Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

Developing A Security Scheme For Banking Networks Based On Honeypot Technology

Hanaa Ali Alghamdi1

Department of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

Dr. Sultan Alshamrani

Department of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

***Abstract*— The banking industry is a vital sector of the global economy. In order to protect financial assets and consumer trust, the banking industry's network security is of utmost importance. The goal of this research is to create a cutting-edge security system that is specifically designed for banking networks and that is built on honeypot technology. Honeypots, misleading network tools intended to entice and capture malicious individuals, have demonstrated potential for improving cybersecurity.**

In this study, we design and analyze the security scheme using the renowned AVISPA program. The effective formal verification tool AVISPA enables a thorough evaluation of security mechanisms. We hope to offer a reliable and mathematically proven security solution for financial networks by using AVISPA in the research framework.

The results of this study not only aid in the creation of a strong security system for banking networks but also show how useful AVISPA is as a tool for security analysis. This research provides a thorough and rigorous way to increasing the security posture of banking networks, The ability of the banking sector to safeguard sensitive financial data and uphold customer confidence in the face of evolving cybersecurity threats is anticipated to be significantly impacted by this study.

***Keywords*—** Cyber Security; Honeypot; Banking Networks; Cyber Attacks; AVISPA; SPAN.

I. INTRODUCTION

The security of banking networks is of utmost importance to both financial institutions and their clients in an increasingly digital environment where financial transactions are carried out electronically. The digitalization of banking services has increased convenience like never before, with a wide range of internet services like electronic funds transfers, mobile banking, and automated teller machines, the banking industry is a leader in technical innovation, but it has also left these networks vulnerable to a wide range of developing cyberthreats. They have introduced vulnerabilities that bad actors are eager to take advantage of.

The pervasiveness of cyberattacks, which can range from sophisticated nation-state-sponsored operations to opportunistic cybercriminal activity, highlights the urgent need for cutting-edge and adaptable security solutions in the financial industry. Banking networks have become top targets for hostile actors looking to acquire illegal access, money, or disrupt financial services due to their quantity of valuable financial data and assets. Cybercriminals target banking networks repeatedly in order to obtain unauthorized access, steal sensitive data, and commit financial fraud. Therefore, it has never been more important to protect the availability, integrity, and confidentiality of banking services. Financial institutions must constantly innovate and adapt to secure their assets and keep their clients' trust as attackers become more sophisticated.

This research acknowledges that, despite their importance, the conventional cybersecurity measures used by financial institutions, such as firewalls and intrusion detection systems, are frequently insufficient to counter the constantly changing strategies of cyber adversaries. So this research sets out to provide a security system that is especially suited to the special difficulties and demands of financial networks in response to the rising threat landscape, and sets out on a crucial trip to tackle this urgent problem by suggesting the creation of a financial network security system that makes use of honeypot technology.

honeypot technology is a deception-based cybersecurity strategy that uses the use of bogus systems and resources to entice, find, and examine harmful activity. As a useful tool in the cybersecurity field, honeypots have attracted attention for their ability to spot new threats, comprehend attack methods, and improve incident response skills.

With its proactive and deceptive approach to cybersecurity, honeypot technology presents a viable way to improve the security posture of financial networks. Assailants are drawn into a controlled environment via honeypots, which are intended to imitate real network assets and give important information about their strategies, techniques, and motivations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

Despite their potential to strengthen financial institutions' defenses against increasingly sophisticated cyber threats, their adoption within the banking sector has been somewhat slow. So by investigating the incorporation of honeypot technology into banking networks as a proactive and strategic way to improve cybersecurity, this research aims to close this gap.

II. CYBER SECURITY

Security in the general concept indicates protection, which previously meant only material possessions, but after the great spread of the Internet and smart and portable devices; We had to redefine security to include more important assets; It has become necessary at the present time to pay attention to cybersecurity and how to protect digital property in the digital space, starting from home to work and all aspects of life. Cybersecurity is one of the most widespread topics in recent years, and has entered all fields due to everyone's dependence on vital infrastructure.

