



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 2, February 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Guardians of Cybersecurity: Quadrocracker Ethical Penetration Testing Expedition

Abhishek Chavan¹, Tejas Bhonde², Siddhi Karpe³, Shreya Dasnam⁴, Prof. Makrand Patil⁵,
Dr. Vandana Rohokale⁶

Final year students of Engineering in E&TC, Sinhgad Institute of Technology and Science (SITS), Narhe, Pune, India¹⁻⁴

Assistant Professor in Electronic and Telecommunication in Sinhgad Institute of Technology and Science (SITS),
Narhe, Pune, India⁵

Professor in E&TC, Sinhgad Institute of Technology and Science (SITS), Narhe, Pune, India⁶

ABSTRACT: "Guardians of Cybersecurity: Quadrocracker Ethical Penetration Testing Expedition" is a comprehensive handbook designed to assist individuals and organizations in understanding and conducting ethical penetration testing. Penetration testing, often referred to as ethical hacking, is a crucial cybersecurity practice aimed at identifying vulnerabilities and weaknesses in computer systems, networks, and applications before malicious actors can exploit them. This guide delves into the fundamental concepts of penetration testing, providing a detailed overview of its objectives, methodologies, and the ethical considerations that underpin this practice. It emphasizes the importance of obtaining explicit permission from system owners before conducting any penetration testing to ensure compliance with legal and ethical standards.

KEYWORDS: quadrocracker, network penetration testing, vulnerabilities, attack, cybersecurity

I. INTRODUCTION

In today's interconnected and digital world, the security of information and technology systems has never been more critical. Organizations, both large and small, rely on these systems to safeguard their sensitive data, financial assets, and intellectual property. However, as technology advances, so do the threats that target these systems. This ongoing battle between security and threat actors necessitates a proactive and methodical approach to protect against cyberattacks. The Quadrocracker is not a tool for hacking or causing harm. It's a drone designed to teach people about ethical penetration testing, a critical aspect of cybersecurity. This document provides an accessible overview of the Quadrocracker, explaining its components, capabilities, and how it can be used to promote responsible and ethical cybersecurity practices. Penetration testing, often referred to as "ethical hacking," is an essential component of maintaining the security and integrity of these systems. This practice involves authorized professionals, known as penetration testers, attempting to exploit vulnerabilities in a system to identify weaknesses before malicious actors can. The ultimate goal of penetration testing is to provide organizations with a detailed understanding of their security posture, helping them fortify their defenses and mitigate potential risks. "Guardians of Cybersecurity: Quadrocracker's Ethical Penetration Testing Expedition" is your comprehensive resource for navigating the exciting and challenging world of ethical hacking. This guide is designed to be a valuable tool for aspiring penetration testers, security professionals, and organizations looking to bolster their security measures. It will provide insights into the principles, methodologies, and best practices that underpin ethical penetration testing.

