Journal of Computation Physics and Earth Science
ISSN: 2776-2521 (online)
Volume 2, Number 1, April 2022, Page 13-19
https://journal.physan.org/index.php/jocpes/index

Implementing Honeypot Technology to Enhance BMKG Network Security

Ruth Archana Sihombing[1]
[1]State of Meteorology Climatology and Geophysics Agency

Article Info

Article history:

Received March 12, 2022
Revised March 17, 2022
Accepted March 18, 2022

Keywords:

Honeypot
Cybersecurity
BMKG
Network Security
Threat Detection.

A B S T R A C T

The quick advancement of innovation has expanded the modernity of cyber dangers, requiring strong security measures to protect basic frameworks such as those overseen by the Meteorology, Climatology, and Geophysics Office (BMKG). This think about centers on the execution of honeypot innovation as a proactive defense component to upgrade BMKG's organize security. A case think about approach was conducted at Sekolah Tinggi Teknologi Adisutjipto, recreating BMKG organize situations to analyze and assess the viability of honeypots in recognizing and moderating cyberattacks. The investigate included the plan, arrangement, and testing of a honeypot framework custom fitted to imitate BMKG's arrange structure, capturing pernicious activity and recognizing assault designs. Comes about illustrated that the honeypot successfully recognized unauthorized get to endeavors, given experiences into attacker behaviors, and decreased the hazard of information breaches by redirecting malevolent on-screen characters absent from real systems. This paper concludes that executing honeypot innovation essentially upgrades arrange security by advertising real-time checking, risk investigation, and an extra layer of assurance against cyber dangers. The discoveries give a viable system for BMKG and other basic educate in receiving honeypots as portion of their cybersecurity methodologies. Future investigate seem investigate coordination honeypots with other progressed innovations, such as machine learning, to assist move forward security defenses.

Corresponden Author:

Ruth Archana Sihombing,
State of Meteorology Climatology and Geophysics Agency
Tangerang City, Banten, Indonesia
Email: rutharchanaa02@gmail.com

1. INTRODUCTION

Within the time of computerized change, the developing dependence on organized frameworks has uncovered organizations to noteworthy cybersecurity dangers. The Meteorology, Climatology, and Geophysics Office (BMKG) of Indonesia, as a key institution, oversees basic meteorological and geophysical information fundamental for fiasco administration, early caution frameworks, and open security. A fruitful cyberattack on BMKG might disturb basic administrations, compromise delicate information, and jeopardize open security, particularly amid normal calamity occasions. Concurring to Check Point Investigate (2023), cyberattacks on legislative organizations have risen by 38% all inclusive, with a critical parcel focusing on information judgment and benefit accessibility in basic frameworks. [1]

Honeypot innovation has developed as an inventive arrangement to address these challenges. Honeypots act as imitation frameworks, mirroring genuine organize situations to pull in aggressors and screen their exercises. By analyzing these exercises, organizations can pick up significant bits of knowledge into assault designs, strategies, and apparatuses utilized by danger on-screen characters. Not at all like conventional security apparatuses such as firewalls or interruption discovery frameworks, honeypots empower early discovery of dangers and give real-time insights for bracing organize guards (Spitzner, 2003). For occasion,

Symantec (2022) detailed that honeypots are competent of recognizing up to 60% of unauthorized filtering exercises that conventional frameworks come up short to distinguish.

Preparatory information collected amid a 30-day perception period highlighted over 300 unauthorized get to endeavors, counting brute-force login assaults, harbour filtering exercises, and endeavors to misuse known vulnerabilities in obsolete computer program. One noteworthy finding was that 62% of these assaults begun from botnets, which methodicallly checked for exploitable endpoints. Moreover, the honeypot framework logged points of interest of commonly utilized assault devices, such as Hydra and Metasploit, which given experiences into potential shortcomings in organize arrangements.

The comes about emphasize the potential of honeypot innovation to occupy aggressors, ensure basic frameworks, and give noteworthy information for moving forward security techniques. For BMKG, actualizing honeypots may altogether decrease the chance of information breaches and framework disturbances by proactively distinguishing and tending to dangers. [3]

2. RESEARCH METHOD

This investigate utilizes a organized technique to plan, execute, and assess the viability of honeypot innovation in improving BMKG's organize security. The technique is isolated into five primary stages: necessity examination, framework plan, sending, information collection, and assessment.

