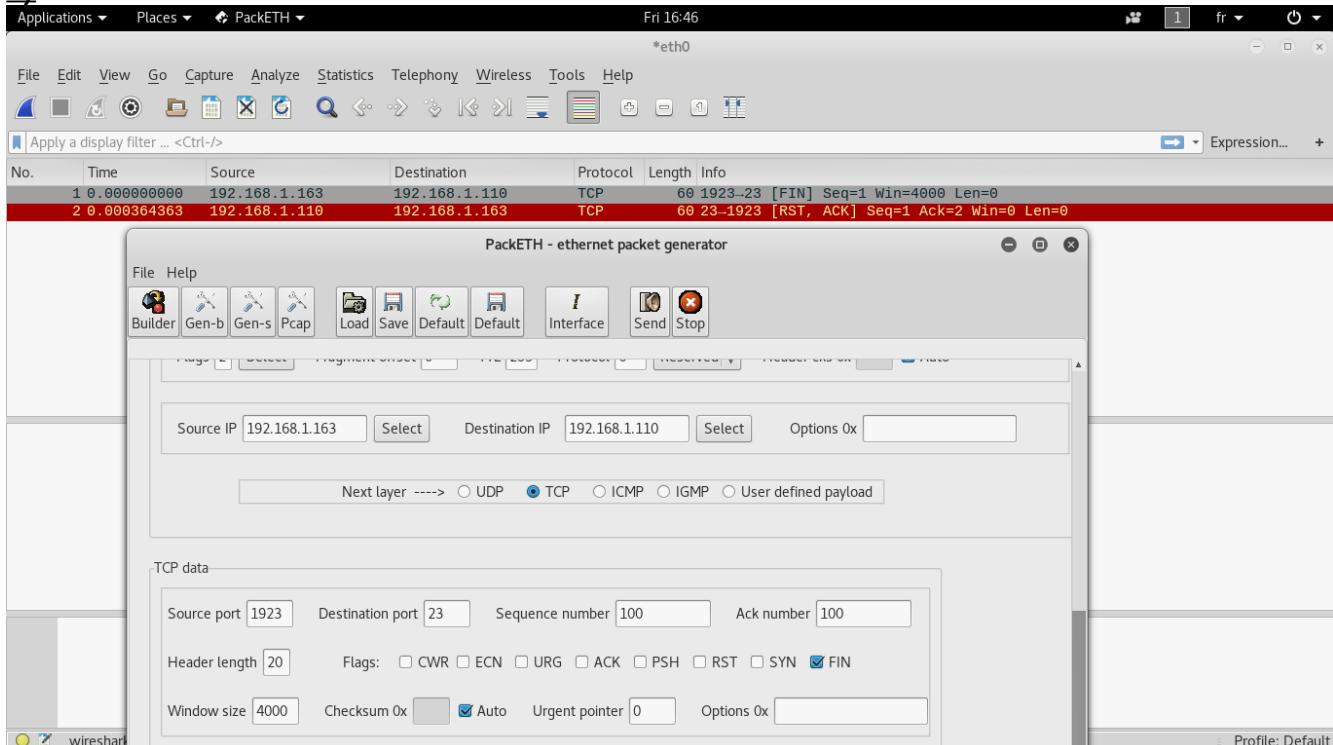
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nc -vznu 192.168.1.110 1-1054 core verbose
(UNKNOWN) [192.168.1.110] 1048 (?) open for connects and final net reads
(UNKNOWN) [192.168.1.110] 1047 (?) openLF as line-ending
(UNKNOWN) [192.168.1.110] 1046 (?) openO mode [used for scanning]
(UNKNOWN) [192.168.1.110] 1045 (?) opens: lo-hi [inclusive]; 1-1054
(UNKNOWN) [192.168.1.110] 1044 (?) open escaped (e.g. 'ftp\-\data').
(UNKNOWN) [192.168.1.110] 1043 (?) open
(UNKNOWN) [192.168.1.110] 1042 (?) open
(UNKNOWN) [192.168.1.110] 1041 (?) openostname port[s] [ports] ...
