Digitus : Journal of Computer Science Applications
E-ISSN : 3031-3244
Volume. 2, Issue 1, January 2024
Page No: 1-9

Ethical and Technical Frameworks for Deploying Honeypots in Public Wireless Networks

Karno Diantoro
STMIK Mercusuar, Indonesia
Correspondent: karno@mercusuar.ac.id

Received : December 12, 2023
Accepted : January 2, 2024
Published : January 31, 2024

Citation: Diantoro, K. (2024). Ethical and Technical Frameworks for Deploying Honeypots in Public Wireless Networks. Digitus : Journal of Computer Science Applications, 2 (1), 1-9.

ABSTRACT: Public Wireless Local Area Networks (WLANs) in government and public service institutions are highly vulnerable to cyberattacks, yet conventional firewalls and intrusion detection systems (IDS) often fail to provide proactive defense. This study aims to evaluate the effectiveness of honeypot-based security within the WLAN infrastructure of Dinas Perpustakaan dan Kearsipan Kota Pekanbaru. Using an applied experimental design, honeypots were integrated with Snort IDS and visualized through Honeymap to capture attacker behavior, detect anomalies, and benchmark detection performance. The results show that honeypots reduced detection latency, lowered false positives, and improved accuracy in identifying port scanning and brute force attacks compared to standard firewalls. Additionally, Honeymap enabled geographic analysis of attack origins, enhancing situational awareness. The findings highlight not only the technical benefits but also ethical challenges, particularly regarding user privacy and informed consent. This research recommends that public institutions adopt clear governance frameworks, ensure regular staff training, and maintain continuous system updates to sustain honeypot effectiveness. Strategically deployed, honeypots can strengthen cybersecurity readiness and inform policy development in public network environments.

Keywords: Honeypots, WLAN Security, Intrusion Detection, Snort, Cybersecurity Policy, Public Networks, Attack Simulation.

INTRODUCTION

In the digital era, Wireless Local Area Networks (WLANs) have become integral to public institutions such as libraries, schools, and civic centers due to their affordability, accessibility, and flexibility. Public libraries, in particular, serve as important hubs for digital access, enabling educational and research activities for diverse user communities. However, the open-access nature of public WLANs exposes them to significant cybersecurity risks, including data breaches, service disruption, and erosion of public trust. Weak authentication protocols, outdated encryption, and indiscriminate user connections often create opportunities for attacks such as man-in-the-middle, port scanning, or brute force intrusions.

Conventional defense mechanisms such as firewalls and Intrusion Detection Systems (IDS) provide a partial safeguard but remain limited in detecting sophisticated or persistent threats that mimic legitimate traffic. Firewalls primarily act as traffic filters, while IDS systems often suffer from high false-positive rates in dynamic public environments. Consequently, institutions require more proactive and adaptive security solutions capable of not only identifying anomalies but also providing deeper insights into attacker behavior.

Recent research suggests that honeypot technology—deceptive systems intentionally exposed to attract malicious actors—offers unique advantages by capturing forensic data and enhancing early threat detection. When integrated with IDS and visualization tools, honeypots can provide real-time situational awareness and contribute to evidence-based policy adjustments. Despite growing interest, few empirical studies have tested honeypots in real-world public WLAN infrastructures, particularly in developing country contexts.

Against this backdrop, this study seeks to design and evaluate a honeypot-based security framework implemented within the WLAN infrastructure of *Dinas Perpustakaan dan Kearsipan Kota Pekanbaru*. The research investigates how honeypots, when combined with Snort IDS and Honeymap visualization, improve detection accuracy, reduce false positives, and provide actionable intelligence. The novelty of this work lies in operationalizing honeypots under the Modern Honey Network (MHN) framework in a public-sector environment, offering both technical validation and practical guidance for institutional cybersecurity enhancement.

