



TWIN GHOSTS: EVIL TWIN ATTACKS IN WIRELESS NETWORKS AND DEFENSE MECHANISMS

İlker Kara¹ 

¹ Çankiri Karatekin University, Department of Computer Engineering, Çankırı, Türkiye,
karaikab@gmail.com

KEYWORDS

Evil twin attack
Security
Wireless access point
Fake access point

ARTICLE INFO

Research Article

DOI

[10.17678/beuscitech.1450756](https://doi.org/10.17678/beuscitech.1450756)

Received 11 March 2024

Accepted 25 December 2024

Year 2024

Volume 14

Issue 2

Pages 58-74



ABSTRACT

With the increasing adoption of wireless network technologies, a variety of attacks targeting these networks have emerged, posing significant threats to user security. One prominent type of attack is the evil twin attack, which involves the creation of fake access points, often referred to as "evil twins." In this type of attack, a malicious actor sets up a fake access point (AP) designed to closely resemble a legitimate one, thereby deceiving users into believing it is trustworthy. By exploiting these fake APs, attackers can capture user credentials and gain unauthorized access to sensitive information, potentially leading to financial exploitation or system breaches. Due to the covert nature of evil twin attacks, they can be highly effective without the users' awareness. In this study, explores the risks posed by evil twin attacks and investigates defense strategies to address the security challenges in wireless networks. To achieve this, a scenario involving an evil twin attack is developed and analyzed. In this scenario, an attacker establishes a fake wireless access point in a café or public area near the targeted institution, replicating the institution's network name and security settings to trick users into connecting to the malicious network. This study underscores the potential impacts of such attacks and outlines critical measures that both users and institutions should implement to safeguard against these threats.

1 INTRODUCTION

The widespread adoption of wireless network technologies in today's world has led to a significant transformation in the field of information and communication [1]. However, along with the proliferation of this technology, malicious attackers have developed various types of attacks targeting wireless networks, posing threats to the security of users. One of the most sophisticated types of these attacks is a form of attack known as the evil twin attack. The evil twin attack is executed through the creation of fake access points [2]. These attacks typically involve the creation of a fake access point that mimics the appearance of a wireless access point that users perceive as trustworthy. As soon as the victim connects to this fake access point, the attack is initiated. Evil twin attacks enable attackers to steal the identities and passwords of legitimate users and gain access to sensitive data using this information [3]. This poses a serious threat to both the security of users and the information security of institutions.

In recent years, the most common analysis methods used for preventing and detecting evil twin attacks involve monitoring and analyzing network traffic, analyzing security protocols, and utilizing artificial intelligence and machine learning techniques [4]. The method based on monitoring and analyzing network traffic relies on analyzing situations where the number and types of packets in the network traffic are different from normal, enabling the detection of a potential evil twin attack. Another method used to prevent evil twin attacks is the use of security protocols. In particular, strong encryption and authentication methods can prevent malicious actors from creating fake access points. By ensuring that users securely connect to the network, this method can reduce the impact of evil twin attacks [4]. Another approach used for detecting and preventing evil twin attacks involves the use of artificial intelligence and machine learning techniques. These methods are used to analyze large datasets to detect abnormalities and signs of attacks. In particular, deep learning algorithms have the potential to identify and block complex evil twin attacks [5].

This study aims to address security threats in wireless networks and specifically examine the potential risks of and protection strategies against evil twin attacks. The overall objective of the study is twofold. Firstly, a case analysis was

conducted to understand how evil twin attacks are carried out. The goal here is to provide concrete recommendations to elucidate the logic behind the attacker's evil twin attack. Secondly, the study aims to explain the complexity of evil twin attacks and their impact on cybersecurity, as well as to develop mechanisms for protection against these attacks. In this study, differentiates itself from existing tools used for modeling evil twin attacks by proposing a novel prevention mechanism that incorporates advanced security protocols and user education. While most existing literature focuses primarily on the process of executing the attack, this paper provides an in-depth analysis of both the technical aspects of the attack and the effective countermeasures that can be employed to mitigate such threats.

Within this scope, an evil twin attack scenario was created and analyzed. In this scenario, the attacker sets up a fake wireless access point in a cafe or public area near the targeted institution, designing the fake access point to mimic the name and security settings of the target institution to lure users into connecting to the fake network under their control. This study not only highlights the potential impacts of evil twin attacks but also includes significant steps in understanding the strategies of attackers and taking necessary measures to protect users and institutions against such attacks through complementary mechanisms.

2 MATERIAL AND METHOD

This section begins by providing a detailed explanation of the equipment and steps used to carry out the evil twin attack (real case study). Subsequently, a brief description of the events occurring during the attack is provided.

