Null Dubai

Who am I ?

Agenda

Why Infernal Wireless

Q/A

Pentester / Coder by Necessity

3ntr0py1337

- What is wireless security in PT
- A bit of wireless Coding practices
- How IW can help and accelerate ?
- Future of the tool

- Suite of various attacks combined
- Accelerates assessment

Null Dubai

Penetration Testing Methodology and Reporting

- Wireless Penetration Testing Methodology
- Risk Rating of issues
- Reporting the issue
- Proof of Concept
- Codes
- Output results
  –

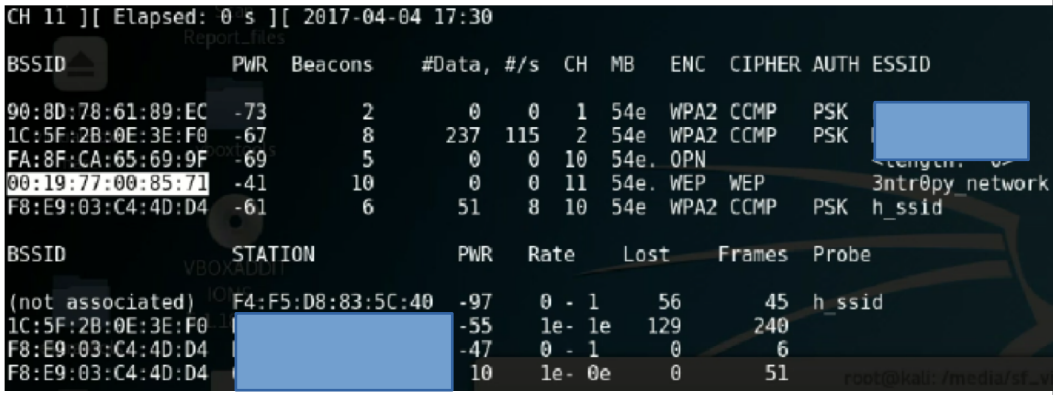
Wireless Penetration Testing methodology

Null Dubai

- There is no defined proper methodology for wireless security assessment like ones defined for others.
- For example: Open Source Security Testing Methodology Manual (OSSTMM)
- Basic and most common phases of assessment are:
  - **Reconnaissance** – Intelligence gathering which doesn't touch the target network by any means
  - **Attack** – actual exploitation, Evil AP and cracking against network
  - **Post Attack** – Involves traffic interception, pivoting into internal network and more

Wireless Penetration Testing – Reconnaissance

- Gather SSID list
- Encryption types
- Channel IDs
- MAC addresses of Access Points in scope of work
- Hosts connected to Access Points
- Probe requests broadcaster by stations



Null Dubai

Wireless Penetration Testing methodology - Attacks

Null Dubai

- Perform attacks against the network to assess its security:
- WEP
- WPA2
- WPA2 Enterprise
- Open Access Points MiTM
- Evil Twin attacks
- WPS Attack
- Deauthentication against STA and clients.
- MiTM

Wireless Penetration Testing methodology – Post Attack

Null Dubai

- Perform post attacks against the network to assess its security:
- Evil Access Point MiTM
- Authentication attacks against administrative and other protocols (SMB, FTP, HTTP, SSH)
- Pivot the attack against internal network

Wireless Penetration Testing methodology – Risk Rating

Null Dubai

- We can use commonly used risk rating developed by OWASP:
- https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- It is critical to provide honest and valid risk ratings taking into account the following:
- Factors of Likelihood
  - Threat Agent
  - Vulnerability Factor
- Factors of Impact
  - Loss of CIAA (confidentiality, integrity and availability, accountability) triangle

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Wireless Penetration Testing methodology – Reporting

Null Dubai

Report

- It is as important as assessment itself
- Good report composition will convey the issues to customers with great impression
- Should contain the issue's description and its impact if exploited
- Should contain recommendation and solution to prevent the attack
- **Should contain:**
  - Destinations that are affected
- **Proof of Concept**
  - Source code, if applicable
  - Output from attack
  - Video demo and screenshots

