Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 12, Issue 5, 2023 | ISSN: 1000-3428

Enhancing Production Network Resilience through Honeypot-Based Defense Strategies

A. K. Ravi Kumar, R. S. Prabhakar Rao

A. K. Ravi Kumar, Department of Computer Science and Engineering, International Institute of Information Technology, Hyderabad, Telangana, India. R. S. Prabhakar Rao, Department of Information Technology, National Institute of Technology, Warangal, Telangana, India.

Abstract

Computer Networks and Internet has become extremely well known now a days since it fulfills individuals with fluctuating needs by giving assortment of fitting services. Computer Networks have reformed our utilization of computers. Online bills, shopping, transactions and numerous other fundamental activities performed in a hurry by only a solitary snap from our homes. In spite of the fact that it is a shelter in this period, it likewise has its own dangers and shortcomings as well. Ventures need to tussle to give security to their networks and in reality impractical to offer a penny for every penny security because of the impalpable knowledge of hackers interfering into the network. This paper misuses the idea of honeypots for giving security to networks of ventures which might not have custom intrusion detection systems or firewalls. The proposed display catches the different procedures utilized by hackers and makes a log of all hacker activities. Subsequently utilizing this log, the production network system can be prevented from attackers.

Indexed keywords: Intrusion, Honeynet, Honeypot, Network.

Article History: Received: 25 February 2023 | Accepted: 05 May 2023 | Published: 18 May 2023

1. INTRODUCTION

The Internet is a network of networks. It depends on the idea of parcel exchanging. Despite the fact that the services offered by Internet are broadly utilized from a layman to multi-tycoon it likewise has its own deformities. Numerous assaults on Internet are being distinguished and reported. A portion of the regular sorts of network assaults are listening in, information alteration, character satirizing, password-based assaults and refusal of administration assaults. To defeat every one of these kinds of assaults and organization more often than not introduces an intrusion detection system to secure the classified information traded over its network. The nearby network is then associated with the Internet in this manner benefiting the representatives to be online on the fly.

Information security has three fundamental targets in particular 1. Information privacy 2. Data respectability 3. Information accessibility.

Information privacy guarantees that the protected information can be gotten to just by authorized people. Information uprightness permits secure alteration of information. Information accessibility guarantees that the information is accessible promptly to authorized people. Little scale enterprises frequently don't favor on intrusion detection systems because of its establishment and upkeep costs.

Honeypots and Honeynets are a productive option for such organizations. A Honeypot can actually be a computer which can go about as a hotspot for assaults. It draws in the hackers to take a stab at hacking it which thusly may log the methods utilized by the attackers. This log is valuable to counteract such assaults to the honest to goodness network. Honeypot computer as a rule don't have any important information or information to be anchored. It just has counterfeit services running on its ports to draw in the attackers. There are numerous sorts of honeypots in view of their organization and outline.

In light of the sending criteria honeypots might be ordered into two sorts specifically 1.Production honeypots 2.Research honeypots. Production honeypots are effortlessly sent in the live condition that may catch just some measure of information about the assaults. Research honeypot

How to cite: A. K. Ravi Kumar, R. S. Prabhakar Rao (2023). Enhancing Production Network Resilience through Honeypot-Based Defense Strategies. Journal of Computer Engineering, 12(5), 68–71. DOI: https://doi.org/10.5281/zenodo.19348801

arrangement is confounded and utilized primarily for look into purposed by government organizations.

Based on plan, honeypots can be partitioned into 1.Pure honeypots, 2.High-connection honeypots, and 3.Low-cooperation honeypots. Unadulterated honeypots are finished production systems. The honeypot computer is connected to the network and taps the assaults. Low-cooperation honeypots permits confined connection with attackers and subsequently they are not tainted by the assaults. High-association honeypots are helpless against assaults. No copying happens and consequently more inclined to get contaminated by assaults. Honeynet is an accumulation of honeypots introduced to trap the aggressor activities and log them.

2. RELATED WORK

The examination about Honeypots has been over 10 years and it is one among the fields which have high degree for research. Most important research papers on honeypots are being talked about in this section.