2.1 Equipment

The equipment used to carry out the evil twin attack consists of several basic components. These are:

1. Kali Linux Operating System: A powerful pentesting operating system like Kali Linux is necessary for the successful execution of the attack. Kali Linux is a Debian-based operating system that includes numerous cybersecurity tools and applications.

2. **Computer:** A suitable computer and monitor are required to execute the evil twin attack. This computer should be compatible with the Kali Linux operating system and will be used to manage the attack. In this study, a Lenovo workstation with an Intel Core i7-10700K processor, 32GB RAM, 1TB HDD, 512GB SSD, and a 5GB Quadro GPU running Windows 11 Pro operating system was used.
3. **Network Interface Card (NIC):** An NIC capable of conducting network discovery and supporting monitor mode is essential for effectively executing the attack. In this scenario, an Alfa Network NIC was used because it supports monitor mode and has the capability to monitor network traffic.

2.2 Attack Steps

This section focuses on the attack steps of evil twin attacks in wireless networks. These steps will explain how attackers create fake networks and acquire user credentials (Figure 1). The attack steps are as follows [6]:

1. **Installation of Kali Linux Operating System:** As the first step, the attacker installs the Kali Linux operating system on a suitable computer. Kali Linux comes pre-loaded with many cybersecurity tools and provides an ideal environment for pentesting operations.
2. **Network Card Settings:** The attacker enables monitor mode using the Alfa Network network card and makes it available to monitor network traffic. This step is crucial for discovering devices on the network and determining targets.
3. **Initiation of Evil Twin Attack:** The attacker initiates the evil twin attack to steal the identities of legitimate users on the target network. This involves generating fake requests or transactions and manipulating network traffic. The attacker creates fake network requests and redirects network traffic to deceive target devices. To achieve this, the attacker runs the Aircrack-ng tool on Kali Linux to detect security vulnerabilities in wireless networks. This step is important for analyzing target networks and identifying potential targets.
4. **Unauthorized Access:** When the evil twin attack is successfully executed, the attacker captures the identities of legitimate users and gains unauthorized

access to systems. This aims to gain access to sensitive data, take control of systems, or perform other malicious activities. For this purpose, the Aircrack-ng tool is used to generate fake requests or transactions and manipulate network traffic.

5. Monitoring and Improvement: The attacker monitors and improves the effectiveness of the attack. By analyzing network traffic, they identify discovered vulnerabilities and develop strategies for future attacks.

These steps provide a general approach to executing an evil twin attack. However, each attack situation is unique and may vary depending on the attacker's goals and environmental factors [7], [8].

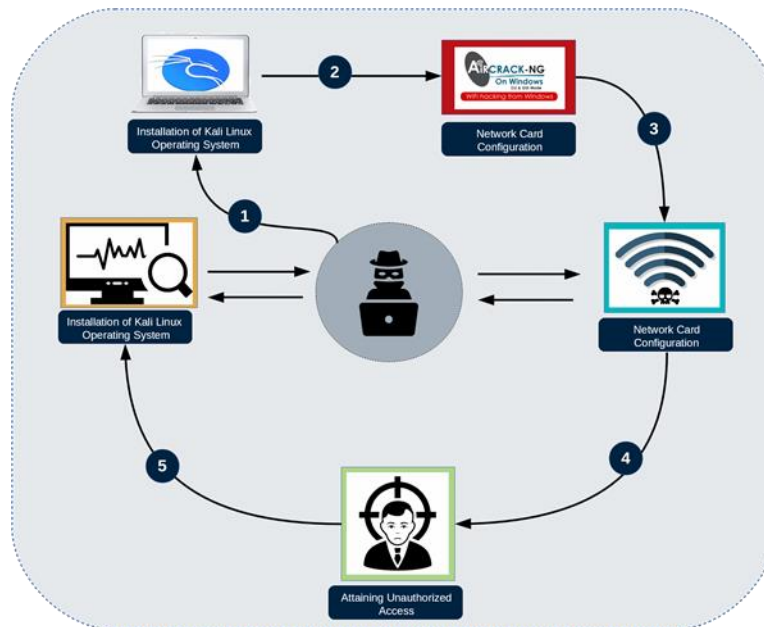


Figure 1. Evil Twin attack steps [9].

