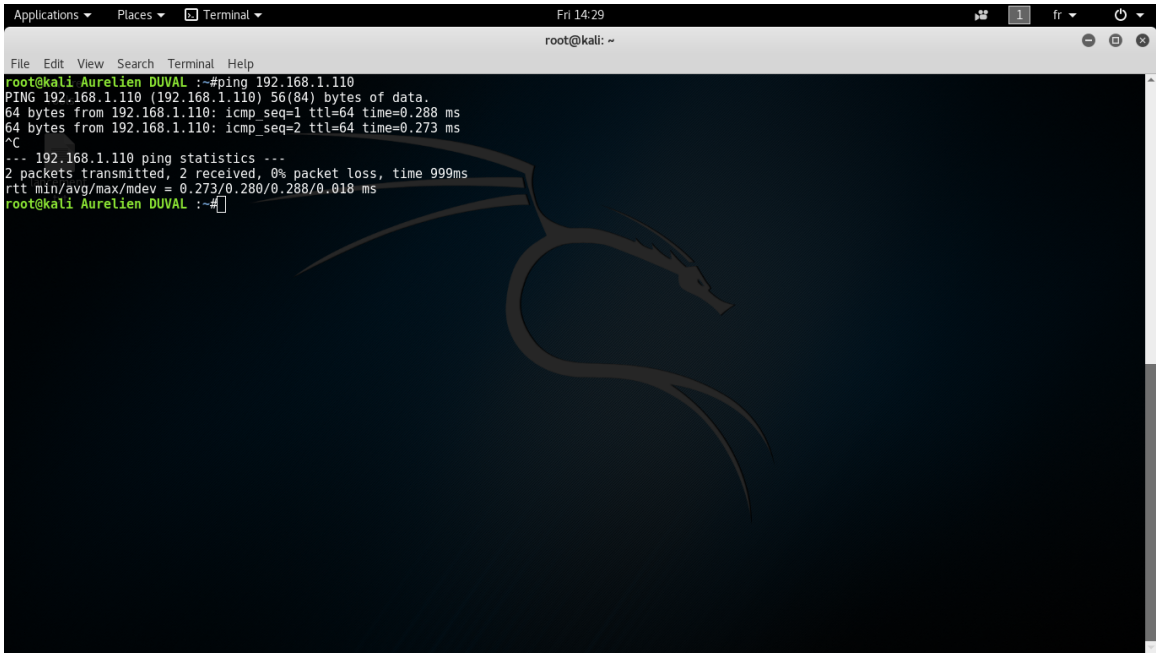
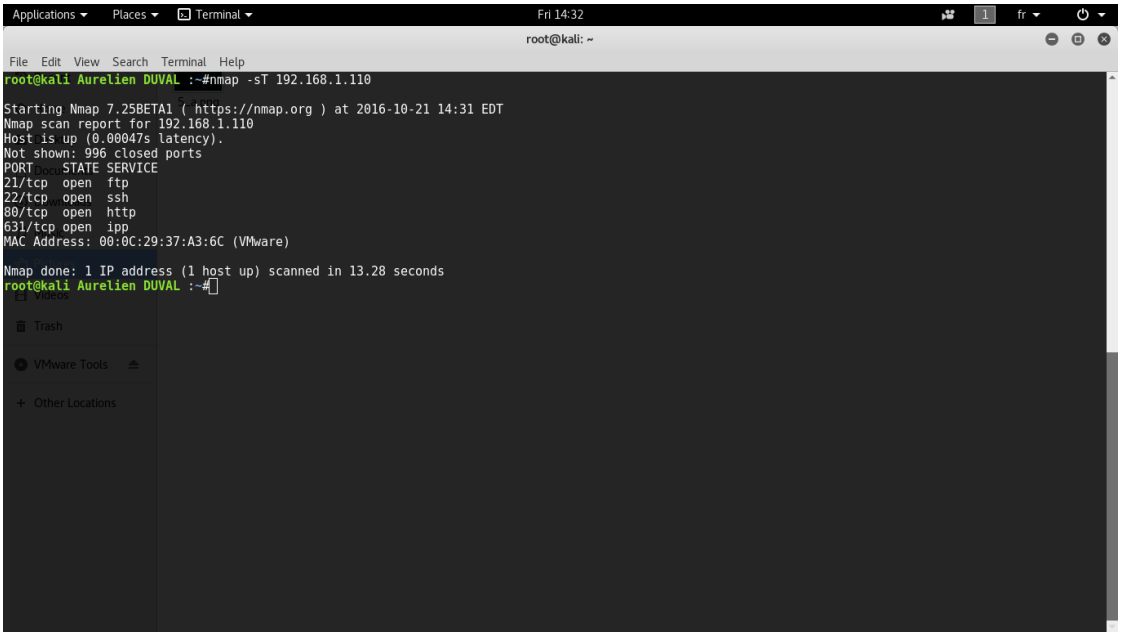
DUVAL Aurélien
NI : 111163937
ip : 192.168.1.163

TP 2 : Scan et footprinting

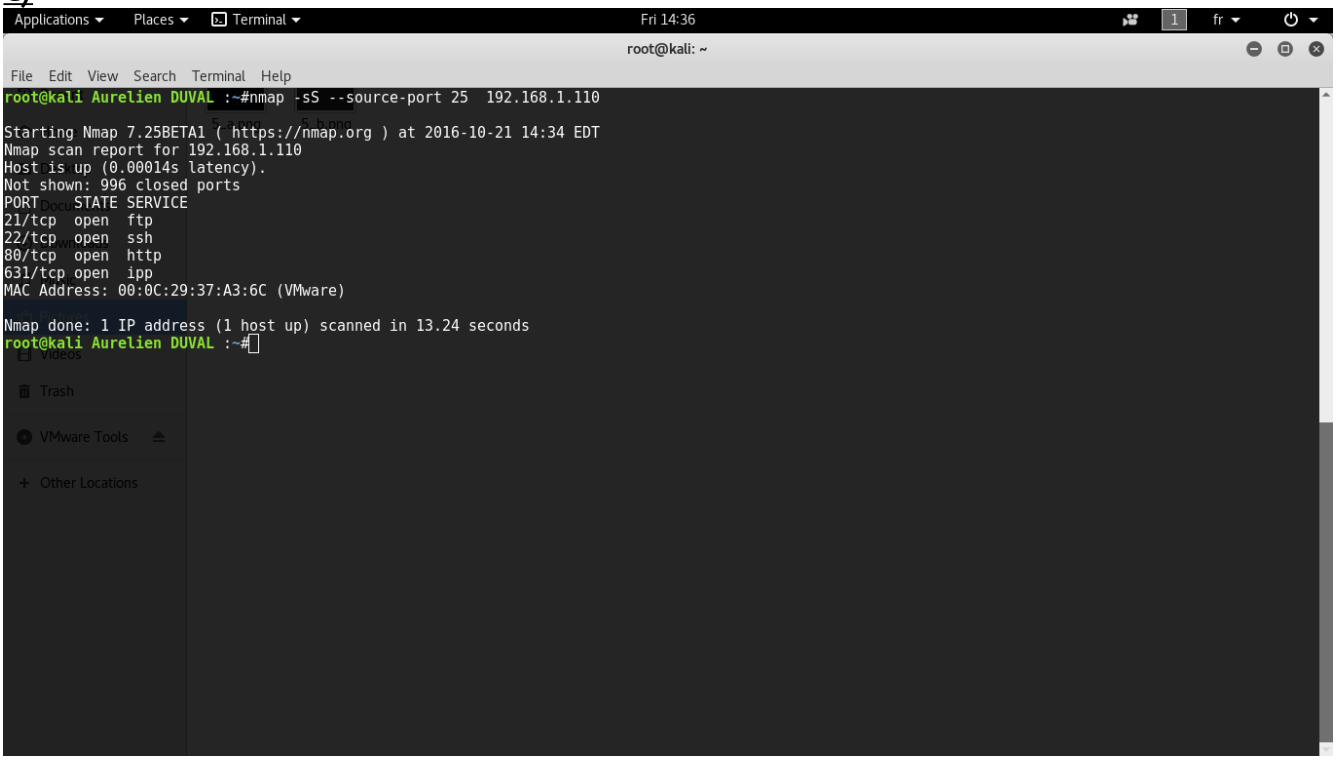
Question 5 : a)



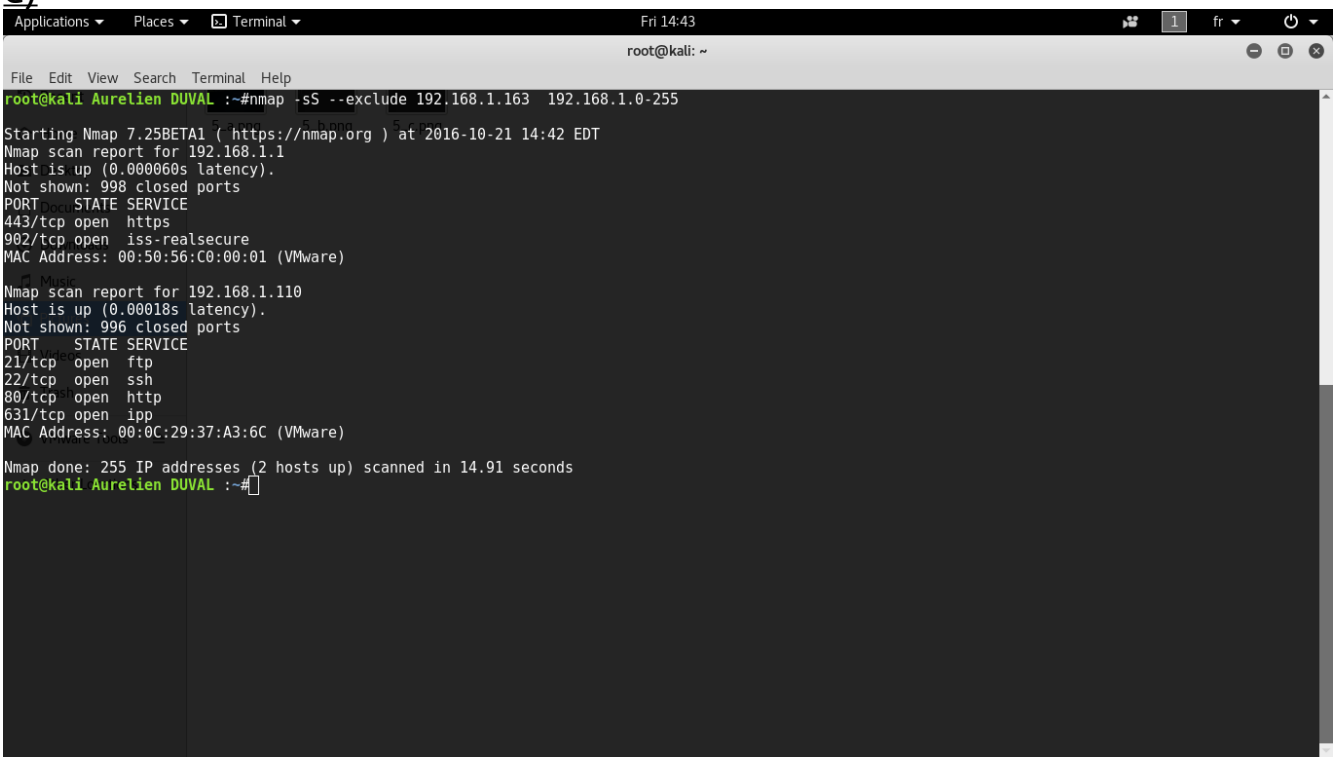
b)