Such as power plants, hospitals, financial services companies, etc. Therefore; Keeping these organizations secure is essential to keeping society functioning and stable [1], but taking effective cybersecurity measures is a major challenge today, as there are more devices than people and attackers have become more creative.

A. The elements of cyber security

Cybersecurity consists of three main elements [2] called the CIA Triad as shown in figure 1:

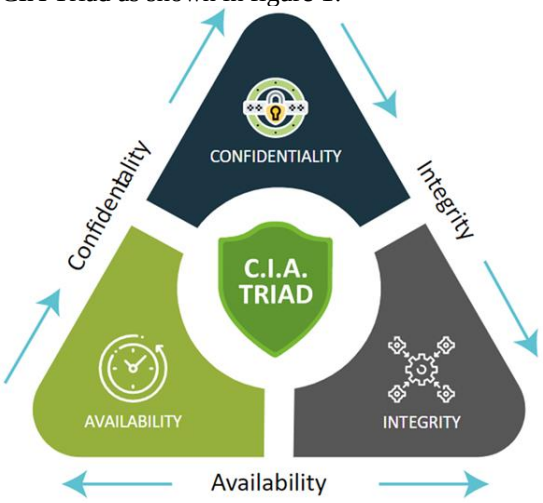

Fig. 1. The elements of cyber security [5].

- Confidentiality: Controlling access to data and making it available only to those who are permitted.
- Integrity: Maintaining the integrity of data and information and protecting it from sabotage attacks or theft.
- Availability: The readiness of all systems, services and information and their availability as requested by the company or its customers.

B. The Types of cyber security

Cybersecurity is classified into several main categories, which are [3]:

- Network Security: It involves securing a computer network from intruders through various software and hardware technologies, whether they are targeted attackers or opportunistic malware. It includes several types, including firewalls, anti-virus programs, honeypots, and intrusion detection systems.
- Application Security: Aims to keep software and hardware free from threats, and most security measures should be implemented at the design stage, long before the software or hardware is deployed.
- Information Security: It is the process of designing and deploying tools to protect important information from damage, modification, or theft. It focuses on the integrity and privacy of data, whether in storage or during transmission, and includes encryption and vulnerability management.
- Operational Security: The risk management process for all elements of internal cybersecurity and includes the processes and decisions for processing and protecting data assets as well as the permissions that users have when accessing a network, and the procedures that determine how and where data can be stored and shared.
- Cloud Security: This involves permanently protecting underlying cloud storage systems due to the massive amounts of data stored on them. It can include business services stored in the data center.
- Infrastructure Security: It is a security measure that includes protecting vital infrastructure such as network connections, data center, server, or information technology center, with the aim of reducing the weaknesses of these systems from corruption or sabotage. The infrastructure includes power supply and transmission systems, cooling system, water supply and others.

B. Benefits of cyber security

Cybersecurity he benefits of cybersecurity are countless but can be summarized as follows [4]:

- Protect network and data from unauthorized access.
- Improving the level of information protection and ensuring business continuity.
- Enhancing the confidence of shareholders and stakeholders in the company.
- Recover leaked data faster in the event of a breach in the cybersecurity system.

B. Cyber Attacks

Cybersecurity Cyber attack can be any occurrence that has the potential to undermine information systems' missions, tasks, images, national cyber assets, or personnel through illegal access, information destruction, disclosure, information alteration, or obstruction of (disruptive) service delivery [5].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

Figure 2 depicts the key categories of cyberattacks, Denial of service attacks, logical bombs, abuse tools, snoopers, Trojan horses, viruses, worms, send spam, and botnets are among the most significant cyberattack techniques. The authorized users' access to the system and vice versa are lost while using the denial of service method. Actually, the attacker begins flooding the target computers with messages at one point and obstructing the legitimate flow of data.

Any system cannot access the Internet or interact with other systems as a result. Another technique, known as broad Denial of services, involves simultaneously attacking from many dispersed systems as opposed to a single source. Worms are frequently used to assault the target in this way, multiplying on many systems. The general public can access tools that can find and exploit vulnerabilities in networks at various skill levels [6].