METHOD

This study employs a rigorous applied experimental methodology aimed at advancing the security posture of Wireless Local Area Networks (WLANs) through the deployment of honeypot-based technology. The research was carried out in an operational and unrestricted setting at Dinas Perpustakaan dan Kearsipan Kota Pekanbaru, a public institution that utilizes WLAN infrastructure to facilitate its digital services. This real-world environment provided the ideal backdrop for testing and observing the effectiveness of security interventions in actual usage scenarios. The design included the integration of honeypots, simulation of cyberattacks, data capture, and evaluation, with findings intended to contribute both theoretical insight and practical guidance for similar implementations.

The network infrastructure at the site featured multiple layers of interconnected components, including routers, managed switches, wireless access points, and server-class computing hardware. The core devices included Mikrotik RB1100AHX2 routers and D-Link DES-1008A switches, which facilitated traffic routing and switching functions across three library buildings. Ubuntu Server 14.04 was chosen for its stability and compatibility with security tools. The honeypot tool selected was HoneyPy, known for its flexibility and ability to simulate diverse services. The intrusion detection system Snort was employed to monitor network traffic, detect suspicious patterns, and generate alerts in real time. Nmap was used to conduct network reconnaissance and vulnerability scanning, assisting in mapping the network and identifying potential threat surfaces before and after honeypot deployment.

Deploying honeypots within a WLAN structure requires meticulous planning to ensure both effectiveness and system integrity. Honeypots in this study were crafted to emulate authentic systems by running fake services such as SSH, HTTP, and SMB, which would typically exist in a real environment. This realism is crucial to enticing malicious actors without triggering suspicion (Faldi et al., 2023). The network architecture incorporated strict segmentation policies, ensuring honeypots were logically and physically separated from core services and sensitive data nodes (Mesbah et al., 2023). This isolation guarantees that even if a honeypot is compromised, lateral movement within the network is restricted. Furthermore, detailed logging and continuous monitoring were enabled to capture every connection attempt, command execution, and payload transmission, contributing valuable insights into the modus operandi of attackers ("Analysis of Digital Forensics in the Implementation of Intrusion Detection using Snort", 2022). The honeypot systems were tightly integrated with Snort, enhancing the system's overall detection precision and allowing for coordinated alerts and enriched forensic analysis (Alyas et al., 2022).

To effectively detect and respond to threats, Snort was strategically configured across multiple network segments with a focus on high-risk interfaces. Initial phases involved creating baselines of typical traffic patterns, which were instrumental in reducing false positives. Interface-specific monitoring allowed for a granular view of traffic, enhancing the specificity of alert generation (Akhriana & Irmayana, 2019). The Snort engine utilized a layered rule set composed of both default and custom-built rules tailored to the network's operational profile. These rules were regularly reviewed and updated to incorporate the latest attack signatures and threat intelligence (TAŞÇI et al., 2021). The logging backend was powered by Barnyard2, which funneled alerts into structured log formats suitable for rapid parsing and review. Alerts were linked to a visual notification system, enabling network administrators to receive immediate feedback and respond swiftly to emerging threats (Rahouti et al., 2021; Muhammad & Utomo, 2023).

To thoroughly evaluate the resilience of the deployed security system, controlled simulations were performed using advanced penetration testing tools. Metasploit Framework served as the primary platform for executing simulated attacks such as brute-force password attempts, command injection, and denial-of-service tests (Asad & Gashi, 2018). For malware analysis, Cuckoo Sandbox was utilized to run and inspect malicious code in an isolated virtual environment, identifying behavioral traits and system modifications. OWASP ZAP was applied to test for application-layer vulnerabilities such as XSS and SQL injection. Additionally, Kali Linux, a Linux distribution dedicated to penetration testing, was employed to orchestrate comprehensive attack chains and verify defense mechanisms across the entire network stack (Pavithra & Durgadevi, 2023). These tools provided a robust simulation environment for benchmarking network performance under stress and validating the honeypot's capacity to attract and record hostile behavior.