Wireless coding Sample using Python and Scapy

Null Dubai

```
def packet_sniffer(self, pkt):
    if pkt.haslayer(Dot11Beacon):
        ###################### WIFI SNIFFER WITH ENCRYPTION
##################
        temp = pkt
        while temp:
            ssid_details = []
            global ssid_dictionary
            global ssid_channel_dictionary
            temp = temp.getlayer(Dot11Elt)
            cap = pkt.sprintf("{Dot11Beacon:%Dot11Beacon.cap%}"
"{Dot11ProbeResp:%Dot11ProbeResp.cap%}").split('+')

            if temp and temp.ID == 0 and (pkt.addr3 not in ssids):
                global essid
                global bssid
                global ssid_dictionary
                global ssid_channel_dictionary
                global channel
                global beacon
                global rssi
                #~ print repr(essid)
                if pkt.info:
                    essid = pkt.info
                    ssid_dictionary[bssid] = repr(essid)

                bssid = pkt.addr3
                ssid_dictionary[bssid] = repr(essid)
                ssids.add(bssid)
```

How Infernal Wireless Can Help ?

Being developed since 2014 but very slow

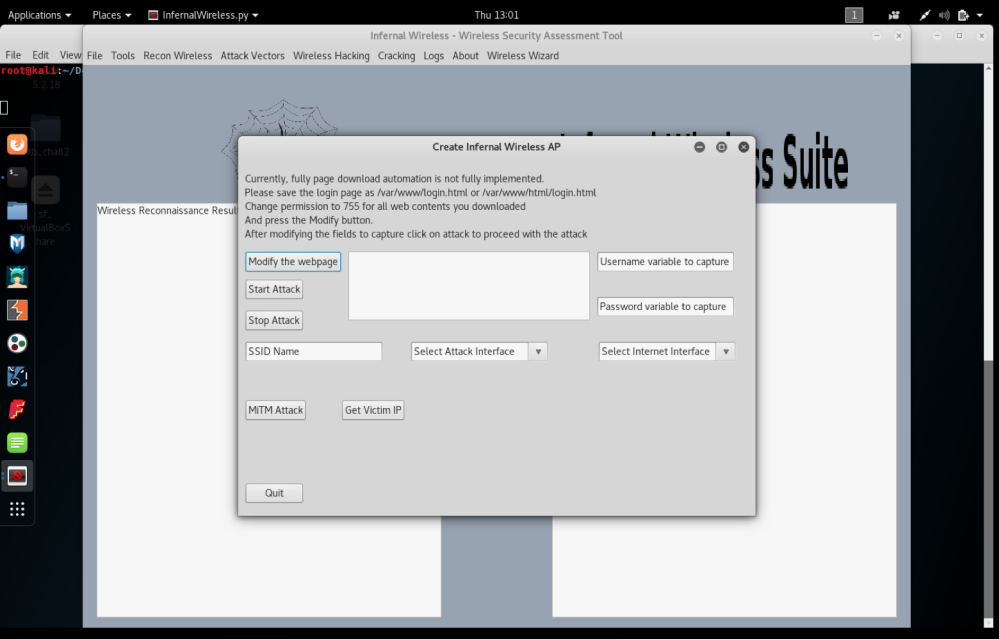
Paused from 2016 till 2018 Sep :(

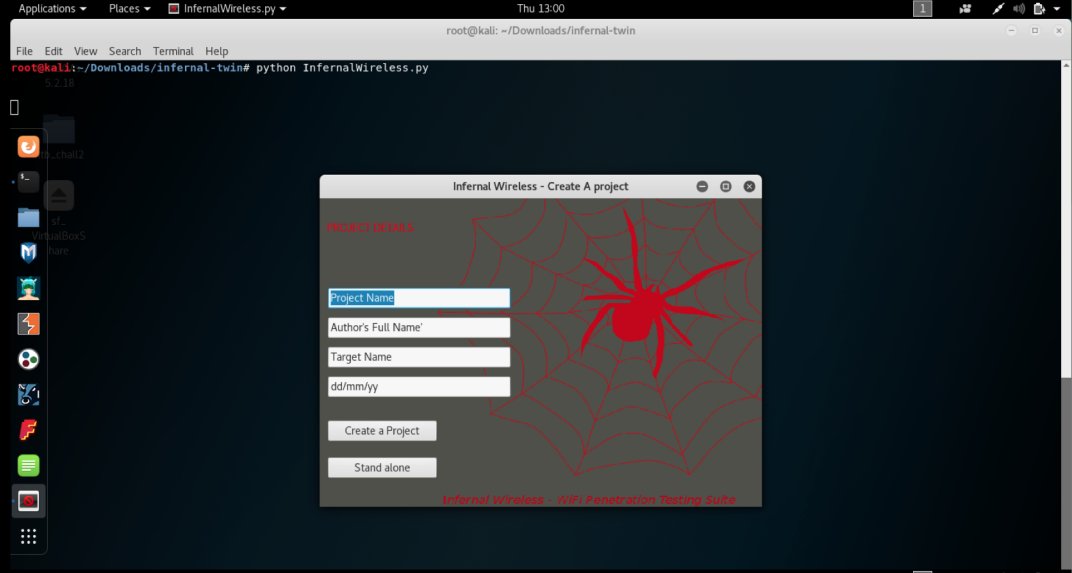
Null Dubai

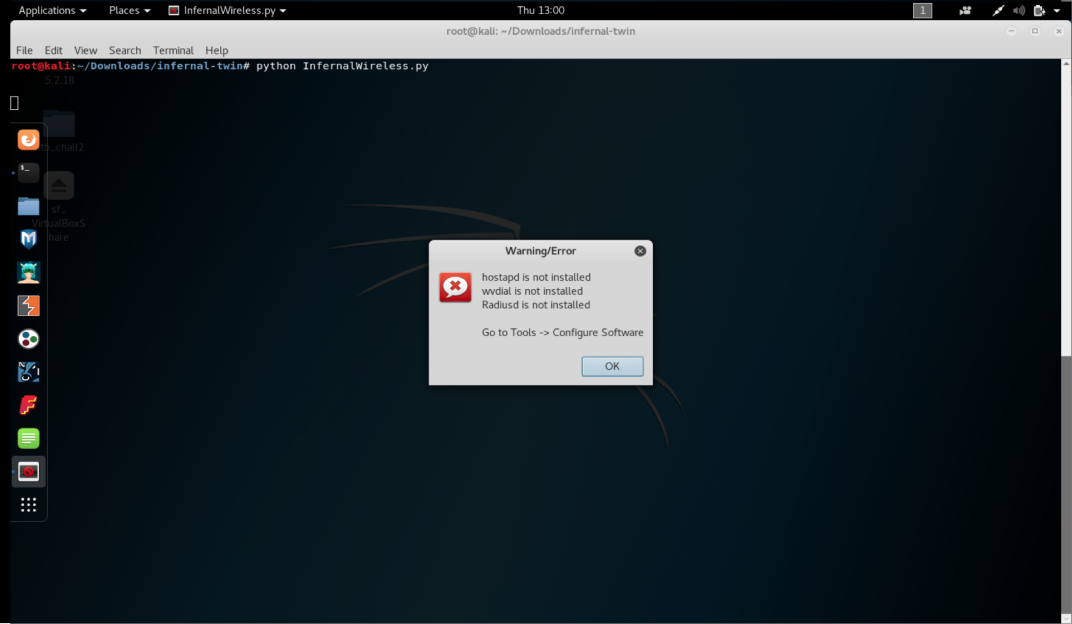
- WPA2 hacking
- WEP Hacking
- WPA2 Enterprise hacking
- Wireless Social Engineering
- SSL Strip
- Report generation
- PDF Report
- HTML Report
- Note taking function
- Data is saved into Database
- Network mapping
- MiTM
- Probe Request
- Added Visual Representation of Wireless Scan
- Added Visual Representation of Probe Requests and Map per SSID requested by Devices
- Project Creation

