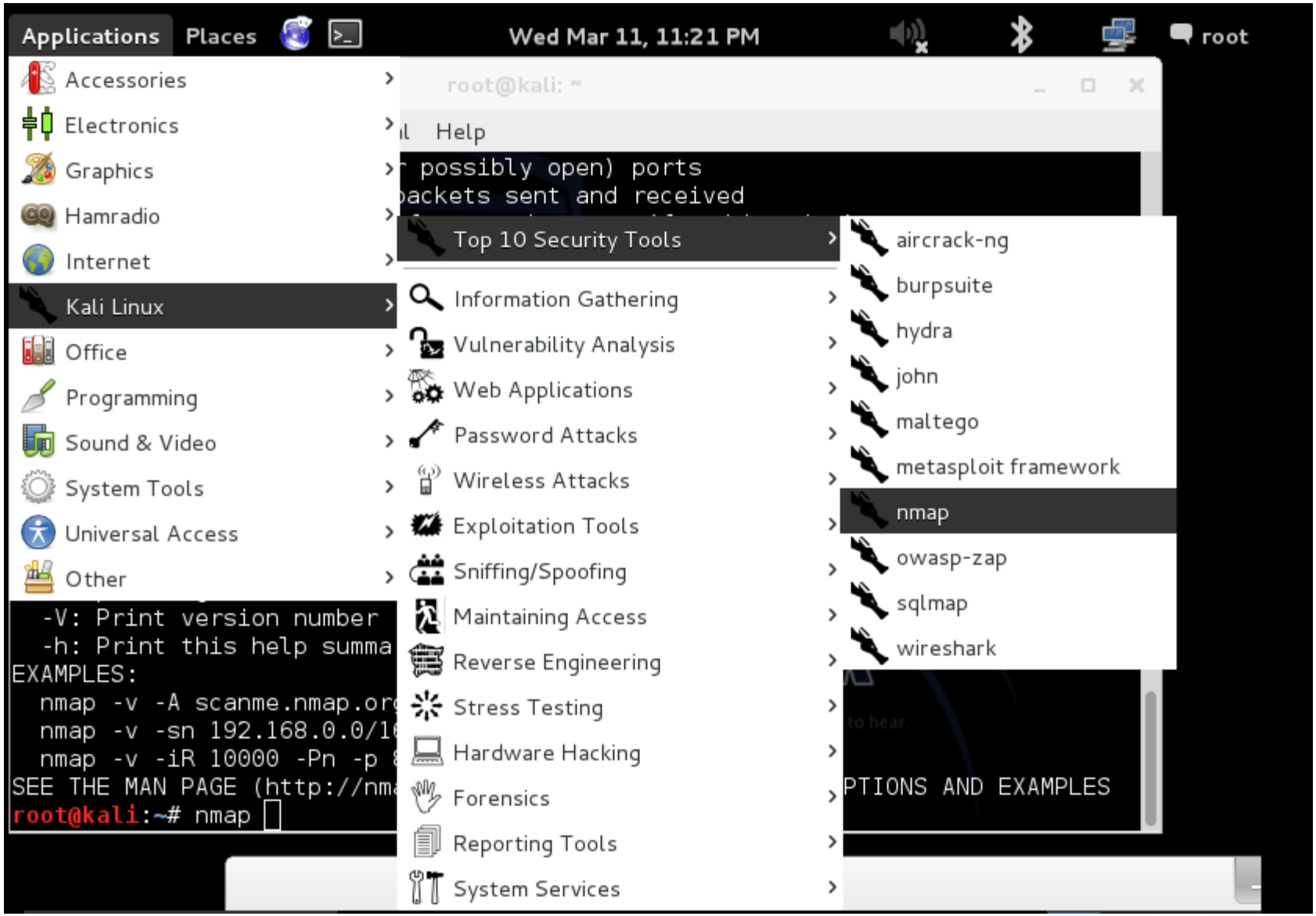
NMAP o ZENMAP Footprinting UTILIZANDO KALI

Clase practica

Jorge Gutiérrez

Cargar Kali


Applications
Places
Wed Mar 11, 11:21 PM
root
Accessories
Electronics
Graphics
Hamradio
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Universal Access
Other
root@kali: ~
Help
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
owasp-zap
sqlmap
wireshark
-V: Print version number
-h: Print this help summa
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16
nmap -v -iR 10000 -Pn -p
SEE THE MAN PAGE (http://nma
root@kali:~# nmap
PTIONS AND EXAMPLES

open (abierto)

filtered (filtrado) FIREWALL

closed (cerrado)

unfiltered (no filtrado).

open|filtered y closed|filtered

-Pn (igual –PN sin ping)

-sn (-sP solo scan ping)

-PS (TCP SYNC ping)

-PA (TCP ACK ping)

-PU (UDP ping)

-PE (ICMP Echo ping)

-PP (ICMP Timestamp ping)

-PM (ICMP Address Mask ping)

-PR (ARP ping)

--traceroute

-n (deshabilitar la resolución dns reverse)

--system-dns (alternative DNS Lookup)

--dns-servers (Manually Specify DNS server(s))

-sL (Create a Host List)

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

`--resume` (scan) `--append_output`

`-iL <targets_filename> -p <port ranges>`

`-F` (Fast scan mode) `-D <decoy1 [,decoy2][,ME],>`

`-S <SRC_IP_Address> -e <interface>`

`-g <portnumber> --data_length <number>`

`--randomize_hosts -O` (OS fingerprinting) `-I` (dent-scan)

`-f` (fragmentation) `-v` (verbose) `-h` (help)

`-n` (no reverse lookup) `-R` (do reverse lookup)

`-r` (don't randomize port scan) `-b <ftp relay host>` (FTP bounce)

NMAP opciones de tiempo

-T Paranoid – serial scan & 300 sec wait

-T Sneaky - serialize scans & 15 sec wait

-T Polite - serialize scans & 0.4 sec wait

-T Normal – parallel scan

-T Aggressive- parallel scan & 300 sec timeout & 1.25 sec/probe

-T Insane - parallel scan & 75 sec timeout & 0.3 sec/probe

--host_timeout --max_rtt_timeout
(default - 9000)

--min_rtt_timeout --initial_rtt_timeout
(default – 6000)

--max_parallelism --scan_delay (between probes)

-f (Fragment packetes)

--mtu (especificar mtu)

-D (usar Decoy)

-sI (Idle Zombies Scan)

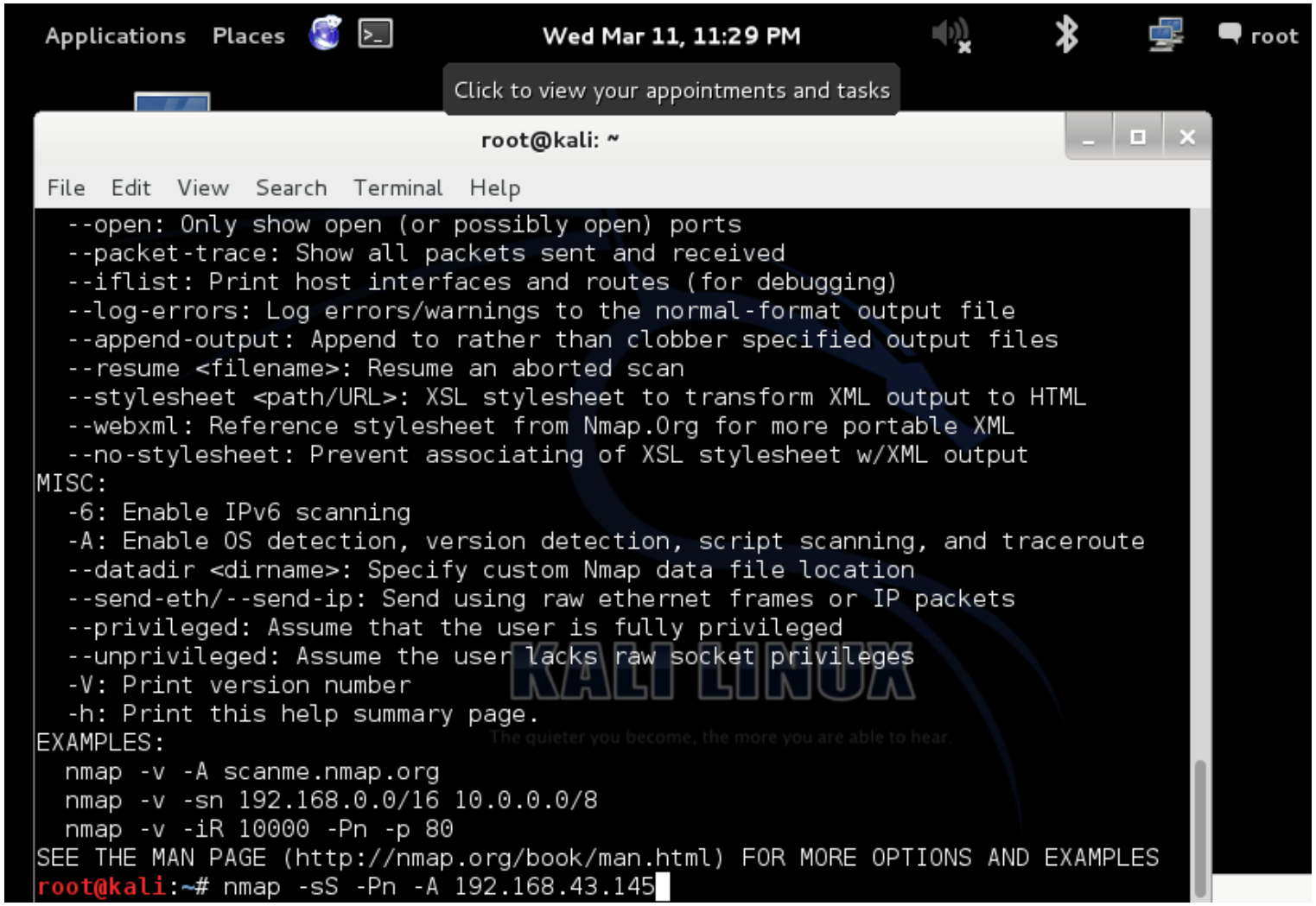
--source-port (cambiar el puerto origen)