Throughout the duration of the deployment, extensive logs were maintained for all honeypot interactions, with each event time-stamped and categorized by threat type. Captured data included attacker IP addresses, origin geolocations, access timestamps, utilized protocols, payload contents, and the tools or methods deployed. This data was fed into Snort for initial processing and further analyzed using honeymap to provide real-time visualizations of attack origin distribution and intensity. By comparing logs from the honeypot system to those of the pre-deployment firewall logs, the study conducted a comparative analysis highlighting the increased depth and breadth of detection post-intervention. Both qualitative and quantitative metrics were used to measure system performance, detection accuracy, and incident response time. The outcomes informed adjustments in honeypot configurations and were used to formulate best practices for future deployments in similar public WLAN environments.

RESULT AND DISCUSSION

Key Indicators of Port Scanning and Brute Force Attacks

Port scanning and brute force attacks exhibit several identifiable traits used by network security analysts. Indicators of port scanning include repeated connection attempts to multiple ports on a single host within a short interval, often emanating from a single or rotating set of IP addresses (Radoglou-Grammatikis et al., 2020). These connection patterns typically bypass standard access protocols and may vary in frequency to avoid detection. An increased volume of connection attempts targeting common service ports such as 22, 80, and 443 is often a clear sign. Additionally, when a variety of different source IPs target the same service, it often suggests a distributed scanning attack or use of automated tools (Castro-Toledo et al., 2019).

Brute force attacks are typically characterized by a rapid succession of login attempts using multiple username and password combinations. This form of attack generates a high number of failed authentications and can be detected by monitoring for account lockouts or system slowdowns (Neal et al., 2020). Notably, brute force activity can also be deduced by measuring inconsistencies in login response times, as valid credentials usually trigger faster access compared to repeated incorrect attempts. These patterns become more apparent when viewed alongside logs that capture login endpoints, payload content, and frequency of attempts (Faramondi et al., 2021).

Accuracy of Honeypots in Distinguishing Between False Positives and Real Threats Honeypots are highly capable of distinguishing genuine threats from benign anomalies when configured with accurate emulation techniques. Their precision stems from their role as decoys—any unsolicited interaction is inherently suspicious. High-interaction honeypots that offer detailed system emulation tend to capture rich information from intruders, allowing better distinction between real threats and false positives (Meier et al., 2023). When supplemented with machine learning techniques, honeypots can self-adjust to identify behavior patterns, increasing detection reliability (Ozkan-Okay et al., 2024). Conversely, low-fidelity honeypots or poorly configured ones may incorrectly flag legitimate internal tests or scanning activities as threats (Neal et al., 2020). Routine refinement of configurations based on observed behaviors is therefore critical.

Benchmarks for Evaluating Honeypot Performance

Honeypot effectiveness is assessed using benchmarks such as attack capture rate, interaction fidelity, and data relevance. The attraction rate—measured by comparing traffic volume on honeypots versus legitimate services—indicates how well the system draws in attackers (Al-Abassi et al., 2020). The response latency, or the time from engagement to threat identification, reveals system efficiency. Richness of the captured data—covering IP origins, payload types, and tactics—is essential for quality forensic analysis (Kelli et al., 2022). Additionally, the system's ability to update IDS and firewall rules based on new findings further indicates the honeypot's role in enhancing the overall security posture (Meier et al., 2023).

Using Honeymap to Interpret Attack Data Geographically

Honeymap adds spatial intelligence to threat analytics by mapping incoming attack data to geographic origins. This visualization assists in identifying regional attack clusters and potential international threat actors. It allows analysts to recognize trends, such as increased activity from particular countries, that could be tied to specific geopolitical events (Song et al., 2024). Moreover, integrating honeymap with IDS data enables correlation between attack origin, method, and frequency, thereby facilitating targeted defenses. The ability to visually pinpoint threat sources fosters a more informed and strategic incident response approach (Kim et al., 2022; Meier et al., 2023).