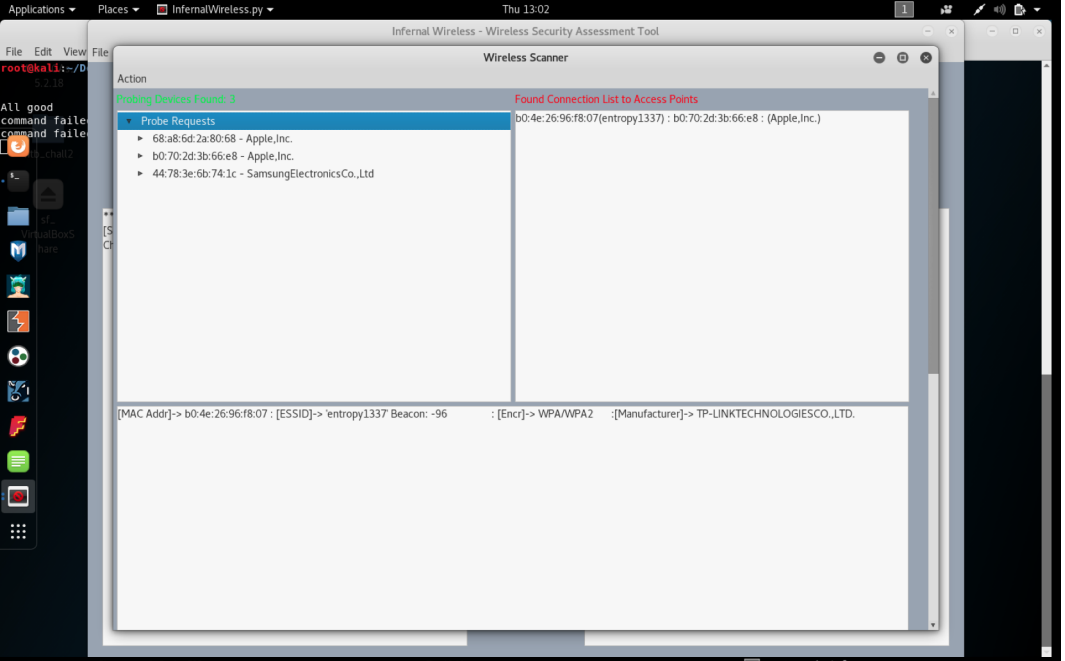
How Infernal Wireless Looks

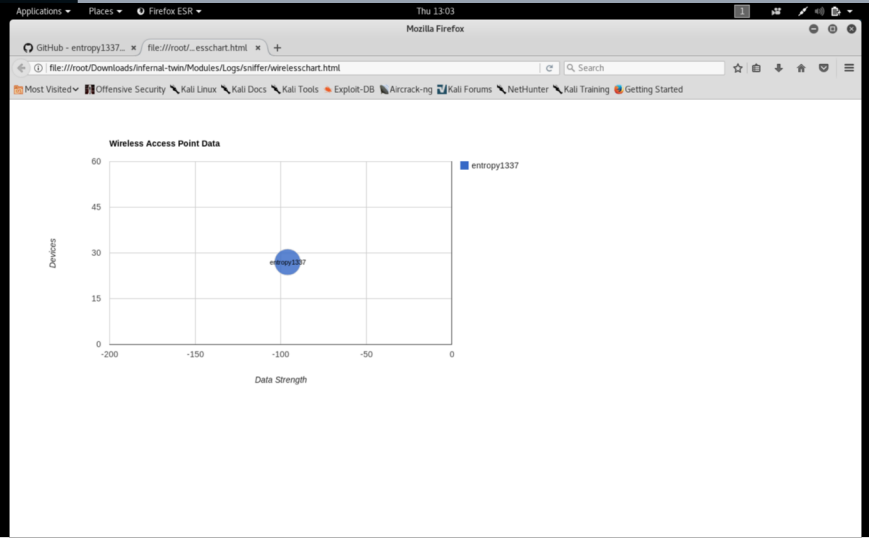
https://github.com/entropy1337/infernal-twin

