IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Quadrocracker – A Guide To Ethical Penetration Testing

[1]Abhishek H. Chavan, [2]Tejas S. Bhonde, [3]Siddhi V. Karpe, [4]Shreya N. Dasnam

[1]Student, [2]Student, [3]Student, [4]Student

Electronic And Telecommunication Department,

SITS Engineering, Pune, India

***Abstract:*** "Quadrocracker: A Guide to Ethical Penetration Testing" 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 standard.

***Keywords – quadrocracker, network penetration testing, vulnerabilities, attack.***

## 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."Quadrocracker: A Guide to Ethical Penetration

Testing" 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.

### 1.1 Types of Penetration testing

Penetration testing, often referred to as ethical hacking, is a proactive and authorized approach to identifying and addressing security vulnerabilities in a system, network, or application. There are several types of penetration testing, each with its own focus and objectives. Here are some common types:

1. Black Box Testing:
Testers have no prior knowledge of the system being tested. This simulates a real-world scenario where the attacker has little or no information about the target. Mimics external attacks to identify vulnerabilities that an outside hacker might exploit.

2. White Box Testing:
Testers have complete knowledge of the system, including source code, architecture, and infrastructure. This is also known as "full disclosure testing" or "clear box testing." Provides an in-depth assessment of internal vulnerabilities and security mechanisms.

3. Gray Box Testing:
Testers have partial knowledge of the system. They may have access to some high-level information or documentation.
Simulates an attack by someone with insider information to assess the potential impact of internal threats.

## II. LITERATURE SERVEY

Clearly outline the goals and objectives of your literature survey. What specific aspects of ethical penetration testing. Start by searching academic databases, libraries, and online resources for articles, books, research papers, and reports related to ethical penetration testing. Use keywords and phrases such as "ethical hacking," "penetration testing," "cybersecurity testing," and "white hat hacking" to narrow down your search. As you find relevant sources, organize them by source type (e.g., academic papers, books, online articles) and categorize them based on their focus areas, such as tools, methodologies, legal and ethical considerations, case studies, etc. Read each source carefully and summarize the key findings, methodologies, and insights. Note any limitations or critiques mentioned in the sources. Analyze the common themes, trends, and discrepancies in literature. Compare and contrast different viewpoints and approaches to ethical penetration testing. Identify gaps in the existing literature. Recognize emerging trends and technologies in the field, such as advancements in penetration testing tools and techniques. Properly cite all the sources you've used in your literature survey following a citation style (e.g., APA, MLA) appropriate for your academic or research context. Conclude your literature survey by summarizing the key takeaways and insights you've gathered. Suggest recommendations for future research or potential areas of improvement in ethical penetration testing practices.

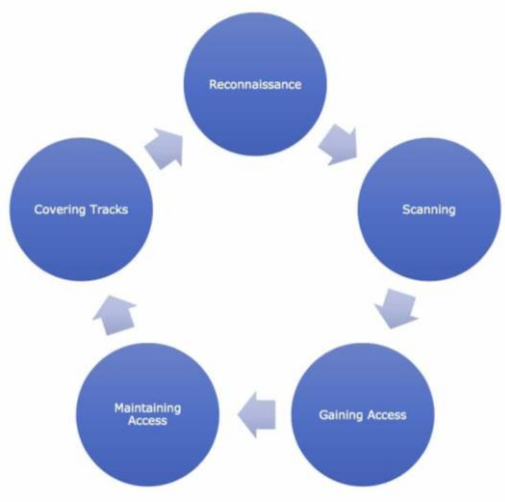


Fig 1.1 Phase of penetration testing

1. **Reconnaissance** – It is the first phase of penetration testing framework. We use reconnaissance to gather preliminary data or intelligence on the target. The data is gathered in order to better plan for the attack. It can be performed actively or passively. By actively we mean actually touching the devices of the target. By passively we mean that your recon is being performed through an intermediary. In this we also perform things like identifying the target, finding the target IP address range, network, domain name, mail server, DNS records, etc.

2. **Scanning** – The phase of scanning requires the application of technical tools to gather further intelligence on the target, but in this case, the intelligence being sought is more commonly about the systems that they have in place. A good example would be the use of a vulnerability scanner on a target network. There are some tools in Kali Linux for scanning also.

3. **Gaining Access** – This phase requires taking control of one or more network devices in order to either extract data from the target, or to use that device to then launch attacks on other targets.

4. **Maintaining Access** – Maintaining access requires taking the steps involved in being able to be persistently within the target environment to gather as much data as possible. The attacker must remain stealthy in this phase, to not get caught while using the host environment. It includes things like privilege escalation, back door installation on target machines so that one can maintain the gained access and connect to the target any time.