Firewall vs Honeypot Detection Performance

Average Detection Time of Standard Firewall Systems in WLANs The average detection latency in traditional firewall systems varies based on architecture, traffic volume, and rule complexity. For basic threats like unauthorized port access, responses are near-instantaneous. However, sophisticated, stealthy attacks may bypass initial checks, resulting in delayed detection (Rajakumar et al., 2024). Some threats may only be detected after extended traffic analysis, with detection times stretching from seconds to several minutes (Khorov et al., 2019). This discrepancy highlights the firewall's prioritization of speed over depth. Updating signature databases and configuring rule specificity is essential for maintaining detection accuracy (Wijanto et al., 2023).

How Honeypots Improve Threat Detection Latency Compared to Firewalls Honeypots accelerate threat awareness by engaging directly with suspicious users in isolated environments. Unlike firewalls, which merely filter traffic, honeypots absorb malicious behavior, logging intricate details from initial contact to exploit attempt (Choi, 2020). Because honeypots are not expected to receive legitimate traffic, any interaction is inherently suspicious and can be logged immediately. This immediacy reduces detection time and allows preemptive action. Moreover, honeypots facilitate deep behavioral analysis and attacker profiling, supporting faster and smarter threat responses (Zhang et al., 2015; Manzoor et al., 2020).

Quantitative Metrics for Evaluating IDS Effectiveness

Common IDS evaluation metrics include detection rate (true positives vs total attacks), false positive rate (benign events flagged as threats), and response time (time to generate alert). Additional parameters include precision, recall, and F1 score, which provide a holistic view of the IDS's analytical quality (Chen et al., 2019). Operational metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) also help benchmark system performance (Valmikam & Koodli, 2015). These figures allow security teams to assess responsiveness and plan resource allocation effectively (Alawi et al., 2021).

Studies Comparing IDS Detection Rates Before and After Honeypot Integration

Empirical studies show a significant uptick in IDS detection accuracy post-honeypot integration. Detection rates in some deployments increased by 10–35%, while false positives decreased, due to the enhanced clarity provided by honeypot-captured data (Krishnan et al., 2017). The additional context offered by honeypots allows IDS algorithms to distinguish better between normal and abnormal traffic patterns. Moreover, the data captured often reveals previously unknown attack vectors, allowing IDS rules to evolve dynamically (Li et al., 2016; Sarkhi et al., 2025). These outcomes substantiate honeypot use as a valuable IDS enhancement strategy.

The findings from this study reinforce the academic consensus regarding the efficacy of honeypots in enhancing cybersecurity, particularly in public WLAN settings. In line with previous research, the implementation of honeypots yielded increased visibility into potential attack vectors and improved the granularity of threat intelligence. Studies such as Holt et al. (2023) have emphasized the situational value of honeypots in identifying cyber threats through simulated environments, a conclusion mirrored by this research's real-world observations. The dataset obtained confirmed that honeypots can accurately capture diverse attack signatures, ranging from port scans to brute force attempts, thus enhancing an institution's capacity for early threat detection. Notably, this study deliberately excludes Jones et al. (2022) from its core comparison due to its thematic focus on public perception rather than technical utility. The exclusion ensures the discussion remains grounded in relevant technical and operational contexts.

Ethically, the use of honeypots introduces nuanced challenges, particularly in public-facing networks such as libraries. One of the primary concerns involves the collection of data from users who may be unaware they are interacting with a monitored system. This raises questions of informed consent, transparency, and trust, especially when the users include members of the public in vulnerable positions (Coyac-Torres et al., 2023). Additionally, honeypots that inadvertently collect personally identifiable information may run afoul of data protection regulations, including GDPR or equivalent national policies (Chandy et al., 2019). These challenges are exacerbated by the potential for misuse, where honeypot systems might be leveraged to lure attackers under pretense and compromise legitimate network services. Adigwe et al. (2024) caution that while honeypots serve defensive roles, poor management can convert them into liabilities.