(UNKNOWN) [192.168.1.110] 1040 (?) open-options] [hostname] [port]
(UNKNOWN) [192.168.1.110] 1039 (?) open
(UNKNOWN) [192.168.1.110] 1038 (?) open; use /bin/sh to exec [dangerous!]
(UNKNOWN) [192.168.1.110] 1037 (?) open to exec after connect [dangerous!]
(UNKNOWN) [192.168.1.110] 1036 (?) openbroadcasts
(UNKNOWN) [192.168.1.110] 1035 (?) openrouting hop point[s], up to 8
(UNKNOWN) [192.168.1.110] 1034 (?) openrouting pointer: 4, 8, 12, ...
(UNKNOWN) [192.168.1.110] 1033 (?) openuft
(UNKNOWN) [192.168.1.110] 1032 (?) openinterval for lines sent, ports scanned
(UNKNOWN) [192.168.1.110] 1031 (?) openpalive option on socket
(UNKNOWN) [192.168.1.110] 1030 (?) openmode, for inbound connects
(UNKNOWN) [192.168.1.110] 1029 (?) open-only IP addresses, no DNS
(UNKNOWN) [192.168.1.110] 1028 (?) openp of traffic
(UNKNOWN) [192.168.1.110] 1027 (?) openort number
(UNKNOWN) [192.168.1.110] 1026 (?) openze local and remote ports
(UNKNOWN) [192.168.1.110] 1025 (?) openter EOF on stdin and delay of secs
(UNKNOWN) [192.168.1.110] 1024 (?) openource address
(UNKNOWN) [192.168.1.110] 1023 (?) opene Of Service
(UNKNOWN) [192.168.1.110] 1022 (?) openTELNET negotiation
(UNKNOWN) [192.168.1.110] 1021 (?) opene
(UNKNOWN) [192.168.1.110] 1020 (?) open [use twice to be more verbose]
(UNKNOWN) [192.168.1.110] 1019 (?) open for connects and final net reads
(UNKNOWN) [192.168.1.110] 1018 (?) openLF as line-ending
(UNKNOWN) [192.168.1.110] 1017 (?) openO mode [used for scanning]
(UNKNOWN) [192.168.1.110] 1016 (?) opens: lo-hi [inclusive];
(UNKNOWN) [192.168.1.110] 1015 (?) open escaped (e.g. 'ftp\-\data').
(UNKNOWN) [192.168.1.110] 1014 (?) open
(UNKNOWN) [192.168.1.110] 1013 (?) open

```

(2)

```
Fri 16:24
root@kali: ~
File Edit View Search Terminal Help
(UNKNOWN) [192.168.1.110] 36 (?) openode
(UNKNOWN) [192.168.1.110] 35 (?) opense [use twice to be more verbose]
(UNKNOWN) [192.168.1.110] 34 (?) openut for connects and final net reads
(UNKNOWN) [192.168.1.110] 33 (?) openCRLF as line-ending
(UNKNOWN) [192.168.1.110] 32 (?) openI/O mode [used for scanning]
(UNKNOWN) [192.168.1.110] 31 (?) openges; lo-hi [inclusive];
(UNKNOWN) [192.168.1.110] 30 (?) opensh escaped (e.g. 'ftp\-\data').
(UNKNOWN) [192.168.1.110] 29 (?) open
(UNKNOWN) [192.168.1.110] 28 (?) open
(UNKNOWN) [192.168.1.110] 27 (?) open hostname port[s] [ports] ...
(UNKNOWN) [192.168.1.110] 26 (?) open [-options] [hostname] [port]
(UNKNOWN) [192.168.1.110] 25 (?) open
(UNKNOWN) [192.168.1.110] 24 (?) opene'; use /bin/sh to exec [dangerous!]
(UNKNOWN) [192.168.1.110] 23 (?) openam to exec after connect [dangerous!]