2.3 Evil Twin Attack Scenario

The steps of the evil twin attack are provided in Figure 1. The attack begins with the attacker installing the Kali Linux operating system on a suitable computer. Then, the attacker runs the Aircrack-ng tool on Kali Linux to detect security vulnerabilities in wireless networks. This step is crucial for analyzing target networks and identifying potential targets. Subsequently, the attacker initiates the evil twin attack to steal the identities of legitimate users on the target network. By using the Aircrack-ng tool, fake requests or transactions are generated, and network traffic is manipulated [10]. When the evil twin attack is successfully executed, the attacker

captures the identities of legitimate users and gains unauthorized access to systems. This step aims to gain access to sensitive data, take control of systems, or perform other malicious activities. Finally, the attacker monitors and improves the effectiveness of the attack. By analyzing network traffic, they identify discovered vulnerabilities and develop strategies for future attacks.

3 ANALYSIS OF CASE STUDY

In this section, a case analysis was conducted to understand how evil twin attacks are carried out. For this purpose, a real-life case example was examined, and a comprehensive analysis was conducted on the methods used to execute the evil twin attack and the results obtained. Airgeddon tool package was utilized for this purpose. Airgeddon is equipped with various features that allow monitoring and controlling of wireless networks, including menu-driven handshake capturing and Evil Twin Attack functionalities.

Figure 2 shows how the necessary preparations for the malicious twin attack are made through the user interface of the Airgeddon tool. Initially, the user needs to redirect their wireless network card to the correct network and activate monitoring mode. Subsequently, by selecting the sixth option, "Evil Twin Attack (AP encryption)," preparations are made to create a fake access point. This fake access point enables the attacker to redirect users of the target network to a login page that appears legitimate, thereby capturing their credentials.

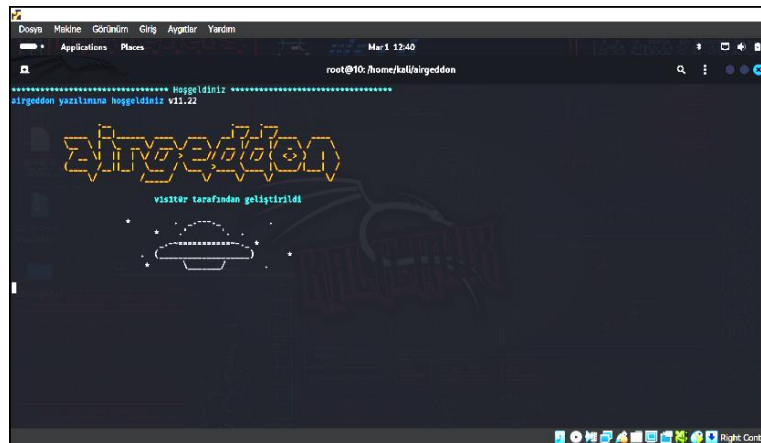


Figure 2. Airgeddon Tool installation page

Figure 2 depicts a desktop environment running the Kali Linux operating system, commonly used for education and research purposes in the field of cybersecurity. Within Kali Linux, the open-source tool Aircgeddon comes pre-installed.

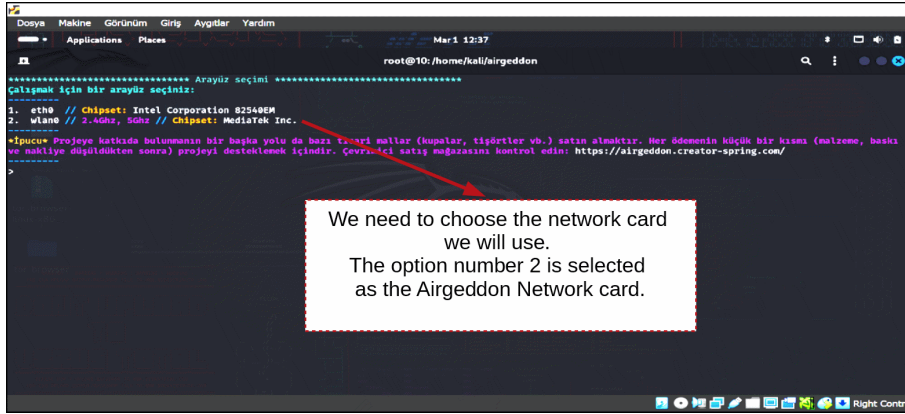


Figure 3. Configuration of Aircgeddon tool.

Figure 3 shows the step where users select their wireless network cards and then configure the necessary settings on these cards for using the Aircgeddon tool. In this step, the network card to be used in the attack is selected. Subsequently, the type of attack to be performed is chosen from the parameters available in the Aircgeddon tool menu (Figure 4).