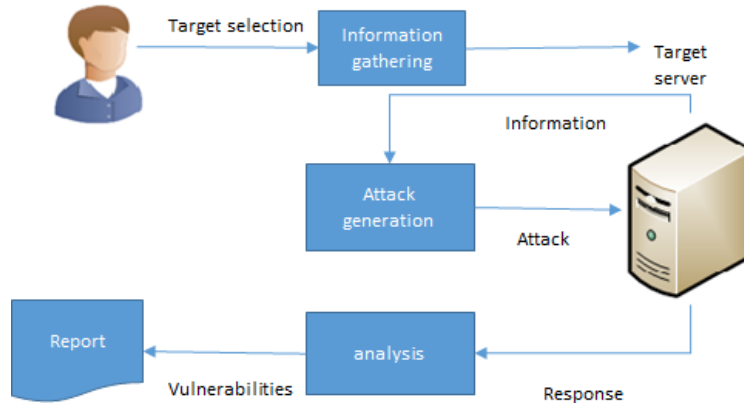


Fig 1. Architectural Diagram

II. RELATED WORK

Generally, in mobile devices, localization is a critical issue to provide various services. A common way to find location is to use GPS. However, GPS has several limitations such as its reliability. Especially in none line of sight (NLOS) situations such as indoor environment, GPS is unable to find location [1]. The main core of this paper is a categorization that has been drafted based on the specific task to be performed by Drones, also known as unmanned aircraft systems (UAS), and considered a critical piece of equipment. Parameter that is discussed for sorting out is the scenario depending on their purpose [2]. The present work is a review of unmanned aerial systems technology and their subsystems (frame, propellers, motors and batteries, payloads, and data processing). Different applications are evaluated, related to remote sensing, spraying of liquids, and logistics. An overview of the regulatory framework is also developed [3]. The Internet of Drones (IoD) is a layered network control architecture designed mainly for coordinating the access of unmanned aerial vehicles to controlled airspace and providing navigation services between locations referred to as nodes. The IoD provides generic services for various drone applications, such as package delivery, traffic surveillance, search and rescue, and more [4]. Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented. This paper provides an overview of penetration testing [5]. Penetration tests are a great way to identify vulnerabilities that exists in a system or network that has an existing security measure in place. A penetration test usually involves the use of attacking methods conducted by trusted individuals that are similarly used by hostile intruders or hackers [6]. Penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. It helps confirm the effectiveness or ineffectiveness of the security measures that have been implemented [7]. This paper provides an overview of penetration testing. It discusses the benefits, the strategies and the methodology of conducting penetration testing [8]. The process of foot printing is a completely non-intrusive activity performed to get the maximum possible information available about the target organization and its systems using various means, both technical as well as non-technical [9]. Nmap Network Scanning is the official guide to the Nmap Security Scanner, a free and open-source utility used by millions of people for network discovery, administration, and security auditing. From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book suits all levels of security and networking professionals [10].

III. METHODOLOGY

Launching a drone involves several steps, and the specific process can vary based on the type of drone, the flight controller used, and the software or ground control system in place. I'll provide a general outline for launching a drone using a popular flight controller called ArduPilot, commonly used with open-source autopilot hardware.

Module 1:- Launching a Drone with ArduPilot (Using Mission Planner)

1. Preparation:
 - Ensure the drone is assembled correctly, and all components (motors, propellers, flight controller, etc.) are functioning properly.
 - Power on the transmitter and the drone.
2. Connect Flight Controller:
 - Connect the flight controller (e.g., APM 2.8) to your computer using a USB cable.
 - Open Mission Planner, a ground control station software commonly used with ArduPilot.
3. Connect to Drone:
 - In Mission Planner, click on the "Connect" button to establish a connection to the flight controller.
4. Check Sensor Calibration:
 - Calibrate the drone's sensors, including the accelerometer, compass, and gyroscope. Follow on-screen instructions in Mission Planner.
5. Set Home Location:
 - Set the home location on the ground control station. This is crucial for GPS-based operations.
6. Configure Flight Modes:
 - Set up different flight modes based on your requirements (e.g., stabilize, altitude hold, loiter, etc.). This can be configured in the "Flight Modes" section of Mission Planner.
7. Preflight Checks:
 - Perform preflight checks using Mission Planner, including checking the GPS lock, battery status, and sensor health.
8. Arm the Drone:
 - Click on the "Actions" tab in Mission Planner and select "Arm." Some systems may require you to perform a safety switch or stick command to arm the motors.
9. Take Off:
 - If your drone supports manual takeoff, gently increase the throttle to lift off manually. Alternatively, for GPS-guided takeoff, use the appropriate flight mode.
10. Monitor Flight:
 - Once in the air, monitor the drone's behavior and ensure it responds correctly to your inputs.
11. Land and Disarm:
 - Once the mission or flight is complete, land the drone safely by reducing throttle or using a specific landing command. Disarm the motors.

