AI-DRIVEN PENETRATION TEST

KAPT

HEYLEAN

First Publishment Date: *August 14, 2025*
Version: *v.1.0.0*

COPYRIGHTS

DISCLAIMERS

This white paper has been prepared by Heylean International, Inc. to provide information on AI-Powered Offensive Black Box Penetration Testing (KAPT). The information in this document is intended to provide a general overview and does not constitute specific consultation or professional advice.

Heylean makes no warranty as to the accuracy, completeness, or currency of the information contained in this document.

The information herein may not be suitable or applicable to a specific situation, and may contain errors or omissions, whether intentional or unintentional.

Heylean International, Inc. cannot be held liable for any loss, damage, or harm arising from the use or non-use of the information in this document. The use of this information is entirely at the reader's own risk.

The KAPT technology mentioned herein is constantly evolving. Therefore, the information in this document may be updated or changed in the future. For the most current information, please contact Heylean International, Inc. directly.

Any mention of third-party products, services, or companies in this document does not constitute an endorsement thereof.

The effectiveness of any security solution depends on numerous factors and cannot be guaranteed. This document is not sufficient for creating a comprehensive security strategy. It is recommended to consult with a security expert to develop such a strategy.

Certain capabilities described in this document are available for use only by Government Entities and are subject to necessary verification.

The copying, reproduction, or distribution of the contents of this document is prohibited without the prior written consent of Heylean International, Inc.

CONTENTS

INTRODUCTION

With its self-learning (Self-AI) and machine learning (ML) powered C5ISR solutions, Heylean builds a dynamic, proactive, and continuously adaptive security architecture in the domains of ***Defense, Intelligence, Cyberspace, and Public Safety***.

In an era where the global security paradigm is being reshaped by constantly evolving asymmetric and hybrid threats, Heylean's purpose is to redefine strategic deterrence. To preserve the sovereignty of nations and corporate resilience, we provide decision superiority that enables not just reaction, but the ability to anticipate events, neutralize threats at their source, and proactively shape outcomes. At the core of our operations lie next-generation solutions that transform uncertainty into clarity and data into strategic advantage.

We treat intelligence not merely as a product, but as the central nervous system of modern defense and security. By fusing multi-layered data streams, we transform noise into meaningful insights. This process enables our partners not only to counter threats but also to maintain the initiative by anticipating their adversaries' next move. The actionable intelligence we deliver converts uncertainty into absolute clarity and strategic advantage.

We recognize that technological superiority is non-negotiable. Therefore, we pioneer the engineering of next-generation cyber-physical systems and autonomous capabilities. Our activities are focused on establishing a proactive, layered security architecture that strengthens the defense postures of nations and enterprises. Our expertise optimizes the decision cycle in mission-critical operations, maximizing readiness and ensuring mission success.

Heylean's unique position in the global security arena stems from our ability to seamlessly fuse advanced intelligence capabilities with our technology. In a rapidly evolving and increasingly complex world, we do not merely anticipate challenges; we engineer the solutions to neutralize them before they emerge. This strategic synthesis provides our clients with an operational tempo and quality of decision-making that their adversaries cannot match.

Behind our technology and our analyses lies our most valuable asset: a multidisciplinary team of strategists, engineers, data scientists, intelligence specialists, and more. A single purpose unites us all: **to build a safer, more secure, and more resilient world.**

OUR STRATEGY AND MISSION

Heylean aims to redefine global security and defense doctrines with the transformative power of artificial intelligence. Our fundamental objective is to transcend reactive defense paradigms by building a next-generation security architecture equipped with proactive, predictive, and autonomous capabilities. In the domains of Defense, Intelligence, Cyberspace, and Public Safety, our C5ISR solutions deliver absolute situational awareness and decision velocity, granting our allies and partners strategic superiority under any circumstances.

OUR STRATEGY

We do not merely apply existing technologies; we shape the technology map of the future. Our experts analyze the potential of technologies such as artificial intelligence and autonomous systems, delivering actionable roadmaps to integrate them into the missions of our allies and partners. Our goal is to transform technological innovation directly into operational value. For us, innovation is not an end in itself, but a means to enable our allies and partners to succeed in their most challenging missions. By deeply understanding the operational realities and strategic objectives of our clients, we offer them not just technology, but holistic solutions and new business models that ensure mission success.

