WiFi Pumpkin

Information Security Inc.

iSEC
information security inc.

Contents

- About WiFi Pumpkin
- Features
- Testing Environment
- Installing WiFi Pumpkin
- Using WiFi Pumpkin
- References

About WiFi Pumpkin

- WiFi-Pumpkin is a very complete framework for auditing Wi-Fi security. The main feature is the ability to create a fake AP and make Man In The Middle attack

Features

- Rogue Wi-Fi Access Point
- Deauth Attack Clients AP
- Probe Request Monitor
- DHCP Starvation Attack
- Credentials Monitor
- Transparent Proxy
- Windows Update Attack
- Phishing Manager

Features

- ARP Poison
- DNS Spoof
- Patch Binaries via MITM
- Karma Attacks (support hostapd-mana)
- LLMNR, NBT-NS and MDNS poisoner (Responder)
- Pumpkin-Proxy (ProxyServer (mitmproxy API))
- Capture images on the fly

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/"
```

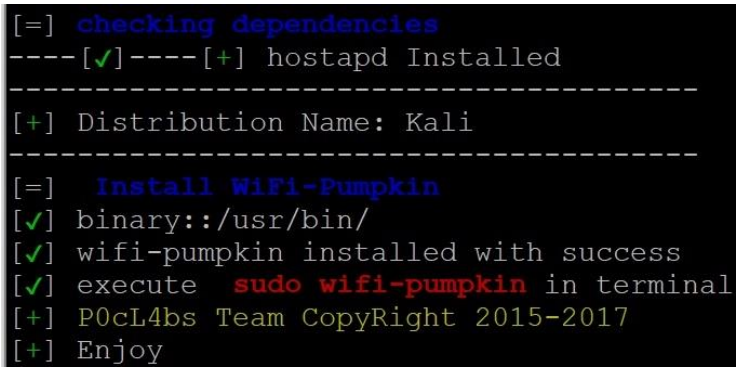
Installing WiFi Pumpkin

- Installing WiFi Pumpkin

```
git clone https://github.com/P0cL4bs/WiFi-Pumpkin.git
cd WiFi-Pumpkin/
./installer.sh --install
```

Installing WiFi Pumpkin

- Installing WiFi Pumpkin



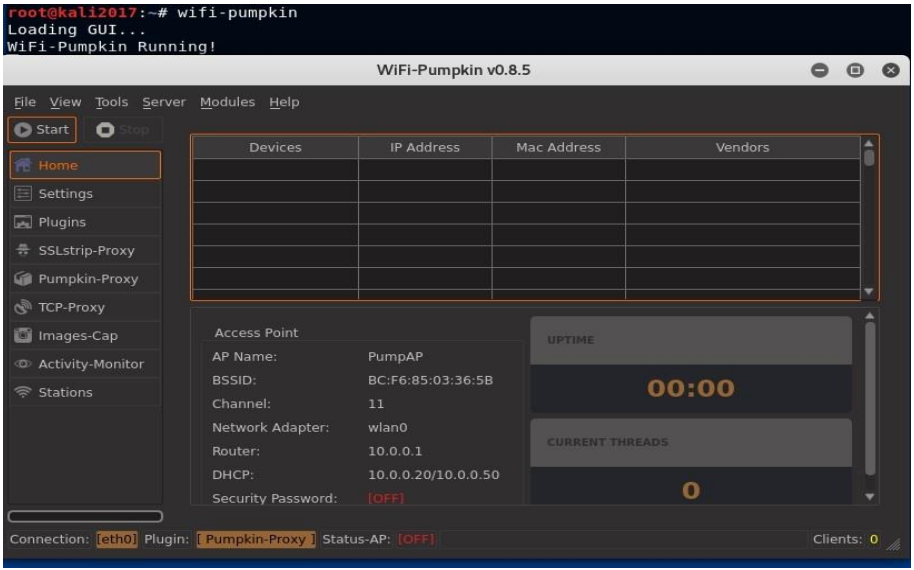
Installing WiFi Pumpkin

- Upgrading lxml

```
root@kali2017:~# pip install --upgrade lxml
Collecting lxml
  Downloading lxml-4.1.1-cp27-cp27mu-manylinux1_x86_64.whl (5.6MB)
    100% |████████████████████████████████| 5.6MB 298kB/s
Installing collected packages: lxml
  Found existing installation: lxml 3.6.0
    Uninstalling lxml-3.6.0:
      Successfully uninstalled lxml-3.6.0
Successfully installed lxml-4.1.1
```

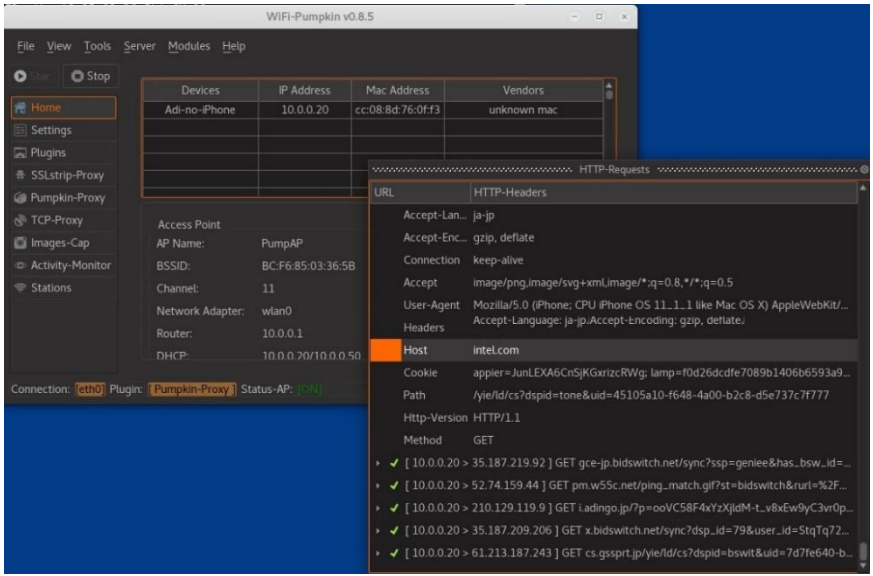
Using WiFi Pumpkin

- Running wifi-pumpkin



Using WiFi Pumpkin

- MiTM



References

- Kitploit
http://www.kitploit.com/2017/05/wifi-pumpkin-v085-framework-for-rogue.html

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