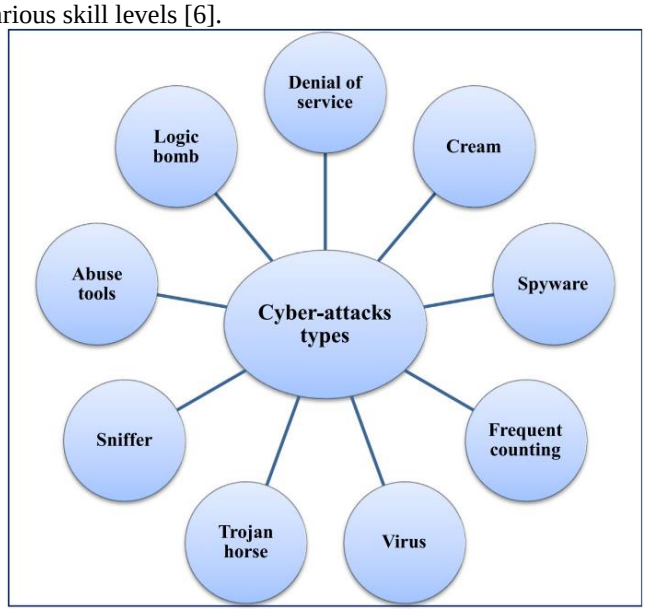

Fig. 2. The primary types of cyberattacks [5].

Another type of assault is a logic bomb, in which a programmer inserts code into a program so that, in the case of a particular circumstance, the software automatically performs a damaging action [7].

Another program called Sniffer examines each packet in the data stream to eavesdrop on routed information and search for specific information like passwords [8]. Trojan horses frequently resemble useful programs that the user is prepared to run while concealing dangerous code [9].

A virus can also corrupt system files, which are frequently used programs, by introducing a copy of itself into such files. These variants function and enable the virus to infect more files by loading infected files into memory. Viruses can only spread through human interaction, unlike worms. On the other hand, the worm is an independent system software that copies from one computer to another in the network in order to replicate itself [10].

Last but not least, a botnet is a network of infected remote control devices that are used to spam, coordinate assaults, and distribute malware. Typically, botnets are installed covertly on the target computer, giving the unauthorized user remote access to the machine to carry out their evil intentions. Another name for botnets is "electronic soldiers" [11].

III. BANKING NETWORK SECURITY OVERVIEW

Banking institutions are often the target of cybercriminals because they hold a lot of valuable and sensitive data. Customer personal information, financial transaction records, and confidential company information are all included in this data. As a result, maintaining the security and integrity of this data is essential for upholding legal requirements as well as customer confidence [12].

Banking network security is the umbrella term for a variety of procedures and tools designed to protect financial organizations from a range of dangers, such as malware, denial-of-service (DoS), insider threats, and data breaches. An efficient security plan needs to be dynamic and ever-evolving in the digital era due to the ever-changing threat landscape [12].

A.Most common cyber security attacks on banking networking

While prevalent cybersecurity attacks on banking networks are always changing, a few types of attacks still represent serious risks to the financial sector. The following are a few of the most frequent cyberattacks on banking networks [13]:

- Phishing Attacks: Cybercriminals try to fool bank staff or customers into disclosing sensitive information like login credentials and financial data by sending phony emails or messages that seem to be from reliable sources.
- Distributed Denial of Service (DDoS) Attacks: These assaults flood a bank's network or online services with excessive traffic, disrupting operations and preventing consumers from using services.
- Malware and Ransomware: Networks connected to banks may be breached by malicious software, which may then use the encrypted data to hold a ransom. Financial losses and significant delays to operations can result from ransomware attacks.
- Insider Threats: Insiders who have access to banking systems run a serious danger when they abuse their privileges. workers or former workers that steal data, conduct fraud, or compromise systems are considered insider threats.
- Man-in-the-Middle (MitM) Attacks: Hackers eavesdrop on conversations between the bank and its clients, changing or obtaining private data in the process. These assaults frequently target compromised devices or unprotected public networks.
- SQL Injection: Cybercriminals modify or extract data by taking advantage of weaknesses in databases or web applications. This may result in sensitive financial data being accessed without authorization.
- Zero-Day Exploits: Attackers focus on unpatched vulnerabilities in hardware or software that the vendor is unaware of. These exploits can be used to get inside the banking network or to make money.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