We recognize that threats are not static. Therefore, our strategy is built on continuous adaptation and evolution. The systems we develop adapt by autonomously learning new threat vectors, providing effective and deterrent protection even where traditional defense mechanisms fall short.

OUR MISSION

In the face of rapidly evolving and increasingly unpredictable global threats, our mission is clear: to fuse qualified human intelligence with superior technology at the right time and place, neutralizing potential threats at their source before they escalate into crises. As Heylean, this strategic vision and unwavering commitment to our mission are what lie behind our pledge to create a safer and more stable world.

WHY HEYLEAN?

The New Equation of Entropy: Beyond Uncertainty

Because we are rewriting the known rules in security and defense. While our competitors solve problems, we reshape possibilities. For us, the equation is to manage entropy, to transform chaos into a predictable system, and to turn uncertainty into a strategic advantage for our allies and partners.

FOUR-STAGE SUPERIORITY

The Signal Within the Noise

Everything begins with data. But data, in isolation, is meaningless. Our advanced data fusion systems fuse trillions of disparate data points—from satellite imagery (IMINT) and cyber network traffic (CYBINT) to human intelligence (HUMINT) and open sources (OSINT)—into a single, live, and holistic operational picture.

From Reactive Defense to Proactive Dominance

We are not content with merely seeing what is; we anticipate what is possible. By analyzing hidden patterns, anomalies, and weak correlations on the holistic data map, our systems detect threats while they are still mere intentions. By continuously simulating potential future scenarios and adversary behaviors, we ensure our partners always stay one step ahead and seize the initiative.

Strategic Clarity in Seconds

At a level of complexity that surpasses human intelligence, our systems generate optimal Courses of Action (COA) in seconds. Each plan is analyzed against critical metrics such as potential risk, probability of success, resource requirements, and second-order effects. This provides the command echelon with absolute decision clarity even in the most challenging moments, pushing the decision cycle beyond the adversary's limits of perception.

A Tailored Solution for Every Mission

Our technology is meaningless unless it operates in perfect alignment with strategic objectives on the ground. We combine our deep technological understanding with the unique operational needs and mission goals of our partners. The result is not just solutions that are technically functional, but mission-specific solutions that shift the operational paradigm.

OUR TECHNOLOGY INFRASTRUCTURE

Sovereign, Secure, and Hyperscale Cloud Architecture

Heylean's technological backbone is built upon the doctrines of the highest levels of security, performance, and scalability required by mission-critical operations. This architecture is fortified by our proprietary engineering layers on top of the global infrastructure of the world's most advanced and trusted cloud providers, Amazon Web Services (AWS) and Microsoft Azure. This strategic foundation allows us to offer our allies and partners an uninterrupted and sovereign operational environment under all conditions.

SECURITY

Security is the most fundamental principle in the design of our infrastructure. Our approach is based on a multi-layered and proactive defense philosophy, designed to exceed even the strictest government and defense industry standards.

Data Sovereignty and Zero Trust Architecture

All data is automatically encrypted at the physical layer before it leaves our facilities. All traffic transmitted over the global network of AWS and Microsoft Azure flows through isolated and encrypted tunnels. This "Zero Trust" approach ensures that sensitive data, regulated workloads, and classified information are under absolute protection at all times. Each region utilizes fully segregated resources and isolated network traffic for maximum security.

Access Management

To eliminate the threat of unauthorized access, we employ authentication protocols that far exceed industry standards. These include methods such as software-defined (SDN) 4-factor authentication (4FA) and hardware-defined (HDN) 5-factor authentication (5FA). Access is managed at the most granular level, based solely on the principles of "need-to-know" and "least privilege."

PROACTIVITY

Our infrastructure is under 24/7 surveillance by advanced AI-powered monitoring systems. These systems instantly detect anomalies and potential threat vectors, triggering automated response mechanisms before threats can escalate into problems. Heylean delivers a holistically managed infrastructure that provides full transparency and control.

COMPLIANCE

Our operations demonstrate full adherence to the most current and leading global security and compliance standards (e.g., ISO, SOC, GDPR).

OPERATIONAL SUPERIORITY

Our infrastructure is designed for the most intensive data processing and analysis tasks. With over 100 Tbps of external network capacity and over 1 Pbps of internal network traffic, it delivers ultra-low latency and high performance even for the most complex workloads.

