Rouge Access Point

Yogaraj Govindarajalu Prabagaran

Table of Contents

[Lab 1 – Rouge Access Point 3](#_Toc162216932)

[Part A 3](#_Toc162216933)

[Task- Investigation of a Wireless Environment. 3](#_Toc162216934)

[Description 3](#_Toc162216935)

[Observations 3](#_Toc162216936)

[Screenshots 4](#_Toc162216937)

[Reflection 5](#_Toc162216938)

[Part B 5](#_Toc162216939)

[Task- Creation of a rogue access point for malicious activity. 5](#_Toc162216940)

[Description 5](#_Toc162216941)

[Preparation 5](#_Toc162216942)

[Observations 6](#_Toc162216943)

[Screenshots 7](#_Toc162216944)

[Reflection 9](#_Toc162216945)

[References 9](#_Toc162216946)

# Lab 1 – Rouge Access Point

# Part A

## Task- Investigation of a Wireless Environment.

## Description

This section underscores proficiency in identifying and evaluating Rogue Access Points, employing the inSSIDer application for meticulous analysis. The task involves strategically choosing a target location to examine all active wireless devices extensively. The focus is on extracting detailed information such as SSID, BSSID, signal strength, encryption type, Wi-Fi mode, and Max Data Rate, utilizing the capabilities of inSSIDer.

## Observations

* The **SSID** is found to be CCSecure.
* The **MAC address** is found to be Hewlett\_B6:0F: B2
* The **Manufacturer** is found to be Unknown.
* The **Signal strength** is found to be **-**59 dbm
* The **encryption type** is found to be **WPA**2-Enterprise
* The **Wi-Fi Mode** is found to be **a**/n/ac Wifi 5
* The **Max Data Rate** is found to be 385.2Mbps

The analysis reveals the presence of a network with the SSID "CCSecure," utilizing the MAC address Hewlett\_B6:0F:B2. However, manufacturer details were assumed to be Conestoga but were initially unknown even with the inSSIDer application. The signal strength is recorded at -59dBm, indicating a robust signal. The encryption type is identified as WPA2-Enterprise, suggesting a secure network configuration. The Wi-Fi mode is a/n/ac Wifi 5, indicative of a high-performance wireless standard. The maximum data rate is 385.2Mbps, reflecting the network's potential speed.

This comprehensive set of observations provides a detailed insight into the characteristics of the identified wireless network, aiding in assessing its security and potential classification as a Rogue Access Point.

## Screenshots

A screenshot of a computer

Description automatically generated

Figure 1.1 This screenshot displays the various Wifi networks available and my connected Wifi with a chain link symbol.

A screenshot of a computer

Description automatically generated

Figure 1.2 This screenshot depicts the router to which my Wi-Fi was connected.

A screenshot of a computer

Description automatically generated

Figure 1.3 This Screenshot displays various types of information, prominently the MAC address information.

## Reflection

As the application unfolded its interface, my connected Wi-Fi CCSecure was adorned with a distinctive star symbol and chain symbol. The application cataloged all routers within its range, succinctly pinpointing the one to which my device was tethered through the consistent chain symbol. Utilizing the binocular symbol on the right side of the network facilitated displaying comprehensive details of the selected option. This intuitive feature seamlessly provided a wealth of data, including SSID, MAC address, signal strength, encryption type, Wi-Fi mode, and Max Data Rate — elements instrumental in scrutinizing the wireless landscape.

The symbology employed, particularly the chain and binocular symbols, streamlined the identification and exploration process, rendering the task of gathering intricate router specifics remarkably efficient. This hands-on experience with inSSIDer showcased its user-friendly design and functionality, contributing to a seamless analysis of the wireless environment. The symbiotic interplay between symbols and data extraction demonstrated the tool's effectiveness in deciphering the nuances of each connected router, laying the foundation for a comprehensive assessment of potential Rogue Access Points.

# Part B

## Task- Creation of a rogue access point for malicious activity.

## Description

This section details the hands-on process of attempting to create a rogue access point using the Airbase-ng command in Kali Linux. It highlights the potential implications in the context of attacker use.