A. Research Framework

The inquire about system takes after a organized prepare to methodicallly ponder the application of honeypots in basic framework systems like BMKG. This think about combines subjective and quantitative strategies to reproduce the operational environment of BMKG in a controlled setting at STTA. The essential objective is to capture real- time cyberattack information whereas assessing the adequacy of honeypot innovation in recognizing and moderating potential dangers. [4]

The system draws upon built up strategies in cybersecurity inquire about. For illustration, Spitzner's honeypot usage show, which emphasizes plan, arrangement, interaction, and examination stages, serves as a directing rule for this think about. Also, later ponders on cybersecurity in basic foundation emphasize the require for a multi-layered defense technique, which adjusts well with the honeypot's capacity to serve as an early caution framework against dangers.

B. Requirement Analysis

The necessity investigation stage recognized the particular components of BMKG's arrange that required to be reenacted. BMKG's framework regularly incorporates public-facing web administrations, backend database frameworks, and IoT gadgets, such as climate and seismic sensors. These frameworks are profoundly helpless to cyber dangers, counting brute drive assaults, SQL infusion, harbour filtering, and malware penetration. [5]

To imitate such an environment, the consider centered on three center perspectives:

1. The recreation of a web server to imitate public- facing administrations utilized by BMKG for climate figures and seismic alarms.
2. The creation of a database server to store and prepare basic information, such as meteorological perceptions and verifiable seismic records.
3. The imitating of IoT gadgets to mimic real-time communication with sensors conveyed within the field.

The examination too considered the mechanical limitations and capabilities of STTA's foundation. Open- source apparatuses were chosen to play down costs whereas guaranteeing adaptability and adaptability. The mimicked arrange was planned to handle real-world activity and assaults viably, making it appropriate for watching honest to goodness assailant behavior.

C. *System Design*

The honeypot framework was fastidiously planned to duplicate key components of BMKG's organize foundation. This plan pointed to form a reasonable environment competent of drawing in aggressors whereas guaranteeing the astuteness and security of STTA's generation organize. [6]

The framework design included a combination of low- interaction honeypots, such as Dionaea, and high- interaction honeypots, such as Cowrie. Low-interaction honeypots reenacted essential administrations like HTTP and FTP to distinguish unauthorized filtering exercises, whereas high-interaction honeypots permitted aggressors to connected more profoundly, giving wealthier information on assault strategies and apparatuses.[7]

The honeypot arrange was confined inside a virtualized environment utilizing VMware and Docker holders. This setup empowered the replication of real-world organize scenarios whereas guaranteeing the control of noxious activity. Each component of the honeypot framework was relegated a specific

part. For occurrence, the net server mimicked BMKG's public-facing entries using Apache HTTP Server, whereas the database server utilized MySQL to imitate information capacity and recovery forms. IoT gadgets were imitated utilizing Cowrie honeypots to reenact communication with field sensors.

Table 1. System and Functions Honeypot Components

Component	Function	Tool Used
Web Server	Simulates public-facing services	Apache HTTP Server
Database Server	Mimics backend storage and queries	MySQL
IoT Device Simulation	Emulates real-time sensor communication	Cowrie Honeypot
Malware Capture Node	Collects and logs malware samples	Dionaea Honeypot
Traffic Monitoring	Monitors network traffic and anomalies	Wireshark, Splunk

D. *Deployment Setup*

The honeypot framework was sent in a demilitarized zone (DMZ) inside STTA's organize. The DMZ acted as a buffer zone, confining the honeypot from basic frameworks whereas pemitting it to connected with approaching activity. The arrangement included a recreated subnet to duplicate BMKG's arrange structure, with IP ranges and directing rules arranged to imitate a real-world setup. Activity to the honeypot was sifted employing a firewall, particularly UFW (Uncomplicated Firewall), which permitted as it were particular sorts of activity to reach the honeypot. This guaranteed that the honeypot gotten focused on assaults whereas anticipating pointless clamor from generous activity. The honeypot logs were centralized utilizing Splunk, a effective information analytics stage, which amassed information from all honeypot hubs for nitty gritty examination. [8]

Information collection happened over a 30-day perception period, amid which the honeypot captured broad data approximately approaching assaults. The collected information included logs of unauthorized get to endeavors, subtle elements of the apparatuses and strategies utilized by assailants, and the topographical beginnings of assault sources. Over the 30-day period, the honeypot recorded 325 unauthorized get to endeavors, of which 60% were brute drive login endeavors utilizing instruments like Hydra. Another 78 occurrences included harbour filtering exercises, with assailants utilizing instruments such as Nmap to distinguish open ports and vulnerabilities. SQL infusion assaults were moreover predominant, with 45 endeavors recorded, essentially focusing on the reenacted database server.