OPERATIONAL CONTINUITY

Business continuity is not an option; it is a guarantee. With a 99.99% uptime service-level agreement (SLA), we commit that your operations will not be interrupted, even at the most critical moments.

OUR COMMITMENT

Heylean is dedicated to providing its allies and partners with a secure, high-performance, and scalable infrastructure capable of countering not only today's threats but also tomorrow's. By continuously investing in technological advancements and innovations in cybersecurity, we ensure our infrastructure always maintains its position as an industry leader.

This commitment to excellence ensures that your data and operations are always protected at the highest level and operate at optimal performance.

WHAT IS THE KAPT

A PARADIGM SHIFT IN CYBER DEFENSE

The cyber battlefield is no longer an arena of static fortresses, but of constantly changing and adapting threats. In the face of this new reality, traditional penetration testing methodologies—approaches based on human expertise, which are time-consuming and limited in scope—are dangerously inadequate. They trap organizations in a reactive defense cycle, unable to keep pace with the adversary.

KAPT is not a tool. It is an autonomous cyber attack platform, driven by artificial intelligence, that continuously learns and adapts. Its purpose is to test the limits of defense systems with a speed, creativity, and depth that lie beyond human imagination and endurance.

HUNT THE KNOWN, DISCOVER THE UNKNOWN

KAPT's game-changing power comes from its AI core, which is inspired by the human brain.

The Prediction Hunter – Supervised Learning Algorithm

The Prediction Hunter operates like a cyber strategist trained on all known attack vectors, tactics, techniques, and procedures (TTPs). It systematically and relentlessly hunts for known vulnerabilities, such as the OWASP Top 10 and CWE Top 25, leaving no room for human error.

The Anomaly Explorer – Unsupervised Learning Algorithm

This is where the rules of the game are rewritten. This core does not know what it is looking for; it knows what is "normal." By detecting the slightest anomalies in system behavior, non-standard data flows, and unexpected correlations, it uncovers yet-to-be-defined "zero-day" vulnerabilities and complex, multi-stage attack paths that traditional scanners would never see.

FROM ILLUSION TO TRUE RESILIENCE

Traditional tests often settle for a penetration depth of ~70%, creating a dangerous "illusion of security." This is akin to believing the walls of a system are solid while being unaware of hidden tunnels.

*However, KAPT elevates this rate to a revolutionary level of ~96.8% through the fusion of AI and real-time intelligence, **making the invisible visible**.*

KAPT STAGES

KAPT does not follow a static checklist. It is a dynamic, AI-driven operational process where each phase feeds into the next.

I. PLANNING AND PREPARATION

This phase forms the foundation of the KAPT process and is critical for a successful test. A detailed planning and preparation process minimizes potential risks and maximizes test efficiency.

I.I: SCOPE DEFINITION

Defining the target systems is the most crucial step of this phase. Through discussions with the client, the systems to be included in the test scope are clearly defined. At this stage, we do not request sensitive information such as system topology, keypairs, passwords, or IP bypass details. Our focus is to broadly outline which systems we will be operating on.

I.II: COMMUNICATION PLANNING

Ensuring a seamless and effective flow of communication throughout the test process is essential. Therefore, communication channels (e.g., email, phone, video conference) are established, and a regular communication plan is created with the client. Concurrently, communication protocols for unexpected situations are also defined.

I.III: EMERGENCY ACTION PLAN (EAP)

An action plan is prepared in advance for potential adverse situations that may arise during the penetration test (e.g., system crash, data loss). This plan details the potential scenarios, responsibilities, and the measures to be taken.

I.IV: RISK ASSESSMENT

Potential risks related to the target systems and test methodology are assessed using a risk matrix. The risk matrix helps in prioritizing and defining risk mitigation strategies by evaluating the likelihood and impact of potential risks.

I.V: REPORTING

Regular reporting to the client is crucial for providing updates on the test's progress and for addressing any potential issues in a timely manner. Therefore, the reporting frequency (e.g., daily, weekly, monthly) is determined in collaboration with the client.

I.VI: DETERMINATION OF LEGAL AND ETHICAL ELEMENTS

The KAPT process is conducted in full compliance with all legal and ethical regulations. Prior to the test, necessary authorizations are obtained and privacy policies are reviewed.