(UNKNOWN) [192.168.1.110] 22 (ssh) openbroadcasts
(UNKNOWN) [192.168.1.110] 21 (fsp) openrouting hop point[s], up to 8
(UNKNOWN) [192.168.1.110] 20 (?) open routing pointer: 4, 8, 12, ...
(UNKNOWN) [192.168.1.110] 19 (chargen) open
(UNKNOWN) [192.168.1.110] 18 (msp) openinterval for lines sent, ports scanned
(UNKNOWN) [192.168.1.110] 17 (?) openepalive option on socket
(UNKNOWN) [192.168.1.110] 16 (?) openm mode, for inbound connects
(UNKNOWN) [192.168.1.110] 15 (?) openic-only IP addresses, no DNS
(UNKNOWN) [192.168.1.110] 14 (?) openump of traffic
(UNKNOWN) [192.168.1.110] 13 (daytime) openumber
(UNKNOWN) [192.168.1.110] 12 (?) openimize local and remote ports
(UNKNOWN) [192.168.1.110] 11 (?) openafter EOD on stdin and delay of secs
(UNKNOWN) [192.168.1.110] 10 (?) open source address
(UNKNOWN) [192.168.1.110] 9 (discard) openf Service
(UNKNOWN) [192.168.1.110] 8 (?) open telnet negotiation
(UNKNOWN) [192.168.1.110] 7 (echo) opene
(UNKNOWN) [192.168.1.110] 6 (?) openose [use twice to be more verbose]
(UNKNOWN) [192.168.1.110] 5 (?) openput for connects and final net reads
(UNKNOWN) [192.168.1.110] 4 (?) open CRLF as line-ending
(UNKNOWN) [192.168.1.110] 3 (?) open I/O mode [used for scanning]
(UNKNOWN) [192.168.1.110] 2 (?) openges; lo-hi [inclusive];
(UNKNOWN) [192.168.1.110] 1 (?) openash escaped (e.g. 'ftp\-\data').
root@kali Aurelien DUVAL :~#
```

c)



Question 8 :

b) (1)

The screenshot shows two terminal windows side-by-side. Both are running on a Kali Linux system (root shell).

Terminal 1 (Left):

```
root@kali Aurelien DUVAL :~/Desktop/dnmap# cat commandes.txt
nmap -sS --top-ports 10 192.168.1.110
root@kali Aurelien DUVAL :~/Desktop/dnmap# dnmap#dnmap_server -f commandes.txt
+-----+
| dnmap_server Version 0.6|nmap_results# ls
| This program is free software; you can redistribute it and/or modify |
| it under the terms of the GNU General Public License as published by |
| the Free Software Foundation; either version 2 of the License, or |
| (at your option) any later version.|
| Last is up (0.0012s latency).|
| Author: Garcia Sebastian, eldraco@gmail.com |
| www.mateslab.com.ar |
+-----+
23/tcp closed telnet
=| MET:0:00:00.000412 | Amount of Online clients: 0 |=
+ Client ID connected: 192.168.1.163:44122 (Anonymous)
=| MET:0:00:05.000446 | Amount of Online clients: 1 |=
Clients connected toios-ssn
-----+
https
Alias      #Commands  Last Time Seen (time ago)    UpTime   V
ersion  IsRoot  RunCmdXMin  AvrCmdXMin  Status
Anonymous  0        Oct 21 16:59:40 ( 0' 1")    0h 0m  0
.6       True     0.0        0.0        Online
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
=| MET:0:00:10.004772 | Amount of Online clients: 1 |=
Clients connected p/dnmap/nmap_results#
```

Terminal 2 (Right):

```
root@kali Aurelien DUVAL :~#dnmap_client -s 192.168.1.163
+-----+
| dnmap Client Version 0.6|
| This program is free software; you can redistribute it and/or modify |
| it under the terms of the GNU General Public License as published by |
| the Free Software Foundation; either version 2 of the License, or |
| (at your option) any later version.|
| (nmap.org ) at 2016-10-21 16:57 EDT|
| Author: Garcia Sebastian, eldraco@gmail.com |
| www.mateslab.com.ar |
+-----+
Client Started...