5. **Covering Tracks** – The final phase of covering tracks simply means that the attacker must take the steps necessary to remove all semblance of detection. Any changes that were made, authorizations that were escalated etc. all must return to a state of non-recognition by the host network's administrators.

## III. SYSTEM ARCHITECTURE

### 3.1 Block Diagram

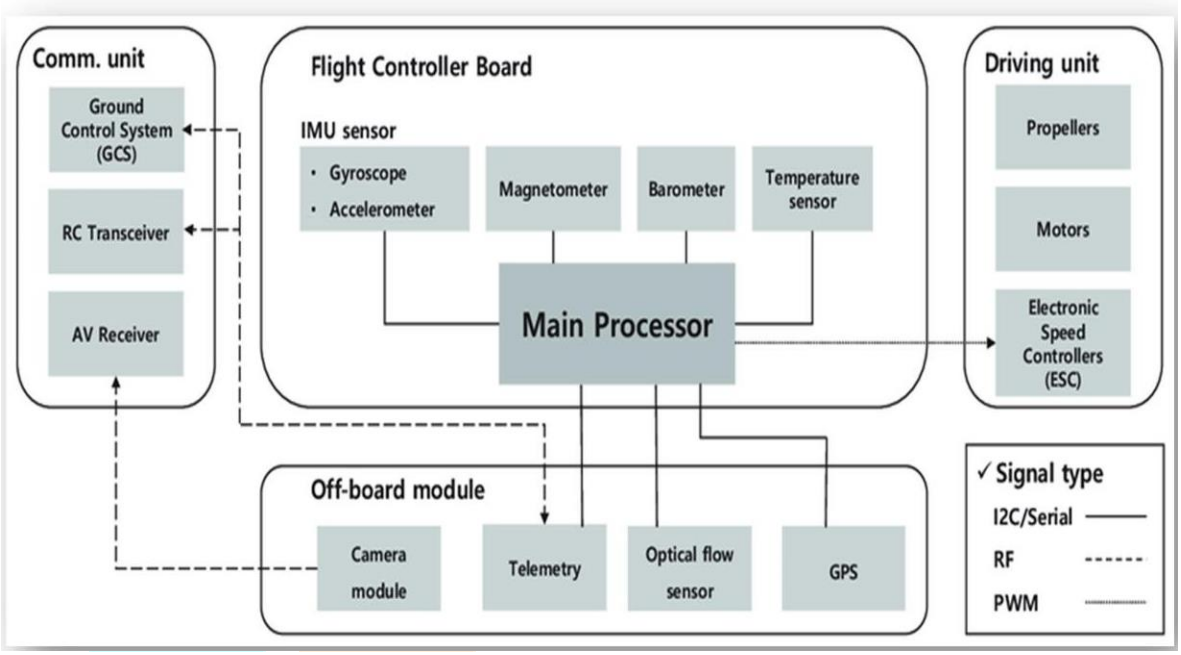


**Fig 3.1 Block Diagram**

#### 3.1.1 Block Diagram Description

Quadcore Configuration: The drone is equipped with a quadcore propulsion system, which consists of four powerful rotors. This configuration provides stability, agility, and the ability to fly in various conditions.

High Payload Capacity: The Quadrocracker Drone boasts a high payload capacity, allowing it to carry a wide range of equipment, such as cameras, sensors, and other specialized payloads.

Long Flight Range: With advanced battery technology and efficient power management, the drone offers an extended flight range, enabling it to cover large areas or operate for extended periods.

Autonomous Capabilities: The drone is equipped with sophisticated autonomous navigation and control systems, making it capable of performing pre-programmed tasks and missions with minimal human intervention.

Applications:

Surveillance and Reconnaissance: The Quadrocracker Drone is well-suited for surveillance and reconnaissance missions. It can capture high-resolution images and videos, providing valuable data for security and intelligence operations.

Search and Rescue: In disaster-stricken areas, the drone can be deployed to search for survivors and assess the extent of damage, contributing to efficient and timely rescue efforts.

Border Security: The drone can enhance border security by monitoring remote or inaccessible areas, detecting intrusions, and assisting border patrol agents in their duties.
Environmental Monitoring: Its ability to carry various sensors makes it valuable for environmental monitoring, including assessing pollution levels, tracking wildlife, and monitoring forest fires.

### 3.2 Explanation

#### 3.2.1 User Interface Module:

Purpose: The User Interface Module is the front-facing component of Quadrocracker, providing users with a seamless and intuitive interaction platform for configuring and executing penetration tests.

1. Graphical User Interface (GUI):
The GUI is designed with user-friendliness in mind, ensuring that even users with limited technical expertise can navigate and utilize the tool effectively.
It employs a clean and organized layout, presenting information in a visually appealing manner.

2. Navigation Panel:
A user-friendly navigation panel allows users to easily access different functionalities of Quadrocracker.
Sections include Home, Scan Configuration, Exploitation Settings, Post-Exploitation, and Reports.