## Preparation

* Installation of VMWare Workstation Pro and the appropriate license was obtained.
* Kali Linux template was downloaded, and the VM task was successfully installed.
* A Wireless adapter (AWUS036NEH IEEE 802.11b/g/n) was used as well.
* Usage of the Airbase-ng command is required.

## Observations

The hands-on exploration involving the creation of a rogue access point using tools like Airbase-ng provided valuable insights into the potential risks associated with such malicious activities.

Understanding the Process:

Initial Setup:

Opening Kali Linux on VMware Workstation marked the initiation of the process, creating an isolated environment conducive to security testing.

Hardware Connection:

The connection of a wireless network adapter to the laptop laid the groundwork for the subsequent steps in creating the rogue access point.

Airbase-ng Command Execution:

Executing the command airbase-ng -e Ygov9578 -c 11 wlan0 demonstrated the simplicity with which a rogue access point can be instantiated, with "Ygov9578" as the designated SSID and channel 11 as the operating channel.

Immediate Wi-Fi Connection Creation:

The rapid creation of a Wi-Fi connection named "Ygov9578," as visually represented in Figure 3.1, underscored the efficiency of tools like Airbase-ng in executing rogue access point attacks.

MAC Address Attribution:

Generating a MAC address for the rogue Wi-Fi connection added an additional layer of camouflage, complicating detection efforts.

Security Vulnerabilities:

The crucial observation that the Wi-Fi connection lacked secure encryption raised concerns. The open and unsecured nature of the connection rendered it accessible to anyone in proximity, exposing a potential avenue for unauthorized network access.

Implications for Attackers:

The hands-on experience shed light on the ease with which attackers could leverage tools like Airbase-ng to deploy rogue access points. The speed at which a seemingly genuine Wi-Fi connection was established and the lack of encryption emphasized the potential risks for unsuspecting users connecting to such rogue networks.

Defensive Considerations:

This practical experiment emphasizes the significance of strong security measures to prevent rogue access point assaults. Network administrators and security experts must be careful in enforcing encryption methods, monitoring unauthorized access points, and teaching users about the dangers of connecting to insecure networks.

In conclusion, this hands-on examination provided a sharp reminder of the real-world vulnerabilities faced by rogue access points and the importance of proactive security measures to limit the risks associated with such malicious activity.

## Screenshots

A screenshot of a computer

Description automatically generated

Figure 3.1 This screenshot illustrates rogue access being generated and the Wi-Fi connection indicating that it is open and unsafe.

A diagram of a network connection

Description automatically generated

Figure 3.2 This image illustrates the working of a Rogue AP that could steal information from the Client.



**Image generated by AI.**Figure 3.3 This fun image helps to visualize hackers deploying a Rogue AP to monitor people’s activity on the Internet.

A screen shot of a computer

Description automatically generated

Figure 3.4 This screenshot demonstrates the victim’s browser activity while connecting with the rogue IP.

## Reflection

In undertaking the task of creating a rogue access point using tools like Airbase-ng, the experience provided a hands-on exploration into the swift and straightforward execution of such malicious activities. The process, involving the setup in Kali Linux on VMware Workstation, connecting a wireless adapter, and running Airbase-ng commands, elucidated the efficiency with which attackers can deploy rogue access points. The immediate creation of an unsecured Wi-Fi connection named "Ygov9578," complete with a unique MAC address, underscored the potential risks for unsuspecting users. This practical exercise revealed the ease with which attackers could exploit vulnerabilities. It emphasized the critical need for robust security measures, including encryption protocols and user awareness, to mitigate the inherent risks of rogue access point attacks.

# References

1. C. H. (2014, March 2). *How To: Create A Fake Access Point On Kali Linux (Rogue AP MItM Attack)*. YouTube. <https://www.youtube.com/watch?v=HePt2J4uSno>
2. L. L. Y. (2018, March 3). *Rogue Access Points with Kali Linux (Cybersecurity)*. YouTube. <https://www.youtube.com/watch?v=MXwOgB-ODmI>
3. S. C. (2018, January 16). *Rogue Access Point and Evil Twin*. YouTube. <https://www.youtube.com/watch?v=FQ5mCHrC91A>