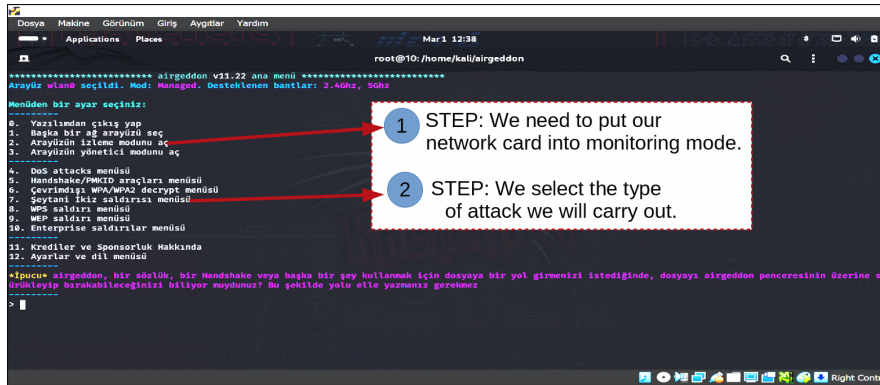


Figure 4. Configuration of Aircgeddon tool.

Figure 4 shows the user interface and usage parameters of the wireless penetration testing tool called Aircgeddon. For this purpose, the first step is to set the network card to monitoring mode. Subsequently, the type of attack to be performed should be determined. A two-step process involving setting the wireless network cards to monitoring mode and selecting the type of attack to be performed is shown. In the first step, users need to select the network card to switch to

monitoring mode, which is a prerequisite for the detection and analysis of wireless networks. In the second step, users need to select the type of penetration testing attack they will perform.

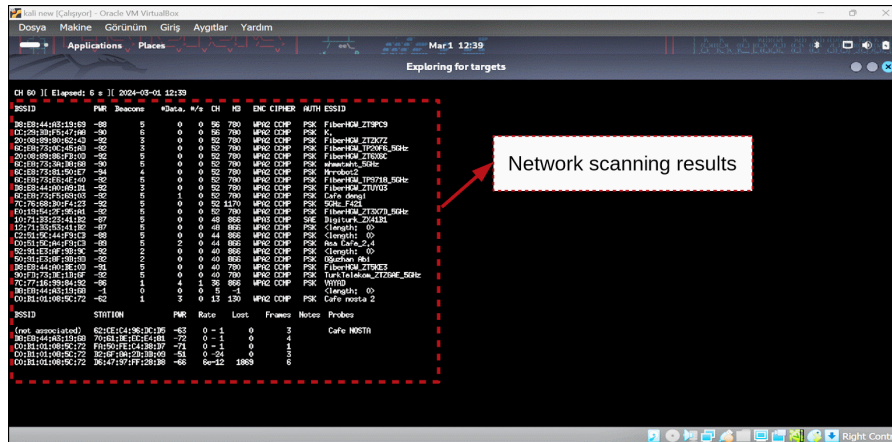


Figure 5. Scanning of Wifi Networks and target identification using Airodump-ng tool.

After configuring the interface and usage parameters of the Airogeddon tool, scanning of Wifi networks and target identification is performed (Figure 5). Network scanning performed using tools like Airodump-ng allows the attacker to determine the signal strength, MAC address, and encryption protocols of the target network. This step is necessary to enhance the credibility of the rogue access point to be set up later. As shown in Figure 5, network scanning is conducted by selecting the Airodump-ng tool.

The scanning performed by the Airodump-ng tool involves the attacker using their wireless network card in monitoring mode to scan the surrounding wireless networks and assess which of these networks could potentially be targeted for a rogue access point in an evil twin attack. From the scan results, the attacker can gather information such as signal strength, ESSID, and MAC address of the networks, which will be utilized to make the rogue access point appear more legitimate and deceive users of the target network.

In the example of a real case where our objective is to obtain passwords associated with the targeted organization, we opted for the 6th method from the menu (Figure 6). This method is crafted to mimic the official modem interface commonly used by users during network connection. Consequently, users are

prompted to enter their credentials, creating an illusion of connecting to the authentic network.