--data-length (agregar datos random)

--randomize-hosts (randon traget scan order)

--spoof-mac (mac adress falsa)
--badsum (enviar checksum malos)

Objetivo: Ver puertos abiertos servicios y versiones



PC Linux o Windows Scaneada x NMAP

Entrar a pc del METASPLOITABLE

meta11 | Windows 7 (2)

```
rtt min/avg/max/mdev = 0.187/4.041/11.207/5.072 ms
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.43.145 netmask 255.255.255
.0 up
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ad:3e:18
          inet addr:192.168.43.145  Bcast:192.168.43.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fead:3e18/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:149 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15160 (14.8 KB)  TX bytes:13099 (12.7 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:49617 (48.4 KB)  TX bytes:49617 (48.4 KB)

msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.43.145 netmask 255.255.255
.0 up_
```

nmap -v //versión
nmap –vv /mas información
nmap –d //debub
nmap scanme.nmap.org //scan normal
nmap ip_metaexplotaible //scan normal
nmap 10.5.27.1-100 //scan multiples tagerts normal
nmap ip –sn //Sn es ping scan, para capa 2 scaning
nmap ipmetaexploitable -A //scan de forma agresiva

nmap -Pn ip //sin ping
nmap -sn 10.5.27.0/24 //ping scan only
nmap -PS ip //tcp syn ping
nmap -PA ip //tcp ack ping
nmap -PU ip //udp ping
nmap -PE ip //icmp Echo Ping
nmap --open 192.168.1.12 //solo los puertos con estado open

nmap -PP ip //icmp timestamp Ping, esto por si los firewall bloquean icmp pero algunos si aceptan icmp timestamp requests
nmap -PM ip //icmp address mask Ping, esto por si los firewall bloquean icmp pero algunos si aceptan icmp address mask ping
nmap --traceroute scanme.nmap.org //traceroute
nmap -n ip //Disable Reverse DNS Resolution
nmap --dns-server 8.8.8.8,8.8.4.4 scanme.nmap.org //manualmente specify DNS server

nmap –T4 –p 21 192.168.1.12 evitar ids
nmap -sP 172.16.15.100-254

nmap -F 192.168.1.12 //escaneo rapido con 100 mas comun puertos
nmap –p 21 192.168.1.12 // escaneo especifico de un puerto
nmap –p 21,22,80 192.168.1.12 //ver varios puertos.

nmap –sV 192.168.1.12 //Version del servicio
nmap –sP 192.168.1.12/24 //ping sweep
nmap –O 192.168.1.12 //Sistema operativo.
nmap –sS 172.16.15.239

Applications Places Wed Mar 11, 11:36 PM root

Access documents, folders and network places

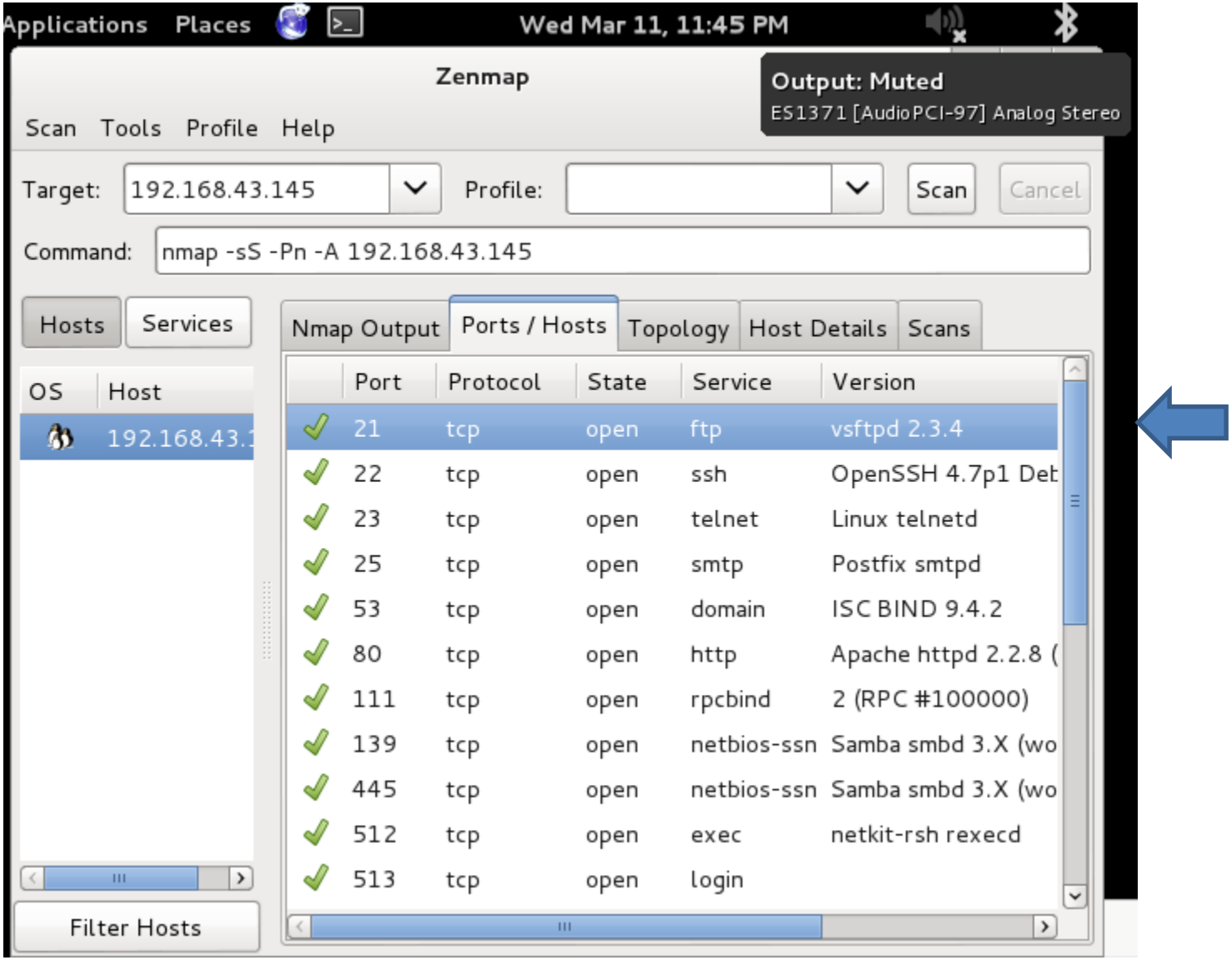
root@kali: ~

File Edit View Search Terminal Help

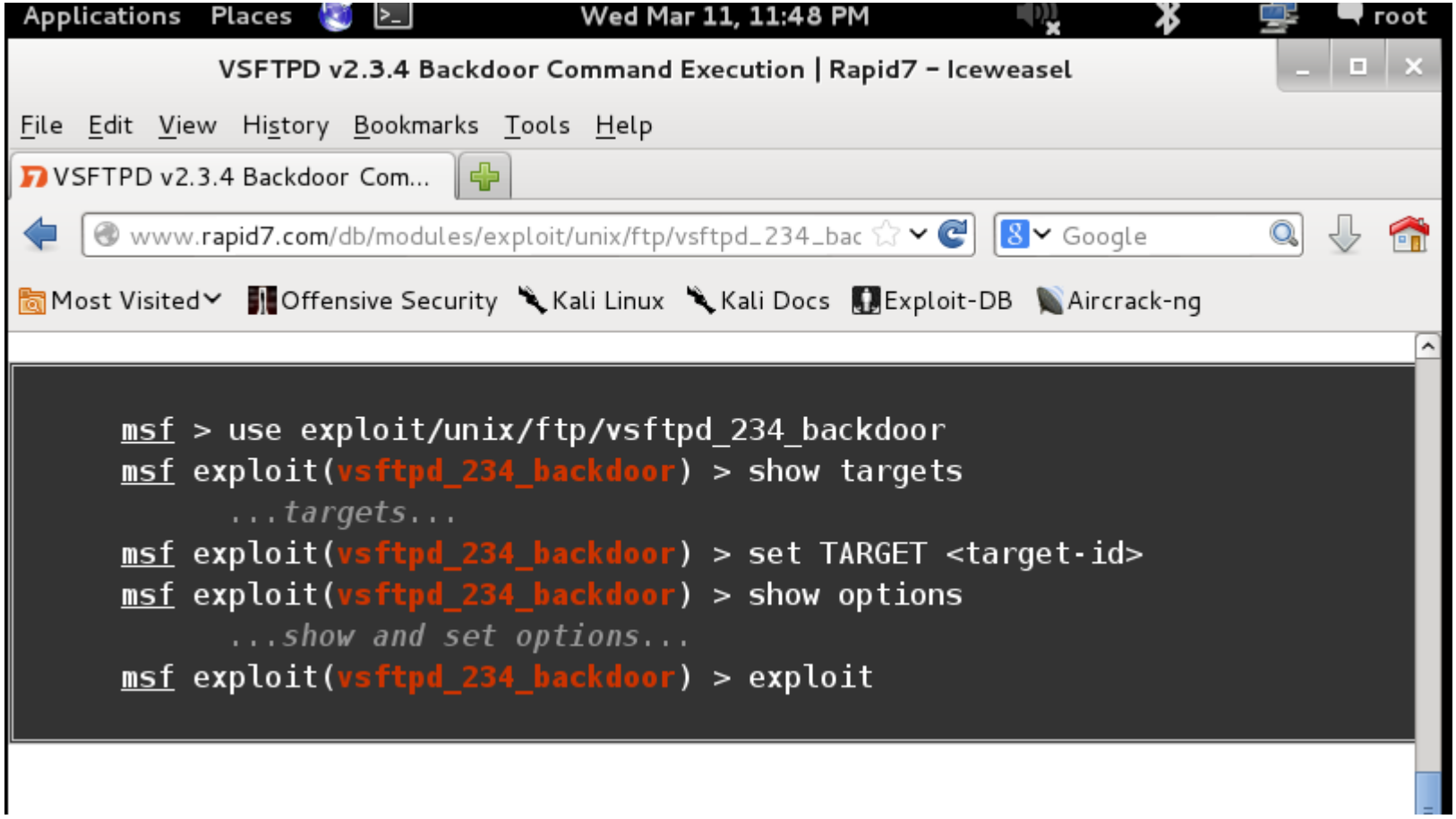
```
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -sS -Pn -A 192.168.43.145

Starting Nmap 6.46 ( http://nmap.org ) at 2015-03-11 23:33 UTC
Nmap scan report for 192.168.43.145
Host is up (0.00056s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ET
RN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOS
A/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45+00:00
|_Not valid after:  2010-04-16T14:07:45+00:00
```

Resultados usando Zenmap



Una vez teniendo lo que requerido, busco el vsftpd 2.3.4 exploit y listo.