- Credential Stuffing: Since many people reuse passwords across many accounts, attackers utilize previously obtained login and password combinations to access bank accounts without authorization.
- Social Engineering: Social engineering techniques are used by cybercriminals to trick bank staff members or clients into disclosing private information or taking actions that jeopardize security.
- Supply Chain Attacks: Third-party suppliers or vendors with access to banking networks' systems may compromise them. To get into the bank's network, attackers sneak into the supply chain.
- ATM Skimming: In physical attacks, skimming devices are affixed to ATMs in order to obtain PINs and card details, resulting in fraudulent transactions.
- SWIFT Attacks: International financial transactions are conducted via the SWIFT network, which stands for Society for Worldwide Interbank Financial Telecommunication. Hackers have targeted SWIFT systems in an attempt to steal money or tamper with financial messages.

Banks use a variety of cybersecurity techniques, including firewalls, intrusion detection systems, encryption, access controls, staff training, and frequent security audits, to lessen these vulnerabilities. Robust cybersecurity strategies in the banking business also require fast incident response, ongoing monitoring, and adherence to industry standards.

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

IV. THE HONEYPOT TECHNOLOGY

Their appearances in the text and in the Reference list. AIMS production requires that each reference has DOI (if there is one). A honeypot is essentially a fake system that attracts attackers to remain on it by storing a lot of "valuable" information that they are searching for. Instead of preventing attackers from exploring the system, a honeypot mimics network services to communicate with them and logs all of their activity.

Any connections to a honeypot are regarded as suspicious since the honeypot is purposefully put within the network. The knowledge gained from observing attack patterns and malware dissemination during the attack might be extremely helpful in developing effective countermeasures [14]. The main tasks of honeypots [15] can be summarized as follows:

1. Diverting the attacker’s attention from the real network to honeypots in order to preserve the actual resources of the system.
2. Exhausting the attacker's resources and slowing down his work, which leads to him running out of time by exploiting fake resources.
3. Capturing new viruses or suspicious movements to benefit from them in the future.
4. Monitor the attacker’s behavior to know his methods, access mechanisms, and techniques used.
5. Identifying system weaknesses, in software or hardware form, that have not yet been discovered.

A. Features of honeypots

The Using honeypots gives the system a lot of features like:

1. Extracted information of high importance: The task of extracting valuable information from stored data about network performance is one of the most important challenges facing the security manager, as huge amounts of data are collected daily, including firewall logs, system logs, and detection system alarms. Most of the data is of this huge size. Most of the time, they are not useful, so it is difficult to extract what is valuable from them, and this process requires a long time. Therefore, the importance of traps lies in their ability to extract much less information [16].
2. Conservation of resources: The most important obstacle to the design of any protection system is the limited availability of resources, or what is called the exhaustion of their capacity, where resource exhaustion occurs when this resource is unable to continue working because it bears a work pressure that is much greater than its capacity [17].
3. Simplicity: This feature is considered one of the most important things that distinguish honeypots from other protection tools, as they do not require complex algorithms, an attack database, or rules to reconfigure them [18].
4. Reinvestment: When firewalls succeed in keeping attackers away from the system, he will become a victim of his successes. In other words, after a period of time has passed and there is no longer any threat to the firewall, it is possible for the network administrator to re-exploit these resources for another task.
   This is because of its limitations, but what he does not know is that this wall has helped reduce the risk, and that investing in other protection technologies such as authentication and encryption faces the same problem, because they are expensive investments that consume resources, time and money, but they can become a victim of successes.
   On the contrary, traps can prove their worth quickly and repeatedly, and even if it turns out that there is no danger, they effectively prove that there is interaction with the attacker, and if it is canceled, the system will be exposed to danger [19].
5. Reducing errors: both positive and negative: Positive errors are those that are generated when an attack does not occur, but the system generates an alarm as if an attack had occurred.
   As for negative errors, they are those that occur when no warning is generated while the attack has occurred, as the system believes that What happened is not an attack, but a natural activity, and therefore honeypots do not fall into this problem because they monitor what is directed at them directly, and these are, of course, suspicious activities [19].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

