Faculdade de Tecnologia SENAC Goiás

Segurança da Informação

Aldo Brito da Costa Filho

Levi Souza

Matheus Marçal

Matheus Oliveira

Relatório estatístico sobre o ataque MITM

Goiânia

2015

Aldo Brito

Levi Souza

Matheus Marçal

Matheus Oliveira

Relatório estatístico sobre o ataque MITM

Relatorio estatístico sobre o ataque MTIM desenvolvido no curso de Segurança da Informação, da Faculdade de Tecnologia SENAC Goiás para o Projeto Integrador do 2° Período

Goiânia

2015

Sumário

1. Introdução

Neste relatório vamos apresentar uma estatística de quantos hosts foram envenenados, quantos hosts foram afetados pelo ataque MITM, throughput de pacotes ARP do atacante e se o servidor com proteção foi afetado pelo ataque.

2. Total de hosts Envenenados

O host envenenado é o host que sofreu o ataque direto do atacante na realização do ataque.

Na rede em que fizemos o ataque, o host envenenado foi:

Nmap scan report for 192.168.1.120

Host is up (0.00057s latency).

MAC Address: 50:E5:49:F7:07:BA (Giga-byte Technology Co.)

Device type: general purpose

Running: Microsoft Windows 7|2008

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8

Network Distance: 1 hop

3. Total de hosts afetados

Os hosts afetados são os que estavam na rede mas não sofreram o ataque do invasor.

No total foram 17 hosts afetados pelo ataque

root@kali:~# nmap -sS -O 192.168.1.0/24

Starting Nmap 6.47 (http://nmap.org) at 2015-12-02 21:40 BRST

Nmap scan report for 192.168.1.1

Host is up (0.00071s latency).

Nmap scan report for 192.168.1.2

Host is up (0.00036s latency).

Nmap scan report for 192.168.1.105

Host is up (0.0013s latency).

Nmap scan report for 192.168.1.107

Host is up (0.00055s latency).

Nmap scan report for 192.168.1.113

Host is up (0.0019s latency).

Nmap scan report for 192.168.1.117

Host is up (0.00050s latency).

Nmap scan report for 192.168.1.120

Host is up (0.00057s latency).

Nmap scan report for 192.168.1.135

Host is up (0.00068s latency).

Nmap scan report for 192.168.1.138

Host is up (0.00044s latency).

Nmap scan report for 192.168.1.141

Host is up (0.00064s latency).

Nmap scan report for 192.168.1.142

Host is up (0.00052s latency).

Nmap scan report for 192.168.1.156

Host is up (0.0010s latency).

Nmap scan report for 192.168.1.166

Host is up (0.00030s latency).

Nmap scan report for 192.168.1.171

Host is up (0.00050s latency).

Nmap scan report for 192.168.1.174

Host is up (0.00044s latency).

Nmap scan report for 192.168.1.183

Host is up (0.00042s latency).

Nmap scan report for 192.168.1.194

Host is up (0.00037s latency).

Nmap scan report for 192.168.1.198

Host is up (0.00040s latency).

#Máquina do atacante

Nmap scan report for 192.168.1.129

Host is up (0.000025s latency).

Network Distance: 0 hops

4. Lista de endereços MAC afetados

root@kali:~# nmap -sS -O 192.168.1.0/24

Starting Nmap 6.47 (http://nmap.org) at 2015-12-02 21:40 BRST

Nmap scan report for 192.168.1.1

MAC Address: F8:B1:56:73:E4:3D (Dell)

Nmap scan report for 192.168.1.2

MAC Address: 50:E5:49:FA:F0:9A (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.105

MAC Address: 00:23:5D:5C:A1:C0 (Cisco Systems)

Nmap scan report for 192.168.1.107

MAC Address: 50:E5:49:FA:F1:DD (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.113

MAC Address: 74:29:AF:65:5B:D5 (Unknown)

Nmap scan report for 192.168.1.117

MAC Address: 80:FA:5B:0C:72:05 (Clevo CO.)

