Comparison of Honeypot System, Types, and Tools

Muhammad Junaid Iqbal[1†], Muhammad Usman Ahmed [2††], Muhammad Asaf[3††]

Lahore Leads University Lahore

Abstract
Network security is now more crucial than ever for consumers, companies, and military clients. Security has elevated to the top of the priority list since the Internet's creation. The evolution of security technology is now better understood. The area of community protection as a whole is broad and dynamic. News from the days before the internet and more recent advancements in community protection are both included in the topic of observation. Recognize current research techniques, previous Defence strategies that were significant, and network attack techniques that have been used before. The security of various domain names is the subject of this article's description of bibliographic research.

Keywords
Internet, information security, and bibliography research

1. Introduction

The connection between the sectors is strengthening with the development of the web and the new Web era. Globally, there is a wealth of data available on people, businesses, marinas, and agencies on the network infrastructure. Because it is so simple to purchase a huge number of things via the Internet, communal security becomes crucial. Authorization is the first step in establishing cyber security, typically requiring a call and password. Network administrators can prevent and show unwanted access to personal PC vendors and shared networks, which is a modification, misuse, or rejection of equipment, as part of the network protection process. Public security is the authority that approves the accurate input of local events, and the network administrator is in charge of this input. According to the information, this is important for both personal computer buyers and sellers. If permitted, the firewall will compel access to laws, such as those governing which products members of the community are permitted to access. This element would not be capable of verifying dangerous content, such as PC worms or Trojans communicated over the network, in addition, to preventing unauthorized connection to your machine. Malware can be found using an anti-virus or a detection system (ID) system. Anomalies can now be logged for later analysis and study in the system, protecting the community against threats like the twine shark trade. The two hosts' chat community's goal is likely to use encryption to safeguard users' online privacy. A house or small management center would need basic protection at the same time, however, major organizations might need intensive maintenance and cutting-edge gear and software to safeguard them against spam attacks and hostile hacker attacks. The community's protection is continually changing as a result of the expansion of transportation, the development of uses, and the evolution of harmful situations. For instance, the widespread use of social networks, cloud computing, and apps to share your tools brings new challenges and serious threats for existing complicated groups. The British government defines recording security as: "Get the finest registration status possible.

Control, listen to, modify, transmit, and other uses by a person with the necessary abilities" (Delivery: UK Online business). If indeed the factual system is to be trusted, it must unwind. Considering numerous businesses Utilizing its data model for Security can be considered a vital component in regulating particular behaviors while creating major company strategies (such as websites, manufacturing schedules, and transaction processing). The major issues with information security are examined by looking at the following points:

- Network security folder
- Easy-to-use Internet network architecture and security components
- Types of Internet attacks and security policies
- Secure access with Internet
- Modern development of hardware and software programs for network security.

When considering cyber security, the focus should be on the whole community to stay relaxed. Community security is not the most effective objective of the security of the structure of laptops every time the chain of communication is abandoned. Even when transmitting statistical information, the chat channel should not be exposed to the risk of attack now: in this threat, the possibility of the threat will be more evident Hackers may also want to manage verbal communication channels, obtain statistical records, decrypt and re-enter incorrect information. So to be honest, protecting your network is just as important as securing your laptop and encrypting your messages. That requires personal storage. When building a relaxed community, the following factors should be taken into account

Manuscript received November 5, 2023
Manuscript revised November 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.11.21

1. Accessibility: offers legal users a way to speak to a specific network.
2. Confidentiality: statistics within the community are not made public and broadcasters should not easily get results.
3. Three. Identity verification - to ensure that customers in the community are, consumers should be the ones to say.
4. Four Integrity: To ensure that the message has not been changed during transmission, the content must be the same as the content at the time of sending.
5. Non-repudiation: make sure that the buyer does not now refuse to use the community.

By understanding security issues, capacity attackers, the required security phase, and the factors that make the community vulnerable to attack, you can develop a powerful network security plan. When doing research on the company, people observed the scales concerned with knowledge: it is a relaxed community, made up of the Internet or other aspects. There is currently preferred security in PC installations associated with the community. The security protocol sometimes appears from time to time in the unmarried layer of the reference version of the Osi network. The current painting is done in-house using a layered method to simplify the layout of the community. We have carried out an elegant micro-protection method, based entirely on most security levels. This security method has a powerful and inexperienced design and can avoid many common security problems.