6. The ability to work in an IPV6 environment: Honeypots are distinguished by their ability to work within an IPV4 and IPV6 environment, unlike many protection technologies that do not support IPV6 [18].

V. PREVIOUS WORKS

Much research has been done in the field of network security for the banking industry to handle the dynamic threat landscape. This subsection provides a thorough synopsis of six previous research publications that have made major contributions to the subject of banking network security scheme development. Also a comparison between all of them.

A. The first paper [20].

In order to draw in the malevolent attacker and examine behavioral patterns, a hybrid honeynet that is installed in Docker and uses the Tuning Of firewall (H-DOCTOR) technique has been employed in this research to detect attacker activity. This is a type of bait used to identify or stop attacks, or to draw the focus of an attacker away from the services that are authorized and adjust the firewall.

B. The second paper [21].

This paper highlights existing methods that can be used as counters to such assaults and explores the blockchain idea and pertinent aspects that offer a full analysis of prospective security attacks. This paper also presents ways to improve blockchain security by outlining important ideas that can be used to create different blockchain systems and security tools that address security flaws.

C. The third paper [22].

This paper discussed a variety of mobile banking topics, including the main motivations for it, potential risks, and security specifications. discussed several security measures and their limitations for mobile banking threats as well. And highlight the difference between user authentication models: two-factor user authentication and three-factor user authentication.

D. The fourth paper [23].

This paper examined the alternatives for efficiently protecting a financial system's network perimeter with honeypot lures. A low-interactive application honeypot, whose goal is to safeguard open Secure Shell ports on servers of the banking network infrastructure, has been used to conduct the analysis.

E. The fifth paper [24].

This study provides an in-depth review of the current state of conventional cryptocurrencies and the CBDC scheme prototype, outlining the purpose and security needs of CBDC. Based on this, a three-tier blockchain-based framework for the CBDC was created, which is shown in figure 9, comprising a supervisory layer, network layer, and user layer.

F. The sixth paper [25].

This paper proposed an architecture for detecting malware using honeypot and machine learning. The Support Vector Machine (SVM) and Decision Tree algorithms are used in this study's categorization in order to maximize the efficiency and accuracy of the technique. Supervised machine learning using labeled datasets was used in this study.

These studies all make significant contributions to the discipline and provide insightful information. It is imperative to recognize their limitations, though, and this is what our suggested approach seeks to do. Given these constraints, our study suggests a new and all-encompassing security plan that capitalizes on the advantages of the previously discussed research while mitigating its drawbacks.

With an increased degree of defense against the constantly changing cyber threat landscape, our architecture aims to equip financial networks with an adaptable, compliance-aware, and threat intelligence-driven security framework.

VI. THE PROPOSED MODEL

In this section we introduce our proposed security model, which is called HBNSF, it is an abbreviation term that refers to the following sentence: Honeypot-Enhanced Banking Network Security Framework. It is a security framework model that aims to protect banks' banking networks from repeated cyber attacks to which they are constantly exposed.

This section introduces and describes the architecture of the proposed HBNSF model. In addition to a detailed explanation of the system components of the proposed model.

A. The architecture of the proposed HBNSF model.

Figure 3 includes the architecture of the proposed HBNSF model, This structure includes three sections, from the left: the regular Internet network, followed by the bank network, but not the actual network, but rather the honeypot network, followed by the actual protected bank network.