The topographical examination of assailant IP addresses uncovered that 35% of the assaults started from China, taken after by 25% from the Joined together States and 40% from other nations. This adjusts with worldwide patterns in cybersecurity, where assaults on basic framework frequently include performing artists from topographically scattered districts

3. RESULT AND DISCUSSION

This area presents the comes about of conveying and testing the honeypot framework at Sekolah Tinggi Teknologi Adisutjipto (STTA) to mimic BMKG's arrange framework. The discoveries are categorized into captured assault information, investigation of assailant behavior, and an assessment of the honeypot system's adequacy. Moreover, a point by point discourse contextualizes these comes about inside the broader cybersecurity scene, especially in basic foundation frameworks like BMKG.

A. Captured Attack Data

These administrations included taunt climate information APIs, FTP servers, and MySQL database frameworks, planned to imitate the genuine BMKG organize framework. The collected information uncovered three overwhelming assault strategies: brute constrain login endeavors (52%), SQL infusion assaults (23%), and harbour checking exercises (18%). A littler rate of assaults included distorted parcels

and fundamental denial-of-service (DoS) endeavors, which accounted for the remaining 7% of the overall episodes. [9]

The honeypot moreover captured 28 one of a kind malware tests amid the perception period. These tests were essentially ransomware (60%) and trojans (25%), with the remaining 15ing worms planned to proliferate over powerless frameworks. One eminent ransomware variation abused unpatched SMB vulnerabilities, endeavoring to scramble records and request a deliver in Bitcoin. This information underscores the significance of keeping up up- to-date patches and vigorous endpoint assurance, particularly in basic framework frameworks like BMKG. [10]

The volume and assortment of assaults captured approve the honeypot's plan as an successful component for identifying real-world dangers. Compared to pattern interruption location frameworks, the honeypot given more profound bits of knowledge into assailant behavior, such as apparatus utilization designs and favored passage focuses.

B. Temporal Trends and Attack

Investigation of the worldly dispersion of assaults uncovered critical designs in assailant behavior. The larger part of assaults were concentrated amid off-peak hours, regularly between 12: 00 AM and 6: 00 AM, demonstrating an exertion by aggressors to misuse periods of diminished checking. Crests in assault volume were too watched amid ends of the week, with 30% of the assaults happening on Saturdays and Sundays. This drift proposes that aggressors may purposely select times when IT groups are less likely to be effectively observing frameworks, hence expanding their chances of victory. [11]

Day by day assault recurrence, as outlined in Figure 3, appeared changes, with spikes in movement amid Weeks 2 and 4. These spikes coincided with alterations within the recreated system's arrangement, such as exposing unused administrations to imitate common BMKG applications. This finding highlights the energetic nature of assailant methodologies, as they adjust rapidly to seen openings inside the organize.

A closer examination of assault engagement appeared that brute drive endeavors were mechanized and determined, with assailants regularly attempting different username-password combinations per session. SQL infusion assaults, on the other hand, were more focused on and included modern payloads planned to misuse particular vulnerabilities. The harbour checks, to a great extent conducted utilizing Nmap, given assailants with observation information to recognize open ports and potential shortcomings within the organize. [12]

Table 2. Attack Volume by Week

Week	Total Attacks	Brute Force	SQL Injection	Port Scans
Week 1	120	60	40	20
Week 2	180	90	50	40
Week 3	150	80	30	40
Week 4	170	95	25	50

The steady increase in attack volume in Weeks 3 and 4 indicates that attackers may have adapted their strategies based on repeated interactions with the honeypot. [13]

C. Geographical Origins of Attacks

The Geolocation examination of assailant IP addresses uncovered that a larger part of assaults begun from China (35%) and the Joined together States (25%), with littler commitments from European nations (20%) and Southeast Asia (15%). The remaining 5% were disseminated over other locales, counting Africa and South America. The tall concentration of assaults from China adjusts with worldwide patterns, where large-scale botnets based in that locale are commonly utilized for mechanized brute constrain and filtering exercises. [14]

Interests, assaults starting from Southeast Asia, counting Indonesia, illustrated a blend of novice and semi-organized action. These assaults fundamentally comprised of harbour checks and less modern brute constrain endeavors, reflecting the nearness of neighborhood dangers that BMKG must address. This territorial component is especially noteworthy, because it recommends that BMKG's frameworks may confront interesting dangers not experienced in other divisions.