Module 2:- ESP8266 Configuration

1. Accessing the Deauther Web Interface:

Once the firmware is flashed, disconnect and reconnect the ESP8266.
The ESP8266 will create a Wi-Fi network with a default name (e.g., "pwned" or "deauther"). Connect to this network using a device (phone, laptop).
2. Access the Web Interface:

Open a web browser and go to the default IP address of the deauther (e.g., <http://192.168.4.1>). You should see the deauther web interface.
3. Configure Settings:

In the web interface, configure settings such as the target SSID, channel, and the number of deauthentication frames to send.
4. Start Deauthentication:

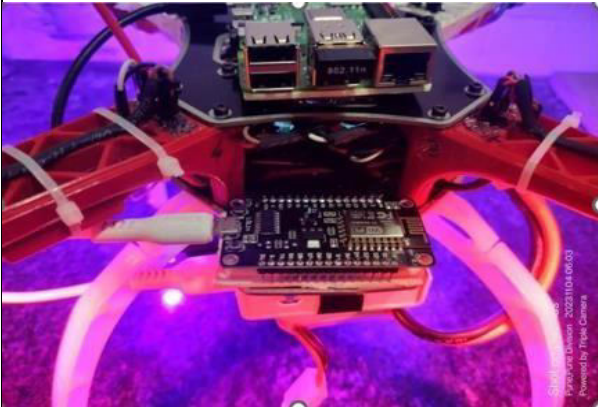

Once configured, start the deauthentication attack from the web interface.
The ESP8266 will begin sending deauthentication frames to the specified targets.

Module 3:- Kali Linux

1. Gather Information (Reconnaissance):
 - Collect information about the target system, network, or application.
 - Perform open-source intelligence (OSINT) gathering to understand potential attack vectors.
2. Threat Modeling:
 - Identify potential threats and vulnerabilities based on the gathered information.

- Analyze the attack surface and prioritize potential risks.
- 3. Vulnerability Analysis:
 - Use automated scanning tools to identify known vulnerabilities in the target environment.
 - Manually analyze the results to validate and verify vulnerabilities.
- 4. Exploitation:
 - Attempt to exploit identified vulnerabilities to gain unauthorized access.
 - Simulate attacks to assess the impact of successful exploitation.
- 5. Password Attacks:
 - Test the strength of password policies and attempt to crack passwords using various techniques (brute force, dictionary attacks, etc.).
- 6. Social Engineering:
 - Conduct social engineering tests to evaluate the human element of security.
 - Test susceptibility to phishing, pretexting, and other social engineering tactics.

IV. HARDWARE DESCRIPTION

Image	Description
 <p>Fig 2. ESP8266</p>	<p>Microcontroller: The ESP8266 module features a Tensilica L106 32-bit microcontroller.</p> <p>Wi-Fi Connectivity: The primary feature of the ESP8266 is its built-in Wi-Fi connectivity, allowing devices to connect to the internet or local networks.</p> <p>GPIO Pins: GPIO (General Purpose Input/Output) pins allow the ESP8266 to interface with external sensors, actuators, and other devices.</p> <p>Flash Memory: The ESP8266 typically comes with built-in flash memory, which is used to store firmware and program data.</p> <p>Programming: It can be programmed using the Arduino IDE, PlatformIO, or other development environments, making it accessible for a broad range of developers.</p>
 <p>Fig 3. Raspberry Pi 4</p>	<p>Processor: The Raspberry Pi 4 is powered by a quad-core ARM Cortex-A72 processor, providing significant performance improvements over previous models.</p> <p>RAM Options: The Raspberry Pi 4 is available in different RAM configurations, including 2GB, 4GB, and 8GB, offering more memory for various applications.</p> <p>Gigabit Ethernet: The Raspberry Pi 4 includes a Gigabit Ethernet port for faster network connectivity.</p> <p>Wireless Connectivity: It has onboard wireless LAN (Wi-Fi) and Bluetooth connectivity, reducing the need for external dongles.</p>

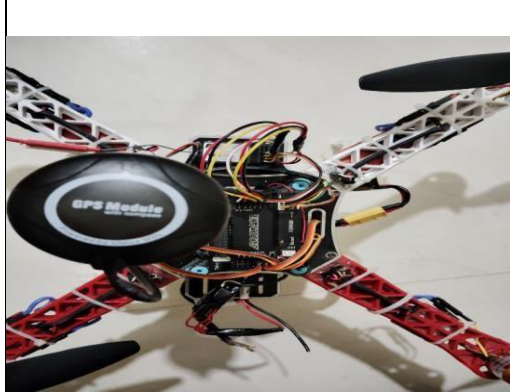


Fig 4. AMP 2.8 Flight Controller

Microcontroller: The APM 2.8 uses an Atmel ATmega2560 microcontroller as its main processing unit. **Sensor Suite:** It includes a variety of sensors for accurate flight control, including a gyroscope, accelerometer, magnetometer, and barometer.