Network Scanner

En kali

Network Scanner

Usando Netdiscover

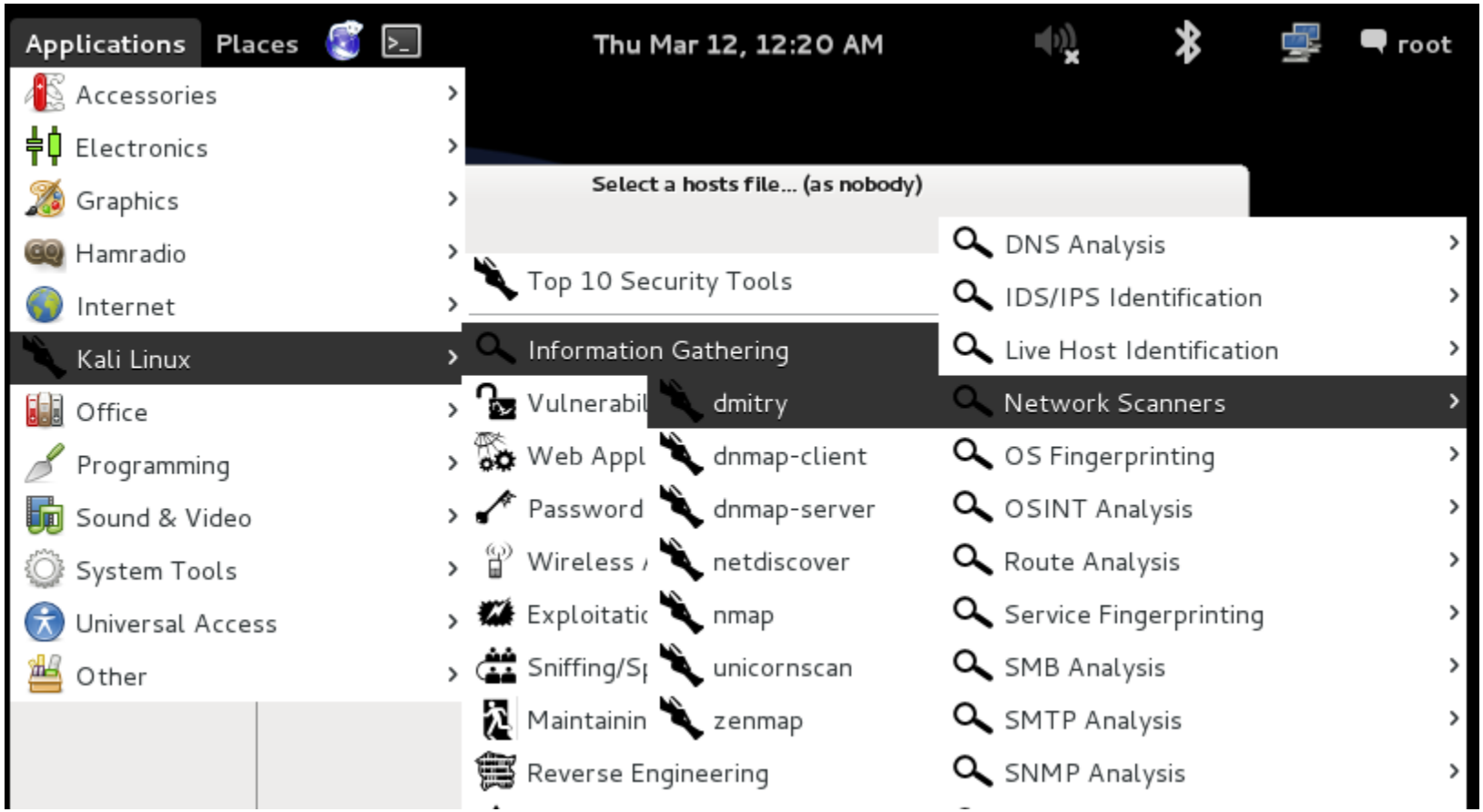
```
Click to view your appointments and tasks

File  Edit  View  Search  Terminal  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count  Len   MAC Vendor
-----------------------------------------------------------------------------
192.168.235.1   00:50:56:c0:00:08    01    060   VMWare, Inc.
192.168.235.2   00:50:56:f7:7a:1a    01    060   VMWare, Inc.
192.168.235.129 00:0c:29:1d:99:4e    01    060   VMware, Inc.
192.168.235.254 00:50:56:f2:a3:27    01    060   VMWare, Inc.

root@kali:~# netdiscover -i eth0 -r 192.168.235.0/24
```

Para Hacer un whois de un dominio utilizando dmitry



Resultados del scan.

```
Applications  Places                    Thu Mar 12, 12:25 AM
                                  Click to view your appointments and tasks
File  Edit  View  Search  Terminal  Help
root@kali:~# dmitry -iwnse www.udem.edu.ni
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:190.106.58.132
HostName:www.udem.edu.ni

Gathered Inet-whois information for 190.106.58.132
---------------------------------

inetnum:     190.106.58.128/29
status:      reallocated
owner:       Universidad de Managua
ownerid:     NI-UNMA-LACNIC
responsible: Mario Vallle
address:     Semaforos Hospital Velez Paiz 1c este, Rpto Belmonte, MANAGUA, ,
address:      - Managua -
country:     NI
phone:       +505  2652632 []
owner-c:     JOW3
tech-c:      JOW3
abuse-c:     JOW3
created:     20140211
```

Applications Places Thu Mar 12, 12:27 AM

root@kali: ~

File Edit View Search Terminal Help

```
HostIP:190.106.58.132
HostName:leninvasquez.udem.edu.ni
HostIP:190.106.58.132
HostName:guillermogarcia.udem.edu.ni
HostIP:190.106.58.132
HostName:pabloemiliohurtado.udem.edu.ni
HostIP:190.106.58.132
HostName:raulvega.udem.edu.ni
HostIP:190.106.58.132
HostName:profmariocabrera.udem.edu.ni
HostIP:190.106.58.132
HostName:lyzbethflores.udem.edu.ni
HostIP:190.106.58.132
HostName:belenmercado.udem.edu.ni
HostIP:190.106.58.132
HostName:juancarlosrochaortiz.udem.edu.ni
HostIP:190.106.58.132
HostName:carlosroman.udem.edu.ni
HostIP:190.106.58.132
HostName:noelmartinez.udem.edu.ni
HostIP:190.106.58.132
HostName:marbeliduarte.udem.edu.ni
HostIP:190.106.58.132
```

Who IS en Kali

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
 &?                Muestra este mensaje.

&NOTA:
 &Si se busca informacion sobre un dominio este debe pertenecer al ccTLD .mx
root@kali:~# whois yahoo.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Server Name: YAHOO.COM.ACCUTAXSERVICES.COM
   IP Address: 98.136.43.32
   IP Address: 66.196.84.168
   Registrar: WILD WEST DOMAINS, LLC
   Whois Server: whois.wildwestdomains.com
   Referral URL: http://www.wildwestdomains.com

   Server Name: YAHOO.COM.AU
   Registrar: WILD WEST DOMAINS, LLC
   Whois Server: whois.wildwestdomains.com
   Referral URL: http://www.wildwestdomains.com
```

root@kali: ~

File Edit View Search Terminal Help

```
   Server Name: YAHOO.COM.ZZZZZZ.MORE.INFO.AT.WWW.BEYONDWHOIS.COM
   IP Address: 203.36.226.2
   Registrar: INSTRA CORPORATION PTY, LTD.
   Whois Server: whois.instra.net
   Referral URL: http://www.instra.com

   Server Name: YAHOO.COM.ZZZZZZZ.GET.ONE.MILLION.DOLLARS.AT.WWW.UNIMUNDI.COM
   IP Address: 209.126.190.70
   Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
   Whois Server: whois.PublicDomainRegistry.com
   Referral URL: http://www.PublicDomainRegistry.com

   Domain Name: YAHOO.COM
   Registrar: MARKMONITOR INC.
   Sponsoring Registrar IANA ID: 292
   Whois Server: whois.markmonitor.com
   Referral URL: http://www.markmonitor.com
   Name Server: NS1.YAHOO.COM
   Name Server: NS2.YAHOO.COM
   Name Server: NS3.YAHOO.COM
   Name Server: NS4.YAHOO.COM
   Name Server: NS5.YAHOO.COM
   Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibite
```

Footprinting con dnsenum

```
root@kali: /usr/share/dnsenum
File  Edit  View  Search  Terminal  Help
root@kali:/usr/share/dnsenum# dnsenum --enum udem.edu.ni
dnsenum.pl VERSION:1.2.3
Warning: can't load Net::Whois::IP module, whois queries disabled.