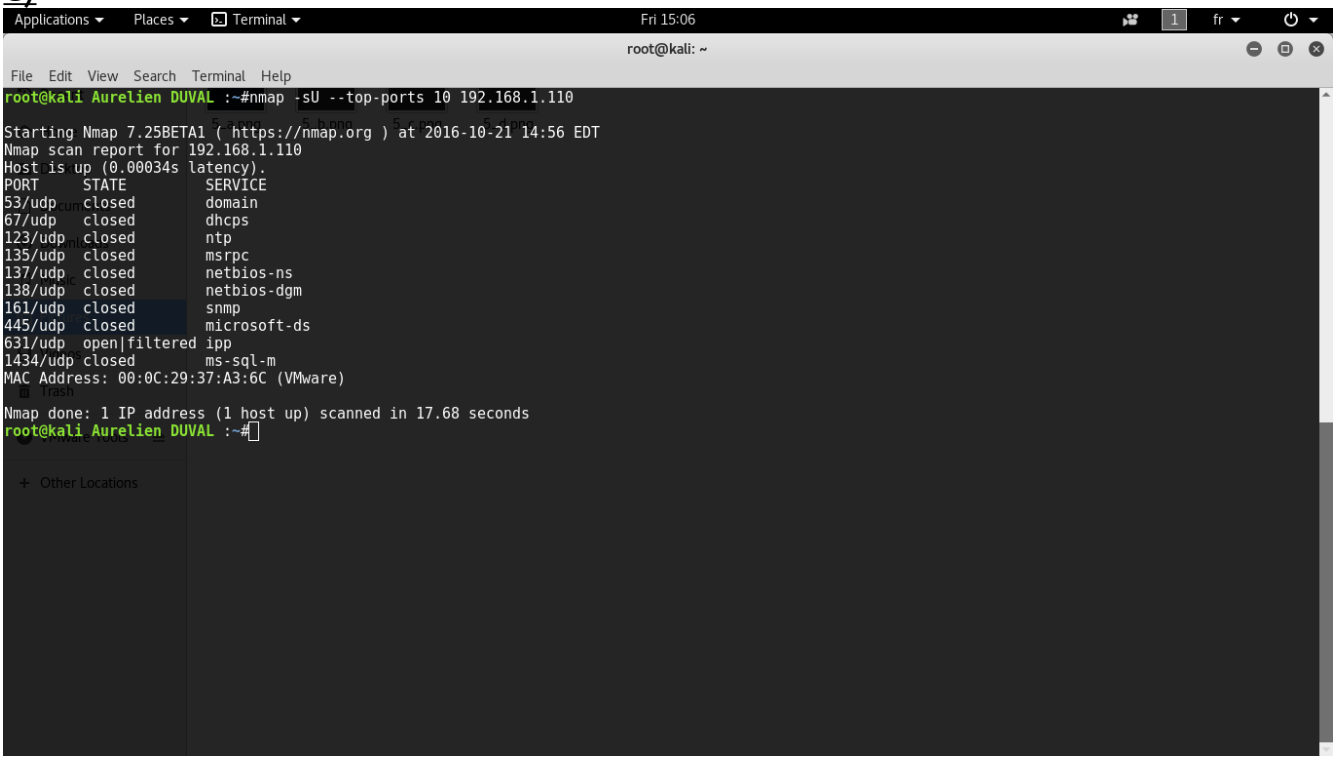
c)


Applications
Places
Terminal
Fri 14:36
fr
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 :~#
Trash
VMware Tools
Other Locations

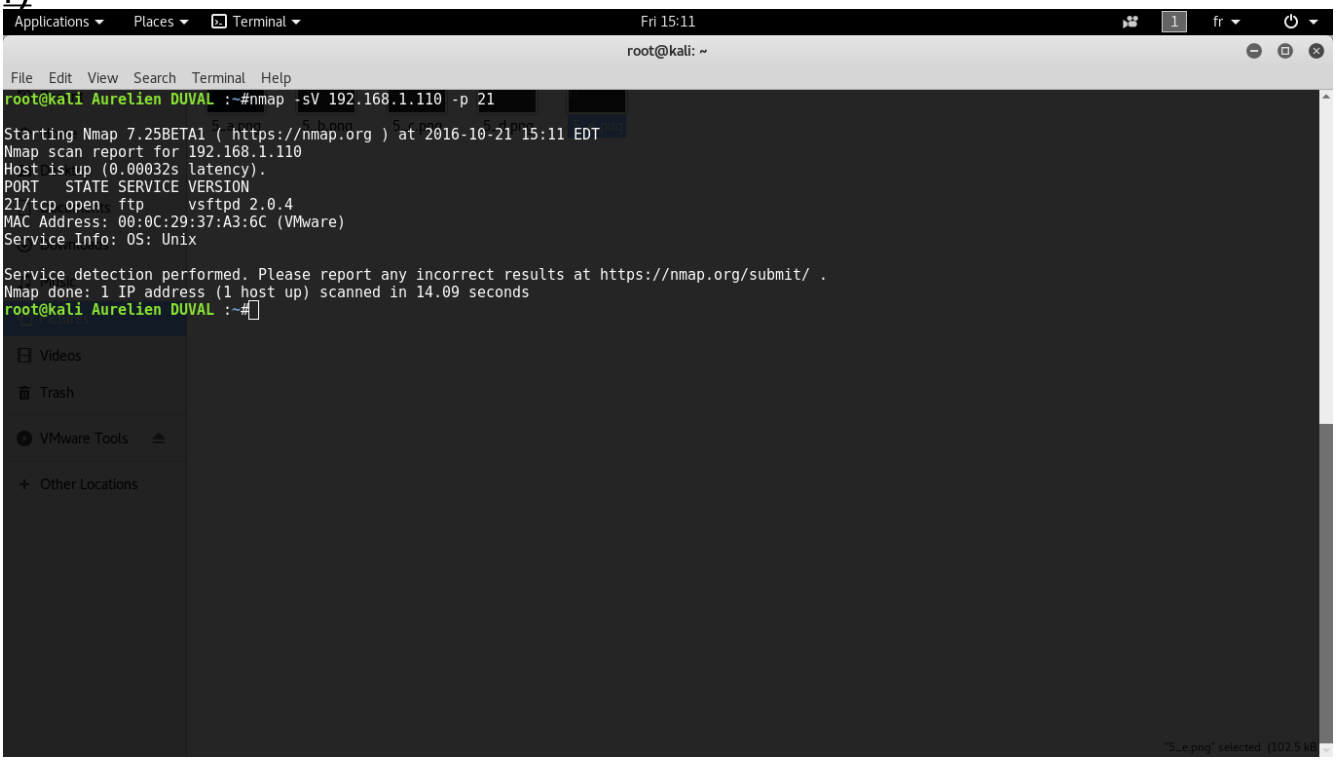
d)


Applications
Places
Terminal
Fri 14:43
fr
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 :~#

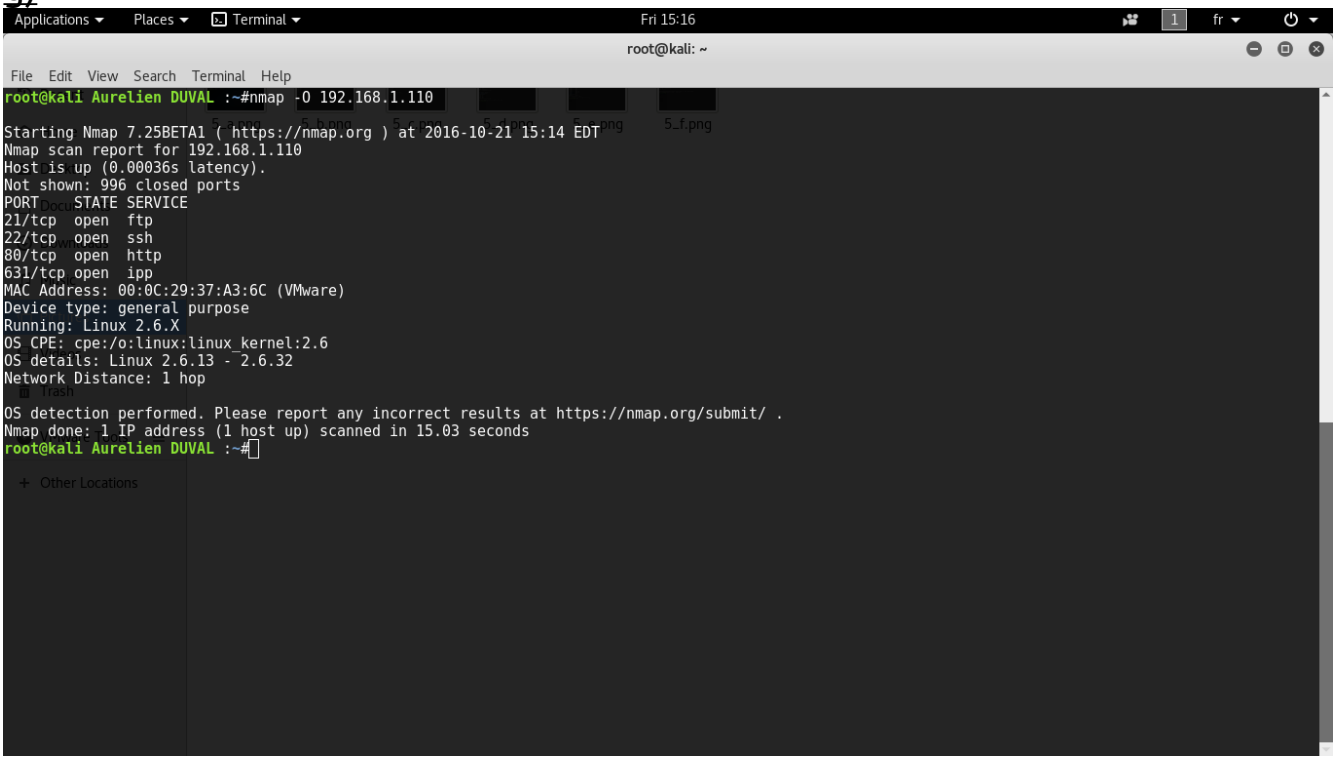
e)


Applications
Places
Terminal
Fri 15:06
fr
root@kali: ~
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

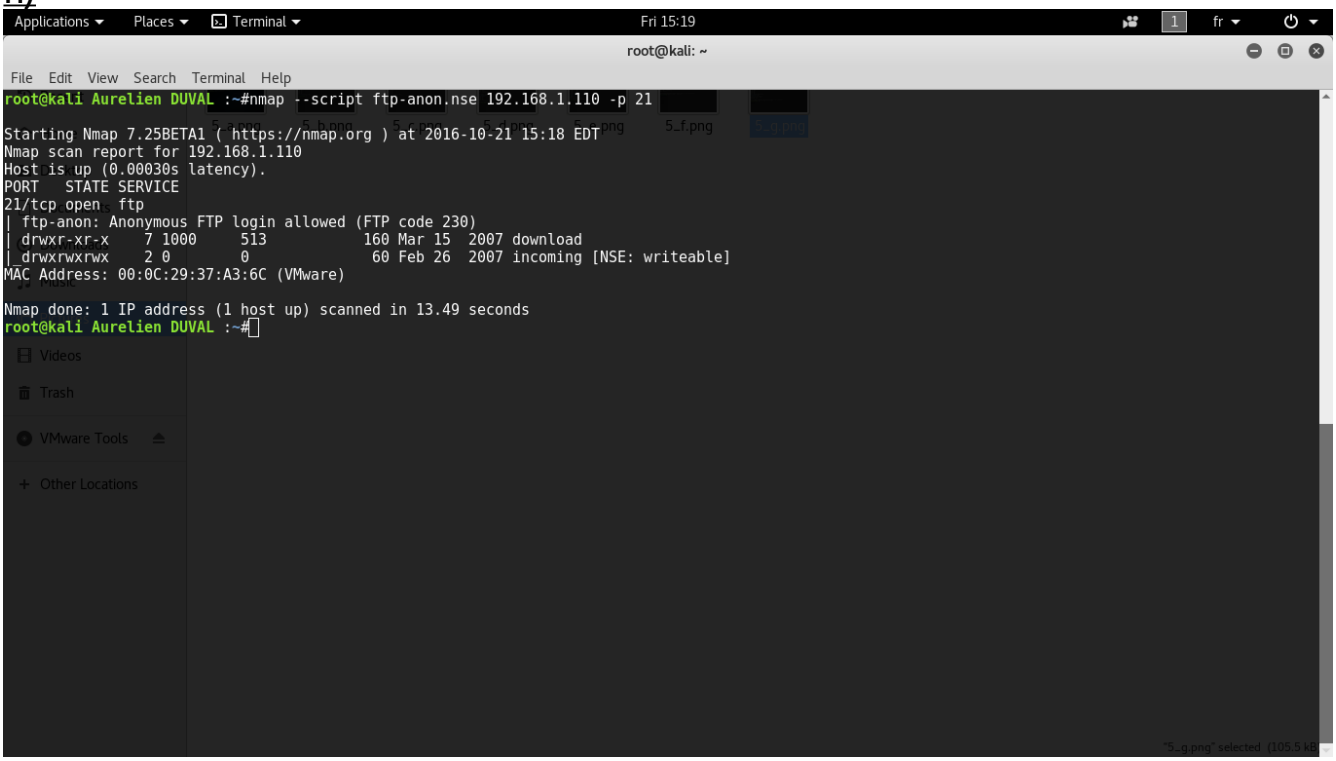
f)


Applications
Places
Terminal
Fri 15:11
fr
root@kali: ~
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