Nmap output files stored in 'nmap_output' directory...
Starting connection...
Client connected successfully...
Waiting for more commands...
^CConnection lost. Reason: Connection to the other side was lost in a non-clean fashion: Connection lost.
Trying to reconnect in 10 secs. Please wait...
root@kali Aurelien DUVAL :~#
```

(2)

The screenshot shows two terminal windows side-by-side. Both are running on a Kali Linux system (root shell).

Terminal 1 (Left):

```
root@kali Aurelien DUVAL :~/Desktop/dnmap/nmap_results# cd ~
root@kali Aurelien DUVAL :~#cd Desktop/dnmap/nmap_results/
root@kali Aurelien DUVAL :~/Desktop/dnmap/nmap_results#ls commandes.txt
87824535.nmap
root@kali Aurelien DUVAL :~/Desktop/dnmap/nmap_results#cat 87824535.nmap
Client ID:192.168.1.163:44118:Alias:AnonymousStarting Nmap 7.25BETA1f ( https://nmap.org ) at 2016-10-21 16:57 EDT: version 2 of the License, or
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).; either version 2 of the License, or
PORT STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
23/tcp closed telnet
25/tcp - closed smtp
80/tcp open  http
110/tcp closed pop3  | Amount of Online clients: 0 |=
139/tcp closed netbios-ssn|192.168.1.163:44122 (Anonymous)
443/tcp closed https | Amount of Online clients: 1 |=
445/tcp closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 00:0C:29:37:A3:6C (VMware)seen (time ago)    UpTime   V