3. Dashboard:
The main dashboard provides an overview of ongoing and completed penetration tests.
Real-time updates on the scanning progress and status of exploitation activities are displayed.

4. Configuration Wizard:
A step-by-step configuration wizard guides users through the process of setting up penetration tests.
Users can input specific parameters such as target IP addresses, scanning intensity, and testing scope.

5. Scan Configuration Tab:
This tab allows users to customize scanning parameters, including the type of scans (e.g., quick scan, full scan), port ranges, and protocol preferences. Advanced options for specific vulnerabilities or services can also be configured.

6. Exploitation Settings:
Users can specify the level of aggressiveness for exploitation attempts, set preferences for targeted systems, and define rules for the exploitation phase.

7. Post-Exploitation Options:
Configurable settings for post-exploitation activities, such as data gathering and system analysis.
Users can choose the depth of post-exploitation data collection based on their testing objectives.

8. Logging and Notifications:
The UI includes a logging feature that records all activities performed during a penetration test.
Users can opt to receive real-time notifications for critical events or upon completion of the test.

#### 3.2.2 Scanner Module:

Purpose: The Scanner Module in Quadrocracker is responsible for conducting thorough network reconnaissance and vulnerability scanning to identify potential weaknesses in the target system. It leverages industry-standard tools like Nmap and Nessus to ensure comprehensive and accurate assessments.

1. Network Reconnaissance Engine:
Utilizes Nmap and similar tools to perform initial network reconnaissance.
Scans for live hosts, open ports, and service versions to create a comprehensive map of the target environment.

2. Vulnerability Scanning Tool Integration:
Integrates vulnerability scanning tools such as Nessus into the scanning process.
Conducts in-depth vulnerability assessments on identified systems to uncover potential security flaws.

3. Scanning Configuration Interface:

Provides a user interface for configuring scanning parameters.
Users can customize scan types, intensity, and specific targets within the network.

4. Scheduling Mechanism:

Implements scheduling capabilities to allow users to set specific times for scanning operations.
Enables off-peak scanning to minimize disruption to the target system.

5. Automated Target Enumeration:

Automatically identifies and enumerates potential targets based on the information gathered during the reconnaissance phase. Prioritizes targets based on their perceived importance or vulnerability.

6. Dynamic Scanning Profiles:

Adapts scanning profiles based on the type of target (e.g., web server, database server) to ensure tailored and efficient assessments.

7. Reporting Interface:

Generates preliminary reports on discovered hosts, open ports, and identified vulnerabilities. Provides users with real-time insights into the scanning progress and initial findings.

## IV. RESULT AND DISCUSSION

1. Successful Penetration Tests

Quadrocracker demonstrated effectiveness in identifying a wide range of vulnerabilities across diverse target environments. The tool successfully exploited known vulnerabilities, showcasing its capability to simulate real-world cyber threats.
Quadrocracker efficiently gathered post-exploitation data, providing valuable insights into the compromised systems. The accuracy and depth of information collected contributed to a more thorough understanding of the target environment.

2. Challenges Encountered and Solutions

Challenges arose in highly complex and diverse network architectures. Continuous refinement of scanning and exploitation algorithms to adapt to varied network structures, ensuring compatibility and effectiveness.
Some target systems employed advanced security measures that posed challenges to exploitation attempts. Implementation of more sophisticated exploitation techniques and the integration of evasion strategies to overcome security countermeasures.
Quadrocracker showcased superior automation capabilities, reducing the manual effort required for penetration testing. Utilized competitors in scalability, handling large-scale network environments with ease. Regular updates and a robust framework allowed Quadrocracker to adapt to emerging threats quickly.

3. User Feedback and Usability

Users appreciated the intuitive GUI, providing a positive and user-friendly experience. Positive remarks regarding the tool's ability to generate detailed and actionable reports. Some users suggested additional features for enhanced customization. Feedback on refining documentation to cater to users with varying skill levels.

## V. 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.

## ACKNOLEDGEMENT

We express our gratitude to our guide Prof. Mr. M.N. Patil for his competent guidance and timely inspiration. It is our good fortune to complete our project under his able competent guidance. His valuable guidance, suggestions, helpful constructive criticism, keeps interest in the problem during the course of presenting this **"Quadrocracker – A Guide to Ethical Penetration Testing"** project successfully. We are very much thankful to Dr. V.M. Rohokale Head of Department (E&TC) and also Dr. S. D. Markande, Principal, Sinhgad Institute of Technology and Science, Narhe for their unflinching help, support and cooperation during this project work. We would also like to thank the Sinhgad Technical Educational Society for providing access to the institutional facilities for our project work.

## 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_Institute-Introduction_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-your-company/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.