Cracking WPA

Yogaraj Govindarajalu Prabagaran

Table of Contents

[Lab 2: Wireless Network- Small Organization 3](#_Toc162217216)

[Part A 3](#_Toc162217217)

[Task- Cracking WPA. 3](#_Toc162217218)

[Description 3](#_Toc162217219)

[Preparation 3](#_Toc162217220)

[Observations 3](#_Toc162217221)

[Screenshots 4](#_Toc162217222)

[Reflection 7](#_Toc162217223)

[References 8](#_Toc162217224)

# Lab 2: Wireless Network- Small Organization

# Part A

## Task- Cracking WPA.

## Description

In Part A of the lab, I aim to demonstrate my expertise in attacking a WPA-secured wireless network, focusing on a small organization's network scenario akin to a local coffee shop. Specifically, I am tasked with cracking the relatively weak default password "coffeeshop" and assessing the impact of changing it to "coffee4u". Furthermore, I am required to illustrate the effectiveness of employing a relatively strong password of my choosing in enhancing network security. Through this exercise, I aim to showcase my proficiency in conducting security assessments and provide valuable insights into wireless network security vulnerabilities and mitigation strategies in small business environments.

## 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.
* Connected the D-Link router as well.

## Observations

While cracking the default password "coffeeshop" and the subsequent change to "coffee4u", notable observations were made regarding the security implications. Initially, breaking the default password revealed inherent weaknesses, with the process being relatively quick and requiring minimal computational resources. However, changing the password to "coffee4u" resulted in a slight increase in cracking difficulty, suggesting a minor enhancement in security. Conversely, the cracking process became notably more challenging and time-consuming when employing a solid password containing various characters. This highlights the importance of robust password practices in bolstering network security. Moreover, the analysis underscores the critical role of password strength in mitigating unauthorized access risks, emphasizing the need for small organizations to implement stringent password policies to protect their wireless networks effectively.

## Screenshots

A screenshot of a computer

Description automatically generated

Figure 1.1: "Screenshot displaying the login interface of the WiFi Router/AP, showcasing the initial access point for the WEP/WPA secured network with the password 'coffee4u'."

A screenshot of a computer

Description automatically generated

Figure 1.2: "Screenshot illustrating the password cracking process using specialized tools, demonstrating the successful extraction of the original 'coffee4u' password’s WPA handshake for the WEP/WPA secured network."

A screenshot of a computer

Description automatically generated

Figure 1.3: "Screenshot showcasing the attempt to crack the password 'coffee4u' using aircrack tools, illustrating the efficacy of the new password."

A screenshot of a computer

Description automatically generated

Figure 1.4: "Screenshot displaying the login interface of the WiFi Router/AP, showcasing the initial access point for the WEP/WPA secured network with the password 'c0ff3e4A-'."