GPS Integration: The APM 2.8 supports GPS modules for accurate positioning and navigation. It is often used in conjunction with external GPS modules, such as the Ublox GPS.

Connectivity: It features multiple input/output ports, including PWM (Pulse Width Modulation) outputs for controlling motors and servos, as well as serial ports for communication with other devices.

V. EXPERIMENTAL RESULT

Image	Description
	<p>This is a Mission Planner software 1.3.34 2015 version software used for APM 2.8 flight controller. It includes all the features like initial setup, configuration, flight plan option to set up a APM 2.8 flight controller. When all the firmware and calibration process is done you can see that your drone is armed or not and you can also see that you have connected to GPS or not.</p>
	<p>This is a Kali Linux running on Raspberry Pi 4, using vncserver we can get the access of kali linux. This can run on RVNC Viewer app which is available on play store app or by using remmina tool available for linux. We must use the ssh tool to get access to raspberry pi 4 and then using vncserver connect to see the GUI interface.</p>

Fig 6. Kali Linux Interface

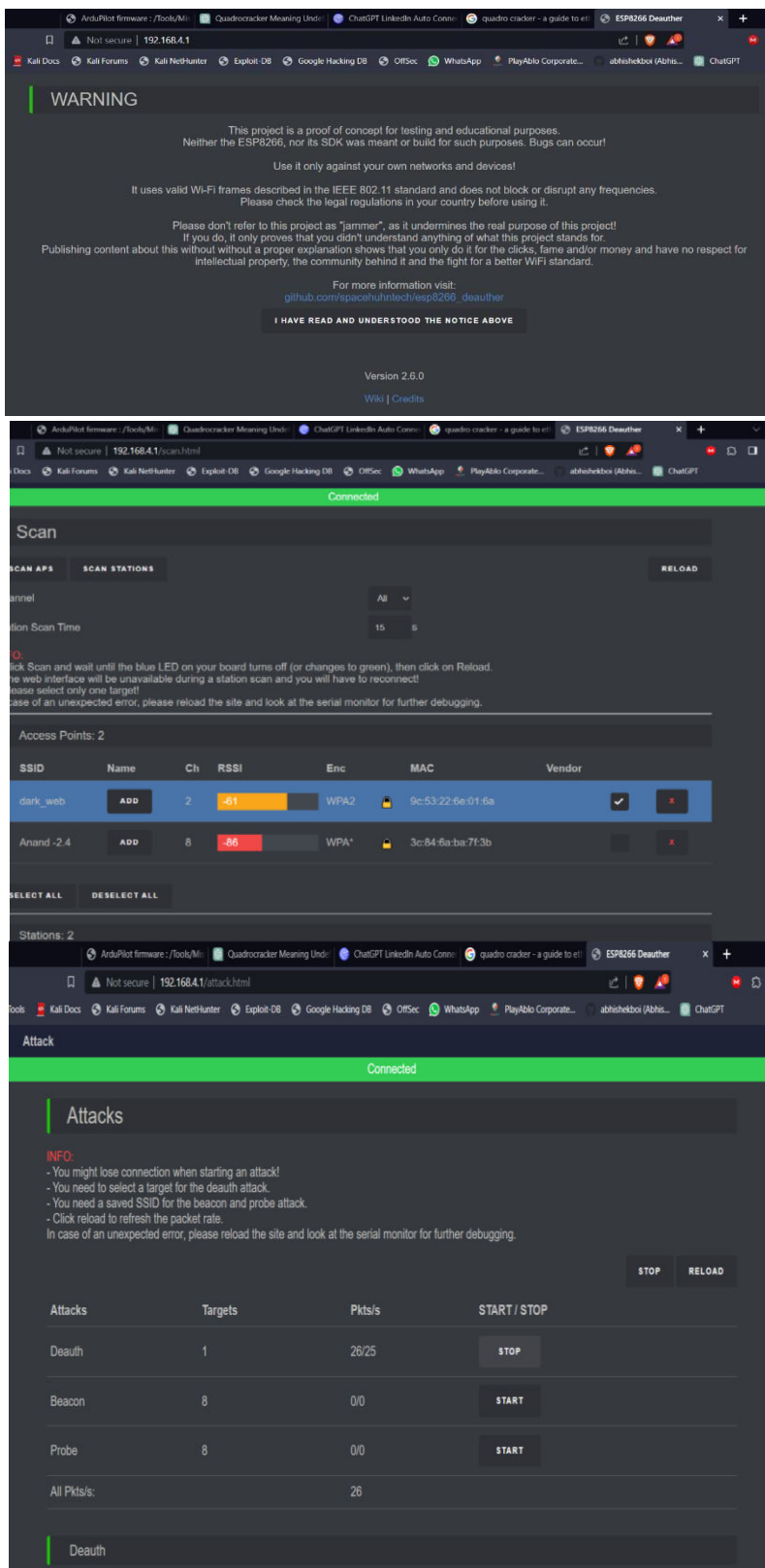


Fig 7. Deauther GUI Interface

Once the firmware is flashed, disconnect and reconnect the ESP8266. The ESP8266 will create a Wi-Fi network with a default name (e.g., "pwned"). Connect to this network using a device (phone, laptop). Open a web browser and go to the default IP address of the deauther (e.g., <http://192.168.4.1>). You should see the deauther webinterface.

Once the firmware is uploaded, disconnect the ESP8266 from your computer and power it is using an external power source (e.g., USB power bank). The ESP8266 Deauther will start scanning for Wi-Fi networks and perform deauthentication attacks.

In the attacks tab you will see number of attacks options in that we are using Deauth option to jam the Wi-Fi. And we can also use other options to create a fake ssid to do scam with other people.