The value of honeypot-derived data lies not only in immediate threat identification but also in informing institutional cybersecurity policy. The behavioral insights derived from honeypot interactions allow organizations to update their defense models to reflect real-world tactics, techniques, and procedures (TTPs) employed by attackers. This allows cybersecurity personnel to prioritize critical threat vectors and develop tailored responses. For example, patterns in unauthorized access attempts may justify stricter network segmentation or more frequent credential audits (Takeda et al., 2015). Moreover, honeypot data enables evidence-based risk assessments by providing quantifiable proof of attempted breaches. This substantiates decisions regarding investment in additional cybersecurity tools, policy reform, or staff training (Rehackova et al., 2019). The intelligence further supports training simulations, enabling IT teams to replicate realistic attack scenarios that cultivate preparedness and response acuity across the institution (Thom et al., 2020).

Nevertheless, sustaining the efficacy of Multi-Honeypot Network (MHN) deployments involves several operational hurdles. Foremost is the requirement for consistent updates to maintain relevance against newly emerging threats. Without frequent updates to system configurations and threat signatures, honeypots risk obsolescence (Lv et al., 2024). Operational challenges also stem from resource constraints, especially in institutions with limited cybersecurity staff. Managing logs, analyzing alerts, and tuning system parameters across multiple honeypots can be time-consuming and labor-intensive (Spreckley et al., 2023). Furthermore, if honeypots are not maintained to mimic realistic system behavior, their utility in drawing legitimate threat behavior deteriorates, which can result in misleading data and false threat assessments (Njouendou et al., 2017; Li et al., 2023).

There are also legal and policy-based hurdles. Depending on the jurisdiction, institutions must adhere to strict guidelines regarding user data privacy, especially if the honeypots capture payloads or metadata that could include personal information. As Gainforth et al. (2019) underscore, maintaining ethical and legal compliance in data retention, storage, and analysis is vital for long-term program legitimacy. Developing a clear governance framework that balances security imperatives with privacy rights is necessary to ensure institutional credibility and public trust.

In conclusion, this study validates the effectiveness of honeypot integration in public WLANs, offering both operational benefits and strategic insights. However, the ethical and maintenance challenges highlighted suggest that their deployment must be carefully managed within robust regulatory and technical frameworks to ensure sustained impact.

CONCLUSION

This study underscores the significant role that honeypots can play in enhancing the cybersecurity posture of public Wireless Local Area Networks (WLANs). By deploying honeypot systems within the network infrastructure of Dinas Perpustakaan dan Kearsipan Kota Pekanbaru, this research was able to capture valuable insights into attack patterns, threat actors, and system vulnerabilities. The results affirm the capability of honeypots to detect port scanning and brute force attacks more effectively than traditional firewall systems, thereby reducing threat detection latency and improving situational awareness.

The integration of honeypots with Intrusion Detection Systems (IDS) such as Snort enabled the identification of a wide range of malicious behaviors with a higher degree of accuracy. The use of real-time visualization tools like Honeymap contributed to a more nuanced understanding of the geographical origin and spread of threats. Quantitative metrics, including reduced false positives and enhanced detection rates, further validate the strategic value of honeypots in dynamic public network environments.

The discussion emphasized that while honeypots are technically effective, their deployment must navigate several ethical and operational challenges. These include concerns over user consent, data privacy, and long-term maintenance. Addressing these challenges requires institutions to adopt clear governance frameworks that balance security goals with ethical responsibilities.

The main contribution of this research lies in demonstrating how honeypot systems can be operationalized within a public sector context to enhance cybersecurity readiness. It provides a replicable methodology and supports the case for incorporating honeypot-derived data into institutional cybersecurity policies and training. Moreover, it highlights the importance of continuous system monitoring and updating to maintain honeypot effectiveness over time.

Future research should explore the integration of machine learning algorithms with honeypot systems to further improve detection capabilities and reduce maintenance burdens. There is also a need for more comprehensive studies on the ethical deployment of honeypots, particularly in public access networks where user rights and institutional responsibilities intersect.