ersion  IsRoot  RunCmdXMin  AvrCmdXMin  Status
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
.6       True     0.0        0.0        Online
root@kali Aurelien DUVAL :~/Desktop/dnmap/nmap_results#
```

Terminal 2 (Right):

```
root@kali Aurelien DUVAL :~#dnmap_client -s 192.168.1.163
+-----+
| dnmap Client Version 0.6|
| This program is free software; you can redistribute it and/or modify |
| it under the terms of the GNU General Public License as published by |
| the Free Software Foundation; either version 2 of the License, or |
| (at your option) any later version.|
| (nmap.org ) at 2016-10-21 16:57 EDT|
| Author: Garcia Sebastian, eldraco@gmail.com |
| www.mateslab.com.ar |
+-----+
Client Started...
Nmap output files stored in 'nmap_output' directory...
Starting connection...
Client connected successfully...
Waiting for more commands...
^CConnection lost. Reason: Connection to the other side was lost in a non-clean fashion: Connection lost.
Trying to reconnect in 10 secs. Please wait...
root@kali Aurelien DUVAL :~#
```

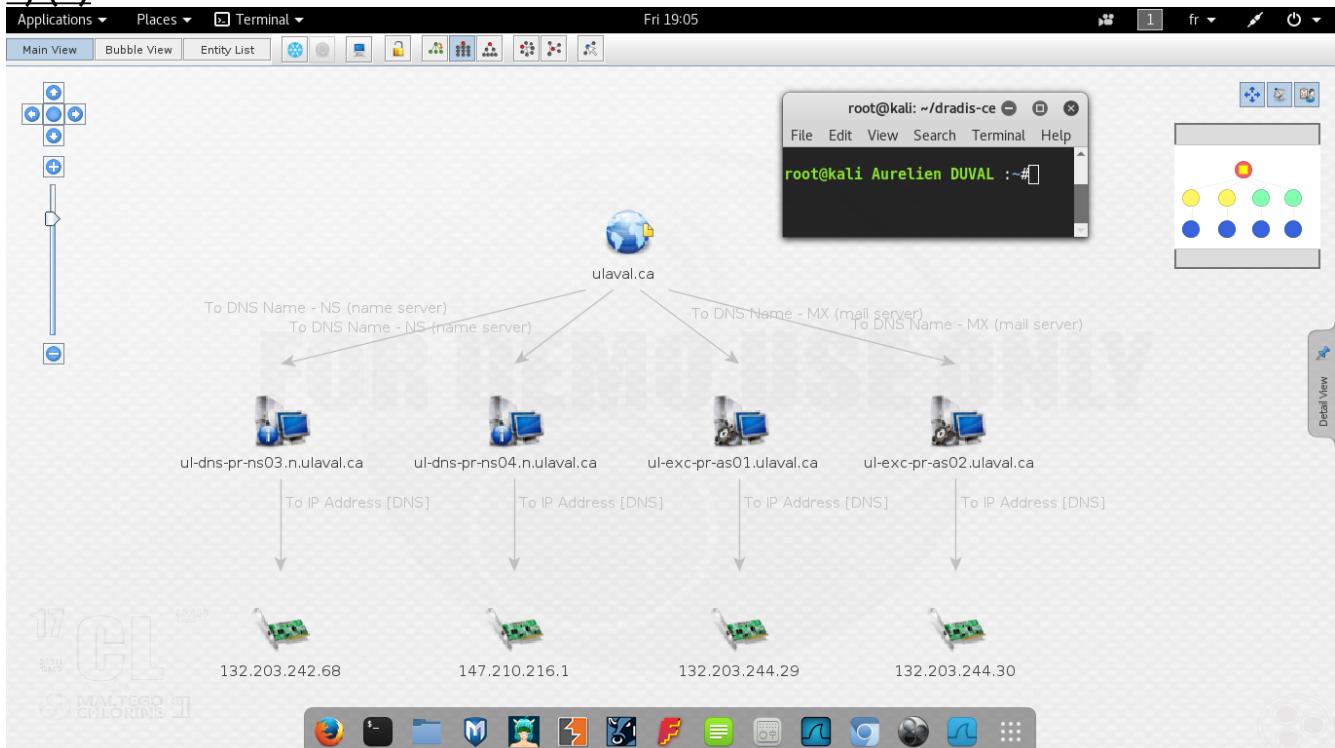
Question 9 :

a)

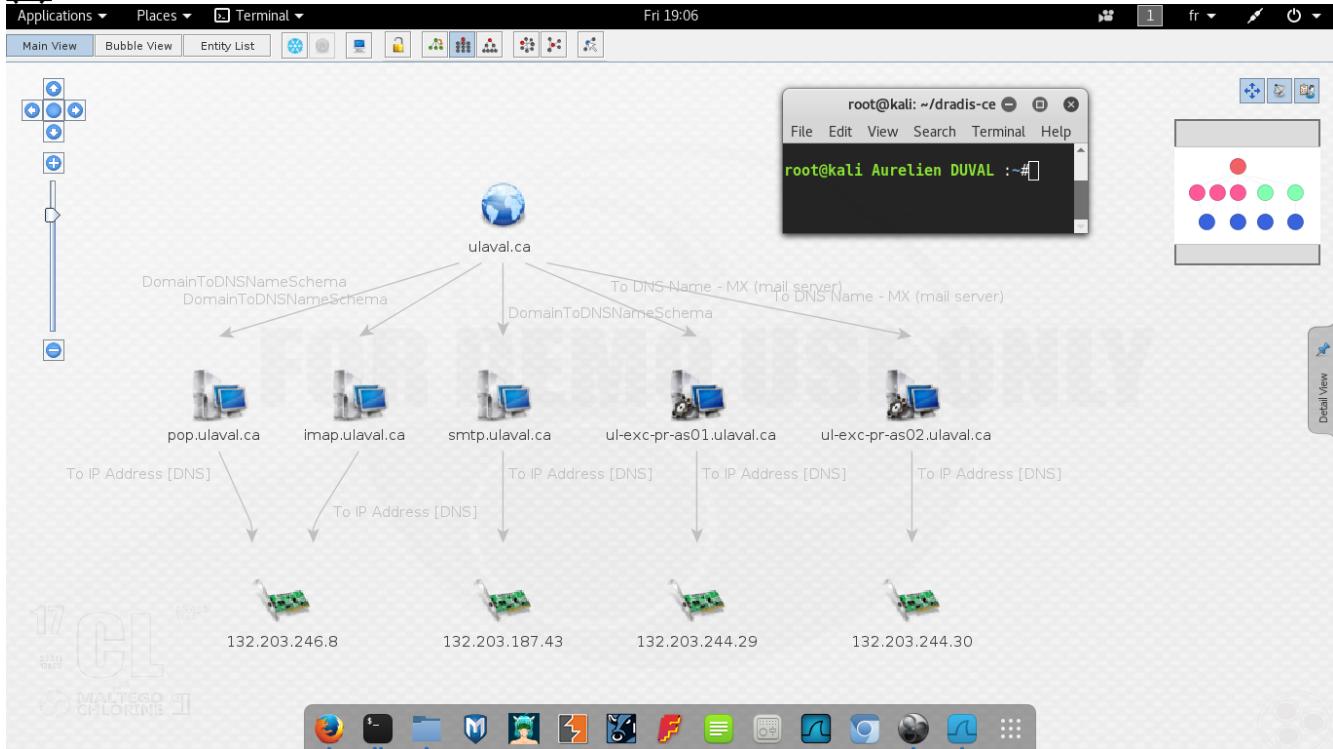
The screenshot shows the Dradis CE interface. On the left, there's a sidebar with 'Nodes' expanded, showing 'M110' and '192.168.1.110'. The main panel displays 'Host properties' for '192.168.1.110'. Under 'Notes', it lists: 21/tcp is open (syn-ack), 