Wireless Sniffing com Scapy

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

Segurança em Redes Sem Fio

A segurança é um ponto fraco das redes sem fio pois o sinal propaga-se pelo ar em todas as direções e pode ser captado a distâncias de centenas de metros utilizando qualquer dispositivo com interface de rede sem fio o que torna as redes sem fio inerentemente vulneráveis à interceptação.

Nesta aula, você aprenderá a descobrir os endereços MAC de todos os dispositivos que estão em sua proximidade, inclusive dos pontos de acesso que estão utilizando rede Wi-Fi.

Para isso será necessário instalar os seguintes componentes em sua máquina:

- sudo apt-get install aircrack-ng
- sudo pip install termcolor
- sudo apt-get install python-scapy

Modo Monitor da Interface de Rede Wi-Fi

Modo Monitor, também chamado de Modo de **Monitoramento** ou modo RFMON, permite que um computador com uma placa com interface de rede wireless (WNIC) realize monitoramento de todo o tráfego recebido da rede wireless.

Diferente do modo **promíscuo**, que também é utilizado para sniffar pacote, o modo monitor permite que pacotes sejam capturados sem precisar de associação com um Ponto de Acesso ou rede Ad-hoc primeiro.

Modo monitor cabe apenas às redes wireless, enquanto modo promíscuo pode ser usado em redes cabeadas. Este modo é um dos quatro modos que placas wireless 802.11 podem operar: Master ou **Mestre** (age como um Ponto de Acesso), **Gerenciado** (cliente, também conhecido como estação), **Ad-Hoc** e **Monitor**.

Habilitando o modo monitor da interface wireless

```
tim@charles:~$ sudo airmon-ng start wlp3s0


Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
901     avahi-daemon
911     avahi-daemon
1015    NetworkManager
2087    wpa_supplicant
3427    dhclient
Process with PID 3427 (dhclient) is running on interface wlp3s0


Interface       Chipset         Driver

wlp3s0          Atheros AR9485  ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

Entendendo o Script

Abaixo temos a importação dos módulo **scapy** necessário para trabalhar com a rede wifi, **termcolor** para imprimir colorido a saida no terminal.

```
1  #!/usr/bin/env python
2  import logging
3  from scapy.all import *
4  from termcolor import colored, cprint
5  import argparse
6  import datetime
7  import sys
8
9  mac_list = []
10 interface = "mon0"
```

Após a habilitação do modo Monitor da rede sem fio, foi definido a interface **mon0** para trabalharmos com sniffen de pacotes.

Entendendo o Script

Abaixo temos a função **analisadorPacotes** que é executado a todo novo pacote capturado pela interface **mon0**.

```
20 def analisadorPacote(pacote):
21
22     if pacote.haslayer(Dot11):
23         if pacote.type == 0 and pacote.subtype == 8:
24             if pacote.addr2 not in mac_list:
25                 mac_list.append(pacote.addr2)
26                 imprimirPontoAcesso(pacote.addr2, pacote.info)
27
28         if pacote.haslayer(Dot11ProbeReq):
29             if pacote.addr2 not in mac_list:
30                 mac_list.append(pacote.addr2)
31                 if pacote.info != "":
32                     imprimirCliente(pacote.addr2, pacote.info)
33
34 sniff(iface=interface, prn=analisadorPacote, store=0)
```

Com **Dot11** é certificado se o pacote é 802.11. **type** 0 e **subtype** 8 indicam que o pacote é direcionado a um ponto de acesso.

Entendendo o Script

Abaixo temos a função **imprimirPontoAcesso** que imprime as informações de um pacote do Ponto de Acesso.

```
12 def imprimirPontoAcesso(mac, ssid):
13     print colored("* Encontrado * ", "red", \
14      attrs=["bold"]) + "%s" % (mac), \
15      colored("Ponto de Acesso", "yellow", \
16      attrs=["bold"]), "do SSID:", \
17      colored(ssid, "green", attrs=["bold"])
18
19 def imprimirCliente(mac, ssid):
20     print colored("* Encontrado * ", "red", \
21      attrs=["bold"]) + "%s" % (mac), \
22      colored("Cliente", "yellow", \
23      attrs=["bold"]), "do SSID:", \
24      colored(ssid, "green", attrs=["bold"])
```

A função **imprimirCliente** imprime as informações de um Cliente.

INSTITUTO FEDERAL

Execução do Script

Para executar o script é necessário dar permissão de administrador ou executar com **sudo**. Segue uma saída do script.

```
tim@charles:~$ sudo python wifi.py
* Encontrado * 90:f6:52:5a:13:ba Ponto de Acesso do SSID: cartman
* Encontrado * 10:7b:44:82:92:39 Ponto de Acesso do SSID: My ASUS
* Encontrado * 00:1e:58:24:23:5b Ponto de Acesso do SSID: IFSPCJO
* Encontrado * 48:74:6e:b1:4d:d4 Cliente do SSID: Moto G Play 7313
* Encontrado * 5c:c9:d3:42:7e:ff Cliente do SSID: cartman
* Encontrado * f0:db:f8:ab:a3:3a Cliente do SSID: IFSPCJO
* Encontrado * 5c:c9:d3:1e:46:84 Cliente do SSID: IFSPCJO
* Encontrado * 14:d6:4d:27:49:40 Ponto de Acesso do SSID: SALA 14
* Encontrado * 30:cb:f8:66:7e:15 Cliente do SSID: IFSPCJO
* Encontrado * 32:96:a9:a3:4b:66 Cliente do SSID: Luiz.
* Encontrado * d8:9e:3f:02:d5:86 Cliente do SSID: cartman
* Encontrado * 98:39:8e:07:01:d7 Cliente do SSID: RV
* Encontrado * 5c:c9:d3:44:35:3b Cliente do SSID: IFSPCJO
* Encontrado * c4:6e:1f:bd:b3:f5 Ponto de Acesso do SSID: Wireless_Cassio
```

Na saída é possível ver os endereços MAC dos clientes conectados a um Ponto de Acesso e também os endereços MAC dos Pontos de Acesso.

Atividades

Você deverá construir um scritp que irá determinar aonde se encontra um dispositivo de uma determinada marca em um determinado local através de redes sem fio.

Para isso, você deverá executar as seguintes atividades.

- Faça uma busca na Internet e encontre arquivos **Vendors MAC** que contêm lista de endereços MAC referentes a diversas marcas (encontre uma base grande);
- Modifique o script apresentado na aula de forma que ele aceite como entrada uma determinada marca;
- O script então irá fazer uma varredura constantes nas redes sem fio de forma a encontrar MAC relacionado a marca;
- Ao encontrar imprima o endereço MAC, o nome completo da marca, e o Ponto de Acesso que o dispositivo está enviando;
- O script só para se o usuário finalizar o script.