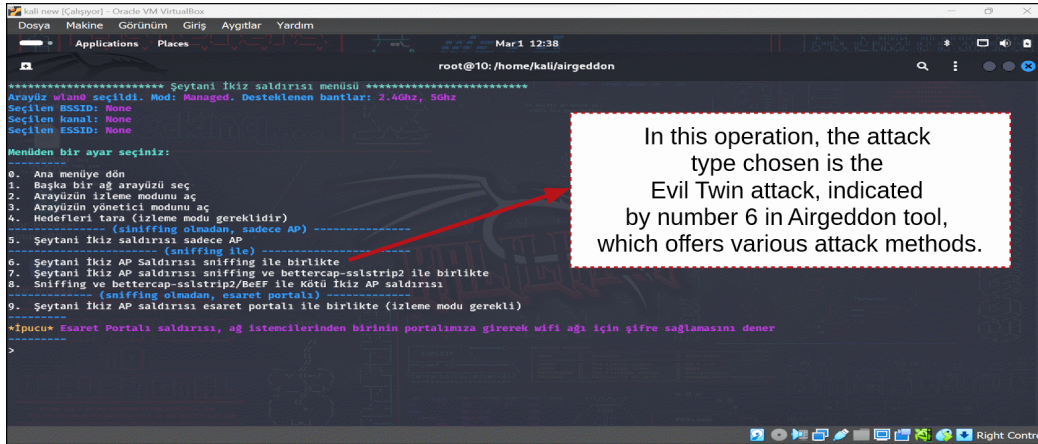


Figure 6. Selection of an Evil Twin attack type using the Airgeddon tool.

Following this step, the target network is identified, and the Evil Twin attack is initiated using the Airgeddon tool. As the attack commences, the perpetrator enters a waiting phase, displaying a series of interfaces and screens. In this attack methodology, the expected waiting time typically varies between 1 to 45 minutes (ref). During the attack, the perpetrator forcibly disconnects users from the current network through a deauthentication (death) process, compelling them to connect to the perpetrator's fake network (Figure 7). This strategy aims to deceive users into connecting to the fake network, resembling a genuine one, in order to obtain the victim's credentials.



Figure 7. Selection of an Evil Twin attack type using the Airgeddon tool.

Among the various deauthentication methods available in the Airgeddon tool, the perpetrator selects the one they consider most effective, often identified as

“Death aireplay attack” (number 2) (Figure 7). This method targets all devices on the network using the aireplay-ng tool, causing them to disconnect from the network and thus forcing users to reconnect. Once the channel hopping feature is disabled and the selected interface is confirmed, the perpetrator awaits users to connect through the fake network (Figure 7).

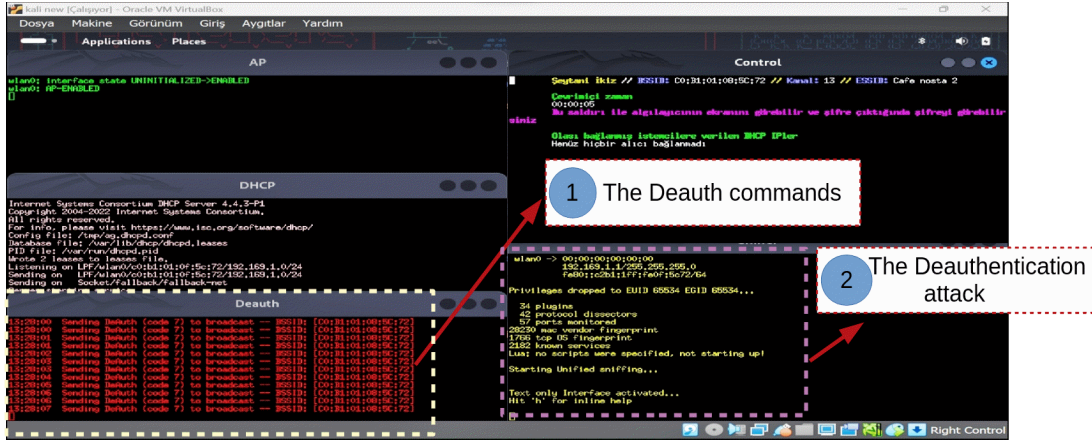


Figure 8. The Death commands and the moment of deauthentication attack.

In Figure 8 (1), continuous “Death” commands are observed. This method is used to disconnect users from the legitimate network and force them to connect to the perpetrator's fake network. The deauthentication attack disrupts users' current connections, prompting them to automatically reconnect to the strongest signal, which in this case would be the perpetrator's fake network.

