Personal Research Project (PRP) on

How do Evil Twin WiFi attacks factor into corporate risk assessments, and what measures can organizations take to effectively address this threat?

By Aleksandar Garkov

Page numbers

Problem Definition or Project Goal

This project aims to investigate and demonstrate the security vulnerability of the Evil Twin WiFi attack. This attack involves setting up a rogue WiFi access point similar to a legitimate network to intercept network traffic, steal sensitive information, or perform various malicious activities. The project aims to understand the underlying mechanisms of the attack, its potential impact on users, and methods to defend against it.

Research Questions:

* What is the Evil Twin WiFi attack, and how does it work?
* What are the potential risks and consequences associated with the Evil Twin attack?
* How can individuals and organizations detect and cope with the Evil Twin attacks?
* What are the legal and ethical considerations surrounding the testing and demonstrating evil twin attacks?

These questions will be answered throughout the whole project in different document points.

Planning per Sprint

Sprint 1- Research and Understanding

* Conduct a review on wifi security and Evil Twin attacks.
* Define research questions and project objectives.
* Identify and document common techniques used in Evil Twin attacks.
* Explore case studies and real-world examples of Evil Twin attacks.
* Draft documentation outlining the project scope and goals.

Sprint 2- Experimenting and Demonstration

* Set up a test environment for emulating Evil Twin wifi attacks.
* Experiment with different tools and techniques for creating and detecting Evil Twin networks.
* Document the process of setting up and executing an Evil Twin attack.
* Explore defense strategies against evil twin attacks.
* Prepare a demonstration of an Evil Twin attack.

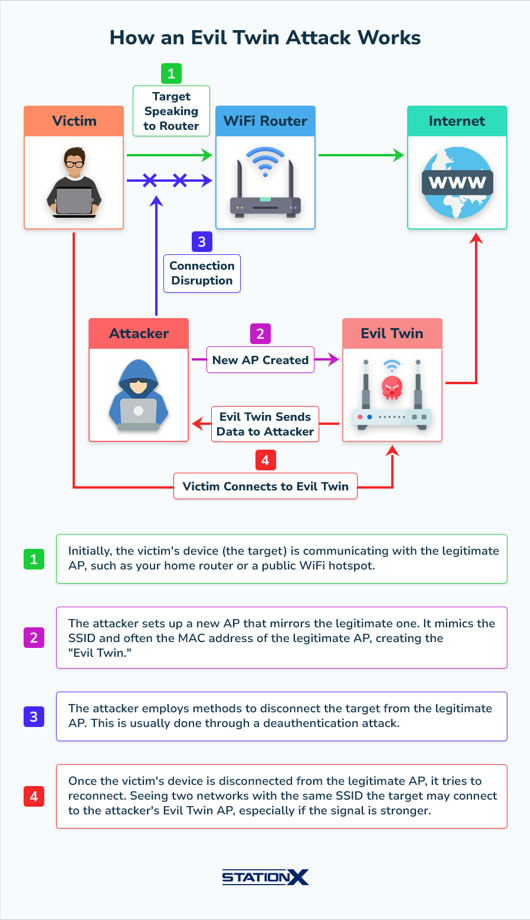
Sprint 3-Analisis and Reporting

* Analyze the results of the experimentation phase.
* Evaluate the effectiveness of various defense mechanisms against Evil Twin attacks.
* Consider legal and ethical implications related to the testing and demonstration of security vulnerabilities.

Imagine you're at your favorite coffee shop, sipping on a latte and browsing the web on their free WiFi. What you don't know is that the network you're connected to isn't the official coffee shop network at all. It's a nearly perfect duplicate set up by someone with ill intentions. You've connected to an Evil Twin. Black Hat hackers deploy Evil Twins to intercept sensitive information from unsuspecting users. By duping users into connecting with the Evil Twin, they can capture crucial data like login details and credit card information.

Ethical hackers employ the Evil Twin approach to help fortify organizational network security. By simulating Evil Twin attacks, they identify and patch up network vulnerabilities before they can be exploited maliciously.