II. RECONNAISSANCE AND INFORMATION GATHERING

In this phase, as much information as possible is gathered about the target systems. This information is used to increase the effectiveness of the attacks to be carried out in subsequent phases. The Integrated Intelligence Network developed by Heylean International, Inc. plays a significant role in this stage.

II.I: INTEGRATED INTELLIGENCE NETWORK

A comprehensive information-gathering process is conducted on the target systems using intelligence disciplines.The specific intelligence disciplines to be used are determined by the characteristics of the target systems and the scope of the test. The use of all disciplines may not be necessary for every system.

II.II: AI DRIVEN

SL and USL Algorithms are used to analyze the collected data and extract meaningful information. These algorithms can rapidly process large datasets and uncover hidden connections. For example, Unsupervised Learning algorithms can be used to detect anomalies in systems, while Supervised Learning algorithms can be used to recognize known attack patterns.

III. SCANNING AND CLASSIFICATION

In this phase, automated, manual, and AI-powered scanning operations are performed on the target systems. The identified security vulnerabilities are classified according to their severity.

III.I: AUTOMATED SCANNING

Known security vulnerabilities in the systems are identified using automated scanning tools. These tools can quickly and effectively scan for a wide range of vulnerabilities.

III.II: AI-DRIVEN SCANNING

An AI-powered scanning process is carried out using a Supervised Learning Algorithm and an Unsupervised Learning Algorithm. The Supervised Learning Algorithm operates on pre-prepared datasets. The Unsupervised Learning Algorithm seeks to discover previously undiscovered (Zero-Day) security vulnerabilities.

III.III: MANUAL VERIFICATION

In the final stage, following the automated and AI-powered scanning, vulnerabilities are manually scanned. Additionally, the vulnerabilities discovered during the automated and AI-powered scanning processes are verified and reproduced. This process eliminates false-positive findings.

IV. REPORTING

In this phase, the test results are presented in a detailed report. The report includes the identified security vulnerabilities, their impacts, and recommended solutions. The report is enriched with technical details, explanations, and screenshots, enabling the client to understand the vulnerabilities and take the necessary measures. The report also contains information about the methodology used, the test scope, and its limitations.

The report provides recommended solutions and improvement suggestions for each identified vulnerability. These recommendations help the client strengthen their security posture and protect against future attacks.

KAPT offers a more comprehensive, rapid, and effective approach compared to traditional penetration tests. AI-powered algorithms analyze large datasets to uncover hidden threats and enable security experts to make more strategic decisions.

With KAPT, Heylean helps its clients strengthen their cybersecurity posture and protect their digital assets.

KAPT CAPABILITIES

OWASP TOP 10

The OWASP Top 10 is a list of the most critical security risks in web applications, published by the Open Web Application Security Project (OWASP). This list is intended to raise awareness and guide developers, security professionals, and organizations in making their web applications more secure.

CWE TOP 25

The CWE Top 25 is a list of the 25 most common and impactful security weaknesses. This list is created by the Common Weakness Enumeration (CWE). CWE is an industry standard used to categorize and define software weaknesses and vulnerabilities.

ZERO-DAY

A zero-day vulnerability is a security flaw in software or hardware that is unknown to its developers. These vulnerabilities are exploited by cybercriminals to gain unauthorized access to systems, steal data, or conduct other malicious activities.

INTERNAL RELAY ATTACK

An Internal Relay Attack is a type of cyber attack where an adversary uses a compromised device (typically a computer or server) as an intermediary or "relay" to gain unauthorized access to a victim's internal network.

LATERAL MOVEMENT

After infiltrating a network, artificial intelligence can automatically perform lateral movement to reach target systems and escalate access privileges.

CYBER ESPIONAGE

Cyber espionage, also known as cyber spying, is the act of a state or a state-sponsored group secretly infiltrating the computer systems and networks of another state, company, or organization to gather sensitive information and data.

POLYMORPHIC AND METAMORPHIC ATTACKS

Polymorphic and metamorphic attacks are sophisticated techniques used by malware to make detection more difficult.

STEGANOGRAPHY ATTACK

A Steganography Attack is a type of cyber attack where sensitive information is concealed within a seemingly harmless carrier file (e.g., an image, audio file, video, or text). This concealment is done to hide the existence of the data and prevent its detection.