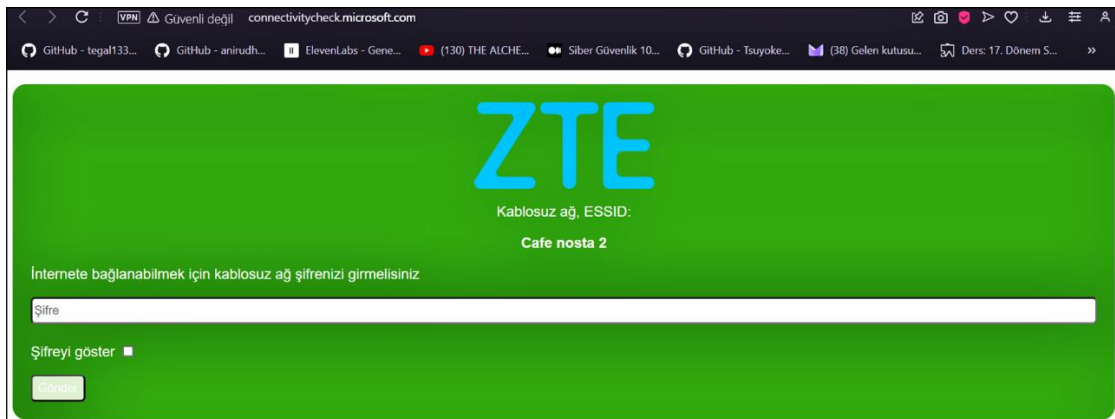
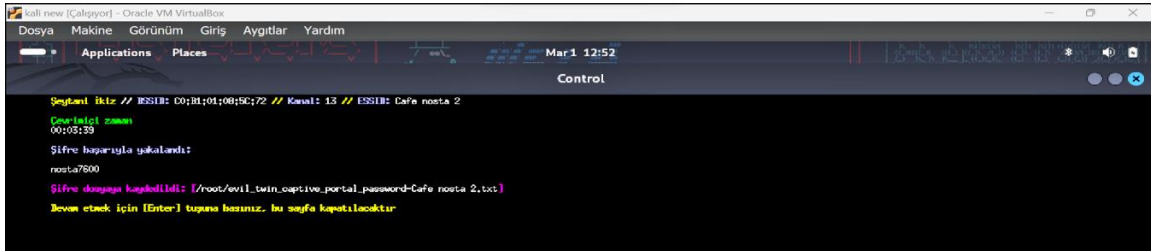


Figure 8. Configured login portal for victim connection.

Upon connection, the user will be greeted with a page prompting them to enter a specially configured WiFi password. This page can be customized to withhold internet access until the user provides the requested information (Figure 9). Additionally, even if an incorrect password is entered, internet access will not be

granted; only when the correct password is entered will the victim be granted internet access. These measures are designed to enhance information security and prevent unauthorized access.



```

koll new (Çalışıyor) - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
Applications Places Mar 1 12:52
Control
Şeybeni İkiz // ESSID: D0:B1:01:00:5C:72 // Kanal: 13 // ESSID: Cafe_nosta_2
Çevrimiçi zaman: 00:03:39
Sifre başarıyla saklandı:
nosta7600
Sifre dogayla kaydedildi: [/root/evil_twin_captive_portal_password-Cafe_nosta_2.txt]
Izlem etmek için [Enter] tuşuna basınız. İki sayfa kapatılmaktadır

```

Figure 9. Demonstration of successful completion and results of Evil Twin attack.

Figure 9 shows the successful completion and results of a wireless network attack scenario. At this stage, it is evident that a user has entered a password into the fake network portal, and this entry has been captured by the attacker. Alongside a message confirming the successful entry, it is indicated that the password entered by the user has been saved to a file and reflected in the Linux terminal. This outcome demonstrates how, within the context of an Evil Twin attack, the attacker gathers and stores authentication information obtained from the target user. By convincing the user to connect to their controlled fake network and enter the network password, the attacker gains access to this information.

4 DISCUSSION

Evil Twin attacks stand out as a significant security threat in wireless networks. These types of attacks aim to capture users' information by creating fake access points. This type of attack can seriously threaten the information security of users and organizations, leading to financial losses. Therefore, it is important to develop and implement effective protection strategies against Evil Twin attacks. Hence, this study conducted a real case analysis to address the potential risks of Evil Twin attacks and the measures to be taken.

Such attacks are often carried out without users' awareness and can result in the capture of sensitive information or the deception of users. In this context, it is important for users to be aware of and implement protection strategies against Evil Twin attacks. Additionally, the effects of Evil Twin attacks on organizations and businesses should be examined. These attacks can jeopardize the reputation and

credibility of businesses and put customers' security at risk. Therefore, it is necessary for businesses to strengthen their defense strategies against Evil Twin attacks and take necessary measures to protect sensitive information.

The methods used to carry out the attack need to be evaluated in the case analysis examined in the study. Firstly, it is important that such tools are used within a legal framework. The usage of hacking tools and unauthorized access to networks are illegal in many countries and can have serious legal consequences. Therefore, it is important that these tools are used only for legal and ethical purposes. Additionally, the usage of these tools brings ethical considerations. Cybersecurity experts should respect personal privacy and security while using these tools and should not engage in unauthorized access.