-----   udem.edu.ni   -----


Host's addresses:
__________________

udem.edu.ni.                             5          IN    A        190.106.58.132


Name Servers:
______________

ns1.udem.edu.ni.                         5          IN    A        190.106.58.132
ns2.udem.edu.ni.                         5          IN    A        190.106.58.133


Mail (MX) Servers:
___________________

aspmx3.googlemail.com.                   5          IN    A        64.233.186.27
```

Footprinting

root@kali: /usr/bin

Output: Muted
ES1371 [AudioPCI-97] Analog Stereo

File Edit View Search Terminal Help

```
   -v                          Show attempts in the bruteforce modes.
root@kali:/usr/bin# ./dnsrecon -d udem.edu.ni
[*] Performing General Enumeration of Domain: udem.edu.ni
[-] DNSSEC is not configured for udem.edu.ni
[*]      SOA ns1.udem.edu.ni 190.106.58.132
[*]      NS ns1.udem.edu.ni 190.106.58.132
[*]      NS ns2.udem.edu.ni 190.106.58.133
[-]      Recursion enabled on NS Server 190.106.58.133
[*]      Bind Version for 190.106.58.133 dnsmasq-2.75
[*]      MX aspmx3.googlemail.com 64.233.190.26
[*]      MX alt1.aspmx.l.google.com 173.194.211.27
[*]      MX alt2.aspmx.l.google.com 64.233.190.27
[*]      MX aspmx.l.google.com 74.125.30.27
[*]      MX aspmx2.googlemail.com 173.194.211.26
[*]      MX aspmx3.googlemail.com 2800:3f0:4003:c01::1b
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:4002:c09::1a
[*]      MX alt2.aspmx.l.google.com 2800:3f0:4003:c01::1b
[*]      MX aspmx.l.google.com 2607:f8b0:4002:c06::1b
[*]      MX aspmx2.googlemail.com 2607:f8b0:400c:c10::1a
[*]      A udem.edu.ni 190.106.58.132
[*] Enumerating SRV Records
```

Footprinting

```
root@kali:/usr/bin# ./dnsmap google.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for google.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.google.com
IPv6 address #1: 2607:f8b0:4008:80b::200d

accounts.google.com
IP address #1: 216.58.192.109

admin.google.com
IPv6 address #1: 2607:f8b0:4008:80b::200e

admin.google.com
IP address #1: 190.212.166.35
IP address #2: 190.212.166.24
IP address #3: 190.212.166.25
```

Footprinting

```
root@kali:/usr/bin# fierce -dns udem.edu.ni
DNS Servers for udem.edu.ni:
        ns2.udem.edu.ni
        ns1.udem.edu.ni

Trying zone transfer first...
        Testing ns2.udem.edu.ni
                Request timed out or transfer not allowed.
        Testing ns1.udem.edu.ni

Whoah, it worked - misconfigured DNS server found:
udem.edu.ni.    3600    IN      SOA     ns1.udem.edu.ni. webmaster.udem.edu.ni. (
                                        2012074317      ; Serial
                                        900     ; Refresh
                                        600     ; Retry
                                        86400   ; Expire
```

Footprinting

Click to view your appointments and tasks

File Edit View Search Terminal Help

```
root@kali:~# dig udem.edu.ni mx

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> udem.edu.ni mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30941
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;udem.edu.ni.                   IN      MX

;; ANSWER SECTION:
udem.edu.ni.            5       IN      MX      5 alt1.aspmx.l.google.com.
udem.edu.ni.            5       IN      MX      5 alt2.aspmx.l.google.com.
udem.edu.ni.            5       IN      MX      1 aspmx.l.google.com.
udem.edu.ni.            5       IN      MX      10 aspmx2.googlemail.com.
udem.edu.ni.            5       IN      MX      10 aspmx3.googlemail.com.

;; Query time: 22 msec
;; SERVER: 192.168.235.2#53(192.168.235.2)
;; WHEN: Thu Feb 25 06:18:28 2016
;; MSG SIZE  rcvd: 162
```

Footprinting