SIDE-CHANNEL ATTACK

A Side-Channel Attack is an indirect attack method used to bypass a system's security mechanisms. These attacks attempt to obtain secret information by analyzing "side channels" such as a system's performance, timing, or other observable side effects. For instance, an attacker might monitor minor variations in a device's power consumption to steal an encryption key or other sensitive data.

TARGETED ATTACK

A Targeted Attack is a cyber attack where adversaries target a specific person, organization, or system. In these attacks, adversaries select a specific target rather than random ones, and the attack is customized for that target. It is carried out on an individual or institutional basis.

POISONING ATTACK

A Poisoning Attack is a type of attack used to manipulate machine learning models. The attacker injects malicious data into the model's training data, causing the model to make incorrect predictions or behave in unexpected ways.

FIRMWARE | HARDWARE ATTACK

A Firmware/Hardware attack is a type of cyber attack where malicious actors gain access to and take control of a device's firmware. Although these attacks are often difficult and complex, they can have devastating consequences when successful.

APT ATTACK

APT (Advanced Persistent Threat) is a type of targeted cyber attack used to gain unauthorized access to organizations or systems and to remain undetected for an extended period. The objective of these attacks is typically data theft, espionage, or system sabotage.

SUPPLY CHAIN ATTACK

A Supply Chain Attack is a type of cyber attack that targets the external parties an organization relies on to deliver its products or services.

WATERING-HOLE ATTACK

A Watering Hole attack is a cyber attack method used to infect individuals within a targeted group or organization. In this attack, adversaries identify websites frequently visited by the target audience (e.g., an industry forum or a popular news site) and plant malicious software on them. When a user from the target audience visits this compromised website, their device becomes infected with malware.

MOBILE DEVICE ATTACK

A Mobile Device Attack is any type of cyber attack that targets mobile devices such as smartphones and tablets. These attacks are orchestrated to access sensitive data stored on the device, take control of the device, install malware, or use the device's resources to conduct other attacks.

IOT/OT ATTACK

IoT/OT attacks are cyber attacks carried out by exploiting the security vulnerabilities of internet-connected devices (IoT) and operational technology (OT) systems.

Internet of Things (IoT): Everyday devices that can connect to the internet (e.g., smart home systems, wearable technologies, smart city infrastructures, medical devices, industrial sensors).

Operational Technology (OT): The hardware and software that control critical infrastructures, industrial processes, and production lines (e.g., SCADA systems, PLCs, DCSs).

SOCIAL ENGINEERING

Social Engineering attacks are a type of cyber attack that targets human vulnerabilities rather than technical flaws. Adversaries use psychological manipulation, deception, and trust-building tactics to trick and manipulate their victims into divulging information or granting unauthorized access to systems.

DISINFORMATION ATTACK

A Disinformation Attack is the deliberate dissemination of false information to achieve a specific objective. It is generally used to manipulate an audience, create confusion, or support a particular viewpoint. Disinformation can take various forms, such as propaganda, smear campaigns, and psychological warfare.

TEMPEST ATTACK

A TEMPEST attack is a side-channel attack that attempts to obtain information by analyzing the electromagnetic emanations from a device. Electronic devices such as computers, monitors, and keyboards normally emit electromagnetic waves while operating. Although these waves are invisible, they can be detected and analyzed with specialized equipment.

CYBER PANIC ATTACK

A Cyber Panic Attack is a sub-branch of social engineering attack perpetrated by falsely exaggerating or entirely fabricating the threat of a real cyber attack. The objective is to weaken the victims' ability to think logically by creating fear and panic, forcing them to make hasty and erroneous decisions.

ADVERSARIAL AI ATTACK

An Adversarial AI Attack is a malicious act where an attacker targets artificial intelligence (AI) systems and algorithms to disrupt, manipulate, or take control of their functions.

PHYSICAL HACKING ATTACK

A Physical Hacking Attack is a type of cyber attack that uses physical access, social engineering tactics, or a combination of both to breach a system's security. This type of attack is characterized by the attacker gaining direct physical access to the computer system, network hardware, or data.

QUANTUM ATTACK

A Quantum Attack is a theoretical type of attack aimed at breaking modern cryptographic algorithms using the power of quantum computers. While classical computers use transistors that represent information as bits of 0 or 1, quantum computers use qubits. Due to the principle of superposition, qubits have the ability to be both 0 and 1 simultaneously. This allows quantum computers to perform certain calculations much faster than classical computers.