The emergence of computers is becoming more and more common: the popularization of computers in society is a welcome step towards modernization, but society hopes to be more adaptable to the tensions linked to the time new hacking techniques are used to infiltrate the community, and security vulnerabilities generally go undiagnosed. Which causes problems for security experts and aims to trap hackers. In education, the problem of failure to update on time due to security concerns is due to the lack of statistical data today. The current objective of the research is to integrate high-quality protection education into the rapidly changing era. The protection of online networks aims to provide an in-depth understanding of the security principles of todays networked computer systems. It covers ideas and basics of personal computer security, early knowledge of security selection in infrastructure design, strategies to make complex systems comfortable and a real talent for managing many systems, laptops private infrastructure. On a large scale.

In this article we can quickly explain the idea of community protection and how to implement it in the future. With the advent of the Internet and its increasing use, we have deepened our research on how security threats penetrate our devices. We have stressed the maximum value of various attacks that occur frequently in any Network (with family, workplace and organization). In the last part, we have analyzed many protection mechanisms, which may need to be maintained. The comfort of the network. In this section, we will cover most of today's ideas, which may be applicable to provide the security necessary for today's hackers and viable attacks

Types of Attacks

It is difficult for the network to attack malicious resources. With the advent and increase of network connections, the growth of network connections is becoming more common. The basic categories of attacks can come from the following categories: "passive", even if community intruders intercept statistical information transmitted over the network; "alive", in the intruder sends commands to prevent the normal functioning of the community. The system must be able to limit damage and recover accidentally in the event of an attack... There are also some great attacks to consider:

A. Passive attack

Passive attacks filter unencrypted visitors and viewing of clear passwords and confidential records that can be used for one-time attacks.

Chat channels that track and monitor unauthorized consumers are called passive attacks. Includes visitor evaluation, tracking insecure communications, decryption of website visitors with weak encryption, Obtain authentication records, including passwords. Passive interception of network operations allows adversaries to visualize future operations. Passive attacks show facts or documents to attacker without authorization or knowledge of techniques

B. Active bay attack

In an acute attack, the attacker tried to skip or insert a secure form in the language transaction that the region needed. This can be done by stealth programs, viruses, worms, or Trojans. Dynamic attacks include attempts to evade or undermine security functions, introduce malicious code, and steal or steal statistical data. The truth that unauthorized user video viewers notice and change

the communication channel is called energy attack. These attacks are carried out in a position opposite the backbone of the community, using transient recordings to electronically enter the enclave or attack remote authenticated users when they tried to connect with the enclave. Persistent attacks result in the modification or disclosure of files, files, or factual information.

C. Attributed attack

Distributed attacks force opponents to introduce code containing worms or door-to-door software into "trusted" software elements or programs, which are then distributed to many different businesses and customers. Software in the production plant or in the distribution process. These attacks introduce malicious code into the backdoor of the product in order to gain unauthorized access to information or functionality of the gadget in the future.

D. Insider Attack

According to the cyber protection observational survey, 21% of security vulnerabilities are caused by insiders, and 21% of the reasons could be insider actions. In other ongoing surveys, More than half of those surveyed said it is much more difficult to detect and overcome insider attacks than it was in 2011, and 53% of those surveyed are increasing their security budget. Respond to insider threats. At the same time, since a large number of violations are caused by malicious or dissatisfied employees or former employees, many of them are well-intentioned employees. Try to do your business right. Byod software and files Sharing and collaborating on products (like Drop box) means that presenting organizational statistics to the appropriate employees can be more difficult than ever for employers and means that employees are irresponsible no matter what they are. Just try it Do your business well. The Byod app and collaboration and document sharing products (including Drop box) mean that it will be more difficult than ever to get business metrics under control of the organization in front of the right employees, which means few, no matter how irresponsible the team of employees

Technologies for providing security to the network

As long as the recordings are available and broadcast online, cyber threats will become the top priority in the industry. A unique protection and detection mechanism has been developed to resolve the above attacks. This section mentions some of these reinforcement mechanisms and concepts. A type. Encryption

A. System One type. Cryptography is a useful and widely used tool in today's security engineering. You are interested in using codes and passwords to turn records into distorted statistics.