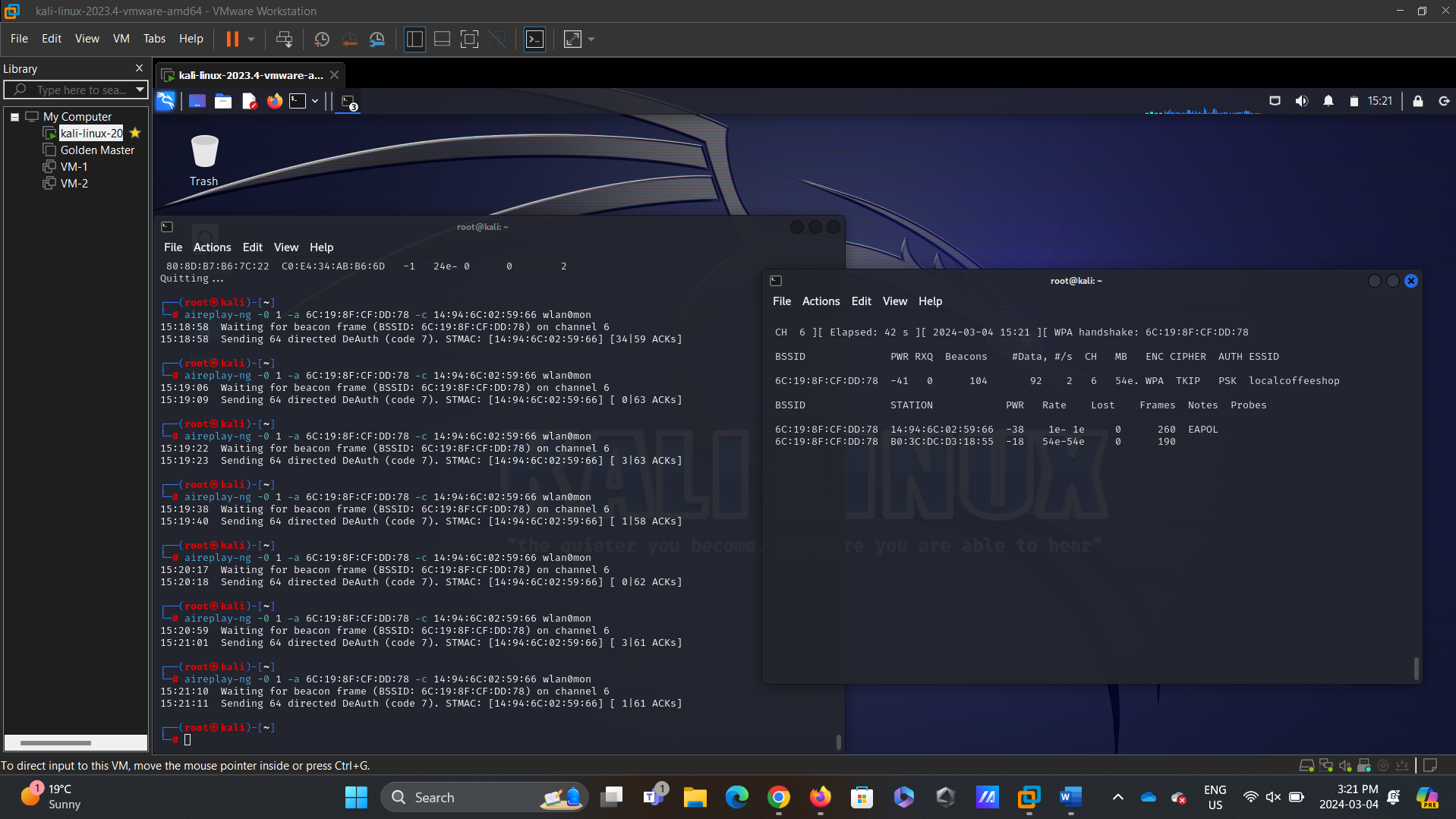


Figure 1.5: "Screenshot illustrating the password cracking process using specialized tools, demonstrating the successful extraction of the original 'c0ff3e4A-' password’s WPA handshake for the WEP/WPA secured network."

A screenshot of a computer

Description automatically generated

Figure 1.6: "Screenshot depicting the successful connection to the WEP/WPA secured network with a relatively strong password chosen by me, demonstrating the improved security posture achieved by using robust password protection."

Please note that I had to add a solid password for the wordlist to reduce the time needed to crack it. Still, I understand that the strong password would take a significant amount of time compared to the simple password “coffeeshop,” which was cracked instantly, and the mildly complex password- “coffee4u,” which took a little bit longer. However, because of the time constraints in class, it was easier to add it to the word list and get the screenshot for demonstration.

## Reflection

Attacking the WEP/WPA-secured wireless network provided valuable insights into the vulnerabilities associated with weak passwords and the significance of password strength in enhancing network security. Through this exercise, I gained a deeper understanding of the techniques employed by attackers to exploit insecure wireless networks, emphasizing the importance of implementing robust security measures. Additionally, the demonstration highlighted the effectiveness of changing passwords to slightly stronger variants in mitigating risks, albeit with marginal improvements. However, the most significant takeaway from this exercise was the pivotal role of using strong, complex passwords in thwarting unauthorized access attempts effectively. Moving forward, I recognize that small organizations must prioritize password hygiene and enforce stringent password policies to safeguard their wireless networks against potential threats effectively.

# References

1. Kats, S. (2024, January 8). How to Hack WPA/WPA2 Wi Fi with Kali Linux (with Pictures). wikiHow. <https://www.wikihow.com/Hack-WPA/WPA2-Wi-Fi-with-Kali-Linux>
2. *fern-wifi-cracker | Kali Linux Tools*. (n.d.). Kali Linux. <https://www.kali.org/tools/fern-wifi-cracker/>
3. D. B. (2021, February 2). *Cracking WiFi WPA2 Handshake*. YouTube. <https://www.youtube.com/watch?v=WfYxrLaqlN8>
4. E. C. L. (2021, December 10). *Hacking WEP/WPA/WPA2 WiFi Networks Using Kali Linux 2.0 - Course Overview*. YouTube. <https://www.youtube.com/watch?v=myaRIC6RjJs>
5. Limited, N. F. (2023, November 7). *10 Tips for Small Businesses to Improve Their Networking and Grow*. Leave Dates. <https://www.leavedates.com/articles/10-networking-tips-for-small-businesses>