```
root@kali:~# tcptraceroute www.udem.edu.ni
traceroute to www.udem.edu.ni (190.106.58.132), 30 hops max, 60 byte packets
 1  192.168.235.2 (192.168.235.2)  0.308 ms  0.232 ms  0.218 ms
 2  host-132-58-106-190.ibw.com.ni (190.106.58.132) <syn,ack>  82.137 ms  83.117
 ms  87.986 ms
root@kali:~# itrace -i eth0 -d www.yahoo.com
 1(1)   [192.168.235.2]
```

dmitry -iwnse targetdomain

dmitry -s yahoo.com //subdominios

dmitry –i udem.edu.ni//con whois ip

dmitry –w targetdomain//con whois domain

dmitry –p targetdomain //TCP port scan

dmitry –wnsepb udem.edu.ni

Whois yahoo.com

Cd /usr/share/dnsenum/

Dnsenum –enum udem.edu.ni
Dnsenum yahoo.com

Dnsenum -help
Dnsenum –enum google //equivalente treat 5

Tool para investigar servidores dns

Cd /usr/bin

./dnsrecon -d google.com
./dnsrecon –h udem.edu.ni

./dnsmap google.com

Fierce scaneo de dominio
fierce -dns google.com
Fierce –dns udem.com

dig google.com
dig google.com MX
dig google.com –t MX
dig google.com AAAA
dig +qr google.com any

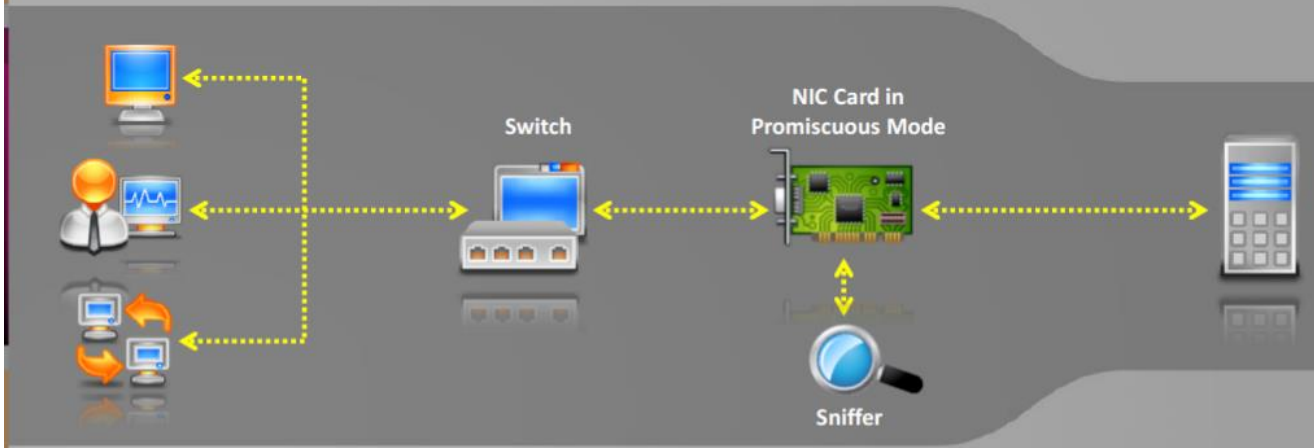
Traza
Tcptraceroute www.yahoo.com

SNIFING

How a Sniffer Works

Promiscuous Mode

Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment

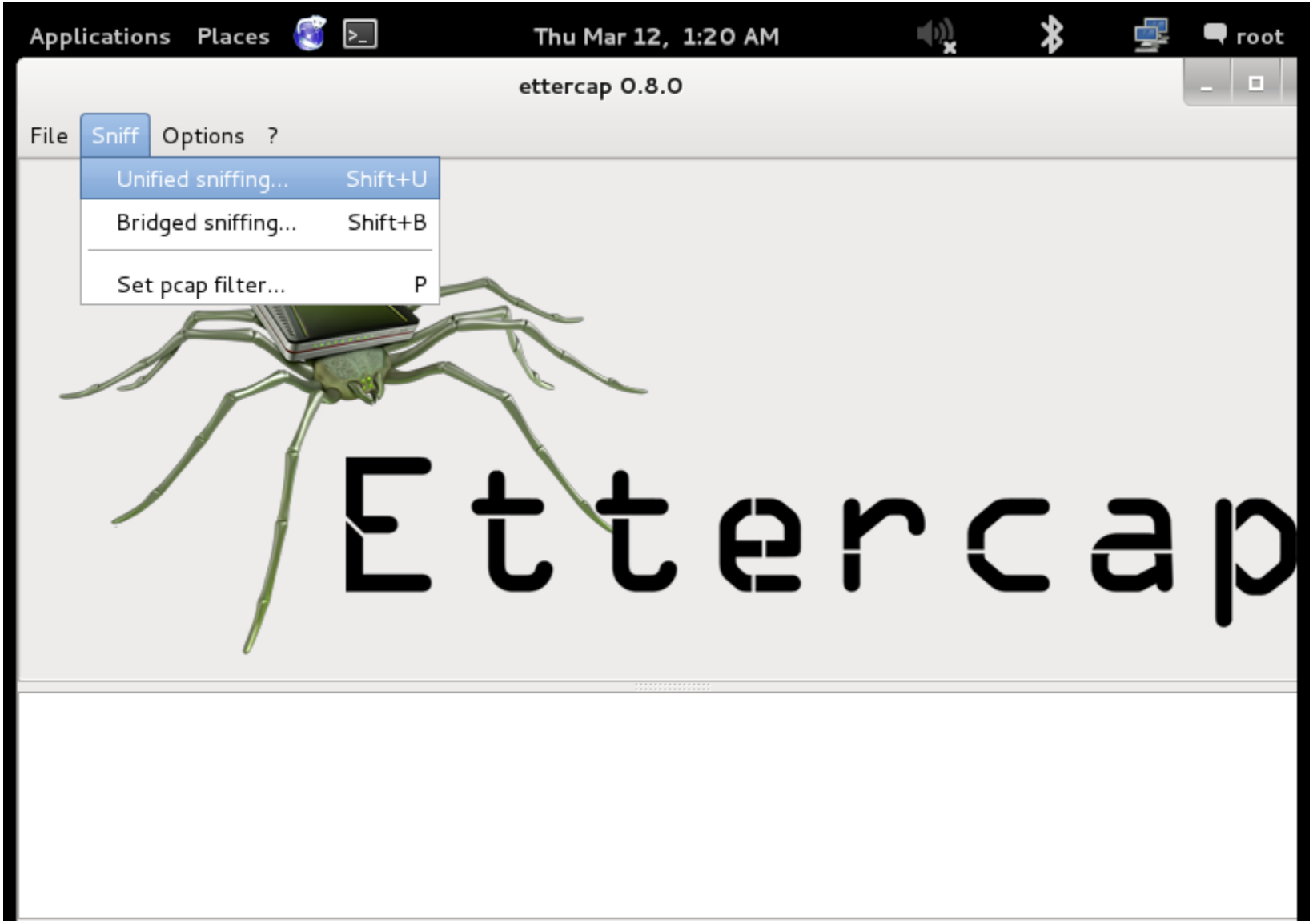


A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet

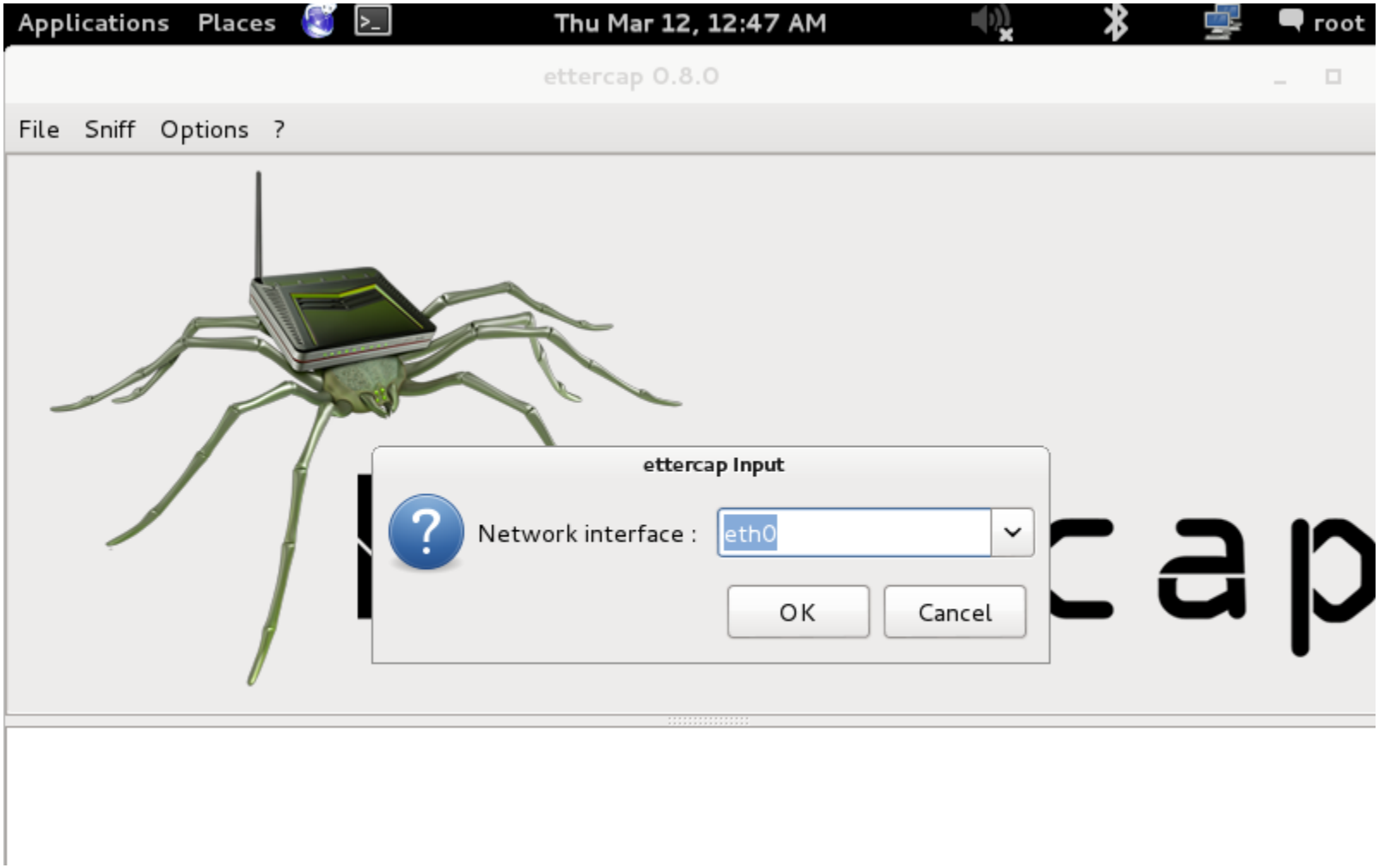
Decode Information

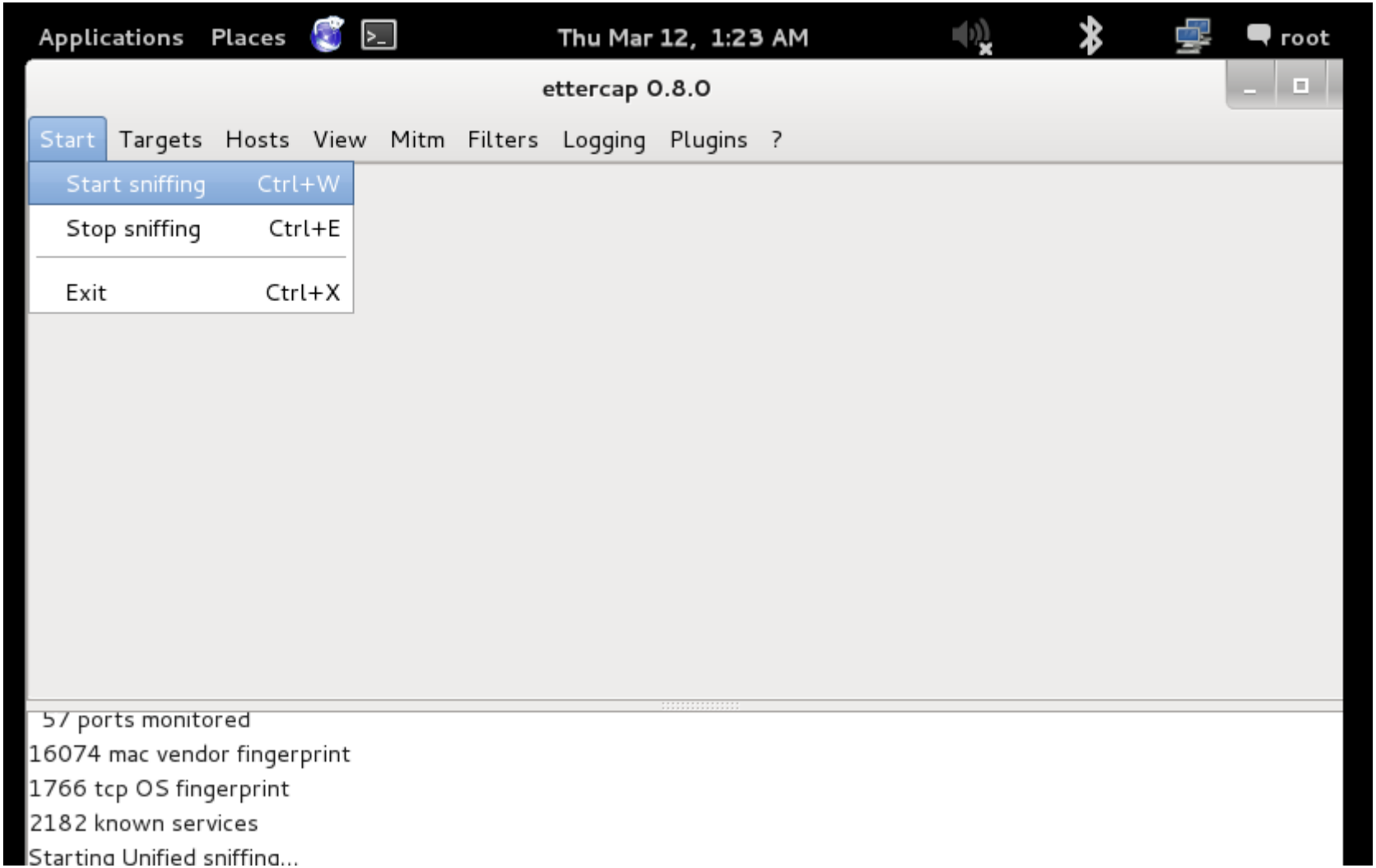
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

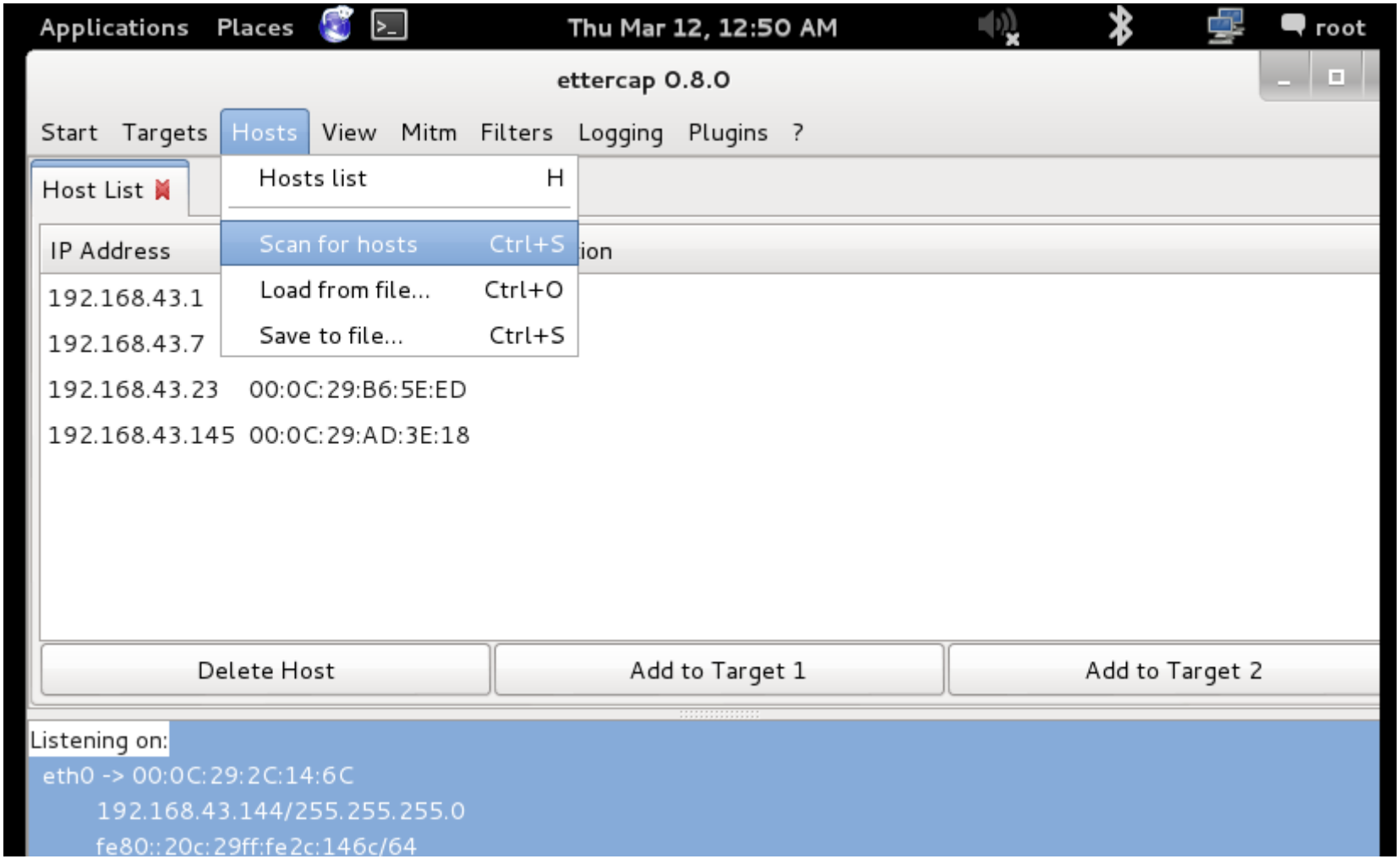
SNIFER en kali ettercap



Seleccionar la interfaz para toda la red




Applications
Places
Thu Mar 12, 1:23 AM
root
ettercap 0.8.0
Start
Targets
Hosts
View
Mitm
Filters
Logging
Plugins
?
Start sniffing Ctrl+W
Stop sniffing Ctrl+E
Exit Ctrl+X
57 ports monitored
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Starting Unified sniffing...


Applications Places
Thu Mar 12, 12:50 AM
root
ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Host List
Hosts list H
Scan for hosts Ctrl+S
Load from file... Ctrl+O
Save to file... Ctrl+S
IP Address
192.168.43.1
192.168.43.7
192.168.43.23 00:0C:29:B6:5E:ED
192.168.43.145 00:0C:29:AD:3E:18
Delete Host
Add to Target 1
Add to Target 2
Listening on:
eth0 -> 00:0C:29:2C:14:6C
192.168.43.144/255.255.255.0
fe80::20c:29ff:fe2c:146c/64

Applications Places Thu Mar 12, 12:57 AM root

ettercap 0.8.0

Output: Muted
ES1371 [AudioPCI-97] Analog Stereo

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List | Connections | Statistics

Host	Port	-	Host	Port	Proto	State	Bytes
192.168.43.144	46856	-	192.168.43.145	23	T	idle	146
192.168.43.145	138	-	192.168.43.255	138	U	idle	459
192.168.43.144	40029	-	192.168.43.1	53	U		
192.168.43.144	39559	-	192.168.43.1	53	U		
192.168.43.144	43611	-	192.168.43.1	53	U		
192.168.43.144	46073	-	192.168.43.1	53	U		
192.168.43.144	54807	-	192.168.43.1	53	U		

View Details Kill Connec

Connection Details (as nobody)

Source MAC address : 00:0C:29:2C:14:6C
Destination MAC address : 00:0C:29:AD:3E:18

Source IP address : 192.168.43.144
Destination IP address : 192.168.43.145

Protocol: TCP
Source port: 46856
Destination port: 23 telnet

Transferred bytes: 1469

Close

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Starting Unified sniffing...

root@kali: ~ | ettercap 0.... | [root@kali: ~] | [root@kali: ... | Connection ...

Applications Places Thu Mar 12, 1:08 AM root

ettercap 0.8.0

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List | Connections | Statistics | Profiles

IP Address	Hostname
23.201.103.90	api.bing.com
204.79.197.200	www.bing.com
54.225.181.150	ping.chartbeat.net
131.253.61.98	login.live.com
108.162.232.201	ocsp.msocsp.com
63.245.216.132	addons.mozilla.org
205.234.175.175	crl4.digicert.com
63.245.217.115	blocklist.addons.mozilla.org
208.80.154.234	bits.wikimedia.org
208.80.154.240	upload.wikimedia.org

Purge Local | Purge Remote | Convert to Host List | Dump to File

Listening on:
eth0 -> 00:0C:29:2C:14:6C
192.168.43.144/255.255.255.0
fe80::20c:29ff:fe2c:146c/64

Applications Places Thu Mar 12, 1:18 AM root

Click to view your appointments and tasks

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List | Connections | Statistics | Profiles | Connection data

Host	Port	-	Host	Port	Proto	State	Bytes
192.168.43.144	47160	-	192.168.43.145	23	T	closed	143
192.168.43.144	47161	-	192.168.43.145	23	T	idle	175
192.168.43.23	138	-	192.168.43.255	138	U	idle	201
192.168.43.7	68	-	255.255.255.255	67	U	idle	600
192.168.43.7	64738	-	224.0.0.252	5355	U	idle	44
192.168.43.7	137	-	192.168.43.255	137	U	active	2250
192.168.43.7	52491	-	224.0.0.252	5355	U	idle	44
192.168.43.7	60840	-	224.0.0.252	5355	U	idle	44
192.168.43.7	56432	-	224.0.0.252	5355	U	idle	44
192.168.43.7	55543	-	224.0.0.252	5355	U	idle	44

View Details | Kill Connection | Expunge Connections

DHCP: [192.168.43.1] ACK : 0.0.0.0 255.255.255.0 GW 192.168.43.1 DNS 192.168.43.1

Unified sniffing was stopped.

Applications Places Thu Mar 12, 1:16 AM root

ettercap 0.8.0

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List | Connections | Statistics | Profiles | Connection data

192.168.43.144:47161