CYBER DRONE ATTACK

Cyber attacks carried out with drones are situations where adversaries use unmanned aerial vehicles (UAVs) to initiate or facilitate a cyber attack against a target. These attacks can take various forms and pose a growing threat.

OSI LAYERS

KAPT can perform comprehensive penetration tests across all seven layers of the OSI model, including TEMPEST attacks. By leveraging advanced artificial intelligence algorithms, KAPT transcends traditional penetration testing methods, delivering faster, more effective, and more comprehensive security analyses. Below is a detailed description of KAPT's capabilities for each layer.

PYHSICAL LAYER

KAPT can be used to detect and analyze threats at the physical layer, such as TEMPEST attacks. This includes analyzing electromagnetic emissions to detect data leakage and simulating attacks that can be executed through physical access to network cables. Furthermore, it can detect data theft attempts by analyzing light leakage from fiber optic cables.

DATA LINK LAYER

At this layer, KAPT can simulate attacks such as MAC address spoofing, ARP poisoning, VLAN hopping, and STP manipulation. KAPT can analyze network traffic to detect anomalies and identify potential attack vectors. For example, KAPT can uncover MAC address spoofing by detecting multiple devices with the same MAC address or detect ARP poisoning attacks by monitoring ARP requests and responses. KAPT can also analyze STP configurations to detect unauthorized access between network segments.

NETWORK LAYER

KAPT can simulate and detect network layer attacks such as IP spoofing, ICMP tunneling, routing protocol attacks, and Denial of Service (DoS) attacks. KAPT can analyze network traffic to detect abnormal IP addresses or packet flows and identify potential sources of attack. Additionally, it can provide protection against routing protocol attacks by analyzing routing tables and detecting manipulated routing updates.

TRANSPORT LAYER

KAPT can detect and analyze transport layer attacks such as TCP SYN floods, UDP floods, port scanning, and session hijacking. KAPT can identify these types of attacks by monitoring network traffic in real-time and detecting abnormal connection attempts or packet flows. Furthermore, it can detect and analyze DoS attacks that consume system resources and cause service disruptions.

SESSION LAYER

KAPT can be used to detect vulnerabilities in session management protocols. This includes detecting unauthorized login attempts, simulating session hijacking attacks, and identifying weaknesses in session management mechanisms.

KAPT can identify potential vulnerabilities by analyzing session data and detecting anomalies.

PRESENTATION LAYER

KAPT can detect vulnerabilities in data encryption and decryption mechanisms. This includes detecting weak encryption algorithms, attempting to crack encryption keys, and verifying data integrity.

KAPT can test different encryption algorithms and assess their resistance to being broken.

APPLICATION LAYER

KAPT can detect and analyze web application vulnerabilities (e.g., SQL injection, cross-site scripting, session management vulnerabilities), API vulnerabilities, and other application layer attacks. KAPT can automatically launch attacks against web applications and analyze the results to detect vulnerabilities.

Furthermore, it can assess API security by testing APIs and detecting unauthorized access or data leakage.

KAPT demonstrates superior performance in detecting and analyzing attacks across these layers by using artificial intelligence and machine learning algorithms. Thanks to its continuous learning capability, it can rapidly adapt to new threats and attack methods and develop more effective defense strategies.

KAPT vs COMPETITORS

Heylean develops innovative and advanced technologies in the field of AI-powered C5ISR solutions. Our AI-powered penetration testing service, KAPT, offers unique features that differentiate it from our competitors.

Dependent on Static and Rule-Based Approaches

These approaches can be effective in detecting known vulnerabilities but fall short against complex attacks such as zero-day vulnerabilities and Advanced Persistent Threats (APTs).

KAPT, in contrast, offers a more comprehensive and proactive penetration testing service by using AI algorithms that continuously learn and adapt to the dynamic threat environment.

Offers Limited Automation

Manual penetration testing processes are time-consuming and expensive.

KAPT, through AI-powered automation, accelerates the testing process, reduces costs, and minimizes human error.

Insufficient in Integrating Intelligence

Many of our competitors struggle to integrate current threat data into their penetration tests.

KAPT makes attack simulations more realistic and effective by using real-time intelligence.

Lacking in Reporting and Visualization

Presenting complex data in an understandable manner is critical for an effective penetration test.

KAPT, with its user-friendly interface and customizable reporting features, clearly outlines vulnerabilities and risks, and provides actionable insights.