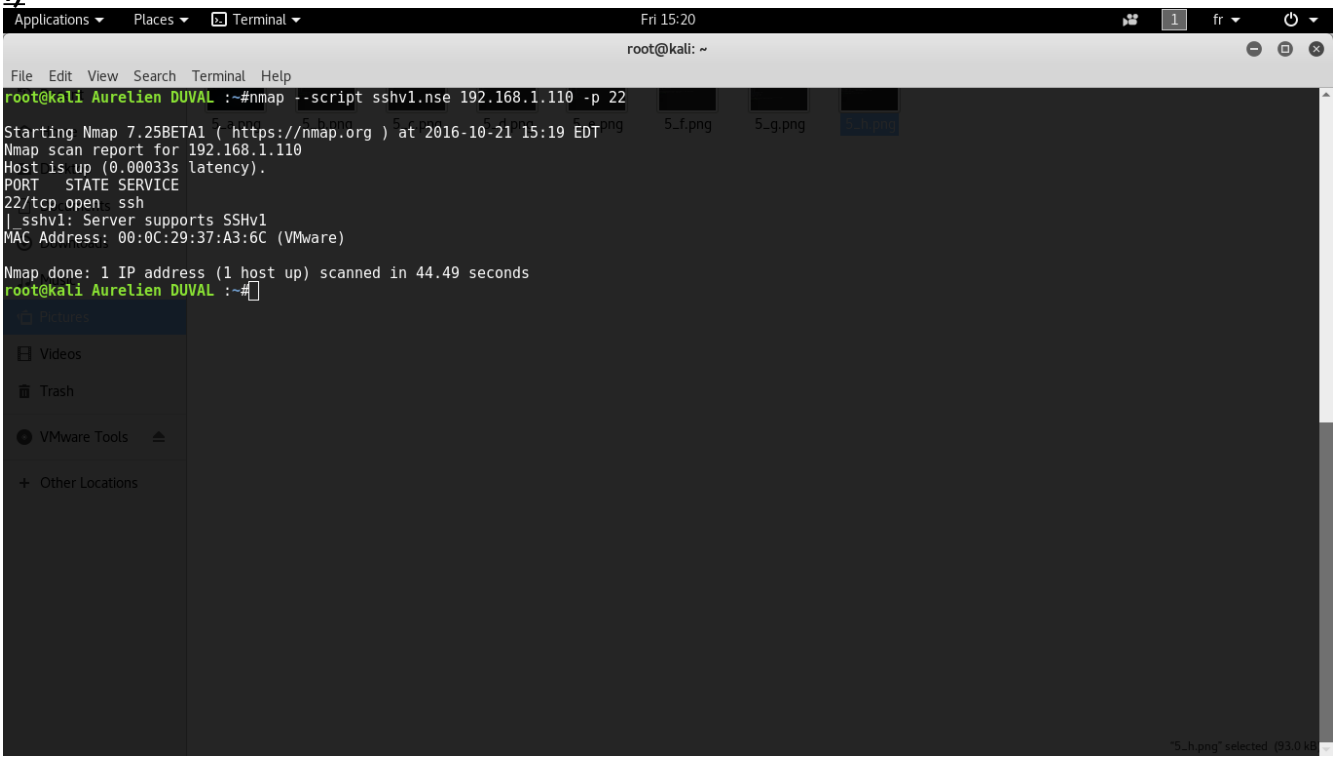
g)


Applications
Places
Terminal
Fri 15:16
fr
root@kali: ~
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 :~#
Other Locations

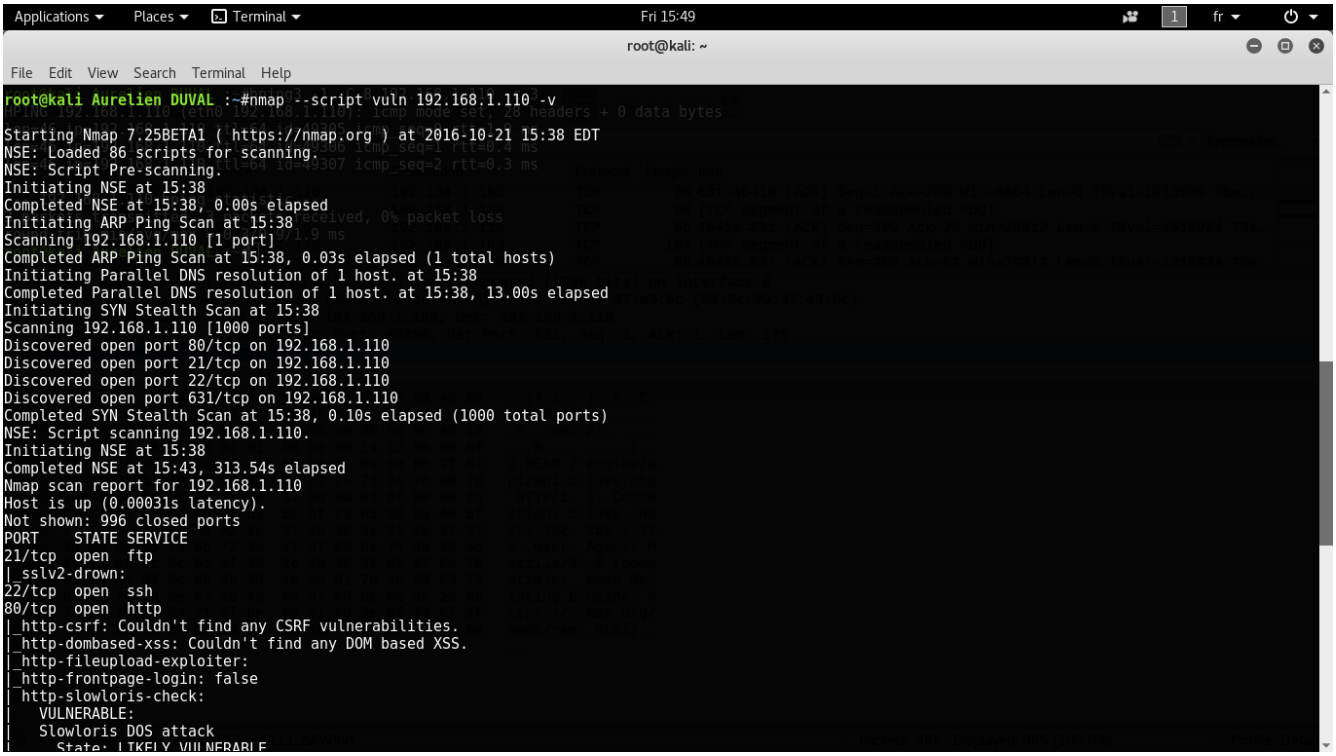
h)


Applications
Places
Terminal
Fri 15:19
fr
root@kali: ~
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

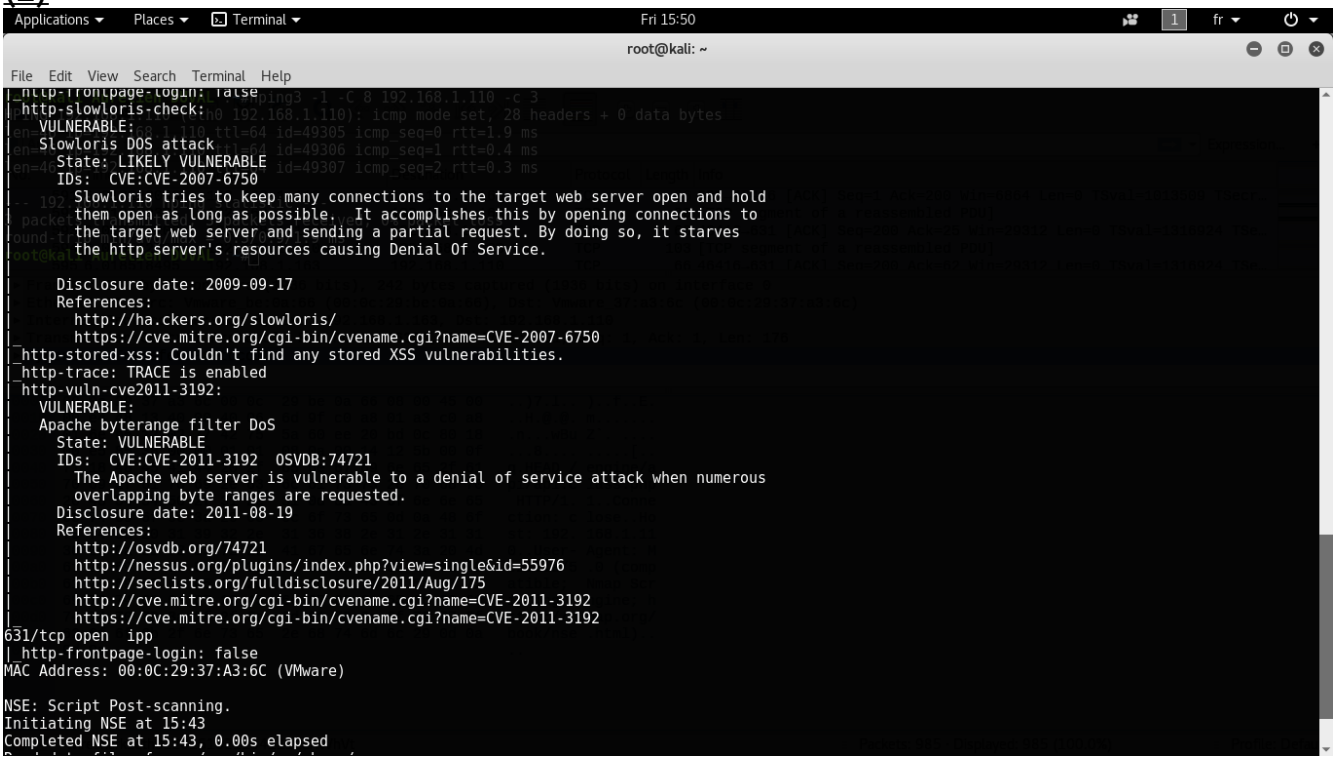
i)


Applications
Places
Terminal
Fri 15:20
root@kali: ~
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 (0.00033s 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 :~#
5_f.png
5_g.png
Pictures
Videos
Trash
VMware Tools
Other Locations

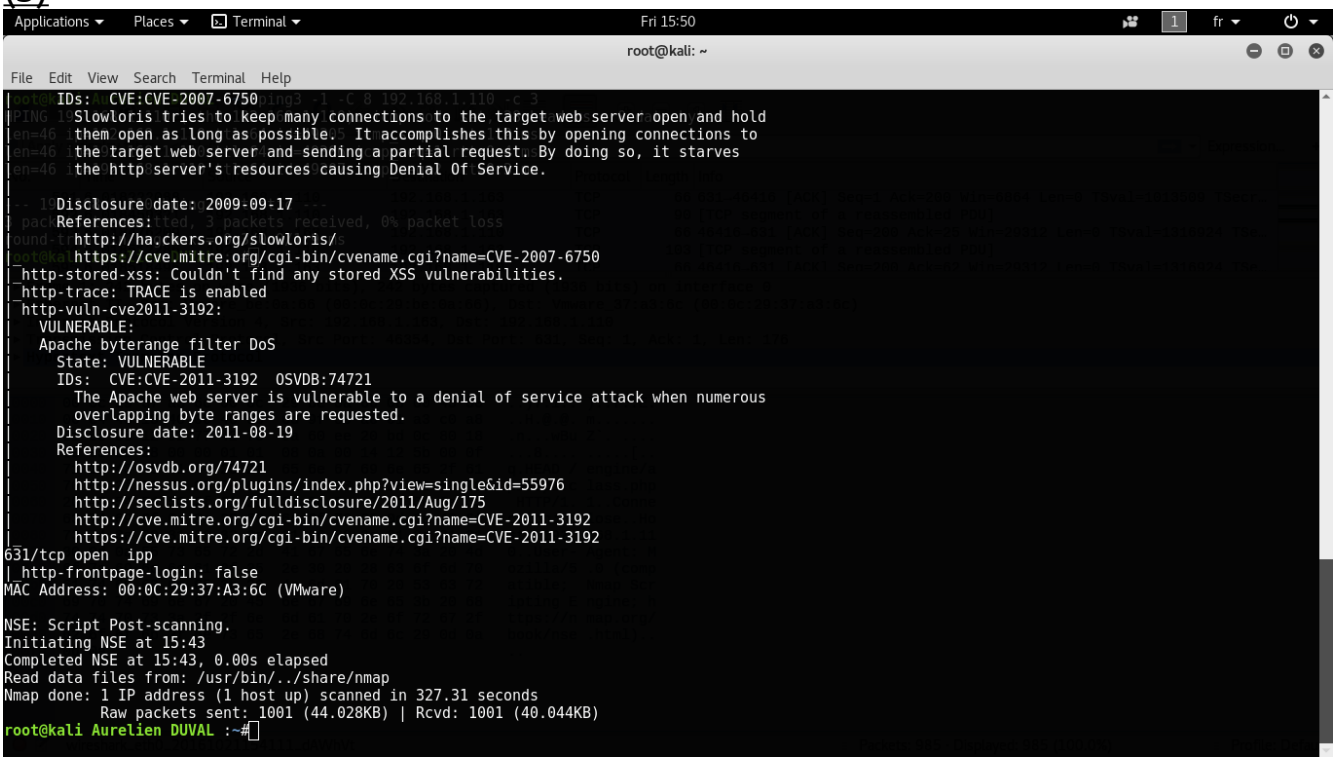
j) (1)


Applications
Places
Terminal
Fri 15:49
root@kali: ~
File Edit View Search Terminal Help
root@kali Aurelien DUVAL :~#nmap --script vuln 192.168.1.110 -v
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 (0.00031s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
21/tcp open ftp
|_sslv2-drown:
22/tcp open ssh
80/tcp open http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-fileupload-exploiter:
|_http-frontpage-login: false
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE

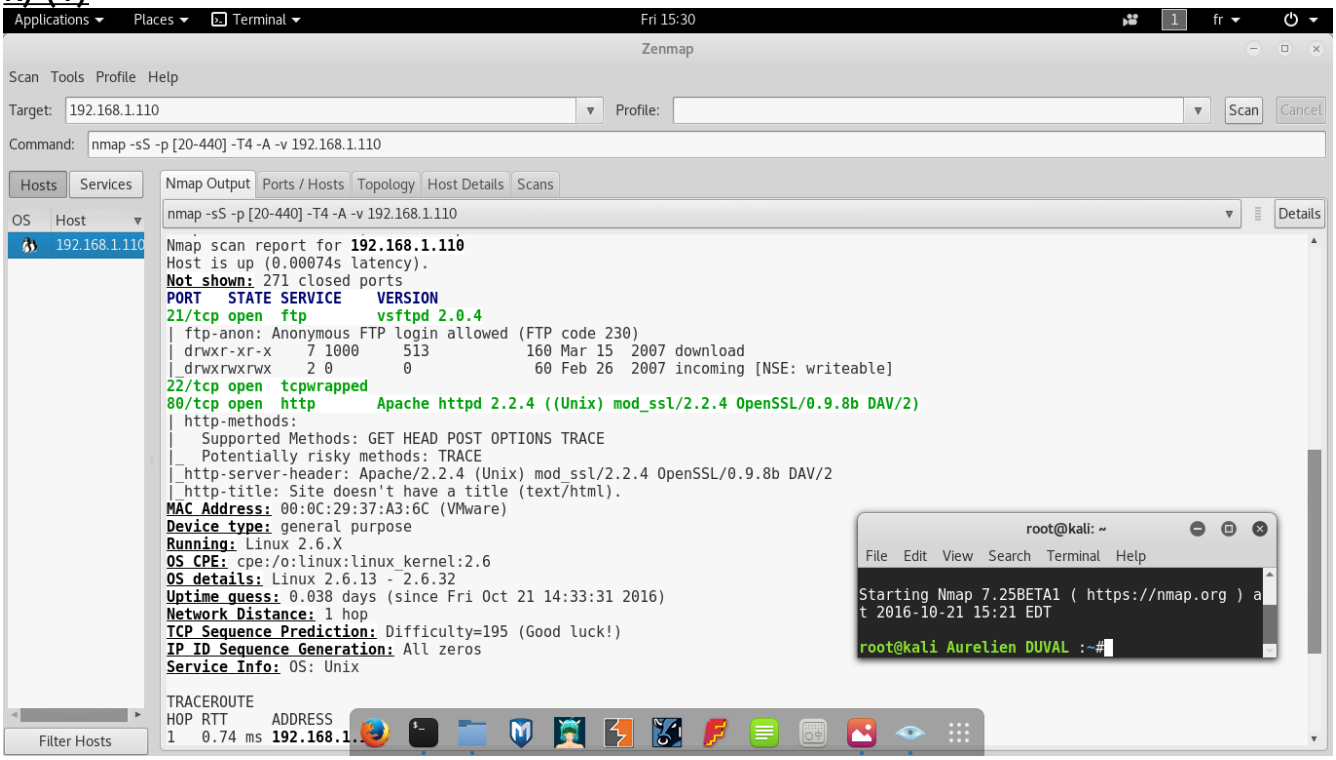
(2)


Applications
Places
Terminal
Fri 15:50
fr
root@kali: ~
File Edit View Search Terminal Help
|_http-frontpage-login: false
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
| http-vuln-cve2011-3192:
| VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| IDs: CVE:CVE-2011-3192 OSVDB:74721
| The Apache web server is vulnerable to a denial of service attack when numerous
| overlapping byte ranges are requested.
| Disclosure date: 2011-08-19
| References:
| http://osvdb.org/74721
| http://nessus.org/plugins/index.php?view=single&id=55976
| http://seclists.org/fulldisclosure/2011/Aug/175
| http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
631/tcp open ipp
|_http-frontpage-login: false
MAC Address: 00:0C:29:37:A3:6C (VMware)
NSE: Script Post-scanning.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed

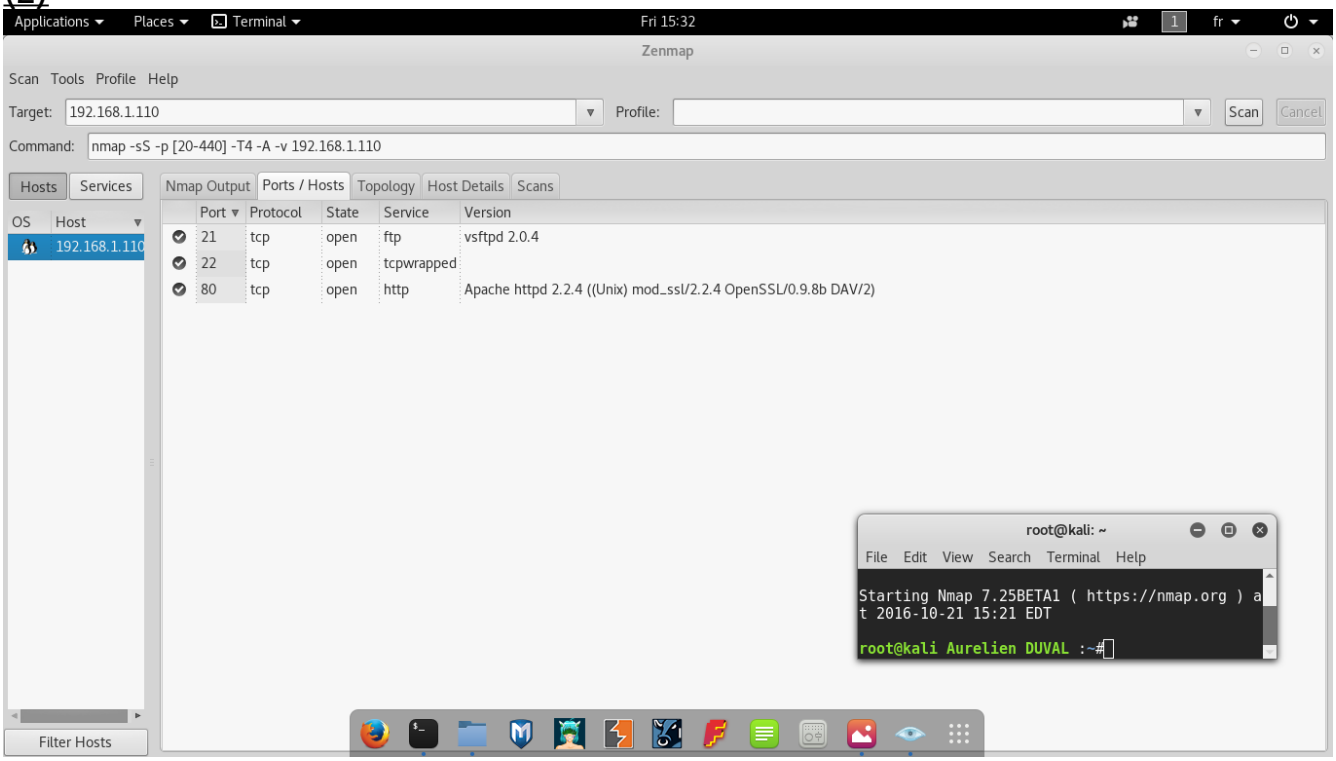
(3)


Applications
Places
Terminal
Fri 15:50
fr
root@kali: ~
File Edit View Search Terminal Help
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
| http-vuln-cve2011-3192:
| VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| IDs: CVE:CVE-2011-3192 OSVDB:74721
| The Apache web server is vulnerable to a denial of service attack when numerous
| overlapping byte ranges are requested.
| Disclosure date: 2011-08-19
| References:
| http://osvdb.org/74721
| http://nessus.org/plugins/index.php?view=single&id=55976
| http://seclists.org/fulldisclosure/2011/Aug/175
| http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
631/tcp open ipp
|_http-frontpage-login: false
MAC Address: 00:0C:29:37:A3:6C (VMware)
NSE: Script Post-scanning.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 Aurelien DUVAL :~#

k) (1)

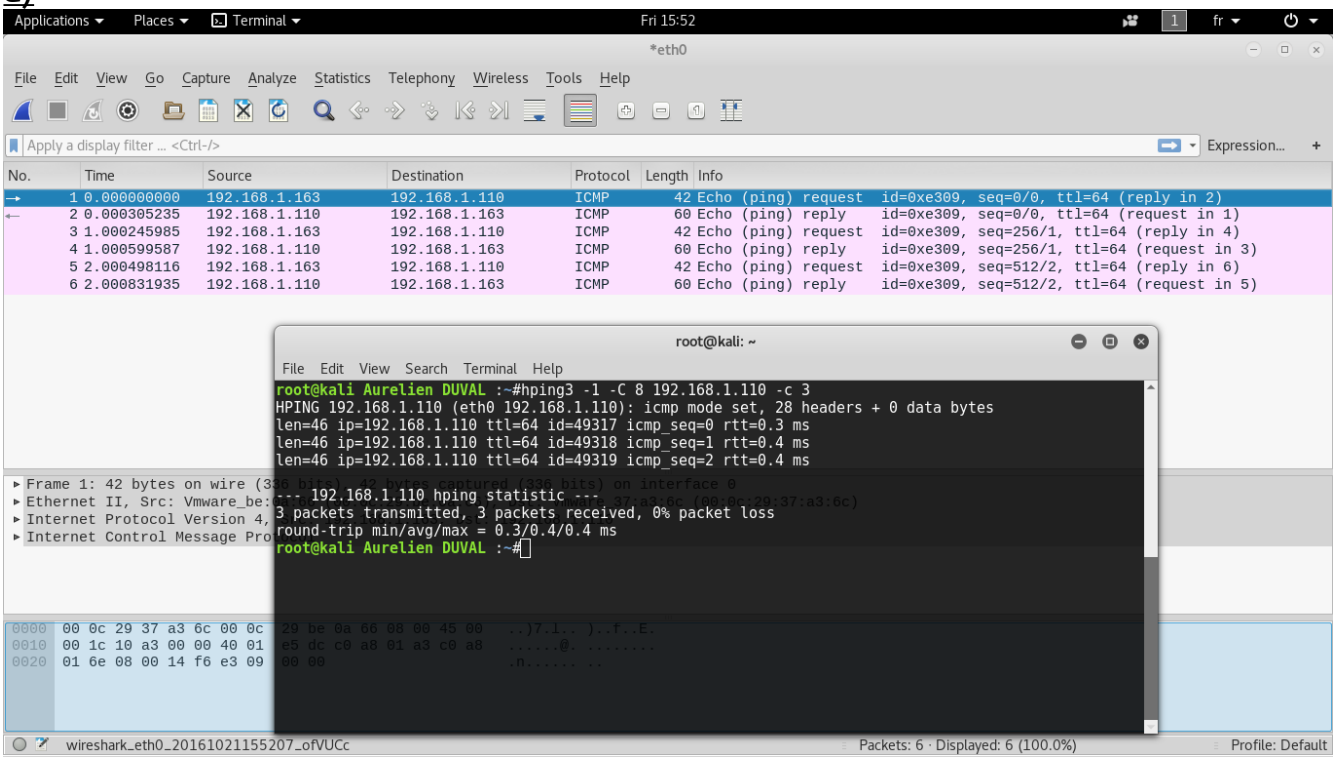

Applications Places Terminal Fri 15:30 fr
Zenmap
Scan Tools Profile Help
Target: 192.168.1.110 Profile: Scan Cancel
Command: nmap -sS -p [20-440] -T4 -A -v 192.168.1.110
Hosts Services
OS Host
192.168.1.110
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -p [20-440] -T4 -A -v 192.168.1.110 Details
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
TRACEROUTE
HOP RTT ADDRESS
1 0.74 ms 192.168.1.1
Filter Hosts
root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.25BETA1 (https://nmap.org) a
t 2016-10-21 15:21 EDT
root@kali Aurelien DUVAL :~#

(2)