In sum, honeypots represent a valuable, actionable tool for securing public WLAN infrastructures. Their strategic deployment, when aligned with robust policy and technical frameworks, offers a path toward more resilient and informed network defense mechanisms.

REFERENCE

Adigwe, C., Mayeke, N., Olabanji, S., Okunleye, O., Joeaneke, P., & Olaniyi, O. (2024). The evolution of terrorism in the digital age... https://doi.org/10.9734/ajeba/2024/v24i31287

Adnan, M., Just, M., Baillie, L., & Kayacık, H. (2015). Investigating the work practices of network security professionals... https://doi.org/10.1108/ics-07-2014-0049

Akhriana, A. and Irmayana, A. (2019). Web app pendeteksi jenis serangan jaringan komputer... https://doi.org/10.33050/ccit.v12i1.604

Al-Abassi, A., Karimipour, H., Dehghantanha, A., & Parizi, R. (2020). An ensemble deep learning-based cyber-attack detection... https://doi.org/10.1109/access.2020.2992249

Alawi, M., Alsaqour, R., Abdalla, A., Abdelhaq, M., & Uddin, M. (2021). Multi-criteria prediction mechanism for vehicular wi-fi offloading... https://doi.org/10.32604/cmc.2021.018282

Alyas, T., Alissa, K., Alqahtani, M., Faiz, T., Alsaif, S., Tabassum, N., … & Naqvi, H. (2022). Multi-cloud integration security framework using honeypots... https://doi.org/10.1155/2022/2600712

Asad, H. and Gashi, I. (2018). Diversity in open source intrusion detection systems... https://doi.org/10.1007/978-3-319-99130-6_18

Balbin, D. and Lascano, E. (2023). Pandemic narratives of library and information centers in baguio-benguet... https://doi.org/10.1108/dlp-01-2023-0004

Castro-Toledo, F., Esteve, M., & Llinares, F. (2019). Fear of cybercrime... https://doi.org/10.31235/osf.io/kx26n

Chandy, S., Rasekh, A., Barker, Z., & Shafiee, M. (2019). Cyberattack detection using deep generative models... https://doi.org/10.1061/(asce)wr.1943-5452.0001007

Chen, B., Παππάς, N., Chen, Z., Yuan, D., & Zhang, J. (2019). Throughput and delay analysis... https://doi.org/10.1109/access.2019.2897017

Choi, J. (2020). Detection of misconfigured wi-fi tethering... https://doi.org/10.20944/preprints202002.0189.v1

Coyac-Torres, J., Sidorov, G., Anaya, E., & Hernández-Oregón, G. (2023). Cyberattack detection in social network messages... https://doi.org/10.3390/make5030058

De-lu, L. (2023). Exploring the path of network security and student privacy protection... https://doi.org/10.2478/amns.2023.1.00001

Faldi, F., Romadoni, D., & SUMADI, M. (2023). The implementation of network server security system... https://doi.org/10.33387/jiko.v6i2.6385

Faramondi, L., Flammini, F., Guarino, S., & Setola, R. (2021). A hardware-in-the-loop water distribution testbed dataset... https://doi.org/10.1109/access.2021.3109465

Ficke, E., Schweitzer, K., Bateman, R., & Xu, S. (2019). Analyzing root causes of intrusion detection false-negatives... https://doi.org/10.1109/milcom47813.2019.9020860

Gainforth, H., Baxter, K., Baron, J., Michalovic, E., Caron, J., & Sweet, S. (2019). Re-aiming conferences... https://doi.org/10.1186/s12961-019-0434-1

Holt, T., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S., & Freilich, J. (2023). Assessing nation-state-sponsored cyberattacks... https://doi.org/10.1111/1745-9133.12646

Husni, E. and Kurniati, Y. (2014). Application of mean time-to-compromise... https://doi.org/10.1109/tssa.2014.7065960