B. firewall

A firewall is a normal perimeter tamper or perimeter defense mechanism. The firewall's motivation is to prevent visitors from leaving; however, it can also be used to block visitors to the dam site from within. A firewall is a main line protection mechanism that prevents intruders from entering the machine. It is a small tool designed to prevent you from entering or leaving non-public networks without permission. The firewall can be used for any hardware and software application software or a combination of both. The greatest known option for solving Internet security problems is a firewall it is a small tool located between the local network and the Internet, which can filter potentially dangerous traffic. The idea of "responses in a container" has a major appeal to many groups and is now so mainstream that it is seen as an important part of business due diligence There are basically three types of firewalls, depending on whether they remove the IP packet layer, the TCP negotiation layer, or the application layer.

Literature Review

In [1] through the use of security concerns and the collection of attack statistics within the cloud network according to the design, a jar of honey is proposed as a solution to mitigate network attacks. The idea is to position the cloud settings and identify security issues by placing jars of honey in the cloud environment. The implementation of the honey pot along the intrusion detection gadget uses entirely proprietary software based on Ubuntu. Actual statistical information is collected, analyzed and specially marked by the contemporary company through the engine on a regular basis. [2] A set of rules is proposed and a completely unique and powerful region-based key technology algorithm is designed and applied, which is entirely based on key transactions based on a dynamic region.

[3] proposed a comprehensive intrusion detection gadget (l-id) based on hop hyperlink values is intended for attacking black holes in the Internet of Things with the help of W.S.N, In addition to fact sets, Sensor nodes are also linked to different nodes via Wi-Fi links and transaction report routing. By integrating the logs transmitted on each hop, the lhv rate can be determined

due to the presence of an attacker. L.H.V is always the same as the actual (av) flow. IPv6 uses the r.p.l routing protocol to manipulate the idea of routing, Attackers use evolving routing loops to stop routing methods. The overall performance of the proposed ID-1 is being evaluated using the latest refined r.p.l routing safety solution. The proposed identification method tests the attacker's life in each statistical transmission from the supply to the target. In addition, it disables the presence of attackers on the network. The basic overall performance of the entire public community provides better results throughout the life cycle of the security solution and in detail represent the state of affairs in the community that cannot be used by black hole attackers. [4] use a full agent-based version to assess how the scammer's network has recovered from danger, their effectiveness monitors the vulnerabilities and recovery times of many fraudulent branches and, through them, we realize which damage technology is most likely to harm a large number of criminal networks.

[5] Implement a general experimental evaluation system that takes into account the uncertainty of the statistical evaluation statistics and uses this uncertainty to convert it into target weights. Combine useful resources, Combine the subjective weights of the evaluation dream with the weight of the evaluation motivation and wait a long time to appreciate the final weight. Therefore, the idea of using clearer evidence for Dempster (d-s) and hazard conversion mainly based on probability (ppt) is used to reach accord on the cyber security risk diploma. [6] Conducted in many related areas: cyber defense physics games, community threats, and community simulations, reruns of website visitors, community topology and general network services. He designed a community from end to end compulsory after components and used netkit-ng as a template for the tool and provided more skills in creating simulation networks.

[7] Describe the need for network protection and privacy for v2g applications and the harsh conditions. It provided a brand new community security facility to help v2g. It also offers a solution with the following privacy and security functions: anonymous authentication, entry of first-class access management authority, anonymous signature, data confidentiality, message integrity, remote testing and billing gadget.