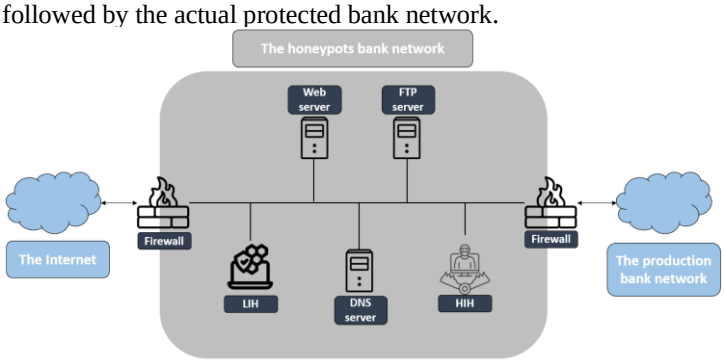

Fig. 3. Architecture of the proposed HBNSF model.

The goal of implementing this structure is to ensure the highest levels of protection for the bank's actual network, which contains very important and sensitive information. Therefore, it must be difficult for attackers so that the actual network is isolated from all potential cyber threats.

Any cyber attack on the banking network is carried out by professional attackers who come through the Internet. Therefore, in this case, when the security framework proposed by us is included, the probability of exposure to an external cyber attack will be reduced by a very high percentage.

In the following subsection, we explain the role of each section of the proposed security framework in enhancing comprehensive protection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

B. The components of the proposed HBNSF model

This subsection provides information about each section present in the proposed system, the role of each section, and why it exists. The following table explains all of these elements:

TABLE I. THE COMPONENTS OF THE PROPOSED HBNSF MODEL.

HBNSF components	Description
Internet	The External world Internet
honeypots bank network	The invisible side of the bank network for the attacker
production bank network	The visible side of the bank network for the attacker
Firewalls	Two of Protection Firewalls
Servers	3 kinds of Servers: Web, FTP and DNS.
LIH	Low interaction honeypot
HIH	High interaction honeypot

The first section is the Internet, which is the actual Internet network that everyone uses. Bank employees use it through their devices inside the bank to enter or modify data or download files necessary for work and many other behaviors, the exploitation of any of which may expose the actual bank network to great danger.

The second section is the network section for honeypots, which is the most important section as it is the focus of the proposed security model. A honeypot is the part of the bank network that is not visible to the attacker. It contains a copy that is exactly similar to the actual bank network, but it is fake. This is the concept of a honeypot.

In this case, when the attacker attacks the bank's network, he will in fact attack the honeypot network, and whatever the extent of the damage he inflicts on the network and whatever the amount of sabotage he causes to the elements and data of the network is a benefit to the bank, as we can monitor the behavior of this attacker and know the security vulnerabilities that he entered. It causes chaos and destruction to the network.

Therefore, using the concept of honeypots does not aim to keep the attacker away, or provide traditional protection methods to identify the attacker when exposed to an attack, but rather includes attracting this attacker to the network to attack it, so that he falls into the trap and becomes a victim of the security network monitor and wastes his time and resources, with the attacker believing that he is attacking the bank's actual network. And he gets the benefits expected by him.

This section initially includes a security firewall. Of course, it is a means of security protection, but it was put in place to avoid wasting the time and resources of the honeypot network in the event of a simple attack or one with a weak impact on the system. Therefore, the firewall includes a set of well-known rules to filter what is coming from the Internet. directly. There is also another security firewall at the end of this section as a final step of protection before entering the bank's actual network system.

This is followed by the presence of several servers, which are fake servers that mimic those in the actual production network and include the same size of data as in the real network, but it is fake or duplicate data, etc., whose goal is to waste the attacker's time before he discovers that what he is attacking is a fake network.

Then there is the low-interaction hacking trap, which is quick to respond to the attacker and does not consume a lot of resources, so it is what interacts with the attacker in the first stage. If the attack is large or includes mechanisms that make it difficult for her to deal with it or expose it to exposure, the interaction is immediately transferred to The attacker goes to a high-reactivity honeypot, which interacts with the attacker with high professionalism and wastes his time until his resources are completely exhausted without him ever suspecting that there is anything suspicious because it is highly reactive.

