



Labels ▼

 Search

Try acunetix v11 FOR FREE

Home » EAPHammer » Evil Twin Attack » http(s) » Kali » Linux » MITM » NetBIOS » NTLM » PowerShell » Python » Responder » SMB » SMB Relay » Toolkit » Wireless » WPA » WPA2 » EAPHammer - Targeted Evil Twin Attacks Against WPA2-Enterprise Networks [Indirect Wireless Pivots Using Hostile Portal Attacks]

EAPHammer - Targeted Evil Twin Attacks Against WPA2-Enterprise Networks [Indirect Wireless Pivots Using Hostile Portal Attacks]

Lydecker Black on 11:18 AM | Post sponsored by FaradaySEC | Multiuser Pentest Environment

```
r00t@r00t-Q470C-500P4C: ~/KitPloit/eaphammer — Konsole
r00t@r00t-Q470C-500P4C:~/KitPloit/eaphammer$ ./eaphammer -h

v0.0.5

usage: eaphammer [-h] [--cert-wizard] [-i INTERFACE] [-e ESSID] [-b BSSID]
                [--hw-mode HW_MODE] [-c CHANNEL] [--wpa {1,2}]
                [--auth {peap,tls,open}] [--creds] [--hostile-portal]
                [--captive-portal]

optional arguments:
  -h, --help                show this help message and exit
  --cert-wizard              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    Specify access point ESSID
  -b BSSID, --bssid BSSID    Specify access point BSSID
  --hw-mode HW_MODE          Specify access point hardware mode (default: g).
  -c CHANNEL, --channel CHANNEL
                            Specify access point channel
  --wpa {1,2}                Specify WPA type (default: 2).
  --auth {peap,tls,open}     Specify auth type (default: open).
  --creds                    Harvest EAP creds using evil twin attack
  --hostile-portal           Force clients to connect to hostile portal
  --captive-portal           Force clients to connect to a captive portal

r00t@r00t-Q470C-500P4C:~/KitPloit/eaphammer$
```

EAPHammer is a toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks. It is designed to be used in full scope wireless assessments and red team engagements. As such, focus is placed on providing an easy-to-use interface that can be leveraged to execute powerful wireless attacks with minimal manual configuration. To illustrate how fast this tool is, here's an example of how to setup and execute a credential stealing evil twin attack against a WPA2-TTLS network in just two commands:

```
# generate certificates
./eaphammer --cert-wizard

# launch attack
./eaphammer -i wlan0 --channel 4 --auth tls --wpa 2 --essid CorpWifi --creds
```

Leverages a lightly modified version of hostapd-wpe, dnsmasq, dnstiff, Responder, and Python 2.7.

Subscribe via e-mail

Subscribe via e-mail [Submit a Tool](#) 

Follow us!

**PenTest Tools**[Like Page](#)

26K likes

Follow @KitPloit 65.7K followers**KitPloit**[Follow](#)

+1

+ 5,159

BY FEEDBURNER

FARADAYCollaborative Penetration Test &
Vulnerability Management Platform[TRY FARADAY](#)www.faradaysec.com

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
- No manual configuration necessary for most attacks.
- No manual configuration necessary for installation and setup process

Upcoming Features

- Perform seamless MITM attacks with partial HSTS bypasses
- Support attacks against WPA-PSK/WPA2-PSK
- Support for SSID cloaking
- Generate timed payloads for indirect wireless pivots
- Integrated PowerShell payload generation
- impacket integration for SMB relay attacks
- directed rogue AP attacks (deauth then evil twin from PNL, deauth then karma + ACL)
- Updated hostapd-wpe that works with the latest version of Hostapd
- Integrated website cloner for cloning captive portal login pages
- Integrated HTTP server

Will this tool ever support Karma attacks?

- At some point yes, but for now the focus has been on directed evil twin attacks.
- If Karma attacks are like a wireless grenade launcher, this tool is more like an easy-to-use wireless sniper rifle

Setup Guide

Kali Setup Instructions

Begin by cloning the **eaphammer** repo using the following command.

```
git clone https://github.com/s01st1c3/eaphammer.git
```

Next run the kali-setup.py file as shown below to complete the eaphammer setup process. This will install dependencies and compile hostapd.

```
python setup.py
```

Other Distros

If you are not using Kali, you can still compile eaphammer. I just haven't written a setup script for your distro yet, which means you'll have to do it manually. Ask yourself whether you understand the following:

- python-devel vs python-dev
- service vs systemctl
- network-manager vs NetworkManager
- httpd vs apache2

If you looked at this list and immediately realized that each pair of items was to some extent equivalent (well, except for service vs systemctl, but you catch my drift), you'll probably have no problems getting this package to work on the distro of your choice. If not, please just stick with Kali until support is added for other distros.