To [8-10] develop the theoretical version of investment protection in the network of interconnected marketing experts. Community connections can introduce a chain reaction, caused by external or internal attacks, depending on the security investment made through the reseller. It breaks down the decomposition of personal income into personal influence and externality, which also allows us to recursively represent incentives for individual investment (taking into account the community thought of removing one agent at a time). Using this decomposition, [11] defined the rapid assessment of the CRN era and checked the related security vulnerabilities and discussed some solutions to threats. His research also focuses on Byzantine attacks or spectral-sensitive statistical forgery attacks, which are not rare specific threats, and reviews important strategies for locating and isolating such attacks via search networks. [12] Proposed a Comprehensive investigation of various protection threats and piracy for each user of social networking sites. In addition, one by one is aware of the various threats caused by the exchange of multimedia content materials within online social networking sites. Then, she proposed the destination route and conveyed some clever reaction strategies to practice, to summarize the reasons for the sincere and comfortable social network environment.

Comparative Analysis

Analysts believe its spending is unlikely to increase in 2013. This economic boom is primarily attributed to cloud computing. More than half of IT companies plan to increase their spending on cloud computing as they develop flexible and fair use of their IT resources. Intel hook runtime technology (Intel txt) is specially designed to enhance the platform to resist attacks from hypervisors, firmware, BIOS, and devices in virtual and cloud environments. Provides a mechanism to verify the integrity of these software programs while it has not yet been started. This ensures that the software has not changed from its perceived state. The txt also indicates that the platform believes that an optimal security program should implement role-based security advisories. Intel txt enforces operations through metering, memory locking, and secret sealing. Nowadays, transfer of information in a safer and secure way over a network has become a major challenge for the industry. The attacks and the network

Security measures define that how using the network security tools, a better, healthy and safe network can be designed and maintained for an organization/industry. This research focuses on the issues through which network security can be managed and maintained more efficiently in an organization. Furthermore, the Security methods and a case study will help a lot in understanding the better

management of the network-security-controlling in an organization.

Table 1: Comparative Analysis of Literature Review

Issues or Problem with Reference	Existing Solution with Reference	Weakness in Existing Solution with Reference	Is Selective?	Is Header Embedded?	Cipher?	Improvement or Research Need?
Security with cloud network	Placing jars of honey in the cloud environment .	It takes more time	No	No	Block	Its speed can be increase by replacing jars of honey closer in cloud environment
Treatment to the vampire attacks	Designed a powerful set of rules for complete neighborhood-based key generation	It is difficult for real men or women to check if the community is under attack.	Yes	Yes	Stream	Its performance can be increase if it becomes user friendly
IoT black hole attack with help from WSN.	Sensor nodes are linked to different nodes via wireless hyperlinks and routing of backup records	By Integrating the transmission of facts in each jump, the price of the lhv can be diagnosed as the existence of an attacker	Yes	Yes	Stream	The overall performance index shows major consequences within the expected ID and improves the reliability of the community.
Difficulties in designing empirical studies of criminal network recovery	Gent-based version to evaluate the curved net recovery method	Monitor vulnerabilities and recovery times for multiple criminal companies	No	No	Block	Higher skills can be observed to harm employers of fraudsters
There is no effective long-term evaluation method to protect the PC community	A unique method for assessing network security risks is proposed, which mixes subjective and target weights under conditions of uncertainty	Evaluate the advisability of evaluating the uncertainty of the records or convert them to target weights using uncertainty measurements.	Yes	Yes	Stream	Can not only effectively evaluate computer network security, but also be widely used in decision-making.
Cyber defense activities, community threats,	The community containing the various elements of	Sftp does not have to join the community. This is due to	No	No	Blocked	The problem was created by a visitor to the community site, which has now been

community simulation, rebroadcasting of community visitors, network topology and public community services	research becomes a community designed and implemented using netkit-ng	a problem in its initial configuration. It is possible to configure an https server using technology equivalent to sftp, which makes using proftpd difficult.				edited to be unmanageable
Challenges of V2G applications.	Present a new network security architecture to support V2G	Anonymous authentication, excellent operational authority, anonymous signature, confidentiality of facts	No	No	Blocked	Designing of large network leads to problem
Cascading failures due to an exogenous or endogenous attack	A tractable decomposition of individual payoffs into an own effect and an externality [8]	When the attack location is endogenized similar forces still operate	No	No	Blocked	Equilibrium may involve too much investment relative to the social optimum.
The Problem of spectrum scarcity.	Cognitive radio network (CRN) is an emerging technology which can resolve this spectrum scarcity problem	Spectrum sensing data falsification (SSDF) attack	No	No	Blocked	This work not done due to ssdf problem.
Safety measures issue and challenge in social network service are studied.	easy-to-apply response techniques to achieve the goal of a trustworthy	Uploaded multimedia content carries information that can be transmitted virally and almost instantaneously within a social networking site and beyond	Yes	Yes	Stream	A novel research direction for security of social network service can increase the speed.