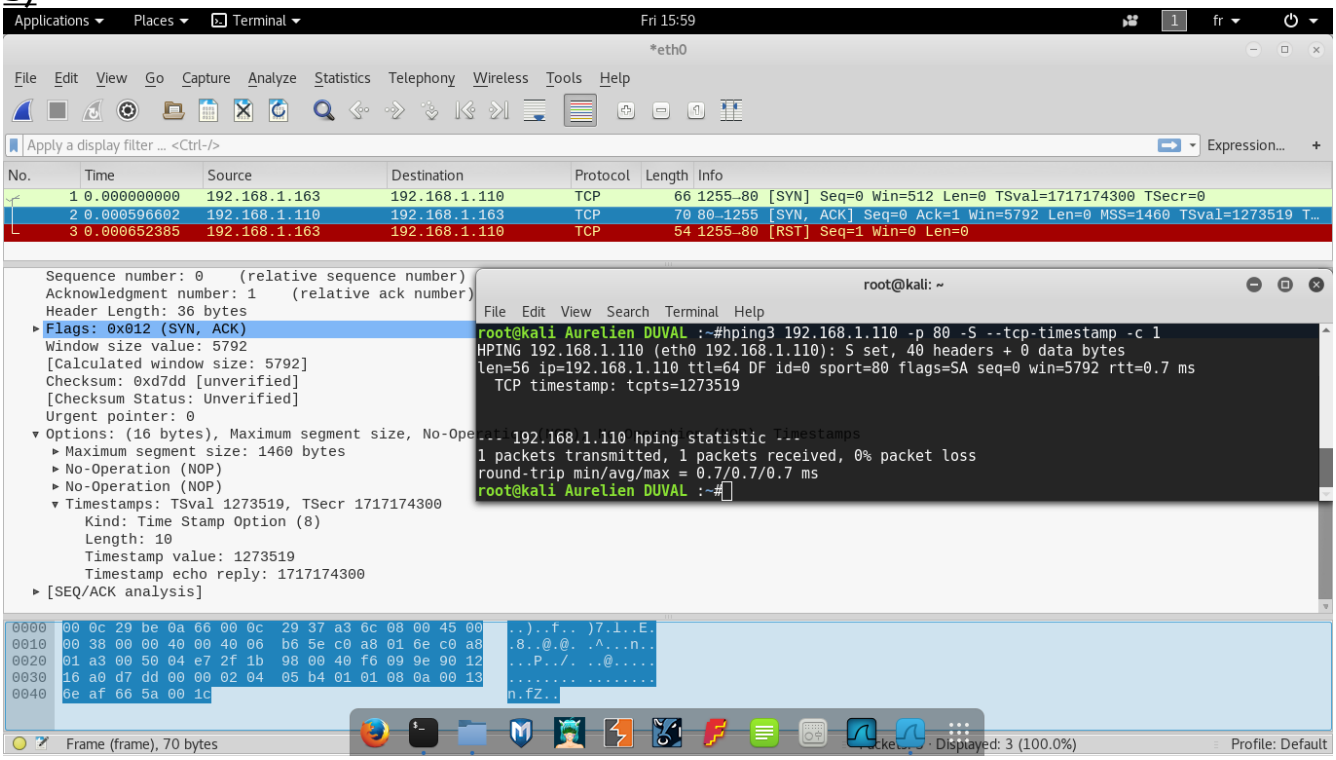

Applications Places Terminal Fri 15:32 fr
Zenmap
Scan Tools Profile Help
Target: 192.168.1.110 Profile: Scan Cancel
Command: nmap -sS -p [20-440] -T4 -A -v 192.168.1.110
Hosts Services
OS Host
192.168.1.110
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
21 tcp 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)
Filter Hosts
root@kali: ~
File Edit View Search Terminal Help
Starting Nmap 7.25BETA1 (https://nmap.org) a
t 2016-10-21 15:21 EDT
root@kali Aurelien DUVAL :~#

Question 6 :

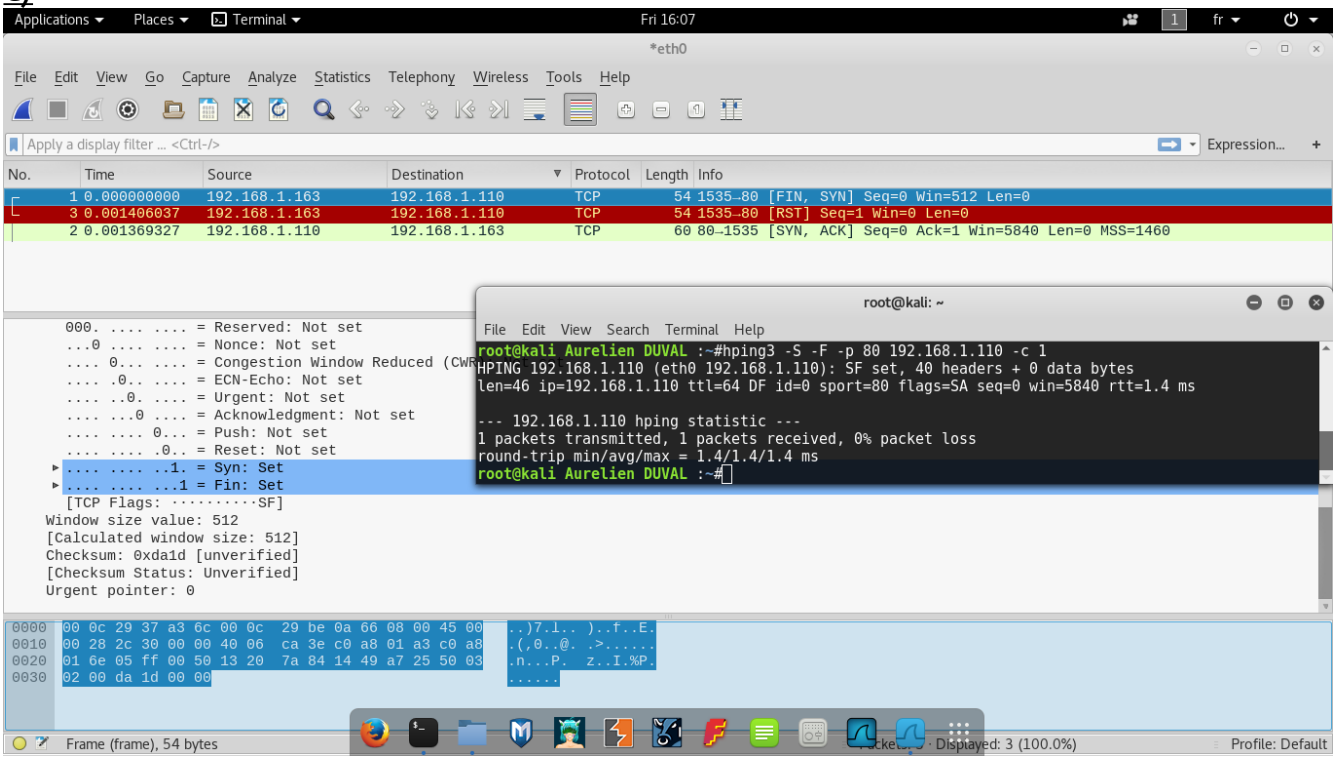
a)



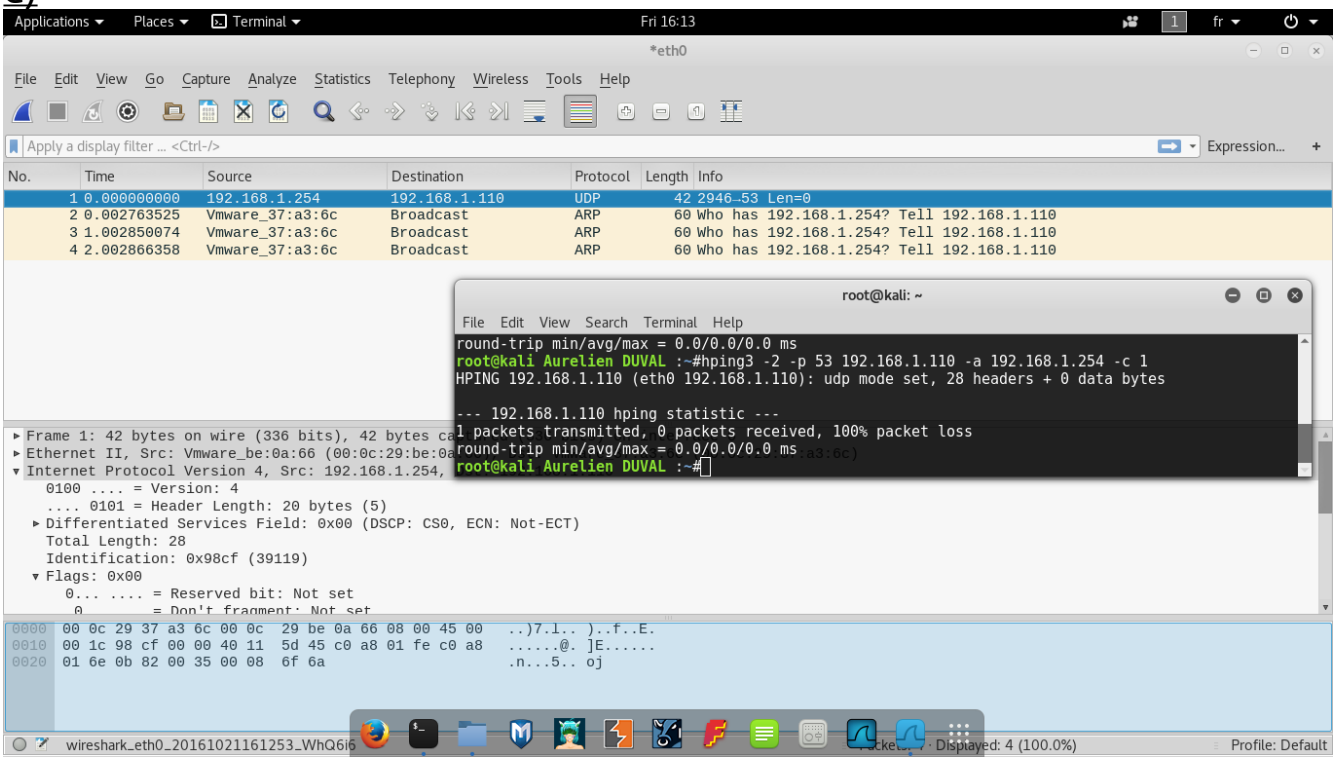
b)



c)

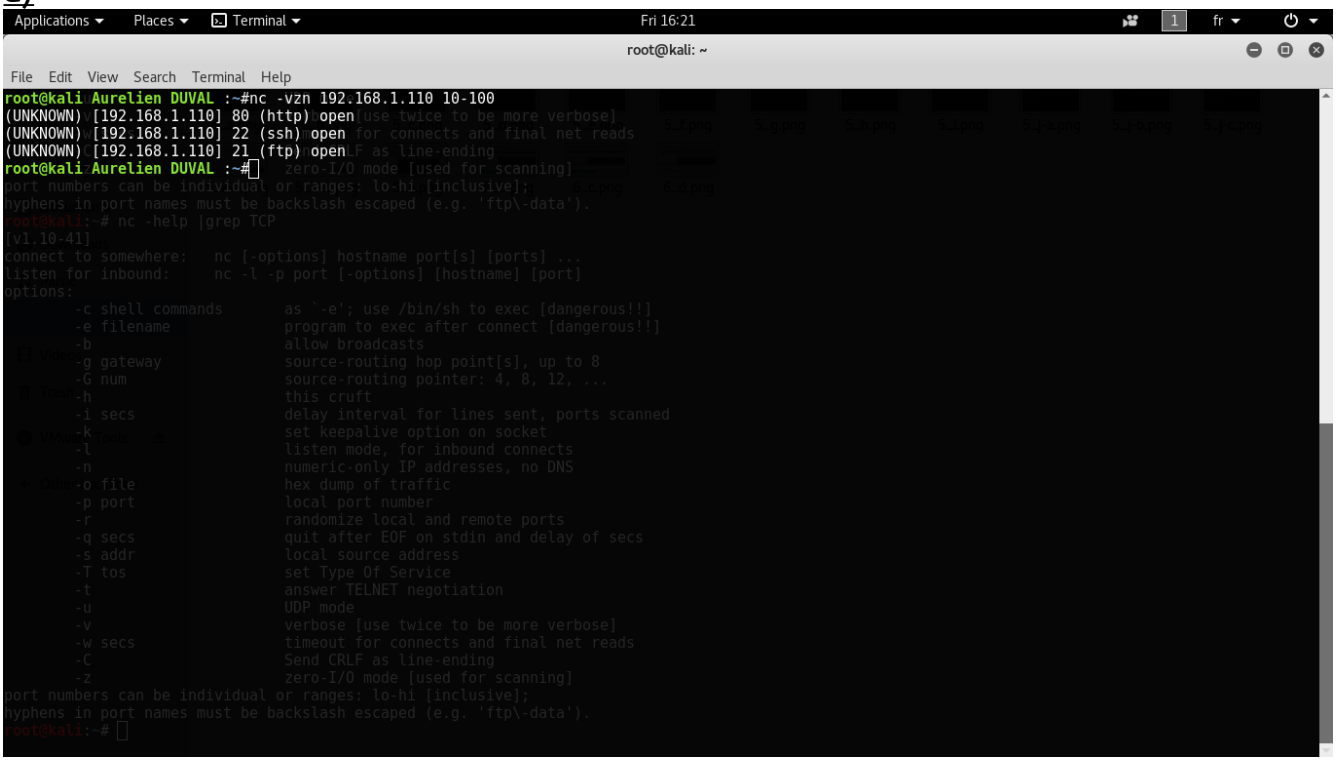

Applications Places Terminal Fri 16:07
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.1.163 192.168.1.110 TCP 54 1535→80 [FIN, SYN] Seq=0 Win=512 Len=0
3 0.001406037 192.168.1.163 192.168.1.110 TCP 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
root@kali: ~
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 :~#
Frame (frame), 54 bytes
Displayed: 3 (100.0%)
Profile: Default

d)