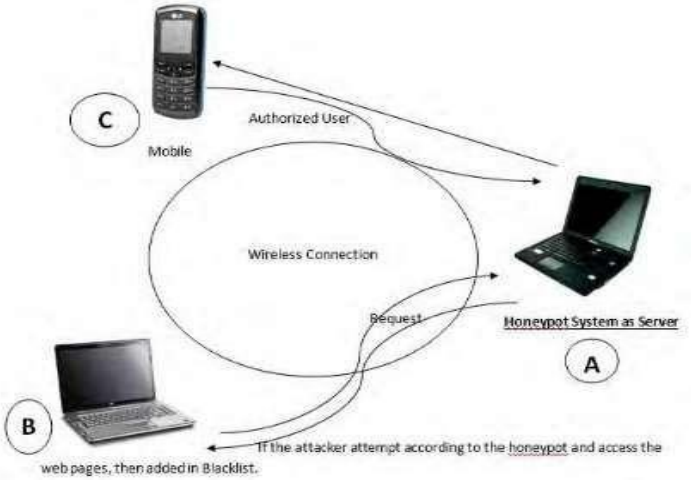
a) LAN security by applying Research

This paper proposes how honeypots can be connected in the LAN system incorporating physical and virtual honeypots. It centers on assortment of technologies like IDS, honeypot technology and firewall.

b) Capturing Network attack traffic using Honeypots

This paper proposed a system to settle the issues looked by honeypots which is an open source honeypot for UNIX. It centers in taking care of the log measure issue by outlining two modules in particular logging and log investigating modules.

Fig 1: Network with Honeypot



c) Intrusion Detection towards Dynamic honeypot

This paper proposed a dynamic honeypot plan for dynamic networks. This model partners dynamic and uninvolved testing and virtual honeypots.

d) Securing WMN using hybrid honeypot system

This paper proposed an ambush detection appear for remote work network using honeypot system. A Honeynet is shown to trap the attackers.

e) Banking security using honeypots

This paper proposed a protected system for banking applications utilizing honeypot technology.

f) Visual analytic approach for SSH honeypots

This paper proposed a diagnostic model that can be utilized by specialists to picture SSH honeypot information. Specialists can be ready to rapidly recognize the sessions to trap the attackers.

g) Honeypots in network security

This paper proposed a security demonstrate for little scale ventures which utilizes a crossover structure made out of snort, NMAP and XPROBE.

3. PROPOSED WORK

In this paper, we have utilized the idea of honeypots for giving security against attackers. A honeypot computer is set up to go about as an effectively assaulted prey than genuine or honest to goodness systems.

For setting up a honeypot there are two objectives

- From the logged information figure out how the attackers probe into the network.
- Collect proper confirmations for intrusions of the attackers to submit to law enforcement officers for legitimate activity.

To accomplish these objectives, the honeypot systems ought to fulfill certain conditions.

- The honeypot computer ought to be like other production systems.
- Usage of fascinating information in honeypots to draw in hackers.

Confine the activity conveyed to the Internet by a gatecrasher.

i) Levels of Tracking

Hacker's information recovered relies upon the level of following set amid setup. It might incorporate firewall logs, system logs and sniffer apparatuses.

a) **Firewall logs**

Setting up a firewall into a network is constantly exceptionally helpful notwithstanding honeypot system. It helps in recognizing the strategies utilized by an interloper to enter into a honeypot computer. Firewalls have distinctive warning capacities like SMS, pager and so forth.

b) System Logs

Windows and UNIX are majority working systems utilized as a part of Internet and supports logging highlight. In Windows, Event Viewer is an apparatus which gives security by logging the occasion's subtle elements. The User Manager gives client administration and services run are caught utilizing netsvc.exe. In UNIX, UTMP, WTMP, BTMP, LASTLOG are the client movement logs and SYSLOGD is a log to a remote server.

c) Sniffer Tools

These apparatuses catch the bundles that are flown between honeypot computer and the firewall. Sniffer devices gather more information about interlopers when contrasted with the system and firewall logs. They additionally offer storage of logs.