Critical discussion

In order to prevent any illegal and appropriate access, misuse, failure, correction, destruction, or disclosure to the actual network infrastructure and to facilitate computer systems, clients, and programmed, a method known as "community protection" is used. Although the daily tasks are the same in a traditional setting, securing the community is accomplished through your tasks and the technology you employ to stop illegal users and programmes from accessing your networks and your devices. Basically, your computer cannot be hacked if a hacker cannot access it through the community. I hardly ever write about identifying difficulties with community safety and provide solutions for how to address such issues, as can be seen in the comparison chart above.

Dionaea, which received 91% of all assaults, was the most often targeted honeypot, second by Glutton (5% of attempts) and Components – (2% of attacks), as shown in Figure 1. Further examination of the acquired data revealed that more than 10 countries, the bulk of which were located in America, Asia, and Europe, were participating in the attacks (Figure 2). Vietnam appears to be the country that conducts the most attacks among them (30%—47,510 attacks), next by Russian and Venezuela. It is important to note that these data show where the assault originated visibly.

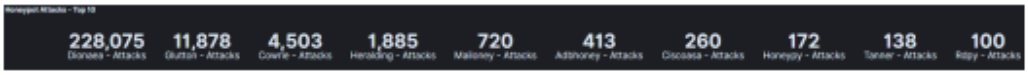
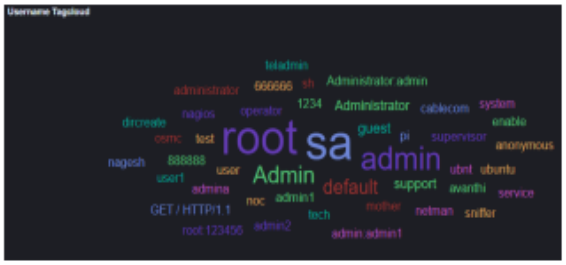


Figure 1: Top 10 AWS Honeypot Attacks.

This is true because the origin of the attack may not be accurately represented by the data given the availability of technologies like VPNs or the possibility that threat actors may use other affected systems as stepping stones. The findings from the Cowrie honeypot point to the usage of automation by attackers as well as predefined credentials and passwords taken from a dictionary to go around authentication (**Figure 3**). Additionally, an examination of the attacker input commands recorded by this honeypot revealed attempts to increase their privileges and conduct (system) information gathering prior to attempting to accomplish their goals

Figure 2: Honeypot Attack Map on AWS.



(**A**) Cloud of Username Tags

(**B**) Cloud of Password Tags

Figure 3: AWS Cowrie Tag Cloud Username and Password.

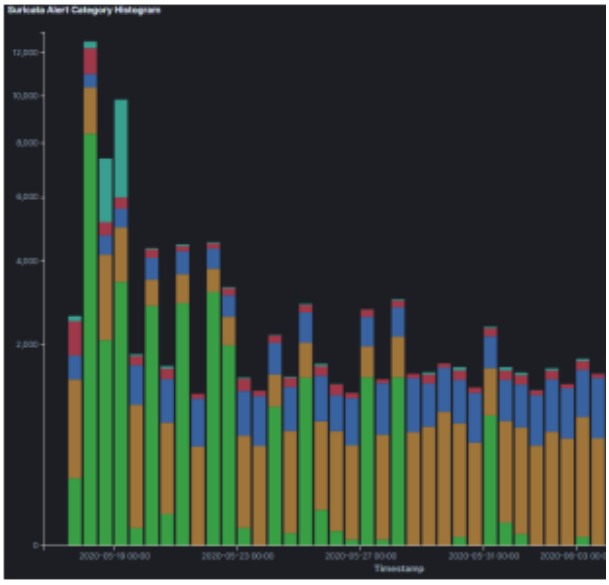


Figure 4: AWS Suricata Alert Category Histogram.