Nmap scan report for 192.168.1.120

MAC Address: 50:E5:49:F7:07:BA (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.135

MAC Address: 50:E5:49:F8:39:1F (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.138
MAC Address: 08:00:27:B3:9D:2A (Cadmus Computer Systems)

Nmap scan report for 192.168.1.141
MAC Address: 50:E5:49:F6:2D:D3 (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.142
MAC Address: 08:00:27:22:B0:8E (Cadmus Computer Systems)

Nmap scan report for 192.168.1.156
MAC Address: 50:E5:49:F7:0F:68 (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.166
MAC Address: 50:E5:49:FA:CC:9F (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.171
MAC Address: 08:00:27:25:6B:FD (Cadmus Computer Systems)

Nmap scan report for 192.168.1.174
MAC Address: 50:E5:49:FA:F0:D9 (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.183
MAC Address: 50:E5:49:F6:33:5F (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.194
MAC Address: 90:2B:34:F5:18:82 (Giga-byte Technology Co.)

Nmap scan report for 192.168.1.198
MAC Address: 50:E5:49:F3:49:3F (Giga-byte Technology Co.)

5. Throughput de pacotes ARP do atacante

O throughput (taxa de transferência) dos pacotes ARP do atacante foi registrada com a utilização do sniffer de rede Wireshark e ficou da seguinte forma:

1378	883.9656780(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1379	884.4110300(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1380	884.6199570(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1381	885.4102510(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1382	885.9657880(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1383	886.4102370(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1384	886.6200640(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1385	887.9659390(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1386	888.6202210(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1387	889.4156290(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1388	889.4182410(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	Who has 192.168.1.120? Tell 192.168.1.153
1389	889.4188500(	Giga-Byt_f7:07:ba	Giga-Byt_f7:0a:93	ARP	60	192.168.1.120 is at 50:e5:49:f7:07:ba
1390	889.9660470(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1391	890.4142820(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1392	890.6203790(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1393	890.6967470(	Giga-Byt_f8:3b:2e	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.149
1394	891.4142370(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1395	891.9661670(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1396	892.6205250(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1397	893.7286510(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153
1398	893.9663060(	Giga-Byt_f7:0a:93	Giga-Byt_f7:07:ba	ARP	42	192.168.1.107 is at 50:e5:49:f7:0a:93
1399	894.6206670(	Giga-Byt_f7:0a:93	Giga-Byt_fa:f1:dd	ARP	42	192.168.1.120 is at 50:e5:49:f7:0a:93 (dup
1400	894.7262670(	Giga-Byt_f7:0a:93	Broadcast	ARP	42	Who has 192.168.1.107? Tell 192.168.1.153

6. Ataque no servidor

Foi realizado um ataque no servidor Linux para ver se a defesa estava funcionando e obtivemos o seguinte resultado

```
root@PC-XXXX: ~
root@PC-XXXX: ~    root@PC-XXXX: ~    root@PC-XXXX: ~
         src IP = <192.168.1.120>
21:53:11 ARP cache, DENY
         src HW = <50:e5:49:f7:a:93>
         src IP = <192.168.1.120>
21:53:11 ARP cache, ACCEPT
         src HW = <50:e5:49:f7:7:ba>
         src IP = <192.168.1.120>
21:53:13 ARP cache, DENY
         src HW = <50:e5:49:f7:a:93>
         src IP = <192.168.1.120>
21:53:13 ARP cache, ACCEPT
         src HW = <50:e5:49:f7:7:ba>
         src IP = <192.168.1.120>
21:53:15 ARP cache, DENY
         src HW = <50:e5:49:f7:a:93>
         src IP = <192.168.1.120>
21:53:15 ARP cache, ACCEPT
         src HW = <50:e5:49:f7:7:ba>
         src IP = <192.168.1.120>
21:53:17 ARP cache, DENY
         src HW = <50:e5:49:f7:a:93>
         src IP = <192.168.1.120>
21:53:17 ARP cache, ACCEPT
         src HW = <50:e5:49:f7:7:ba>
```

O endereço MAC 50:e5:49:f7:a:93 pertence ao atacante e o servidor conseguiu negar suas requisições.