```
........... ..!.."..'.....#....P...... .38
400,38400....#.localhost:0.0....'..DISPLA
Y.localhost:0.0......xterm........msfadmi
n..msadmin..msa.fadmin..msfadmin..ls..cd v
ul       ..ls..
```

192.168.43.145:23

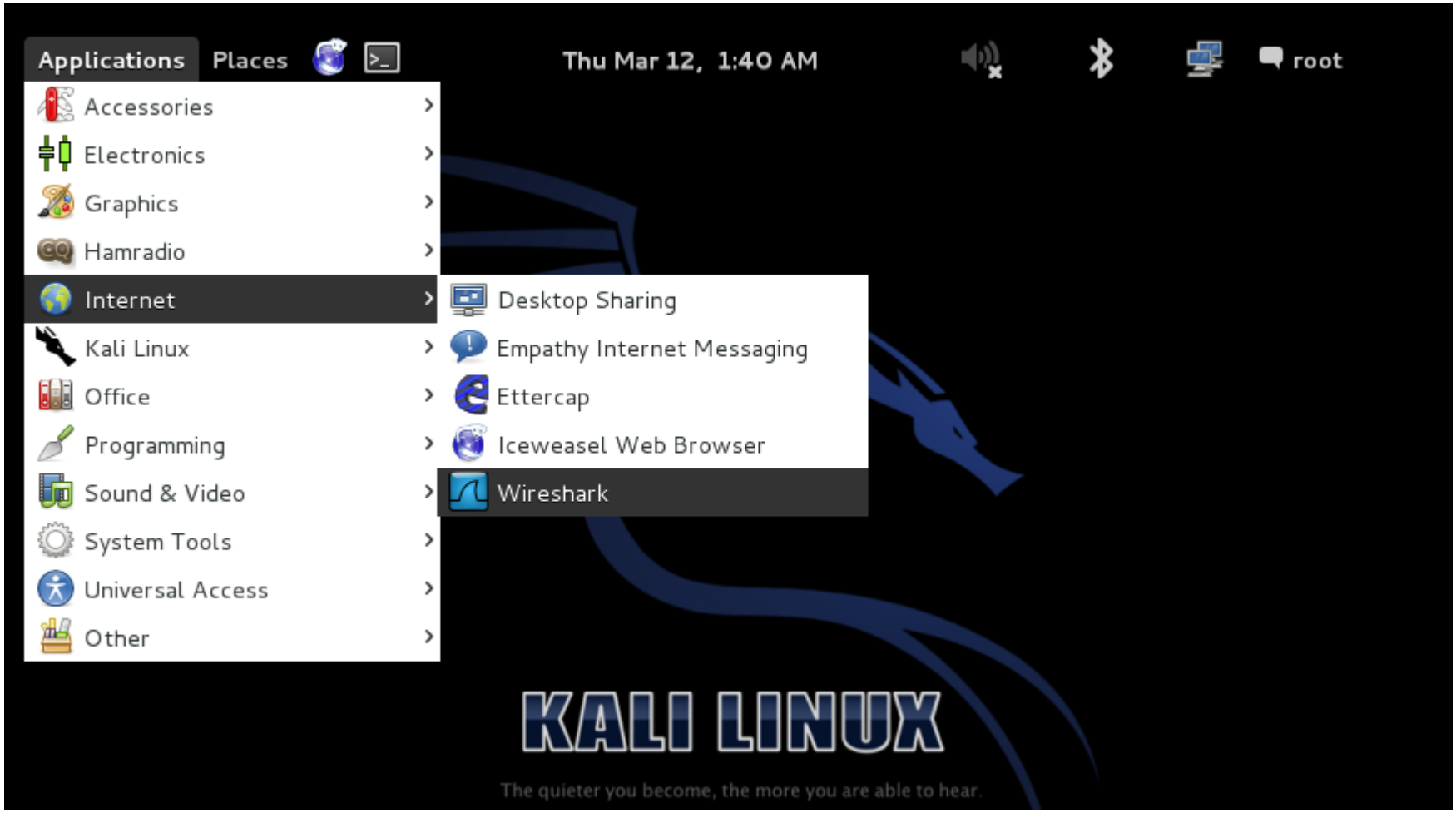
```
.
To access official Ubuntu documentatio
n, please visit:.
http://help.ubuntu.com/.
No mail..
msfadmin@metasploitable:~$ ls.
puertos  vulnerable.
msfadmin@metasploitable:~$ cd vulnerabl
e/.
msfadmin@metasploitable:~/vulnerable$ l
s.
mysql-ssl  samba  tikiwiki  twiki2003020
1.
msfadmin@metasploitable:~/vulnerable$
```

Join Views | Inject Data | Inject File | Kill Connection

DHCP: [192.168.43.1] ACK : 0.0.0.0 255.255.255.0 GW 192.168.43.1 DNS 192.168.43.1

Unified sniffing was stopped.

Wireshark desde Kali



Applications Places Thu Mar 12, 1:42 AM root

Wireshark: Capture Interfaces

Device	Description	IP	Packets	Packets/s
eth0		192.168.43.144	1	1
nflog		none	0	0
any		none	1	1
lo		127.0.0.1	0	0

Help Start Stop Options Close

Tools Internals Help

Expression... Clear Apply Save

ar Network Protocol Analy

4 from /trunk-1.10)

Files

Interface List

Live list of the capture interfaces
(counts incoming packets)

Start

Choose one or more interfaces to capture from, then **Start**

eth0
nflog
any

Open

Open a previously captured file

Open Recent:

Sample Captures

A rich assortment of example capture files on the wik

Ready to load or capture | No Packets | Profile: Default

[root@k... [root@k... [root@k... [La Pren... The Wir... Wiresha...

Wireshark desde Kali

Hacer un telnet al server

root@kali: ~

Output: Muted
ES1371 [AudioPCI-97] Analog Stereo

File Edit View Search Terminal Help