Here's a simplified breakdown of how an Evil Twin attack unfolds:

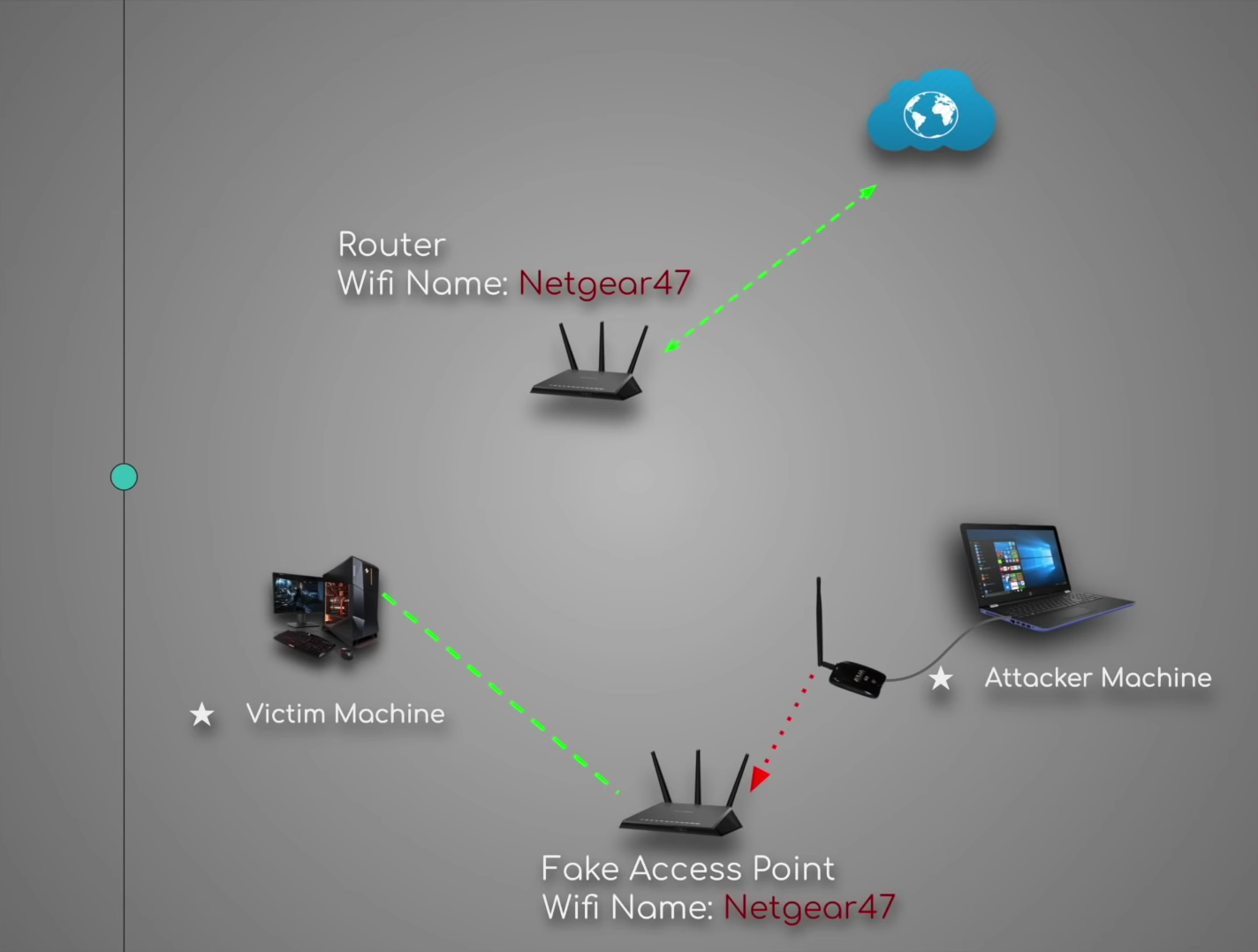


The first and the most obvious sign of an Evil Twin attack is duplicate SSIDs. That means multiple Wi-Fi networks with the same name (SSID).

A second indication might be the signal strength. If the strength is suddenly stronger in an area where the wi-fi has a weaker signal, it could be an evil twin attack.

Network scanning tools like Wireshark, NetStumbler, or Kismet can detect duplicate SSIDs and rogue APs.

This image shows a more in-depth possible attack scenario for an attack. In this case, the bad actor uses a dedicated wireless card to intercept the connection and set up a fake wifi named Netgear47, the same as the original one.