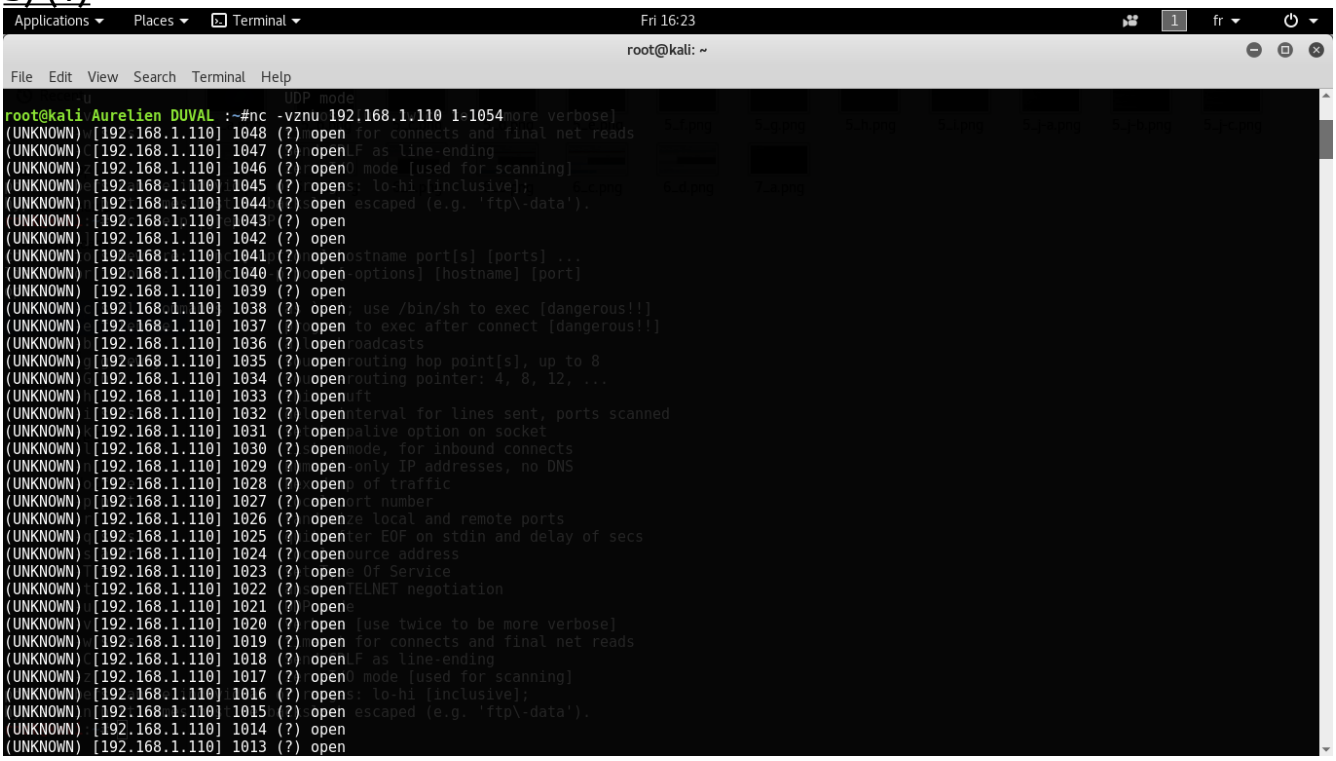

Applications Places Terminal Fri 16:13
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.1.254 192.168.1.110 UDP 42 2946→53 Len=0
2 0.002763525 Vmware_37:a3:6c Broadcast ARP 60 Who has 192.168.1.254? 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
root@kali: ~
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
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali Aurelien DUVAL :~#
wireshark_eth0_20161021161253_WhQ6i6
Displayed: 4 (100.0%)
Profile: Default

Question 7 :

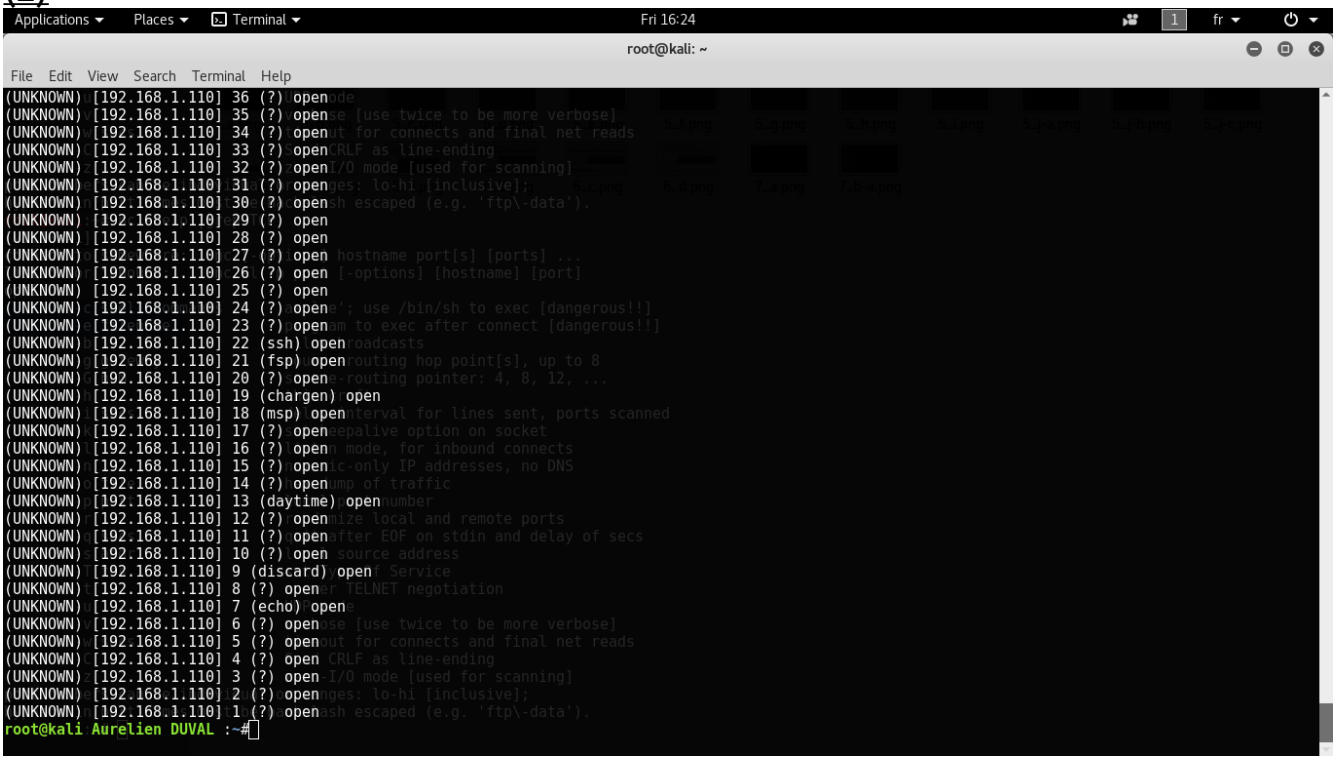
a)



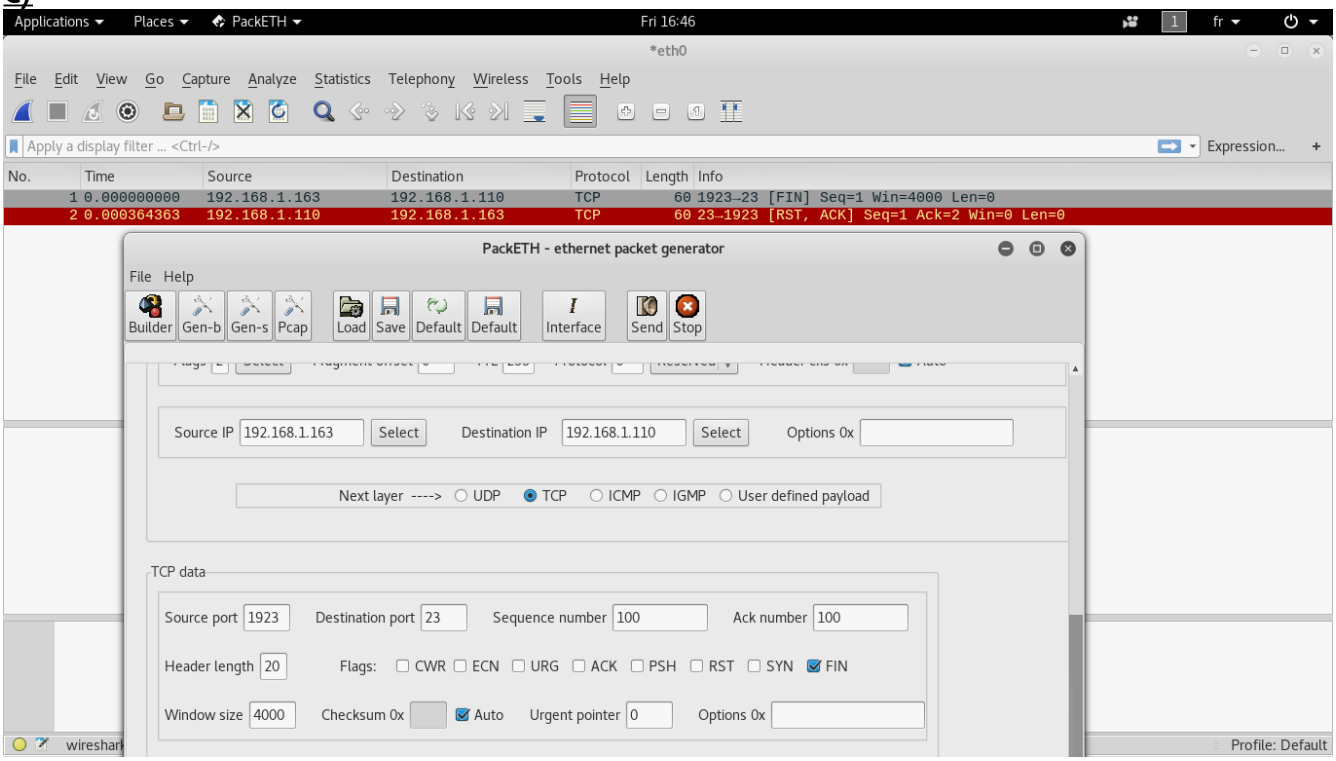
b) (1)



(2)