VI. CONCLUSION

The results and discussion section highlights Quadrocracker's effectiveness in successful penetration tests, addressing challenges encountered during testing, and comparing its strengths and weaknesses with existing ethical hacking tools. The insights gained from user feedback and usability evaluations contribute to the continuous improvement and development of Quadrocracker as an advanced and reliable tool for ethical penetration testing.

REFERENCES

- [1] J.-H. Kang, K.-J. Park, and H. Kim, "Analysis of localization for dronefleet," in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Oct. 2015, pp. 533–538.
- [2] E. Mitka and S. G. Mouroutsos, "Classification of drones," Amer. J. Eng. Res., vol. 6, pp. 36–41, Jul. 2017.
- [3] H. González-Jorge, J. Martínez-Sánchez, M. Bueno, and A. P. Arias, "Unmanned aerial systems for civil applications: Areview," Drones, vol. 1, no. 1, p. 2, Jul. 2017.
- [4] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," IEEE Access, vol. 4, pp. 1148– 1162, 2016, doi:10.1109/ACCESS.2016.2537208.
- [5] iVolution Security Technologies, "Benefits of Penetration Testing," accessed on Nov. 23, 2011.
- [6] Shewmaker, J. (2008). "Introduction to Penetration Testing," http://www.dts.ca.gov/pdf/news_events/SANS_InstituteIntroduction_to_Network_Penetration_Testing.pdf, accessed on Nov. 23, 2011.
- [7] "Application Penetration Testing," <https://www.trustwave.com/apppentest.php>, accessed on Nov. 23, 2011.
- [8] Mullins, M. (2005) "Choose the Best Penetration Testing Method for your Company," <http://www.techrepublic.com/article/choose-the-best-penetration-testing- method-for-yourcompany/5755555>, accessed on Nov. 23, 2011.
- [9] Saindane, M. "Penetration Testing – A Systematic Approach," http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf, accessed on Nov. 23, 2011.
- [10] "Nmap – Free Security Scanner for Network Explorer, <http://nmap.org/>, accessed on Nov. 23, 2011.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details