Furthermore, the potential harms and consequences of using these tools should be taken into account. A step-by-step scenario has been created for the execution of Evil Twin attacks, clearly demonstrating the steps taken by the attacker to gain access to the target network. As a result of these steps, the attacker has gained unauthorized access to systems by capturing the identities of legitimate users, thereby increasing the likelihood of accessing sensitive data, seizing control of systems, and engaging in other malicious activities. However, the impact and damage of the attack can vary depending on the attacker's motivation and the security measures of the target network.

To effectively counteract evil twin attacks, it is essential to implement a comprehensive set of preventive measures and defense strategies. First, employing robust and up-to-date network security protocols and encryption methods is crucial. Network administrators should secure their networks using the latest encryption standards, such as WPA3, and encourage the use of strong, complex passwords to further enhance security. In addition to encryption, regular security vulnerability scans and penetration tests are necessary to identify and mitigate network vulnerabilities. These ongoing scans help administrators understand the evolving techniques used by attackers, enabling them to develop targeted defense strategies against threats like evil twin attacks.

Furthermore, the utilization of firewalls and network monitoring tools by both administrators and users is vital to track network traffic and detect any unusual

activities, facilitating early detection and prevention. Raising end-user awareness is equally significant in creating a multi-layered defense system. By educating users on how to recognize fake access points and avoid connecting to untrusted networks, the overall effectiveness of these preventive measures can be greatly enhanced. Security awareness training provides users with the knowledge needed to understand the risks posed by evil twin attacks and how to protect themselves accordingly.

Assessing the effectiveness of evil twin attacks in different environments is also important for understanding their potential impact in real-world situations. For example, evaluating how these attacks perform on networks using different security standards—such as WPA, WPA2, and WPA3—reveals specific vulnerabilities and indicates which protocols are more resistant. Even advanced encryption like WPA3 may be vulnerable under certain conditions, particularly due to user errors or incorrect configurations.

Acknowledging the limitations of the tools used to execute these attacks is also crucial. The dependency on specific hardware and software, especially when targeting networks with enhanced security measures, can significantly restrict the effectiveness of these attacks. The success of an evil twin attack is often influenced by the capabilities of the tools and the security measures in place within the target network, showing that both environmental and technological factors significantly affect the outcome.

Considering future advancements is essential when discussing the progression of evil twin attacks. The integration of new technologies, such as artificial intelligence and machine learning, could make these attacks harder to detect while allowing attackers to use more advanced techniques. Therefore, it is imperative to strengthen existing defense mechanisms and advance AI-driven detection methods. Such developments will ensure that defense strategies are continuously adapted to counter new and sophisticated threats.

Finally, the protection strategies presented in this study emphasize both enhancing security protocols and increasing user awareness. The adoption of advanced encryption standards and robust authentication mechanisms forms the foundation of a strong defense against evil twin attacks. Moreover, improving user awareness is equally critical—organizations should regularly provide security training

to help end-users recognize and avoid untrusted access points. Empowering users with the skills and knowledge needed to identify potential threats will significantly improve overall resilience to such attacks. These user-centered strategies, in conjunction with technical countermeasures, create a holistic approach to mitigating the risks associated with evil twin attacks.

5 CONCLUSION AND SUGGESTIONS

Evil twin attacks pose a significant cybersecurity threat to both users and companies. These attacks can compromise the identities of legitimate users, gain unauthorized access to systems, and potentially cause extensive financial and reputational damage by compromising sensitive data. The analysis conducted in this study examines a real case of evil twin attacks, focusing on the strategies employed by attackers, the analysis methods of this threat, and defense mechanisms against it.

Understanding the thought process and strategies of attackers is a critical step in preventing evil twin attacks in cyberspace. This understanding can serve as an important tool for cybersecurity experts to anticipate attackers' actions and adjust defense strategies accordingly. Firstly, understanding the motivations and objectives of attackers can help in identifying potential targets and directing their attacks. Secondly, analyzing the techniques and strategies used by attackers can help identify weaknesses in existing defense mechanisms. This is crucial for strengthening defense strategies and effectively preventing attacks. Additionally, a detailed analysis of attackers' pre-attack preparations and behavior during attacks can help cybersecurity experts improve their ability to detect and respond to attacks. These insights can contribute to the development of more effective cybersecurity strategies and the enhancement of stronger defense mechanisms against evil twin attacks in cyberspace.

To effectively mitigate the risks posed by rogue access point attacks, users must adopt a range of precautionary measures, as outlined below:

1. **Avoiding Untrusted Networks:** Users should avoid connecting to wireless networks whose authenticity cannot be verified. This is particularly pertinent

to free Wi-Fi services in public places, as these networks carry a high risk of impersonation.