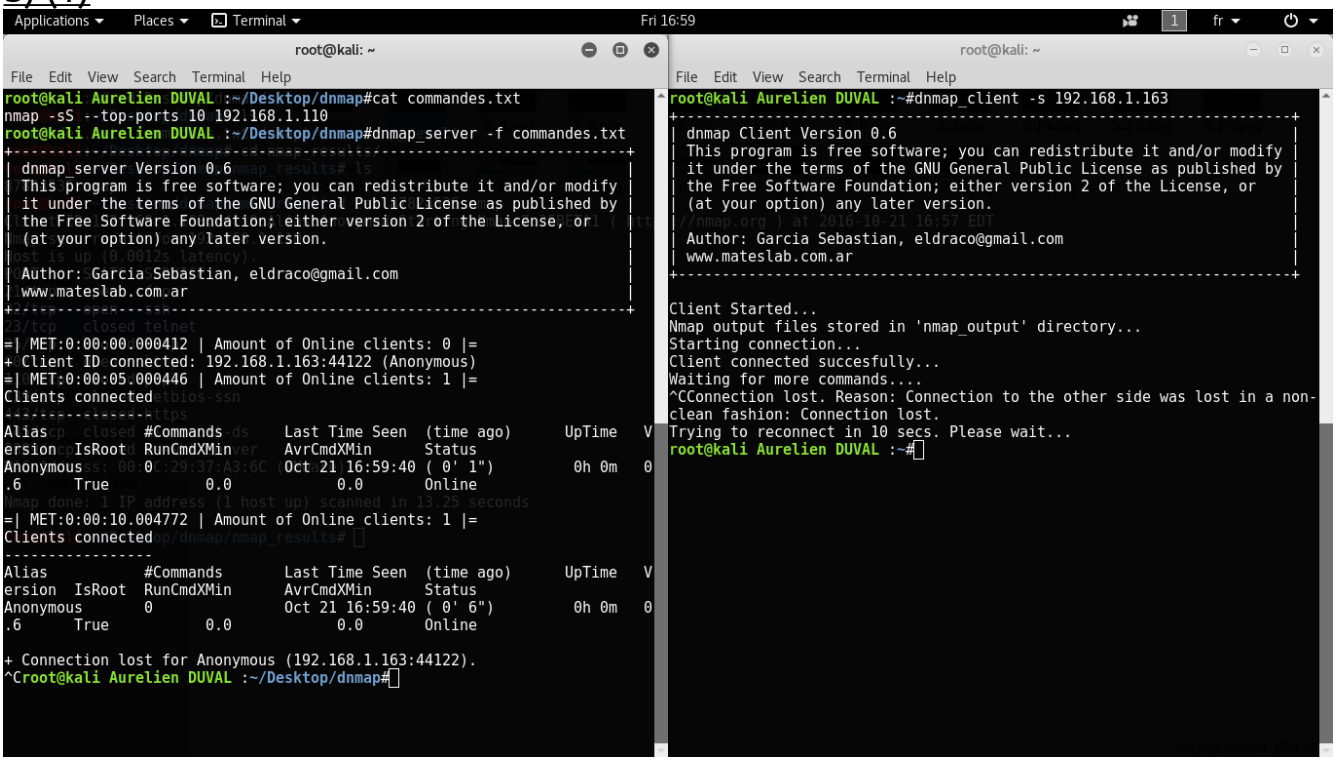

Applications
Places
Terminal
Fri 16:24
root@kali: ~
File Edit View Search Terminal Help
(UNKNOWN) [192.168.1.110] 36 (?) open
(UNKNOWN) [192.168.1.110] 35 (?) open
(UNKNOWN) [192.168.1.110] 34 (?) open
(UNKNOWN) [192.168.1.110] 33 (?) open
(UNKNOWN) [192.168.1.110] 32 (?) open
(UNKNOWN) [192.168.1.110] 31 (?) open
(UNKNOWN) [192.168.1.110] 30 (?) open
(UNKNOWN) [192.168.1.110] 29 (?) open
(UNKNOWN) [192.168.1.110] 28 (?) open
(UNKNOWN) [192.168.1.110] 27 (?) open
(UNKNOWN) [192.168.1.110] 26 (?) open
(UNKNOWN) [192.168.1.110] 25 (?) open
(UNKNOWN) [192.168.1.110] 24 (?) open
(UNKNOWN) [192.168.1.110] 23 (?) open
(UNKNOWN) [192.168.1.110] 22 (ssh) open
(UNKNOWN) [192.168.1.110] 21 (fsp) open
(UNKNOWN) [192.168.1.110] 20 (?) open
(UNKNOWN) [192.168.1.110] 19 (chargen) open
(UNKNOWN) [192.168.1.110] 18 (msp) open
(UNKNOWN) [192.168.1.110] 17 (?) open
(UNKNOWN) [192.168.1.110] 16 (?) open
(UNKNOWN) [192.168.1.110] 15 (?) open
(UNKNOWN) [192.168.1.110] 14 (?) open
(UNKNOWN) [192.168.1.110] 13 (daytime) open
(UNKNOWN) [192.168.1.110] 12 (?) open
(UNKNOWN) [192.168.1.110] 11 (?) open
(UNKNOWN) [192.168.1.110] 10 (?) open
(UNKNOWN) [192.168.1.110] 9 (discard) open
(UNKNOWN) [192.168.1.110] 8 (?) open
(UNKNOWN) [192.168.1.110] 7 (echo) open
(UNKNOWN) [192.168.1.110] 6 (?) open
(UNKNOWN) [192.168.1.110] 5 (?) open
(UNKNOWN) [192.168.1.110] 4 (?) open
(UNKNOWN) [192.168.1.110] 3 (?) open
(UNKNOWN) [192.168.1.110] 2 (?) open
(UNKNOWN) [192.168.1.110] 1 (?) open
root@kali Aurelien DUVAL :~#

c)

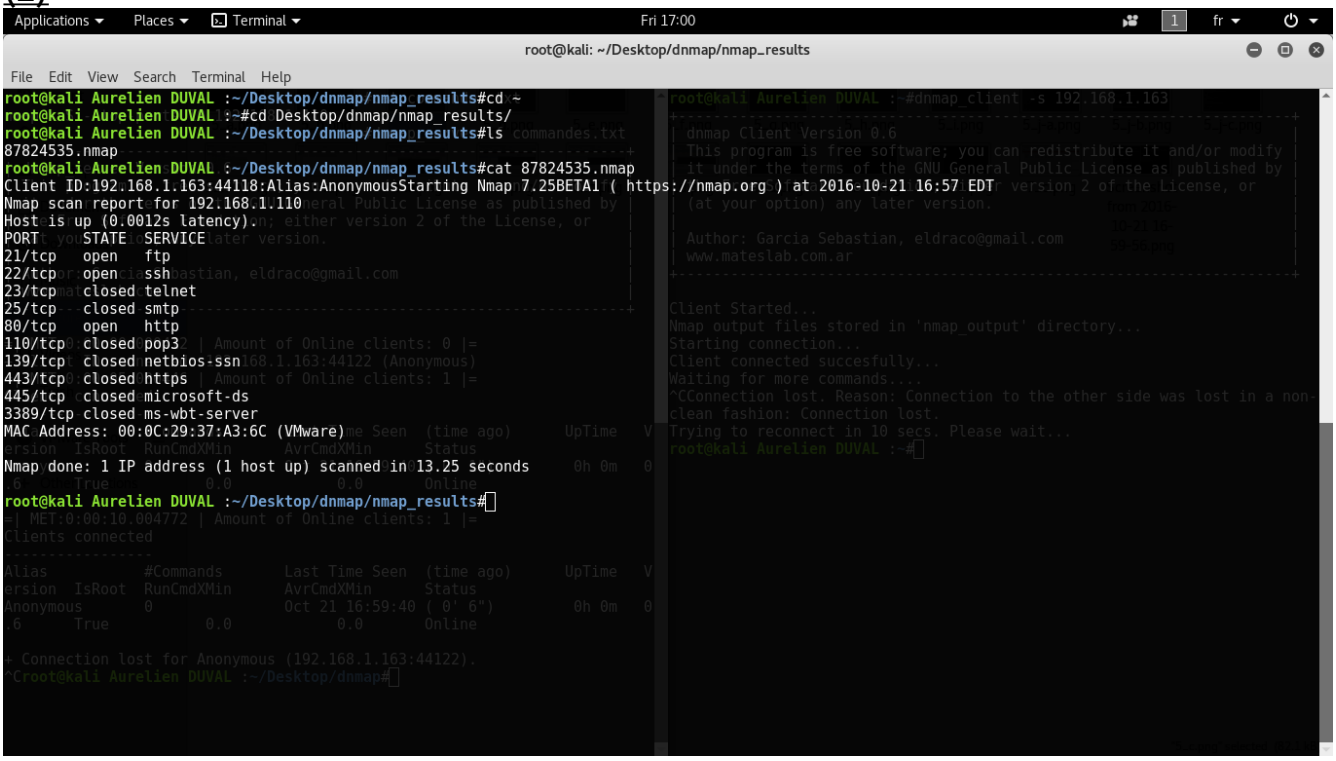

Applications
Places
PackETH
Fri 16:46
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.1.163 192.168.1.110 TCP 60 1923→23 [FIN] Seq=1 Win=4000 Len=0
2 0.000364363 192.168.1.110 192.168.1.163 TCP 60 23→1923 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
PackETH - ethernet packet generator
File Help
Builder Gen-b Gen-s Pcap Load Save Default Default Interface Send Stop
Source IP 192.168.1.163 Select Destination IP 192.168.1.110 Select Options 0x
Next layer ----> UDP TCP ICMP IGMP User defined payload
TCP data
Source port 1923 Destination port 23 Sequence number 100 Ack number 100
Header length 20 Flags: CWR ECN URG ACK PSH RST SYN FIN
Window size 4000 Checksum 0x Auto Urgent pointer 0 Options 0x
wireshark
Profile: Default

Question 8 :

b) (1)

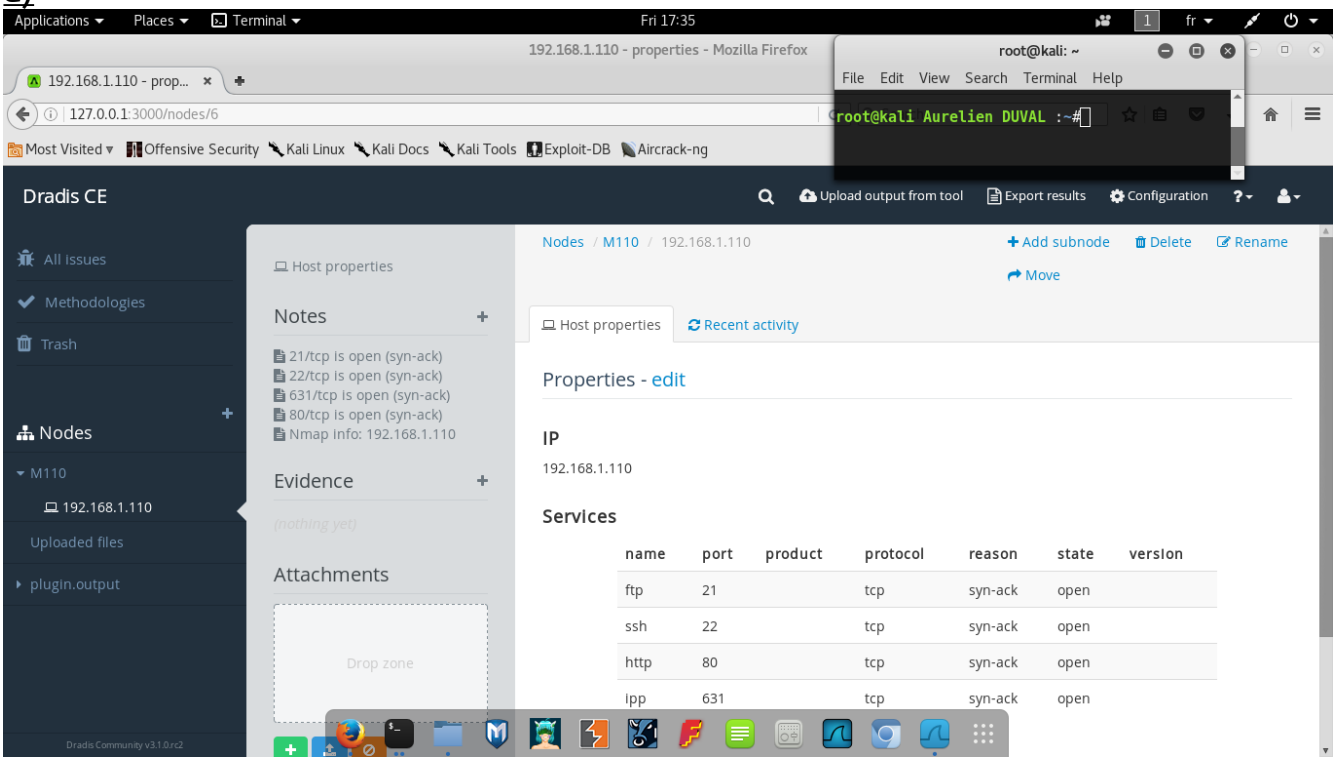


(2)



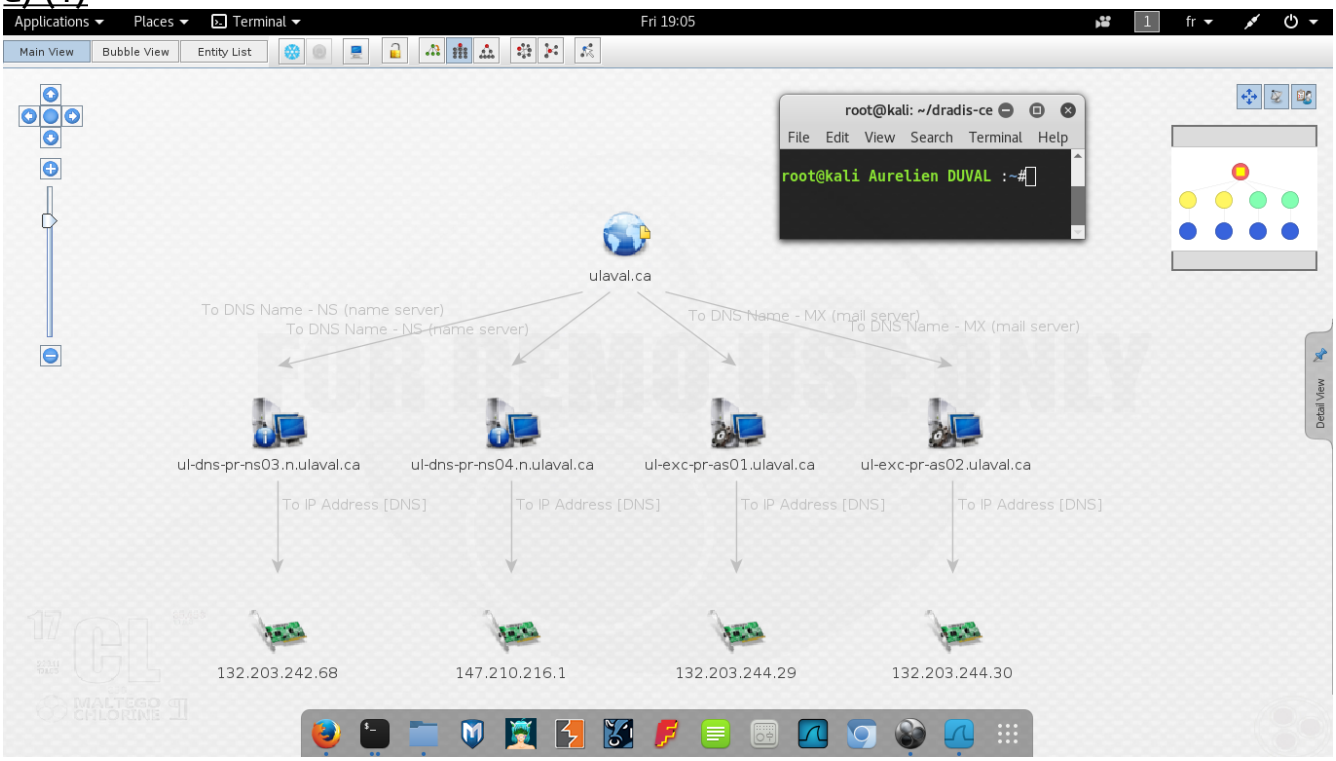
Question 9 :

a)