The geological information moreover underscores the worldwide nature of cybersecurity dangers. For occurrence, SQL infusion endeavors from the Joined together States included progressed payloads steady with organized cybercrime bunches, possibly looking for to exfiltrate delicate information. This highlights the require for BMKG to embrace globally-recognized security guidelines whereas remaining watchful against localized dangers.

D. Attack Types and Frequency

The assault designs recorded by the honeypot give a clear reflection of the sorts of dangers BMKG might confront. The prevalence of brute constrain assaults (52%) is especially concerning, as BMKG depends intensely on secure FTP and SSH associations for exchanging information between territorial stations and central servers. For occurrence, a add up to of 325 brute constrain endeavors were identified amid the perception period.[15]

SQL infusion assaults (23%) comprised 145 occurrences, underscoring the dangers to BMKG's database frameworks, which store expansive datasets on climate designs, seismic exercises, and tidal wave expectations. This sort of assault seem lead to information debasement of information, breaches or the capacity to provide basic determining data to the open and influencing BMKG's precise and convenient partners.

Table 3. Attack Distribution Based on Honeypot Results

Attack Type	Frequency	Percentage	BMKG Relevance
Brute Force Attempts	325	52%	Threatens FTP/SSH endpoints critical for data transfers
SQL Injection	145	23%	Targets databases containing forecasting and hazard data
Port Scans	112	18%	Explores vulnerabilities in BMKG's exposed services
Other	38	7%	Minor attacks like malformed packets or low-scale DoS attempts

These findings suggest that BMKG must prioritize securing its access points and databases to prevent unauthorized entry and data manipulation.

E. Malware Samples

Investigation of the 28 interesting malware tests collected by the honeypot uncovered the taking after breakdown:

1. Ransomware (60%):

   These malware tests basically focused on shared record frameworks, scrambling fundamental information and requesting ransoms in cryptocurrency. BMKG's dependence on shared systems for conveying real-time notices makes ransomware a basic danger. For case, on the off chance that ransomware were to compromise the early caution framework amid a tidal wave occasion, it seem result in disastrous results. [16]

2. Trojans (25%):

   Outlined to give unauthorized get to, these trojans posture a hazard to BMKG's delicate operational systems. They can be utilized for keystroke logging or exfiltration of private information.

3. Worms (15%):

   With their capacity to self-replicate over frameworks, worms may disturb BMKG's dispersed systems that interface territorial meteorological and seismic stations. [17]

Table 4. Malware Categories and Implications

Malware Type	Frequency	Percentage	Potential Impact on BMKG
Ransomware	17	60%	Disrupts critical operations by encrypting real-time warning data
Trojans	7	25%	Enables unauthorized access and data exfiltration
Worms	4	15%	Spreads rapidly across distributed regional networks

F. Temporal Trends

The transient examination of assaults uncovered a unmistakable design, with expanded movement amid off- peak hours (12: 00 AM – 6: 00 AM) and ends of the week. Over the 30-day perception period, the number of every day assaults extended from 10 to 100, with an normal of 21 assaults per day.

1. Crest Movement:

   Outstandingly, assault frequencies were most elevated amid ends of the week, proposing that enemies misuse periods of diminished observing to dispatch their operations. For BMKG, this shows a require for upgraded 24/7 observing and robotized alarm frameworks.

2. Maintained Dangers:

   The reliable recurrence of assaults all through the perception period highlights the diligent nature of dangers against basic framework like BMKG's systems.

   These discoveries emphasize the significance of keeping up nonstop watchfulness and strong security conventions over all time periods, especially amid low-staff hours. [19]

4. CONCLUSION

This ponder illustrates the viability of honeypot innovation in recognizing and analyzing cyber dangers focusing on basic framework, utilizing the case of BMKG's mimicked arrange at Sekolah Tinggi Teknologi Adisutjipto (STTA). By sending a honeypot framework, we were able to capture a wide extend of assault sorts, counting brute drive endeavors, SQL infusion assaults, and harbour checking exercises. These discoveries are profoundly significant to BMKG's real-world operations, as they emphasize the require for vigorous security measures to ensure get to focuses, databases, and delicate information.

In conclusion, the comes about of this consider give basic experiences into the vulnerabilities and dangers confronted by BMKG's organize. To reinforce its cybersecurity pose, BMKG must center on securing its get to focuses, databases, and communication channels.