The last section is the bank's actual network, which includes all servers with all business data, which are fully protected from known and unknown cyber attacks, enabling the bank's employees to deal with all data, work, and complete all procedures simply, easily, and in complete safety.

VII. REQUIREMENTS ANALYSIS

We present below an algorithm that explains the working mechanism of the proposed security system in detail:

Algorithm 1: Filtering incoming packets

Procedure Filter (P)

Input:

Incoming packets CP

Output:

Full Genuine packets FGP

1. **Begin**
2. **In firewall 1:**
3. **Foreach (P in CP) {**
4. **Extract IP Address && Check port header**
5. **If (Source/Destination IP, port) ← Prevented**
6. **P. Reject** // packet is sorted as malicious
7. Block IP and drop P
8. Else
9. **P. Allow** // packet is sorted as genuine
10. **}** // end of if
11. **}** // end of foreach
12. **Transfer** GP to LIH and HIH
13. **Get** GP **to Firewall 2**
14. **Transfer the FGP to production bank network**
15. **END**

The basic process performed by this algorithm is filtering, that is, filtering packets. The income for this algorithm is the packets coming (CP) from the Internet in general, as bank sector employees definitely and permanently use the Internet to complete the work assigned to them, or to analyze required files, or to process various financial transactions, so it is necessary to examine all packets entering the network. The

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

output released by this algorithm is the packets classified as completely authentic, Full Genuine packets (FGP).

When the algorithm begins (line 1), Custom rules placed within the first firewall start running (line 2). This is done by searching each of the incoming packets, and extracting the IP address from them in addition to the port address used (Line 4).

After that, the processing process begins, if both the source and target IP addresses as well as the port address are marked as blocked addresses (Line 5). Then the packet is sorted as malicious packet and the firewall reject it (line 6) also it Block this IP address in order to never get any future messages from it and drop its packets (line 7).

Else the packet is sorted as genuine packet and the firewall allow it to enter the honeypots bank network for more analysis (line 8). Now the output of this stage are the Genuine packets, and now should be transferred to LIH and HIH (line 12).

After that, we enter these packets at a later stage into the second firewall for additional examination and final confirmation that the packets are authentic (line 13). Then as a final step when we are sure that the packets are fully authentic, the Full Genuine packets (FGP) are transfer to real production bank network (line 14).

The requirement analysis stage emphasizes how careful planning is needed to put in place a security solution in a virtualized environment that uses both high and low contact honeypots. This stage establishes the foundation for the following chapter, Experimentation and Evaluation, by defining functional and non-functional requirements and stressing thorough risk assessment. The next chapter will examine how the planned scheme is actually put into practice, utilizing AVISPA and SPAN to evaluate the scheme's effectiveness and confirm that it can protect financial networks against constantly changing cyberattacks.

CONCLUSIONS

The study conducted a thorough investigation of the security measures that are already in place in banking networks. It did this by critically analyzing six important papers that clarify different protection tools and techniques. The result of this thorough literature review was an in-depth comparative analysis that was displayed in a structured table format. The present study exposed intrinsic vulnerabilities present in previous systems, so furnishing a fundamental comprehension for the development of a new security protocol, appropriately named HBNSF, aimed at strengthening financial networks.

The creation of HBNSF required careful planning, which included a detailed strategy outlining its essential elements and operating nuances. The study methodology used made it easier to take a methodical approach, which allowed for a clear explanation of the analytical requirements necessary for the suggested protocol to work.

Significant progress has been made in strengthening the security posture of banking networks as a result of this research project. HBNSF is a significant development in this field, providing a customized solution to solve the weaknesses found in existing systems.

FUTURE WORK

Phase two of the study entails deploying and validating the HBNSF protocol within banking networks as it moves from theoretical formulation to practical implementation. The use of the AVISPA software is scheduled to be the first phase in this implementation process, during which the robustness and functionality of the protocol will be thoroughly evaluated. This stage consists of a set of sequential actions, such as:

1. Implementing the protocol: Including HBNSF in a simulated banking network environment to assess its compatibility and performance.
2. Functional Testing: Testing protocols thoroughly to confirm that they are resilient to known security risks and possible attackers.
3. Deployment in the Real World: Working with industry partners, we will implement HBNSF in real-world financial networks while guaranteeing its scalability and practicality.
4. Constant Improvement: Constantly improving and adjusting the protocol in response to feedback from the real world and changing threat environments.

