Eaphammer

Information Security Inc.

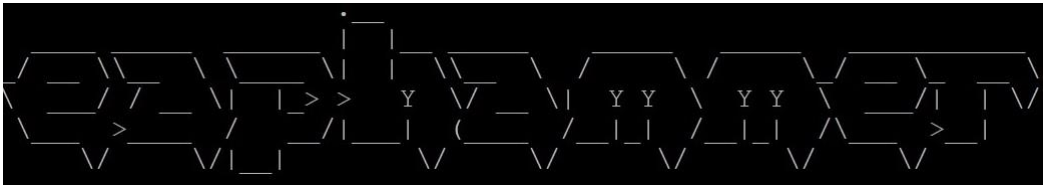
iSEC
information security inc.

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 (1.1.0g-2).
Suggested packages:
  resolvconf
The following NEW packages will be installed:
  dnsmasq 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
```

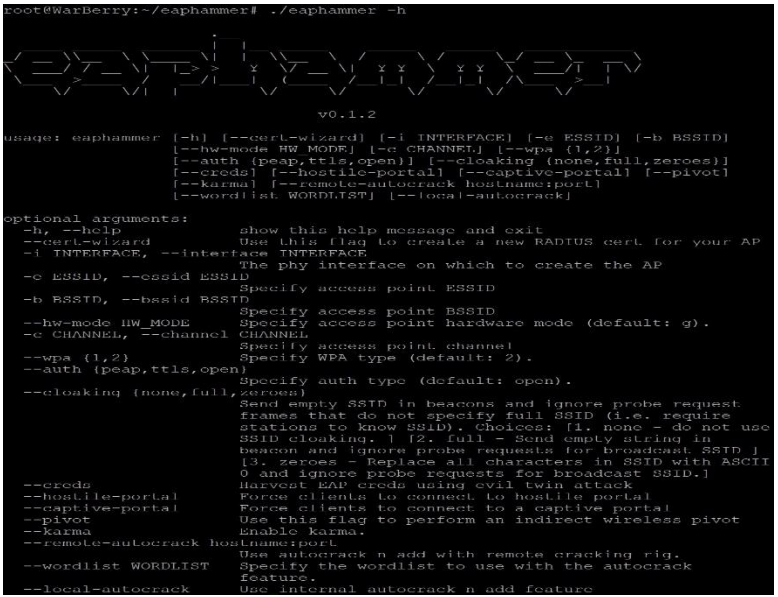
Installing Eaphammer

- Installing Eaphammer

```
HTTP request sent, awaiting response... 200 OK
Length: 53291283 (51M) [application/octet-stream]
Saving to: 'rockyou.txt.tar.gz'

rockyou.txt.tar.gz                  100%[=======================================================>]  50.82M  5.08MB/s    in 10s

2017-11-19 11:03:16 (4.84 MB/s) - 'rockyou.txt.tar.gz' saved [53291283/53291283]

[*] complete!
[*] Extracting default wordlist...
[*] complete!
```

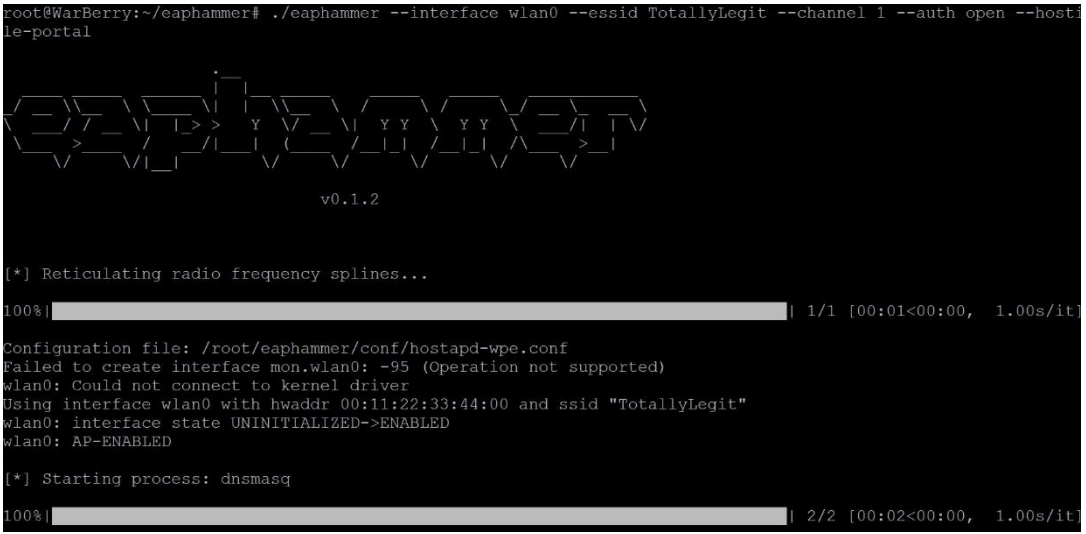
Using Eaphammer

- Running Eaphammer



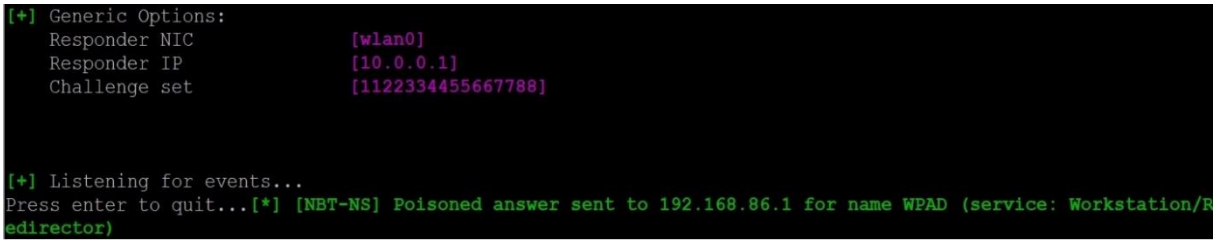
Using Eaphammer

- 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
https://github.com/toolswatch/blackhat-arsenal-tools/blob/master/network_attacks/eaphammer.md