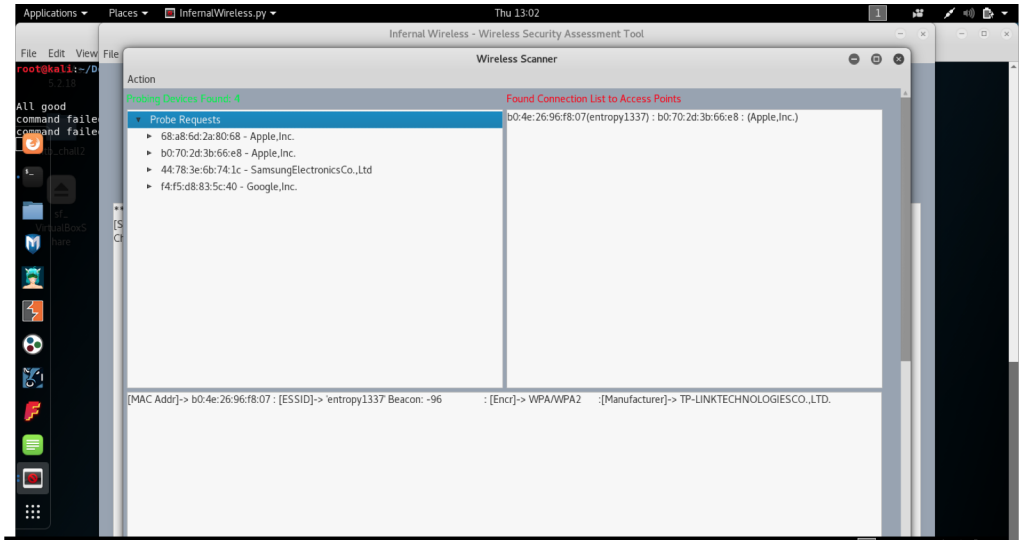


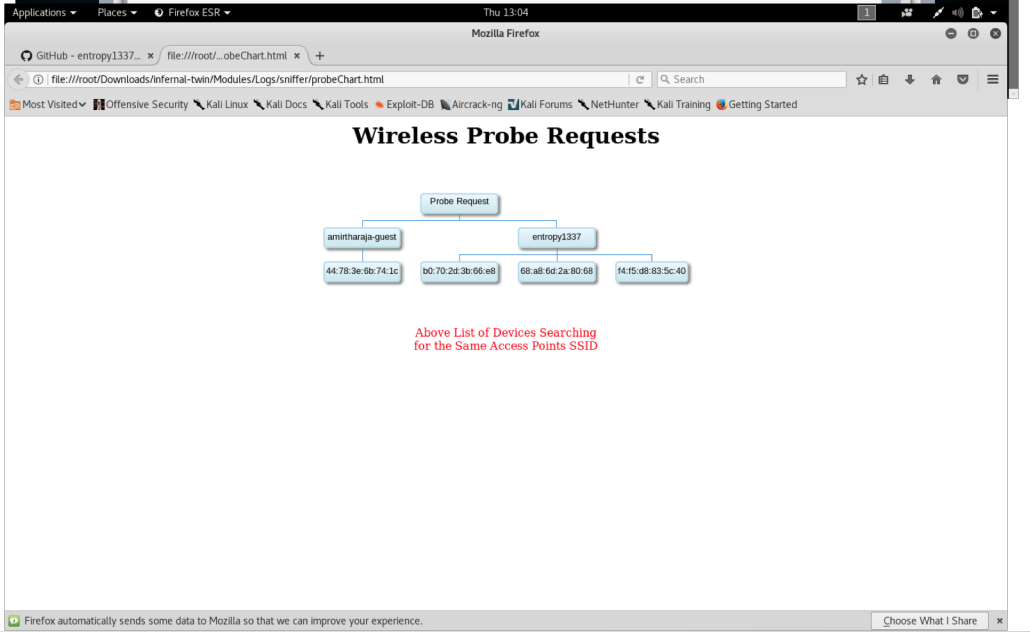




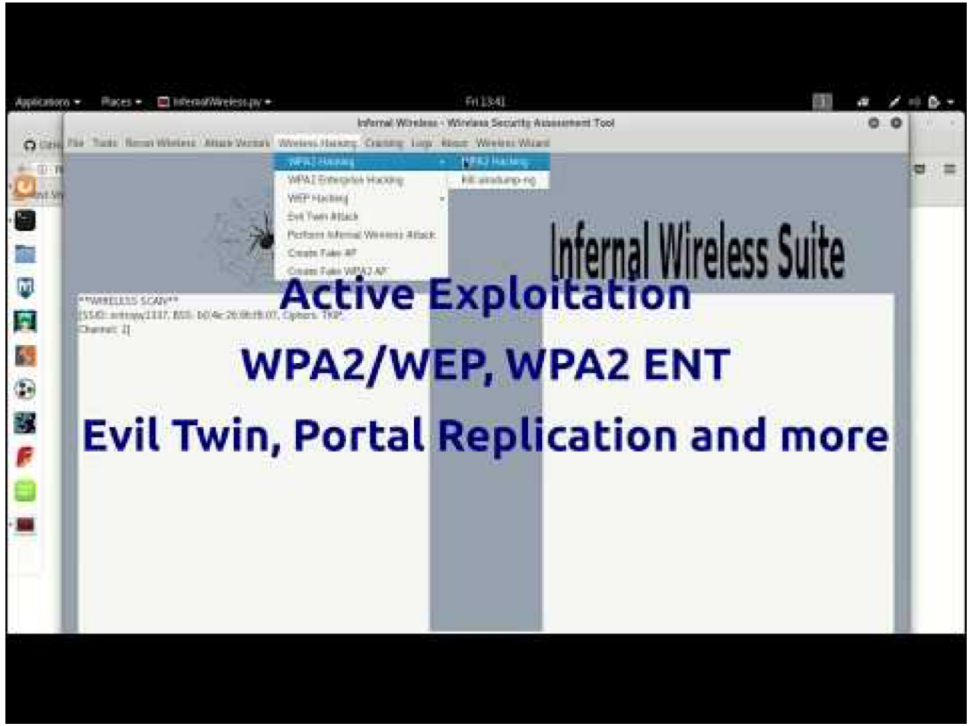

Applications
Places
InfernalWireless.py
Thu 13:02
Infernal Wireless - Wireless Security Assessment Tool
Wireless Scanner
Action
Probing Devices Found: 3
Found Connection List to Access Points
Probe Requests
68:a8:6d:2a:80:68 - Apple,Inc.
b0:70:2d:3b:66:e8 - Apple,Inc.
44:78:3e:6b:74:1c - SamsungElectronicsCo.,Ltd
b0:4e:26:96:f8:07(entropy1337) : b0:70:2d:3b:66:e8 : (Apple,Inc.)
[MAC Addr]-> b0:4e:26:96:f8:07 : [ESSID]-> 'entropy1337' Beacon: -96 : [Encr]-> WPA/WPA2 :[Manufacturer]-> TP-LINKTECHNOLOGIESCO.,LTD.


Applications
Places
Firefox ESR
Thu 13:03
Mozilla Firefox
GitHub - entropy1337...
file:///root/...esschart.html
file:///root/Downloads/infernal-twin/Modules/Logs/sniffer/wirelesschart.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Wireless Access Point Data
entropy1337
Devices
Data Strength
60
45
30
15
0
-200
-150
-100
-50
0


Applications
Places
InfernalWireless.py
Thu 13:02
Infernal Wireless - Wireless Security Assessment Tool
Wireless Scanner
Action
Probing Devices Found: 4
Found Connection List to Access Points
Probe Requests
68:a8:6d:2a:80:68 - Apple,Inc.
b0:70:2d:3b:66:e8 - Apple,Inc.
44:78:3e:6b:74:1c - SamsungElectronicsCo.,Ltd
f4:f5:d8:83:5c:40 - Google,Inc.