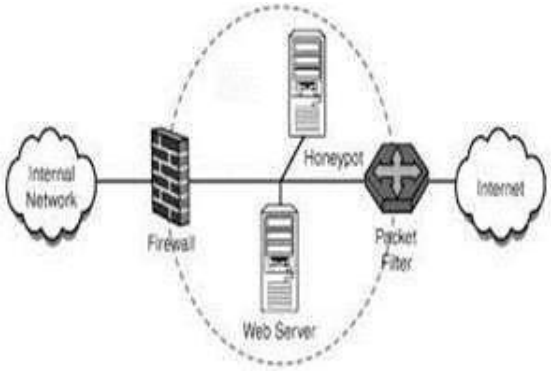


Fig 2: Honeypot Architecture ii)

Building a Honeypot

a. Contingent upon the working system the devices to be utilized for building a honeypot shifts.

b. Major Pre-requisites 3)

1. Computer or Workstation
2. Operating system (either Microsoft NT or RedHat)

4)

There are numerous cash making honeypots promptly accessible in the market specifically Tripwire, CYBERCOP sting and so on. These can be 5) bought from the market and introduced into the nearby network. In this paper, we have executed the honeypot for catching hacker information like 6) government managed savings number and IP address. In a honeypot computer, a phony banking site is made accessible. A login page is shown which requires the login id as the government managed savings number and a password to go into the bank network. Assume a hacker attempts to interrupt into the bank network by giving incorrectly information or utilize SQL infusion 7) methods a log is caught for the given subtle elements. The honeypot enables the

hackers to go into the login page as though his login points of interest were approved and shows the page for 8) doing store exchange which is eventually a phony page and along these lines no damage can be done to the bank. By along these lines, a honeypot can be utilized to catch hacker information interfering into a nearby network utilized by little scale businesses.

4.CONCLUSON

The proposed configuration can square specific IP

ddresses of hackers and furthermore give confirmations like SSN to the legitimate authorities for making lawful move. As a future upgrade more fascinating actualities can be added to pull in the hackers. Because of the fast advancement in honeypot utilization, hackers began to center around the techniques to sidestep the honeypots

nd barge in into the network. Network administrator ought to limit these issues by utilizing solid portals. Log measure is likewise a major limitation to be cared for. Developing logs are dependably a performance bottleneck and reasonable advances ought to be taken for cleansing them in regular intervals.

REFERENCES

1) R.C.Joshi et al, "A Honeypot System for Efficient Capture and Analysis of Network Traffic", IEEE-2008.
2) Iyad Kuwatly et al, "A Dynamic Honeypot Design for Intrusion Detection", IEEE-2010.

Sandeep Chaware, "Saving money Security using Honeypot ", International Journal of Security and Its Jop van der Lelie, Rory Breuk, "A visual diagnostic approach for investigating SSH Honeypots", IEEE2012.

Abhishek Sharma, "HONEYPOTS IN NETWORK SECURITY", International Journal of Technical Research and Applications 2013. Sumalatha Bandela, Ramesh Gadde and Dr. Suresh Pabboju "Survey on Cloud computing Technologies & Security threats" in International Journal of Research and Applications April – June © 2015 Transactions, eISSN: 2349-0020 & pISSN: 2394-4544 Volume2, Issue-6, pp: 296-308. DOI: 10.17812/IJRA.2.6 (53)2015.

Matthias Wählisch, Sebastian Trapp, Christian Keil†, Jochen Schönfelder, "First Insights from a Mobile Honeypot", ACM 978-1-4503-1419-0/12/08.

Shoban Babu Sriramoju, Naveen Kumar Rangaraju, Dr .A. Govardhan, "An improvement to the Role of the Wireless Sensors in Internet of Things" in "International Journal of Pure and Applied Mathematics", Volume 118, No. 24, 2018, ISSN: 1314-3395 (on-line version), url: http://www.acadpubl.eu/hub/ B. Srinivas, Monelli Ayyavaraiah, Shoban Babu Sriramoju, "A Review on Security Threats and Real Time Applications towards Data Mining" in "International Journal of Pure and Applied Mathematics", Volume 118, No. 24, 2018, ISSN: 1314-3395 (on-line version), URL: http://www.acadpubl.eu/hub/. Shoban Babu Sriramoju, "Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol 6, Issue 12, December 2017, [eISSN : 2278-1021, pISSN : 2319-5940].