2. **Verification of Access Point Identity:** Before connecting to a wireless network, users must verify the network name and identity carefully. Any unexpected or unfamiliar network name might indicate a potential attack, in which case users should refrain from connecting.
3. **Enhancing Security Through VPN Usage:** Utilizing a Virtual Private Network (VPN) encrypts internet traffic, thereby enhancing security and preventing attackers from intercepting the data. This measure is especially critical when using public networks to ensure user privacy.
4. **Disabling Automatic Connection Feature:** The automatic connection feature in devices may result in connecting to untrusted networks without the user's knowledge. Disabling this feature can prevent inadvertent connections to potentially harmful networks, thereby increasing security.
5. **Utilization of Updated Security Software and Antivirus:** Keeping security software and antivirus programs up to date is crucial for identifying and mitigating potential threats. This proactive approach strengthens the defense against malicious access points.
6. **Securing Data Using HTTPS Protocol:** Users are encouraged to use the HTTPS protocol during their internet activities to ensure data traffic is encrypted, thereby reducing the risk of sensitive information being compromised. This protocol plays a key role in safeguarding personal information such as credentials.

These measures are intended to reinforce the security of end-users against potential threats that may arise in wireless networks. By implementing such strategies, users can become more resilient to attacks such as the evil twin.

The knowledge and skills required to execute evil twin attacks necessitate expertise in the field of cybersecurity. Therefore, organizations should strengthen their defense mechanisms, provide continuous training for personnel, and regularly update security measures. Additionally, legal and ethical considerations should be

taken into account, and organizations should strive to fully comply with laws and ethical standards.

Future research should focus on developing more effective defense strategies against evil twin attacks. This requires a comprehensive research effort focused on better understanding attack methods, improving defense mechanisms, and advancing cybersecurity technologies. Moreover, increasing collaboration and information sharing can accelerate developments in cybersecurity and support organizations in creating a more secure cyber environment. In this way, organizations can establish a more secure and reliable cyber environment and minimize the impacts of cyber-attacks.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics.

REFERENCES

- [1] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, D. Sicker, "Practical defenses for evil twin attacks in 802.11," *In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010* IEEE. 2010. pp. 1-6.
- [2] P. Shrivastava, J. Mohd Saalim and K. Kotaro, "EvilScout: Detection and mitigation of evil twin attack in SDN enabled WiFi." *IEEE Transactions on Network and Service Management* vol.17.1, pp. 89-102. 2020.
- [3] R. Banakh, A. Piskozub, I. Opirskyy, "Devising A Method For Detecting Evil Twin" Attacks On IEEE 802.11 Networks (Wi-Fi) With Knn Classification Model. *Eastern-European Journal of Enterprise Technologies*, vol.9, pp.123, 2023.
- [4] F. Lanze, A. Panchenko, I. Ponce-Alcaide, T. Engel, "Undesired relatives: protection mechanisms against the evil twin attack in IEEE 802.11," *In Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*, pp. 87-94, 2014.
- [5] L. M. da Silva, V. M. Andregretti, R. A. F. Romero, K. R. L. J. C. Branco, "Analysis and Identification of Evil Twin Attack through Data Science Techniques Using AWID3 Dataset," *In Proceedings of the 6th International Conference on Machine Learning and Machine Intelligence* pp. 128-135. 2023.
- [6] A.S. Guide, "Evil Twins: Handling Repetitions in Attack-Defense Trees," *In Graphical Models for Security: 4th International Workshop, GramSec 2017, Santa Barbara, CA, USA, August 21, 2017, Revised Selected Papers*, Springer. Vol. 10744, p. 17, 2018.
- [7] R. Muthalagu, S. Sanjay, "Evil twin attack mitigation techniques in 802.11 networks," *International Journal of Advanced Computer Science and Applications*, vol.6, pp.12, 2021.

- [8] M.S. Ahmad, S. Lutfi, and S. D. Abdullah. "Extended generic process model for analysis mitm attack based on evil twin." *Journal of Physics: Conference Series*. Vol. 1569. No. 2. IOP Publishing, 2020.
- [9] Q. Lu, H. Qu, Y. Zhuang, X.J. Lin, Y. Zhu, Y. Liu, "A passive client-based approach to detect evil twin attacks," *In 2017 IEEE Trustcom/BigDataSE/ICSS*, pp. 233-239, 2017.
- [10] A. Esser, C. Serrao, "Wi-Fi network testing using an integrated Evil-Twin framework," *In 2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, IEEE. pp. 216-221, 2018.