b0:4e:26:96:f8:07(entropy1337) : b0:70:2d:3b:66:e8 : (Apple,Inc.)
[MAC Addr]-> b0:4e:26:96:f8:07 : [ESSID]-> 'entropy1337' Beacon: -96 : [Encr]-> WPA/WPA2 :[Manufacturer]-> TP-LINKTECHNOLOGIESCO.,LTD.


Applications
Places
Firefox ESR
Thu 13:04
Mozilla Firefox
GitHub - entropy1337...
file:///root/...obeChart.html
file:///root/Downloads/infernal-twin/Modules/Logs/sniffer/probeChart.html
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Wireless Probe Requests
Probe Request
amirtharaja-guest
entropy1337
44:78:3e:6b:74:1c
b0:70:2d:3b:66:e8
68:a8:6d:2a:80:68
f4:f5:d8:83:5c:40
Above List of Devices Searching
for the Same Access Points SSID
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share


Infernal Wireless Suite


Infernal Wireless Suite
Active Exploitation
WPA2/WEP, WPA2 ENT
Evil Twin, Portal Replication and more

How IW Can Help ?

- Faster Recon performance
- Faster attack selection on the results
- wizard feel like attack creation
- more creativity
- single suite for all attacks
- Social Engineering Aspects
- Cracking PSK / Hashes
- MiTM integration

Future of the Tool

- Wizard Based Scanning and exploitation
- Result / Feedback based Attack launch
- Better Reporting layout
- Better GUI
- Adding External Exploitation Modules
- Recreate all code from scratch
- Automatic PoC creation