```
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Mar 11 17:26:25 EDT 2015 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
root@kali:~# telnet 192.168.43.145
```

Wireshark desde Kali

Applications Places Thu Mar 12, 1:48 AM root

Capturing from eth0 [Wireshark 1.10.2 (SVN Rev 51

Output: Muted
ES1371 [AudioPCI-97] Analog Stereo

File Edit View Go Capture Analyze Statistics Telepho

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
4	8.916786000	23.23.102.174	192.168.43.144	TCP	66	http > 370
5	13.38615500(	bc:f5:ac:a3:35:71	Vmware_2c:14:6c	ARP	60	Who has 19
6	13.38621300(	Vmware_2c:14:6c	bc:f5:ac:a3:35:71	ARP	42	192.168.43
7	18.72382200(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat
8	18.72483800(	192.168.43.145	192.168.43.144	TELNET	67	Telnet Dat
9	18.72488300(	192.168.43.144	192.168.43.145	TCP	66	47291 > te
10	18.99341100(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat

Ethernet II, Src: Vmware_2c:14:6c (00:0c:29:2c:14:6c), Dst: Vmware_ad:3e:18 (00:0c:29:ad:
Internet Protocol Version 4, Src: 192.168.43.144 (192.168.43.144), Dst: 192.168.43.145 (1
Transmission Control Protocol, Src Port: 47291 (47291), Dst Port: telnet (23), Seq: 1, Ac

```
0000  00 0c 29 ad 3e 18 00 0c  29 2c 14 6c 08 00 45 10   ..).>... ),.l..E.
0010  00 35 38 23 40 00 40 06  2a 1e c0 a8 2b 90 c0 a8   .58#@.@. *...+...
0020  2b 91 b8 bb 00 17 74 77  2f 44 09 3e 86 11 80 18   +.....tw /D.>....
0030  00 1f a7 88 00 00 01 01  08 0a 00 0e 00 68 00 0b   ........ .....h..
0040  a5 3b 65                                           .;e
```

eth0: <live capture in progress> Fil... Packets: 141 · Display... Profile: Default

Wireshark desde Kali, aplicar filtro

Applications Places Thu Mar 12, 1:50 AM root

Capturing from eth0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: telnet Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Lengtl	Info
7	18.72382200(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat
8	18.72483800(	192.168.43.145	192.168.43.144	TELNET	67	Telnet Dat
10	18.99341100(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat
11	18.99428800(	192.168.43.145	192.168.43.144	TELNET	67	Telnet Dat
13	19.21685800(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat
14	19.21783000(	192.168.43.145	192.168.43.144	TELNET	67	Telnet Dat
16	19.38151900(	192.168.43.144	192.168.43.145	TELNET	67	Telnet Dat
17	19.38259600(	192.168.43.145	192.168.43.144	TELNET	67	Telnet Dat

Ethernet II, Src: Vmware_2c:14:6c (00:0c:29:2c:14:6c), Dst: Vmware_ad:3e:18 (00:0c:29:ad:

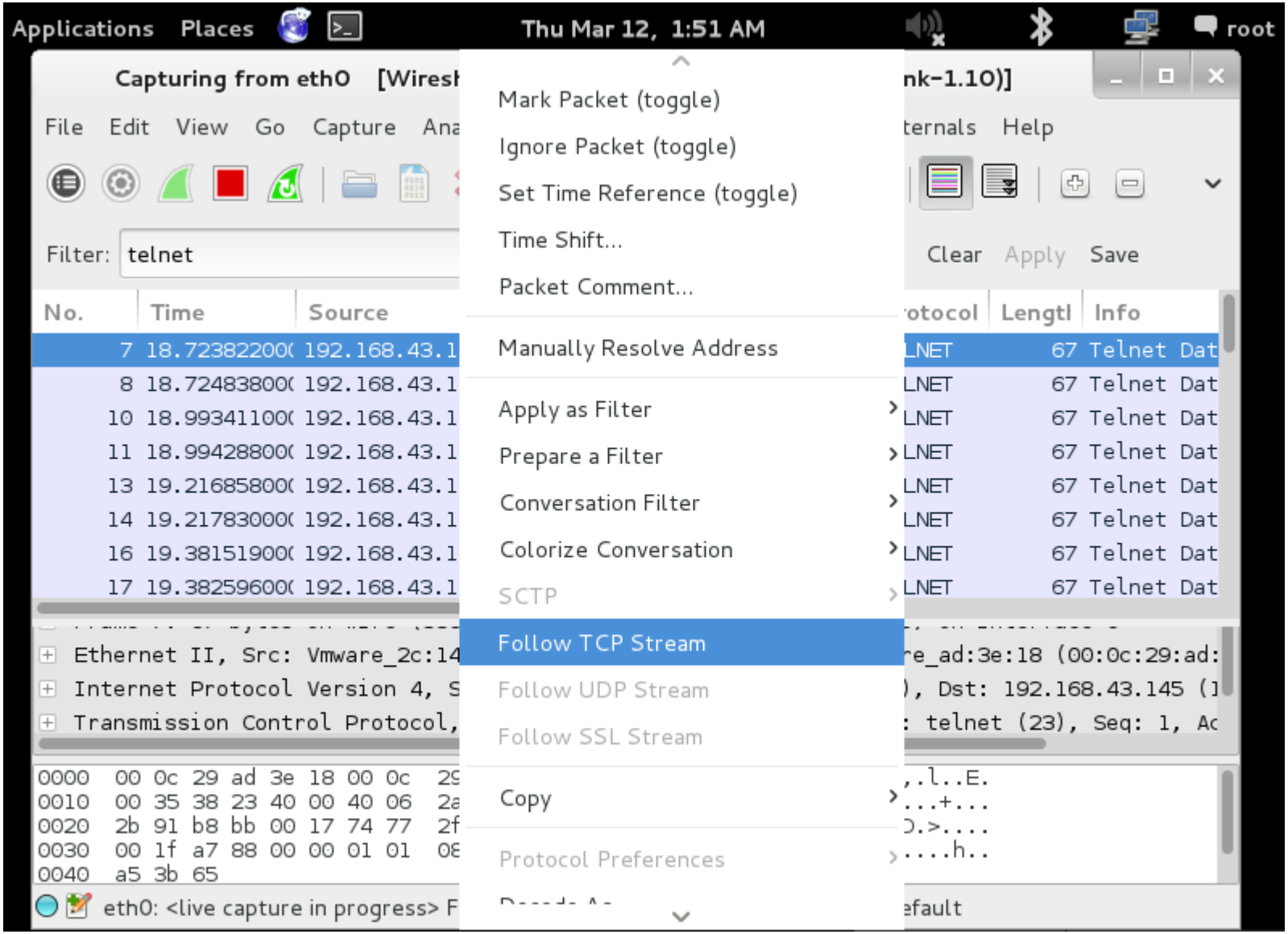
Internet Protocol Version 4, Src: 192.168.43.144 (192.168.43.144), Dst: 192.168.43.145 (1

Transmission Control Protocol, Src Port: 47291 (47291), Dst Port: telnet (23), Seq: 1, Ac

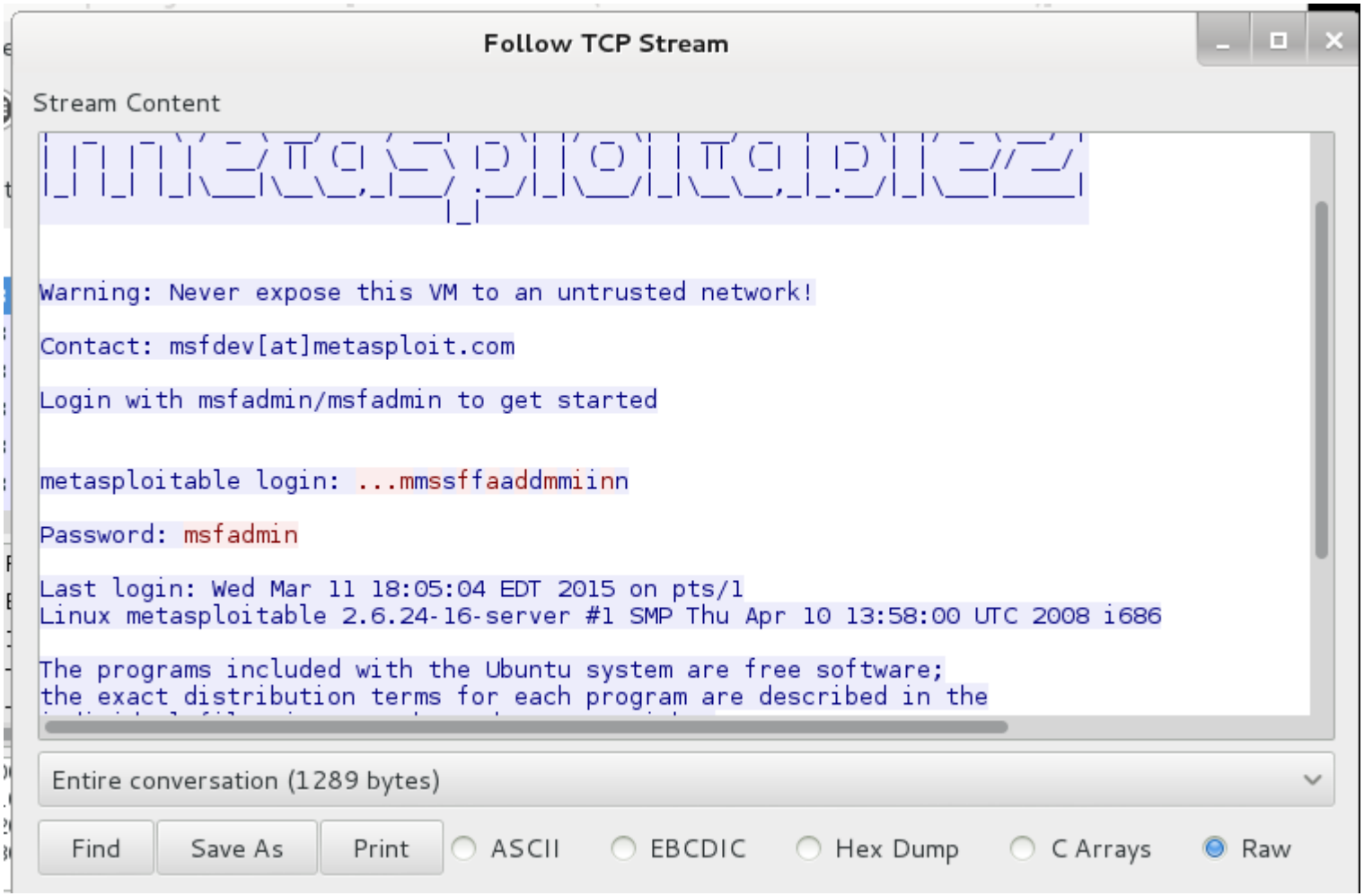
```
0000  00 0c 29 ad 3e 18 00 0c  29 2c 14 6c 08 00 45 10   ..).>... ),.l..E.
0010  00 35 38 23 40 00 40 06  2a 1e c0 a8 2b 90 c0 a8   .58#@.@. *...+...
0020  2b 91 b8 bb 00 17 74 77  2f 44 09 3e 86 11 80 18   +.....tw /D.>....
0030  00 1f a7 88 00 00 01 01  08 0a 00 0e 00 68 00 0b   ........ .....h..
0040  a5 3b 65                                           .;e
```

eth0: <live capture in progress> Fil... Packets: 163 · Display... Profile: Default

Wireshark desde Kali



Wireshark desde Kali



telnet-cooked.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0 | Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	3m-image-lm > telnet
2	0.002525	192.168.0.1	192.168.0.2	TCP	74	telnet > 3m-image-lm
3	0.002572	192.168.0.2	192.168.0.1	TCP	66	3m-image-lm > telnet
4	0.004160	192.168.0.2	192.168.0.1	TELNET	93	Telnet Data ...
5	0.150335	192.168.0.1	192.168.0.2	TELNET	69	Telnet Data ...
6	0.150402	192.168.0.2	192.168.0.1	TCP	66	3m-image-lm > telnet
7	0.150574	192.168.0.2	192.168.0.1	TELNET	69	Telnet Data ...
8	0.151946	192.168.0.1	192.168.0.2	TCP	66	telnet > 3m-image-lm
9	0.153657	192.168.0.1	192.168.0.2	TELNET	91	Telnet Data ...
10	0.153865	192.168.0.2	192.168.0.1	TELNET	130	Telnet Data ...
11	0.154984	192.168.0.1	192.168.0.2	TCP	66	telnet > 3m-image-lm
12	0.155577	192.168.0.1	192.168.0.2	TELNET	84	Telnet Data ...
13	0.155656	192.168.0.2	192.168.0.1	TELNET	75	Telnet Data ...
14	0.156646	192.168.0.1	192.168.0.2	TCP	66	telnet > 3m-image-lm
15	0.159016	192.168.0.1	192.168.0.2	TELNET	90	Telnet Data ...

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Lite-OnC_3b:bf:fa (00:a0:cc:3b:bf:fa), Dst: WesternD_9f:
Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.
Transmission Control Protocol, Src Port: 3m-image-lm (1550), Dst Port: tel