22/tcp is open (syn-ack), 631/tcp is open (syn-ack), 80/tcp is open (syn-ack), and Nmap Info: 192.168.1.110. Under 'Evidence', it says '(nothing yet)'. Under 'Attachments', there's a 'Drop zone' with a file icon. A toolbar at the bottom has icons for file operations like upload, download, and move. On the right, a terminal window shows the root prompt: `root@kali: ~#`.

Question 11 :

a) (1)



(2)

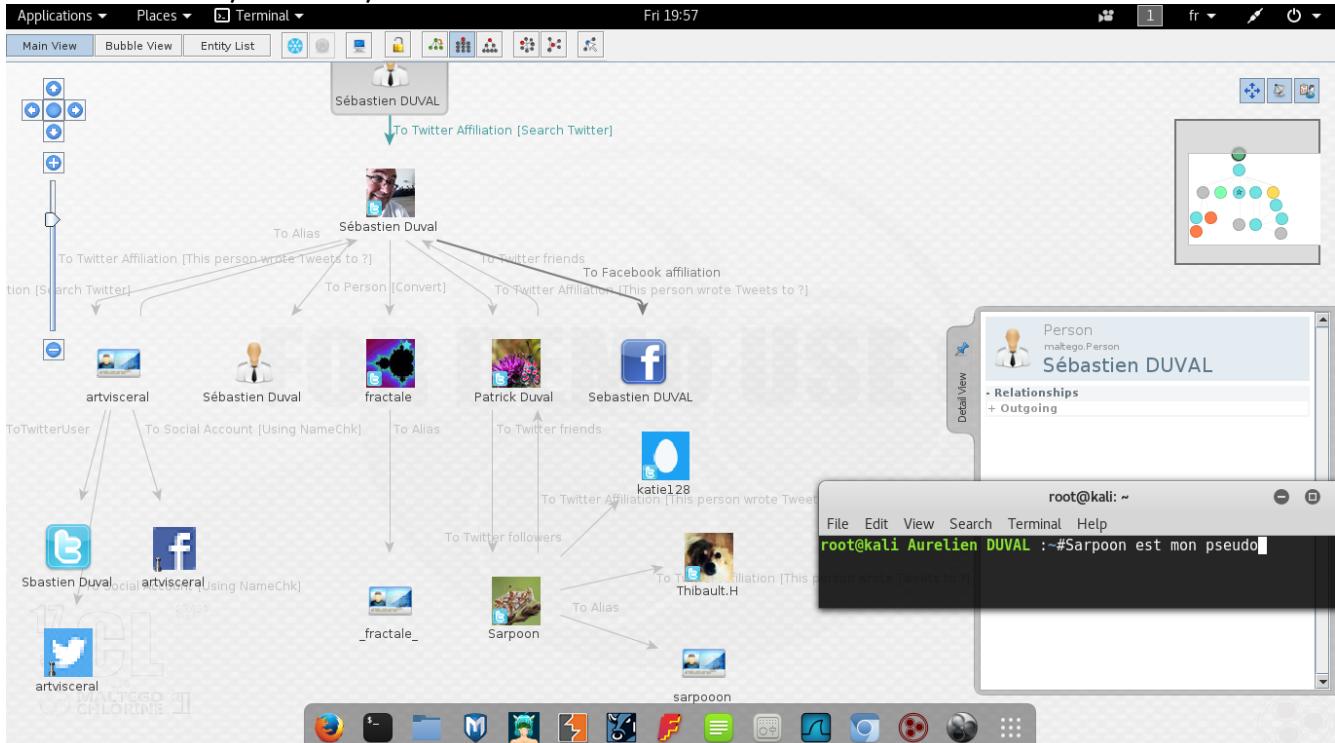


(3)

The screenshot shows the Maltego Kali Linux interface. At the top, there's a toolbar with Applications, Places, and Maltego Kali Linux. Below the toolbar is a menu bar with File, Edit, View, Search, Terminal, and Help. A terminal window is open with the command `root@kali: ~` and the user `Aurelien DUVAL`.

The main area is a table titled "Nodes" with columns: Nodes, Type, Value, Weight, Incoming, Outgoing, and Bookmark. The table lists numerous IPv4 addresses, all categorized as "IPv4 Address". The "Value" column contains IP addresses such as `132.203.227.11`, `132.203.57.253`, `132.203.250.32`, etc. The "Weight" column is mostly set to 100. The "Incoming" and "Outgoing" columns are mostly 0, except for some entries like `132.203.14.74` which has an incoming weight of 2 and an outgoing weight of 0.

b) Je n'ai pas trouvé d'information sur moi directement mais en partant de mon frère Sébastien j'ai pu retrouver mon pseudo : sarpoon, ainsi que plusieurs membres de ma famille : Patrick, Thibault, Cathie ..