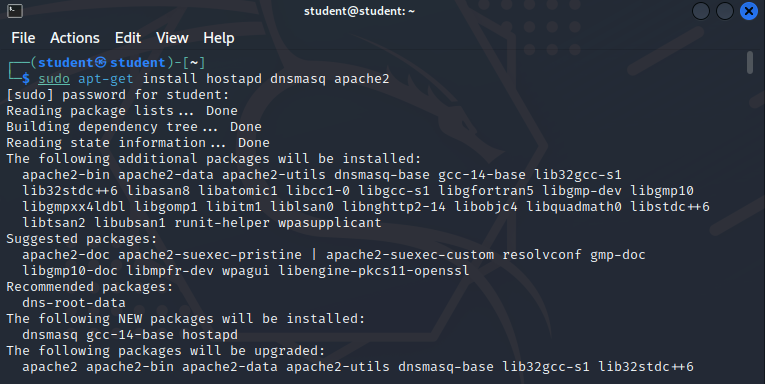


In the next pages, I will try to simulate the same attack on a personal/ permitted device and I will explain step by step my actions towards this goal.

For this task I have equipped myself with a dedicated wifi card called Signal King 300000N.

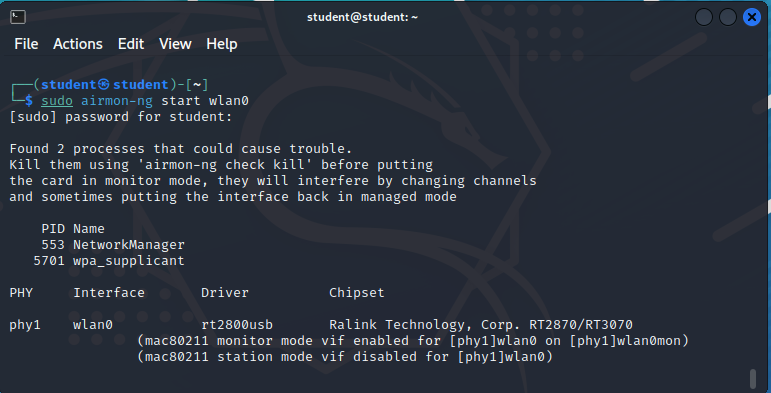


Then I set up a virtual machine with kali Linux, on which I am installing hostapd, a user space daemon software that enables network interface card to act as an access point and authentication server and dnsmasq, providing Domain Name System (DNS) caching, a Dynamic Host Configuration Protocol (DHCP) server, router advertisement and network boot features and Apache HTTP server.

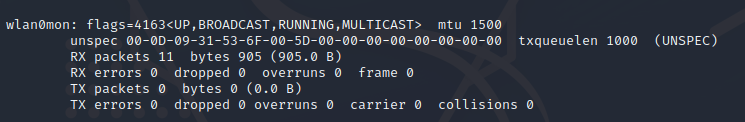


Then we need to check if our wifi card is installed correctly in the VM and if yes, to put it in monitoring mode: A screenshot of a computer program

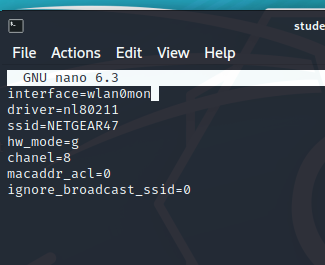
Description automatically generated



And then after ifconfig again, we can see that wlan0 is now called wlan0mon, which stands for monitoring.



Now just to make things organized we will make a new directory in root called FAP (Fake Access Point) and make a new host config file and write the instructions inside it:

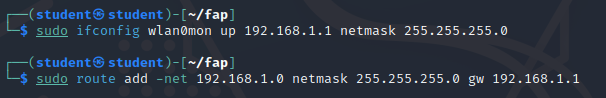


Then we need to create a config file for dns mask and put instructions:

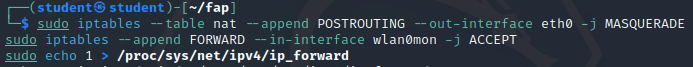
A screenshot of a computer

Description automatically generated

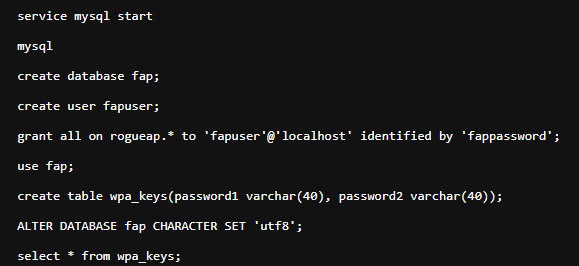
Now we need to assign our wireless adapter a network gateway and a netmask and a routing table:



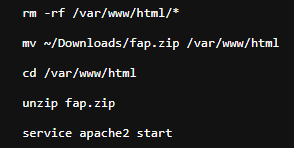
Now to provide internet access to the victim machine when he/she connects to the network, we need to forward the traffic from the virtual wireless adapter, connected to our main machine to wlan0mon:



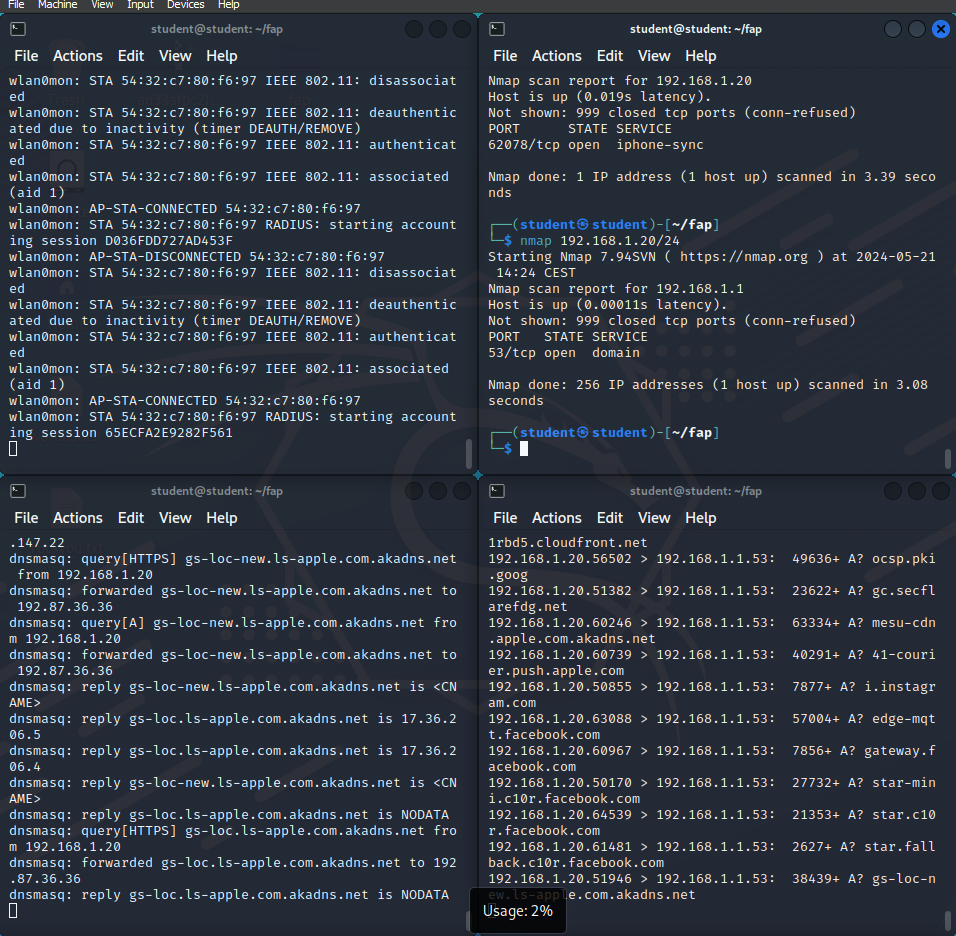
Now it is time to set up our database to store the passwords from the victims by doing the following commands in the terminal:



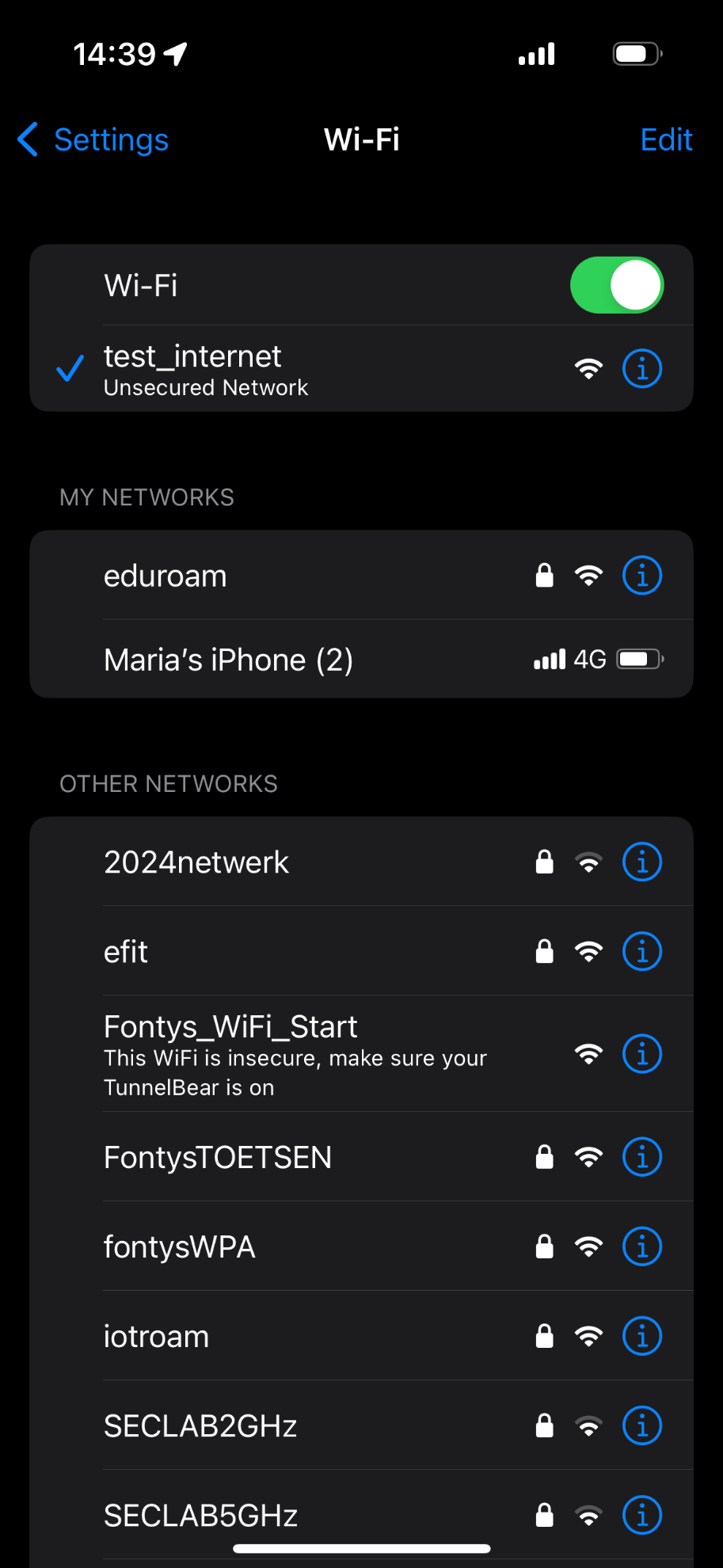
Now we have to set up our captive portal, which I have from a website (down in source). We do this by removing the default Apache files for the web app and replacing them with the downloaded ones.



Now when we run the hostapd, the dnsmasq and the dnsspoof like this:



We can see that a network is available to connect to, from our victim device:



(the network name has changed for testing purposes)

After that, you can see in the video that there is an internet connection and every source is logged in the console:

[](https://www.youtube.com/embed/s8cctm_Pj98?feature=oembed)

To get sensitive information, we will make a website, for example google.com to display not its original page, but an emulated one that we are hosting from our machine, so that when the victim connects to google.com, he/she sees that the URL is indeed google.com, but actually they are looking at a very similar page filled with traps for personal information.

Sources

<https://www.stationx.net/evil-twin-wifi-attack/>

<https://usa.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks>

<https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>

<https://infosecwriteups.com/how-to-perform-an-evil-twin-attack-steal-wi-fi-passwords-4efa60d92f39>

<https://en.wikipedia.org/wiki/Hostapd>

<https://zsecurity.org/wp-content/uploads/2020/08/fapCommands.txt>

<https://zsecurity.org/hack-wpa-wpa2-wifi-without-wordlist-using-evil-twin-attack/>

<https://honoki.net/2015/01/30/how-to-set-up-a-wifi-captive-portal/>

<https://cdn.rootsh3ll.com/captive-portal/captive+portal+guide+-+rootsh3ll.pdf>