With that out of the way, here are the generic setup instructions:

Use your package manager to install each of the dependencies listed in `kali-dependencies.txt`. Package names can vary slightly from distro to distro, so you may get a "package not found" error or similar. If this occurs, just use Google to find out what the equivalent package is for your distro and install that instead. Once you have installed each of the dependencies listed in `kali-dependencies.txt`, you'll need to install some additional packages that ship with Kali by default. These packages are listed below. If you're on a distro that uses `httpd` instead of `apache2`, install that instead.

- `dsniff`
- `apache2`








Compile hostapd using the following commands:

```
cd hostapd-eaphammer
make
```

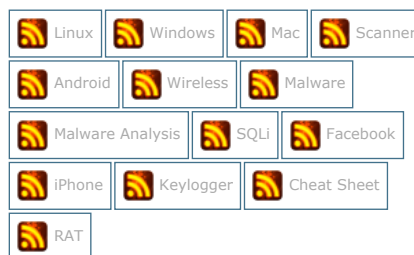
Open `config.py` in the text editor of your choice and edit the following lines so that to values that work for your distro:

```
# change this to False if you cannot/will not use systemd
use_systemd = True
```



Populars	Comments	Archive
	Kali Linux 2017.1 Release As with all new releases, you have the common denominator of updated packages, an updated kernel that provides more and better hardware ...	
	WPSEku - Simple Wordpress Security Scanner WPSEku is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issu...	
	InjectPE - Inject Custom Code into PE File Using this tool you can inject x-code/shellcode into PE file. InjectPE works only with 32-bit executable files. Why you need Inject...	
	Leviathan - Wide Range Mass Audit Toolkit Leviathan is a mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploi...	
	Inspeckage - (Android Package Inspector) Dynamic Analysis With Api Hooks, Start Unexported Activities And More Inspeckage is a tool developed to offer dynamic analysis of Android applications. By applying hooks to functions of the Android API, Insp...	
	Operative Framework v1.0b - Fingerprint Framework This is a framework based on fingerprint action, this tool is used for get information on a website or a enterprise target with multip...	
	PowerStager - A payload stager using PowerShell This script creates an executable stager that downloads a selected powershell payload, loads it into memory and executes it using obfusc...	

Labels



Google+ Followers

```
# change this to 'NetworkManager' if necessary
network_manager = 'network-manager'

# change this 'httpd' if necessary
httpd = 'apache2'
```

Usage Guide

x.509 Certificate Generation

Eaphammer provides an easy-to-use wizard for generating x.509 certificates. To launch eaphammer's certificate wizard, just use the command shown below.

```
./eaphammer --cert-wizard
```

Stealing RADIUS Credentials From EAP Networks

To steal RADIUS credentials by executing an evil twin attack against an EAP network, use the --creds flag as shown below.

```
./eaphammer --bssid 1C:7E:E5:97:79:B1 --essid Example --channel 2 --interface wlan0 --auth
```

The flags shown above are self explanatory. For more granular control over the attack, you can use the --wpa flag to specify WPA vs WPA2 and the --auth flag to specify the eap type. Note that for cred reaping attacks, you should always specify an auth type manually since the the --auth flag defaults to "open" when omitted.

```
./eaphammer --bssid 00:11:22:33:44:00 --essid h4x0r --channel 4 --wpa 2 --auth ttls --int
```

Please refer to the options described in Additional Options section of this document for additional details about these flags.

Stealing AD Credentials Using Hostile Portal Attacks

Eaphammer can perform hostile portal attacks that can force LLMNR/NBT-NS enabled Windows clients into surrendering password hashes. The attack works by forcing associations using an evil twin attack, then forcing associated clients to attempt NetBIOS named resolution using a Redirect To SMB attack. While this occurs, eaphammer runs Responder in the background to perform a nearly instantaneous LLMNR/NBT-NS poisoning attack against the affected wireless clients. The result is an attack that causes affected devices to not only connect to the rogue access point, but send NTLM hashes to the rogue access point as well. The --hostile-portal flag can be used to execute a hostile portal attack, as shown in the examples below.

```
./eaphammer --interface wlan0 --bssid 1C:7E:E5:97:79:B1 --essid EvilC0rp --channel 6 --au

./eaphammer --interface wlan0 --essid TotallyLegit --channel 1 --auth open --hostile-port
```

Performing Indirect Wireless Pivots Using Hostile Portal Attacks

The hostile portal attack described in Stealing AD Credentials Using Hostile Portal Attacks can be used to perform an SMB relay attack against the affected devices. An attacker can use hostile portal attack to perform an SMB relay attack that places timed reverse shell on an authorized wireless devices. The attacker can then disengage the attack to allow the authorized device to reconnect to the targetted network. When the attacker receives the reverse shell, he or she will have the same level of authorization as the attacker.