Question 12 :

Category	Percentage	Count
Usernames	35%	6
Software	24%	4
Emails	0%	0
Paths/Servers	41%	7

User names found:

- Andres Andreu
- d
- Abhishek Kumar
- Jeff Williams
- 7

Software versions found:

- Microsoft Office Word
- Microsoft Word 11.1
- Microsoft Word 9.0
- Microsoft PowerPoint

```

root@kali: ~
root@kali Aurelien DUVAL :~/Desktop/metagoofil#metagoofil -d owasp.org -t pdf,doc,ppt -l 200 -n 5 -o /root/Desktop/metagoofil/ -f /root/Desktop/metagoofil/result.htm
[*] Metagoofil Ver 2.2
[*] Christian Martorella
[*] Edge-Security.com
[*] cmartorella at edge-security.com
[-] Starting online search...
[-] Searching for pdf files, with a limit of 200
    Searching 100 results...
    Searching 200 results...
Results: 104 files found
Starting to download 5 of them:
-----
[1/5] /setprefs?uggon=2
    [x] Error downloading /setprefs?uggon=2
[2/5] /setprefs?safeui=on
    [x] Error downloading /setprefs?safeui=on
[3/5] https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.pdf
    [x] Error in the parsing process
[4/5] https://www.owasp.org/index.php/File:OWASP_Minneapolis_20080908_Jeremiah_Grossman.pdf
    [x] Error in the parsing process
[5/5] https://www.owasp.org/index.php/File:DenimGroup_AJAXSecurityHereWeGoAgain_Content_20060829.pdf
    [x] Error in the parsing process

```