Anticipated future work lays the groundwork for a practical application of research findings, with the dual goals of strengthening banking networks and laying the groundwork for proactive and adaptable security frameworks in the dynamic field of cybersecurity.

REFERENCES

[1] Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128.
[2] Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems, 77, 103201.
[3] Sonkor, M. S., & García de Soto, B. (2021). Operational technology on construction sites: A review from the cybersecurity perspective. Journal of Construction Engineering and Management, 147(12), 04021172.
[4] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on risk and insurance-Issues and practice, 47(3), 698-736.
[5] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
[6] Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems, 122, 149-171.
[7] Magness, J. M. (2020). SLIVer: Simulation-Based Logic Bomb identification/verification for unmanned aerial vehicles.
[8] Glăvan, D., Răcuciu, C., Moinescu, R., & Eftimie, S. (2020). Sniffing attacks on computer networks. Scientific Bulletin" Mircea cel Batran" Naval Academy, 23(1), 202A-207.
[9] Molotkov, S. N. (2020). Trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography. Journal of Experimental and Theoretical Physics, 130, 809-832.
[10] Chen, M., & Yan, M. (2023). How to protect smart and autonomous vehicles from stealth viruses and worms. ISA transactions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 12, December-2023

[11] Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2020). Hybrid deep learning for botnet attack detection in the internet-of-things networks. IEEE Internet of Things Journal, 8(6), 4944-4956.
[12] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 6666.
[13] Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. Authorea Preprints.
[14] Dahbul, R. N., Lim, C., & Capability, J. P. E. H. D. (2019). Through Network Service Fingerprinting. In Internation Conference on Computing and Applied Informatics.
[15] Melhem, H., & Dayoub, Y. (2022). A Hybrid Honeypot Framework for DDOS Attacks Detection and Mitigation, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 11, Issue 11 (November 2022).
[16] Melhem, H., & Dayoub, Y. (2022). A hybrid honeypot framework for DDOS attacks detection and mitigation.
[17] Naik, N., & Jenkins, P. (2018, July). A fuzzy approach for detecting and defending against spoofing attacks on low interaction honeypots. In 2018 21st International Conference on Information Fusion (Fusion) (pp. 904-910). IEEE.
[18] Wang, H., & Wu, B. (2019, March). SDN-based hybrid honeypot for attack capture. In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (pp. 1602-1606). IEEE.
[19] Bonnerji, R. (2020). An approach to enhance low-interaction honeypots by enabling them to detect spoofing attacks via network analysis (Doctoral dissertation, Dublin, National College of Ireland).
[20] Le, T., Park, N., & Lee, D. (2020). A sweet rabbit hole by darcy: Using honeypots to detect universal trigger's adversarial attacks. arXiv preprint arXiv:2011.10492.
[21] Amal, M. R., & Venkadesh, P. (2023). H-DOCTOR: Honeypot based firewall tuning for attack prevention. Measurement: Sensors, 25, 100664.
[22] Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. IEEE Access, 9, 13938-13959.
[23] Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: evolution and threats: malware threats and security solutions. IEEE Consumer Electronics Magazine, 8(2), 56-60.
[24] Lakh, Y., & Shymkiv, R. (2019, October). Using Honeypot Programs for Providing Defense of Banking Network Infrastructure. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 527-532). IEEE.
[25] Han, X., Yuan, Y., & Wang, F. Y. (2019, November). A blockchain-based framework for central bank digital currency. In 2019 IEEE International conference on service operations and logistics, and informatics (SOLI) (pp. 263-268). IEEE.
[26] Matin, I. M. M., & Rahardjo, B. (2019, November). Malware detection using honeypot and machine learning. In 2019 7th international conference on cyber and IT service management (CITSM) (Vol. 7, pp. 1-4