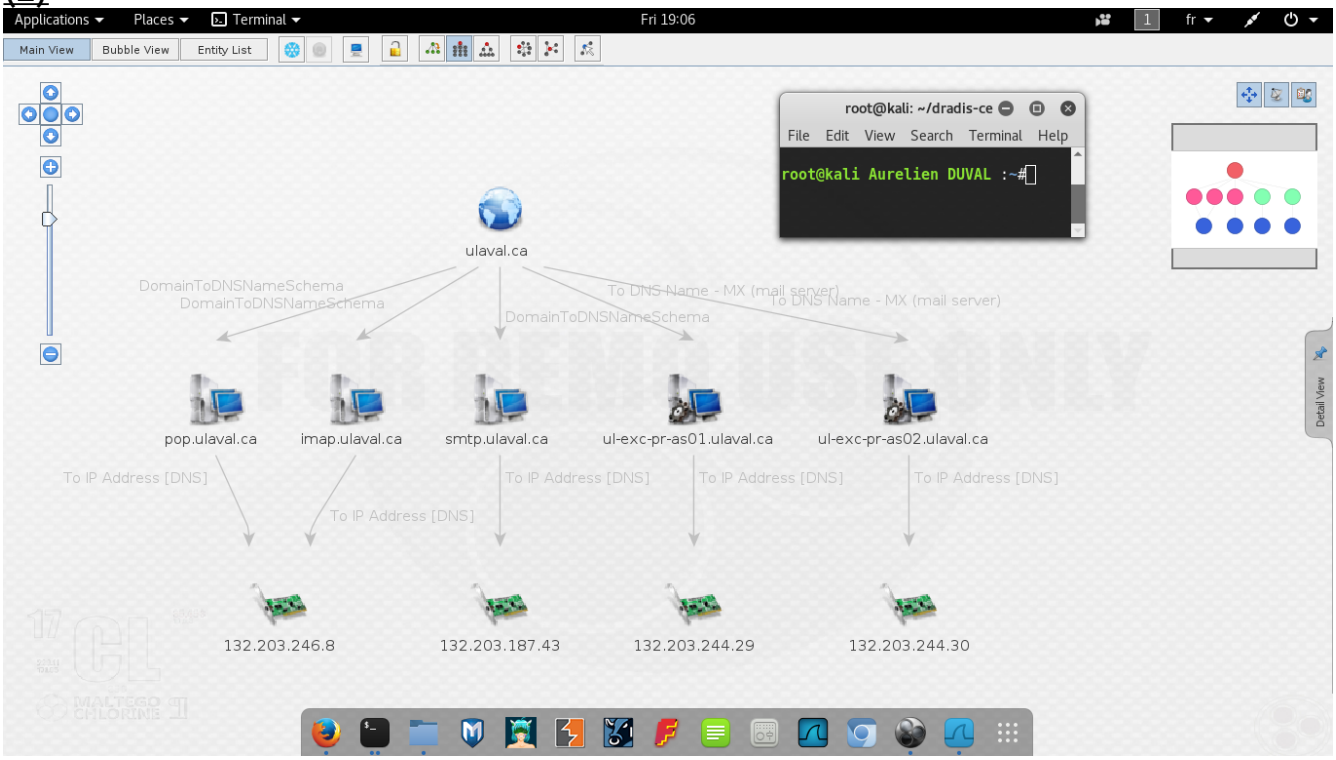


Question 11 :

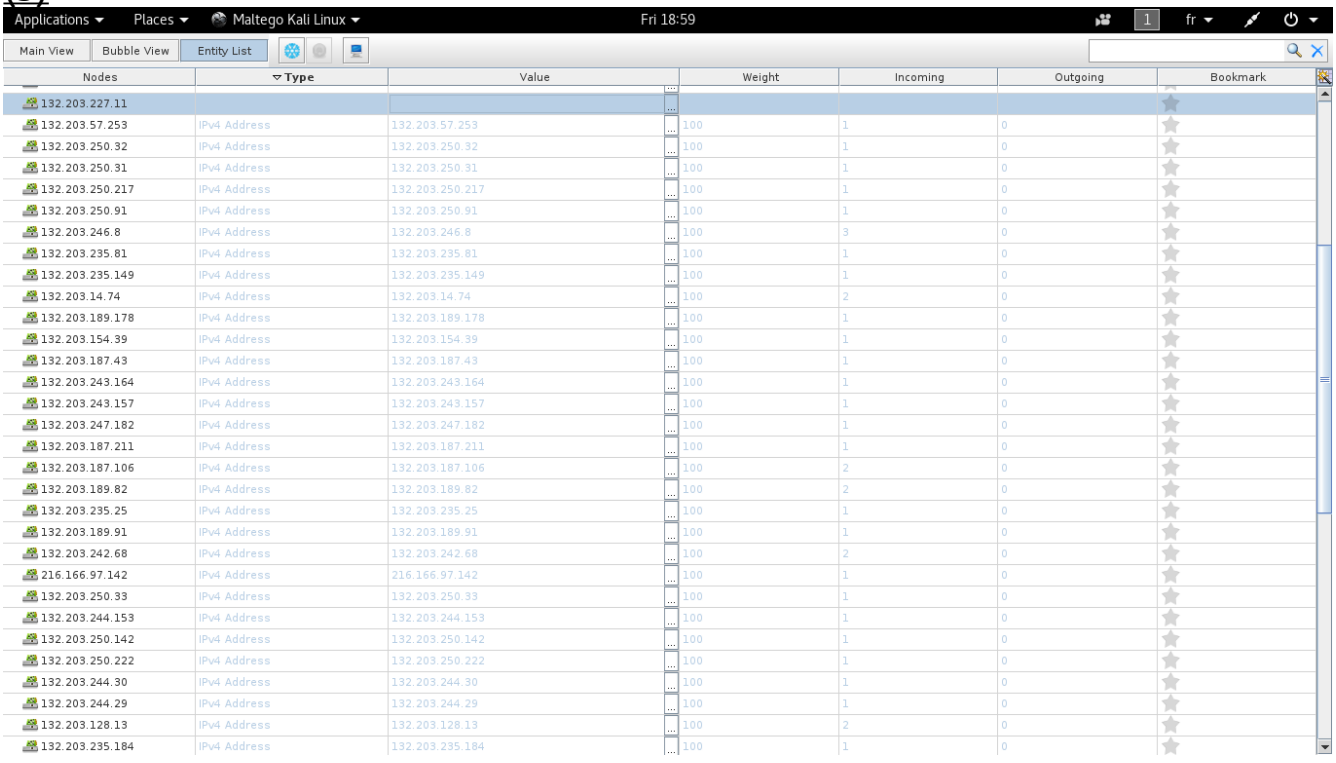
a) (1)



(2)

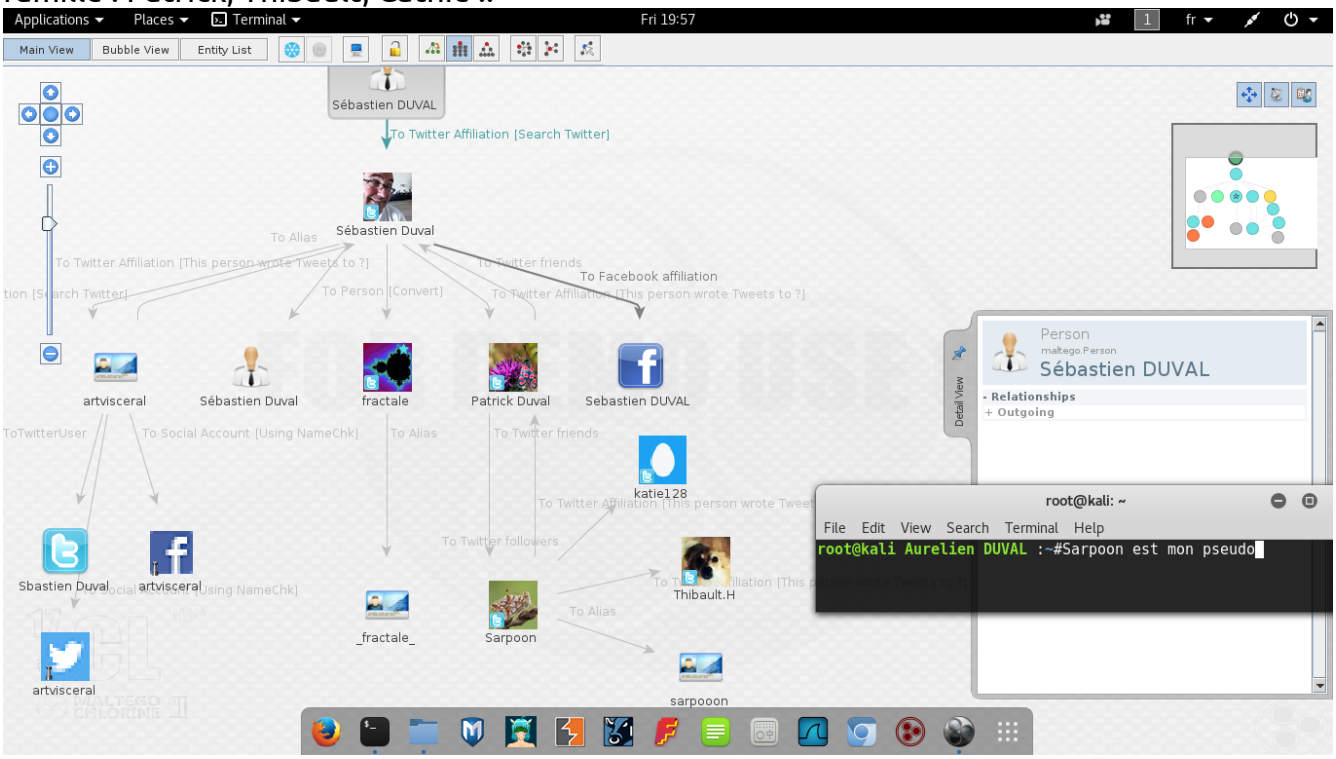


(3)



Nodes	Type	Value	Weight	Incoming	Outgoing	Bookmark
132.203.227.11						
132.203.57.253	IPv4 Address	132.203.57.253	100	1	0	
132.203.250.32	IPv4 Address	132.203.250.32	100	1	0	
132.203.250.31	IPv4 Address	132.203.250.31	100	1	0	
132.203.250.217	IPv4 Address	132.203.250.217	100	1	0	
132.203.250.91	IPv4 Address	132.203.250.91	100	1	0	
132.203.246.8	IPv4 Address	132.203.246.8	100	3	0	
132.203.235.81	IPv4 Address	132.203.235.81	100	1	0	
132.203.235.149	IPv4 Address	132.203.235.149	100	1	0	
132.203.14.74	IPv4 Address	132.203.14.74	100	2	0	
132.203.189.178	IPv4 Address	132.203.189.178	100	1	0	
132.203.154.39	IPv4 Address	132.203.154.39	100	1	0	
132.203.187.43	IPv4 Address	132.203.187.43	100	1	0	
132.203.243.164	IPv4 Address	132.203.243.164	100	1	0	
132.203.243.157	IPv4 Address	132.203.243.157	100	1	0	
132.203.247.182	IPv4 Address	132.203.247.182	100	1	0	
132.203.187.211	IPv4 Address	132.203.187.211	100	1	0	
132.203.187.106	IPv4 Address	132.203.187.106	100	2	0	
132.203.189.82	IPv4 Address	132.203.189.82	100	2	0	
132.203.235.25	IPv4 Address	132.203.235.25	100	1	0	
132.203.189.91	IPv4 Address	132.203.189.91	100	1	0	
132.203.242.68	IPv4 Address	132.203.242.68	100	2	0	
216.166.97.142	IPv4 Address	216.166.97.142	100	1	0	
132.203.250.33	IPv4 Address	132.203.250.33	100	1	0	
132.203.244.153	IPv4 Address	132.203.244.153	100	1	0	
132.203.250.142	IPv4 Address	132.203.250.142	100	1	0	
132.203.250.222	IPv4 Address	132.203.250.222	100	1	0	
132.203.244.30	IPv4 Address	132.203.244.30	100	1	0	
132.203.244.29	IPv4 Address	132.203.244.29	100	1	0	
132.203.128.13	IPv4 Address	132.203.128.13	100	2	0	
132.203.235.184	IPv4 Address	132.203.235.184	100	1	0	

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



Question 12 :