```
0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08 00 45 10   ........ .;....E.
0010  00 3c 46 3c 40 00 40 06  73 1c c0 a8 00 02 c0 a8   .<F<@.@. s.......
0020  00 01 06 0e 00 17 99 c5  a0 ec 00 00 00 00 a0 02   ........ ........
0030  7d 78 e0 a3 00 00 02 04  05 b4 04 02 08 0a 00 9c   }x...... ........
0040  27 24 00 00 00 00 01 03  03 00                     '$...... ..
```

File "C:\Users\admin\Desktop\telnet-cooke... | Packets: 92 Displayed... | Profile: Default

Follow TCP Stream

Stream Content

```
..........  ..!..".. '.....#..%..
%..........  ..!..".. ".........P. ....".....b........b.....B.
.......................".....'.....#..&..&..$..&..&..
$.. .....#.....'........... .9600,9600....#.bam.zing.org:0.0....'..DISPLAY.ba
m.zing.org:0.0......xterm-color.............!..............".............
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:4
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 1

Welcome to OpenBSD: The proactively

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.

$ /sbin/ping www.yahoo.com
PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms
..........
.--- www.yahoo.com ping statistics ---
```

Password revealed in TCP Stream

Entire conversation (1634 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Filter Out This Stream | Close

Macof para inundar un sw

```
Click to view your appointments and tasks
File  Edit  View  Search  Terminal  Help
135605711(0) win 512
53:ed:ad:49:25:62 81:a2:fc:58:51:ee 0.0.0.0.28707 > 0.0.0.0.49879: S 945537655:
945537655(0) win 512
75:84:88:60:29:9d 3b:5:8d:3a:a1:2e 0.0.0.0.5023 > 0.0.0.0.26708: S 379561313:37
9561313(0) win 512
e4:d6:a8:6c:de:ad 55:2a:d5:1f:93:10 0.0.0.0.63334 > 0.0.0.0.24572: S 1838368509
:1838368509(0) win 512
32:20:fc:2a:91:6b 48:e7:c3:2d:ab:c6 0.0.0.0.43609 > 0.0.0.0.51718: S 1460934066
:1460934066(0) win 512
e7:8:3:3b:c4:d1 6e:48:e8:79:b3:83 0.0.0.0.60187 > 0.0.0.0.37893: S 1567634483:1
567634483(0) win 512
bb:21:d:6f:31:55 c8:ae:33:26:f3:5a 0.0.0.0.55085 > 0.0.0.0.56618: S 1495918327:
1495918327(0) win 512
83:24:8e:6b:4f:b e2:22:6d:54:1d:25 0.0.0.0.53003 > 0.0.0.0.31829: S 523205642:5
23205642(0) win 512
f8:b:89:15:23:df c7:57:d0:35:d7:63 0.0.0.0.36135 > 0.0.0.0.19955: S 999745131:9
99745131(0) win 512
dd:10:33:64:cb:32 5:b9:f6:3a:b:ca 0.0.0.0.43568 > 0.0.0.0.25836: S 2112239877:2
112239877(0) win 512
5f:ea:4a:6:fc:c6 35:5f:6c:16:f9:67 0.0.0.0.14635 > 0.0.0.0.15141: S 288436929:2
88436929(0) win 512
de:ce:19:28:73:65 38:27:51:c:8f:84 0.0.0.0.4749 > 0.0.0.0.22131: S 717142420:71
7142420(0) win 512
^Croot@kali:~# macof -i eth0
```

ICMP Ping

```
hping3 -1 10.0.0.25
```

ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 -s
```

Firewalls and Time Stamps

```
hping3 -S 72.14.207.99 -p 80 --
tcp-timestamp
```

SYN scan on port 50-60

```
hping3 -8 50-56 -S 10.0.0.25 -V
```

FIN, PUSH and URG scan on port 80

```
hping3 -F -p -U 10.0.0.25 -p 80
```

Scan entire subnet for live host

```
hping3 -1 10.0.1.x --rand-dest
-I eth0
```

Intercept all traffic containing HTTP signature

```
hping3 -9 HTTP -I eth0
```

SYN flooding a victim

```
hping3 -S 192.168.1.1 -a
192.168.1.254 -p 22 --flood
```