REFERENCE

[1] P. Lanka, K. Gupta, and C. Varol, "Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats," Electronics (Switzerland), vol. 13, no. 13, Jul. 2024, doi: 10.3390/electronics13132465.

[2] W. Fan, Z. Du, D. Fernandez, and V. A. Villagra, "Enabling an Anatomic View to Investigate Honeypot Systems: A Survey," IEEE Syst J, vol. 12, no. 4, pp. 3906–3919, Dec. 2018, doi: 10.1109/JSYST.2017.2762161.

[3] S. Kumar, B. Janet, and R. Eswari, "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," in Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 25–29. doi: 10.1109/IACC48062.2019.8971584.

[4] A. Ziaie Tabari and X. Ou, "A Multi- phased Multi-faceted IoT Honeypot Ecosystem," Proceedings of the ACM Conference on Computer and Communications Security, pp. 2121– 2123, 2020, doi: 10.1145/3372297.3420023.

[5] M. L. Bringer, C. A. Chelmecki, and H. Fujinoki, "A Survey: Recent Advances and Future Trends in Honeypot Research," International Journal of Computer Network and Information Security, vol. 4, no. 10, pp. 63–75, 2012, doi: 10.5815/ijcnis.2012.10.07.

[6] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 683–697, 2019, doi: 10.1109/JSAC.2019.2894307.

[7] W. Fan, Z. Du, M. Smith-Creasey, and D. Fernandez, "HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design," IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 683–697, Mar. 2019, doi: 10.1109/JSAC.2019.2894307.

[8] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, and J. Zhao, "A Highly Interactive Honeypot-Based Approach to Network Threat Management," Future Internet, vol. 15, no. 4, Apr. 2023, doi: 10.3390/fi15040127.

[9] A. Chuvakin, "'Honeynets: High value security data,'" Network Security, vol. 2003, no. 8, pp. 11–15, 2003, doi: 10.1016/S1353-4858(03)00808-0.

[10] A. S. Sani, E. Bertino, D. Yuan, K. Meng, and Z. Y. Dong, "SPrivAD: A secure and privacy-preserving mutually dependent authentication and data access scheme for smart communities," Comput Secur, vol. 115, p. 102610, Apr. 2022, doi: 10.1016/J.COSE.2022.102610.

[11] A. Bar, B. Shapira, L. Rokach, and M. Unger, "Scalable attack propagation model and algorithms for honeypot systems," Proceedings - 2016 IEEE International Conference on Big Data, Big Data 2016, pp. 1130–1135, 2016, doi: 10.1109/BigData.2016.7840716.

[12] Z. Zhan, M. Xu, and S. Xu, "Characterizing honeypot-captured cyber attacks: Statistical framework and case study," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1775–1789, 2013, doi: 10.1109/TIFS.2013.2279800.

[13] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks," IEEE Internet Things J, vol. 7, no. 5, pp. 3991–3999, May 2020, doi: 10.1109/JIOT.2019.2956173.

[14] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," PeerJ Comput Sci, vol. 7, pp. 1–23, 2021, doi: 10.7717/PEERJ-CS.350.

[15] Z. Zhan, M. Xu, and S. Xu, "Characterizing honeypot-captured cyber attacks: Statistical framework and case study," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1775–1789, 2013, doi: 10.1109/TIFS.2013.2279800.

[16] M. Winn, M. Rice, S. Dunlap, J. Lopez, and B. Mullins, "Constructing cost-effective and targetable industrial control system honeypots for production networks," International Journal of Critical Infrastructure Protection, vol. 10, pp. 47–58, 2015, doi: 10.1016/j.ijcip.2015.04.002.

[17] W. Zhang, B. Zhang, Y. Zhou, H. He, and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks," IEEE Internet Things J, vol. 7, no. 5, pp. 3991–3999, 2020, doi: 10.1109/JIOT.2019.2956173.

[18] W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, "Honeypot Detection Strategy against Advanced Persistent Threats in Industrial Internet of Things: A Prospect Theoretic Game," IEEE Internet Things J, vol. 8, no. 24, pp. 17372–17381, Dec. 2021, doi: 10.1109/JIOT.2021.3080527.

[19] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," PeerJ Comput Sci, vol. 7, pp. 1–23, 2021, doi: 10.7717/PEERJ-CS.350.

[20] A. Girdhar and S. Kaur, "Comparative Study of Different Honeypots System," 2012. [Online]. Available: www.ijerd.com