Conclusion

With the development of the Internet, it has attracted more and more attention. Internet security threats and protocols must be analyzed to determine the required security era. The security era consists of widely used software and many hardware tools. Additional community protection includes provisions contained in the underlying PC network infrastructure, strategies supported by community administrators to protect the community, and unauthorized access to network personal items for access rights and the effectiveness (or lack of effectiveness) of these mixed measures. Protecting community security is as important as protecting IT facilities and message encryption. Things to consider when setting up a convenient network are:

1) Confidentiality: the community registration remains private
2) Identity verification: ensure that the community users are what they claim to be
3) Integrity: the message has not been modified during transmission
4) Authorization (access): Provide conversation and
5) Non-repudiation for criminal clients-make sure you, this person will not refuse to use the community.

An effective community security plan must be developed on the basis of understanding security issues, the capabilities of attackers, the required level of protection, and the factors that make the network vulnerable to attacks. Tools to reduce the vulnerability of laptops to the network include encryption, authentication mechanisms, intrusion detection, security audits, and firewalls.

Future Direction:

A very specific review of cyber security issues, architecture responses, and methods. Cyber security research provides current research and has the potential to address future trends, architecture, coverage, and implementation of cyber security protocols. Coverage with community security, comfortable routing, firewall layout, cellular proxy security, Bluetooth security, Wi-Fi sensor network, structural protection, and digital content materials. The major institutions nearby provide reliable documentation on security protocols, architecture, implementation and regulations in modern countries. Participants study sports activities, proposals, research on addiction and modern protective additives, and provide expertise on the future of the industry. Contains technologies for implementing protection mechanisms and technologies, network security function

Reference

[1] S. Puri and M. Agnihotri, "A proactive approach for cyber attack mitigation in cloud network," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017: IEEE, pp. 171-176.

[2] S. Panda, "GPS Hash Table Based Location Identifier Algorithm for Security and Integrity Against Vampire Attacks," in *Cyber Security*: Springer, 2018, pp. 81-89.

[3] G. Soni and R. Sudhakar, "A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT," in *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2020: IEEE, pp. 377-383.

[4] S. W. Duxbury and D. L. J. C. Haynie, "Criminal network security: An agent-based approach to evaluating network resilience," vol. 57, no. 2, pp. 314-342, 2019.

[5] Y. Duan, Y. Cai, Z. Wang, and X. J. A. S. Deng, "A novel network security risk assessment approach by combining subjective and objective weights under uncertainty," vol. 8, no. 3, p. 428, 2018.

[6] S. Chapman, R. Smith, L. Maglaras, H. J. J. o. S. Janicke, and A. Networks, "Can a network attack be simulated in an emulated environment for

network security training?," vol. 6, no. 3, p. 16, 2017.

[7] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. J. I. W. C. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," vol. 24, no. 4, pp. 88-98, 2017.

[8] L. Abualigah, M. Abd Elaziz, P. Sumari, Z. W. Geem, and A. H. Gandomi, "Reptile Search Algorithm (RSA): A nature-inspired meta-heuristic optimizer," *Expert Systems with Applications,* vol. 191, p. 116158, 2022.

[9] F. Adriani and D. Ladley, "Social distance, speed of containment and crowding in/out in a network model of contagion," *Journal of Economic Behavior & Organization,* vol. 190, pp. 597-625, 2021.

[10] A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," *Journal of Economic Surveys,* vol. 36, no. 1, pp. 157-187, 2022.

[11] S. Kar, S. Sethi, M. K. J. I. J. o. C. N. Bhuyan, and D. Systems, "Security challenges in cognitive radio network and defending against Byzantine attack: A survey," vol. 17, no. 2, pp. 120-146, 2016.

[12] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. J. I. s. Park, "Social network security: Issues, challenges, threats, and solutions," vol. 421, pp. 43-69, 2017.

[13] D. Acemoglu, A. Malekian, and A. J. J. o. E. T. Ozdaglar, "Network security and contagion," vol. 166, pp. 536-585, 2016.