Performing Captive Portal Attacks

To perform a captive portal attack using eaphammer, use the --captive-portal flag as shown below.

```
./eaphammer --bssid 1C:7E:E5:97:79:B1 --essid HappyMealz --channel 6 --interface wlan0 --
```

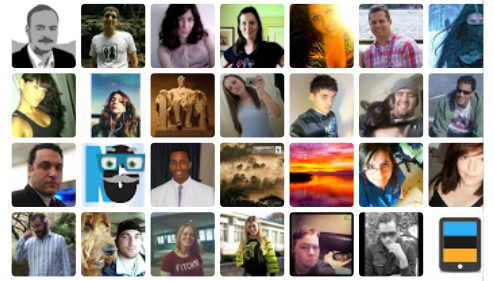
This will cause eaphammer to execute an evil twin attack in which the HTTP(S) traffic of all affected wireless clients are redirected to a website you control. Eaphammer will leverage Apache2 to serve web content out of /var/www/html if used with the default Apache2 configuration. Future iterations of eaphammer will provide an integrated HTTP server and website cloner for attacks against captive portal login pages.

Additional Options

- **--cert-wizard** - Use this flag to create a new RADIUS cert for your AP.
- **-h, --help** - Display detailed help message and exit.
- **-i, --interface** - Specify the a PHY interface on which to create your AP.
- **-e ESSID, --essid ESSID** - Specify access point ESSID.
- **-b BSSID, --bssid BSSID** - Specify access point BSSID.

KitPloit

Follow

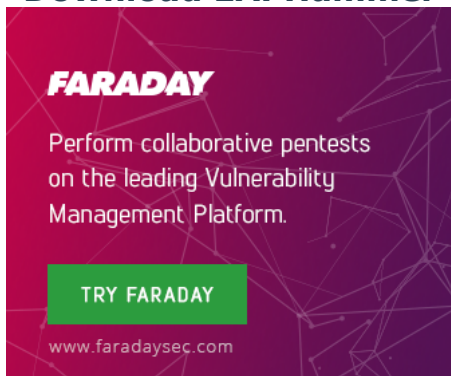


3,746 have us in circles

[View a](#)

- **--hw-mode HW-MODE** - Specify access point hardware mode (default: g).
- **-c CHANNEL, --channel CHANNEL** - Specify access point channel.
- **--wpa {1,2}** - Specify WPA type (default: 2).
- **--auth {peap,tls,open}** - Specify auth type (default: open).
- **--creds** - Harvest EAP creds using an evil twin attack.
- **--hostile-portal** - Force clients to connect to hostile portal.
- **--captive-portal** - Force clients to connect to a captive portal.

Download EAPHammer



Subscribe via e-mail for updates!

Subscribe

Like 127

Tweet

G+1

4

Share

9

Next

This is the most recent post.

Previous

PowerStager - A payload stager using PowerShell

Related Posts

Sponsored

Report ad

0 Comments **KitPloit - Tools for your PenTest Arsenal!**

 **Login**





 **Recommend**  **Share**

Sort by Best



Start the discussion...

Be the first to comment.

 **Subscribe**  **Add Disqus to your site**  **Add Disqus**  **Privacy**

Sponsored

Report ad

Contact Form

Name

Email *

Message *

Send

Recommended:

Best Fails

Blackploit [Pentest]

DedicatedSolutions (Private Cloud)

DedicatedSolutions (Server Products)

DigitalOcean

ExoClick

Funeek!

Th3 R4v3n

7PRO

Underc0de

Sunploit

Site Info
kitploit.com
May 01, 2017

Traffic Rank:
148,338

Links in:
97

Powered by


Follow us!



PenTest T...

Like Page

Follow @KitPloit

65.7K followers

KitPloit

google.com/+KitploitWeb

Hacking and PenTest Tools for your Security Arsenal!

G+

Follow

+1

+ 5,159

BY FEEDBURNER