

Eaphammer

Information Security Inc.



Contents

- About Eaphammer
- Features
- Testing Environment
- Installing Eaphammer
- Using Eaphammer
- References



About Eaphammer

• EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks





Features

- Steal RADIUS credentials from WPA-EAP and WPA2-EAP networks.
- Perform hostile portal attacks to steal AD creds and perform indirect wireless pivots
- Perform captive portal attacks
- Built-in Responder integration
- Support for Open networks and WPA-EAP/WPA2-EAP



Features

- No manual configuration necessary for most attacks.
- No manual configuration necessary for installation and setup process
- Leverages latest version of hostapd (2.6)
- Support for evil twin and karma attacks
- Generate timed Powershell payloads for indirect wireless pivots
- Integrated HTTP server for Hostile Portal attacks



Testing Environment

Kali Linux 2017

```
root@WarBerry:~# 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 Eaphammer

Clone GitHub repository

```
root@WarBerry:~# git clone https://github.com/s0lst1c3/eaphammer.git Cloning into 'eaphammer'...
remote: Counting objects: 982, done.
remote: Total 982 (delta 0), reused 0 (delta 0), pack-reused 982
Receiving objects: 100% (982/982), 2.18 MiB | 1.06 MiB/s, done.
Resolving deltas: 100% (243/243), done.
```



Installing Eaphammer

Installing Eaphammer

```
root@WarBerry:~/eaphammer# ./kali-setup
[*] Installing Kali dependencies...
Reading package lists... Done
Building dependency tree
Reading state information... Done
libnfnetlink-dev is already the newest version (1.0.1-3+b1).
libnfnetlink-dev set to manually installed.
libssl-dev is already the newest version (1.1.0q-2).
Suggested packages:
 resolvconf
The following NEW packages will be installed:
 dnsmasg libnl-3-dev libnl-genl-3-dev
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 127 kB of archives.
After this operation, 617 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



Installing Eaphammer

Installing Eaphammer



Using Eaphammer

Running Eaphammer

```
ot@WarBerry:~/eaphammer# ./eaphammer -h
                    [-h] [-cert-wizard] [-i INTERFACE] [-e ESSID] [-b BSSID] [-hw-mode HW MODE] [-c CHANNEL] [--wpa [1,2]] [--auth (peap,ttls,open)] [--cloaking (none,full,zeroes)] [--crods] [--hostile-portal] [--captive-portal] [--pivot] [--karma] [--remote-autocrack hostname:port]
                    |--wordlist WORDLIST| |--local-autograck|
                              show this help message and exit
                              Use this flag to create a new RADIUS cert for your AP
-i INTERFACE, --interface INTERFACE
                              The phy interface on which to create the AP
-e ESSID, --essid ESSID
-b BSSTD, --bssid BSSTD
                             Specify access point BSSID
--hw-mode HW_MODE
                              Specify access point hardware mode (default: g).
-- auth {peap, ttls, open}
                             Send empty SSTD in beacons and ignore probe request
                             frames that do not specify full SSID (i.e. require
stations to know SSID). Choices: [1. none - do not use
SSID cloaking. | [2. full - Send empty string in
                              beacon and ignore probe requests for broadcast SSTD ]
                              Force clients to connect to a captive portal
                              Use this flag to perform an indirect wireless pivot
                              Enable karma.
                              Use autocrack n add with remote cracking rig.
 -wordlist WORDLIST
                              Specify the wordlist to use with the autocrack
                              feature.
                              Use internal autocrack n add featur
```



Using Eaphammer

Executing a hostile portal attack



Using Eaphammer

Executing a hostile portal attack



References

- Kitploit
 http://www.kitploit.com/2017/05/eaphammer-targeted-evil-twin-attacks.html
- Kali Linux 2017 https://www.kali.org/downloads/
- GitHub <u>https://github.com/toolswatch/blackhat-arsenal-tools/blob/master/network_attacks/eaphammer.md</u>

