International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Network Intrusion Detection System Using Honeypot in Cloud Environment

[1]Himali Gajjar, [2]Dr.Zakiyabanu Malek

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: The issues of cybercrime, allocation of space, site-hosting & loss of data are getting worse every day as the number of internet users rises. Our switch to cloud computing technique resulted in reliable, safe, fast, and cost- effective services. The real advancement in computer technology put malicious people at risk of compromising its security. System security has increased as a result of the adoption of a thorough plan, and harmful traffic has been diverted away from systems. Remember that using Honeypot on servers owned by third-party cloud vendors may present legal issues. One file-sharing programme that is installed on cloud servers makes advantage of the honeypot concept. In this study, we mainly discussed the intrusion detection capabilities of honeypots, and we used many Linux instances.

Keywords: *NIDDS, networkHoneypot, vulnerabilities, knowledge, intrusion detection, DDoS*

1. Introduction

The detection of malicious traffic on a network is performed by a network-based intrusion detection system (NIDS).[8]. In order for NIDS to analyze all traffic, including unicast traffic, it is typically necessary to have promiscuous network access.[1]. Passive NIDS operate without interfering with the traffic they observe.; Fig.1 illustrates the typical architecture of NIDS.When operating in read-only mode, the NIDS examines the firewall's internal interface and uses a different network interface (read/write) to transmit alerts to an NIDS Management server.

2. Honeypot

A system that is connected to the network and used as a bait for online criminals in an effort to detect, thwart, or gather information on hacking attempts to obtain unapproved access to data systems is known as a honeypot.A honeypot's main goal is to look like a valued target or service to attackers on the internet in order to collect all the information about it and alert defenders to any attempts at unauthorised access.

Honeypots aim to assist companies and enterprises in cybersecurity research in solving and defending ongoing attacks against advanced threats carried out by those attackers. Honeypots have been recognized as a valuable tool for organizations to have an active defense against attackers in the future. They are also used in cybersecurity research to uncover the techniques and tools that attackers use.

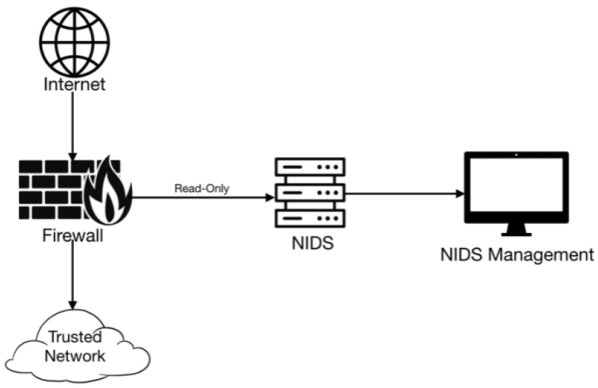

Figure1 : Place of NIDS in network

2.1. Honeypot Classification

The honeypot is built according to the level of interaction and is separated into three sections: high interaction honeypot, medium interaction honeypot, and low interaction honeypot. It is used for both production and research reasons.[2]

[1]*School of Doctoral Research and Innovation, GLS University, Ahmedabad, India*
himaligajjar10@yahoo.com
[2]*Centennial college,Scarborough, Ontario, Canada*
zakiya.malek@gmail.com

Low Interaction	It is also call as Passive IDS, It does not provide info of OS but provides info related ftp, ssh, http Honeyd is deamon which is used on single host to simulate large n/w.
Medium Interaction	It also does not provide info of OS. It checks more than Low interaction. It checks honeytrap, Napenthes. For medium contact honeypot
High Interaction	It is very difficult to plan and execute. It is very time consuming as ti also includes checks of OS. This type of honeypot requires realtime OS activity so risk is also higher.

Table 1 : Types of honeypot

2.2. Below are goals of honeypot

1. The virtual system needs to be as realistic as possible.

2. To prevent major attacks on other systems, it is necessary to monitor the virtualization system.

3. The default system should be similar to a normal system, including files and directories.

2.3. **Advantages of using Honeypot**

1. The ability for honeypots to capture attacks and analyze them allows them to provide additional data about their types.

2. The use of honeypots is allowing for a deeper understanding of future attacks and attackers.

3. Honeypots do not necessitate massive data storage.

4. Honeypots have the ability to concentrate on malicious traffic, which could greatly enhance the investigation.

5. Creating honeypots aids other computers and networks in securing themselves. The more honeypots are used by attackers, the more time they have to break into systems and cause real harm to a significant amount of users.

2.4. Disadvantages of using Honeypot :

Although there are many advantages to using technologies, there are also many disadvantages as below:

1. Hackers can only record data when they are actively attacking the system.
2. Active attacks in another system may make it difficult for the honeypot to detect them.
3. It is easy for an experienced hacker to distinguish between attacking a real system or a honeypot.

2.5. Applications domain of Honeypot:

The Honeypot can be utilized in one of the three most crucial areas or fields, and it can also be utilized as an instructional setting. We mean here that the requirements for students, cybersecurity researchers, and information security specialists are satisfied, allowing them to observe real-time breaches or attacks or monitor malware. Further learning can be done in the honeypot's suitable environment. To avoid security issues and improve our system, the second field can be used to attract hackers and learn their techniques and methods for penetration and gathering information, which may also be useful. Also, the third field may be of use.

The honeypot is utilized to monitor any harmful program and its spread within the systems. For instance, when new viruses emerge that I am unfamiliar with and cannot control, or when malicious worms spread across networks[15].It's easy for me to test them inside the honeypot and observe their effects, and they're clearly visible in the system or network. The third use of these traps is to use them as a defense tool, but this field is not useful due to the honeypot's lack of security and its ease of download, similar to antivirus, in the network.The hacker will be cautious before launching an attack if they are aware of a honeypot trap on the network.The hacker understands that the honeypot will keep track of their movements, leading to their identity being revealed.

3. Honeypot with IDS

IDS separates network traffic from that of attackers and clients. IDS comes in two flavours: anomaly disclosure and misuse detection. In identifying misuse -: To verify the attacks, IDS examines every type of data it has gathered from network traffic and compares it with a sizable database.

In Anomaly detecting:
To make it easier to identify abnormal disposal and

detect deviations from the usual, an IDS can have a honeypot point added.The connection is terminated and sent to the honeypot after the database examines the received packet to see whether any malicious packets were received. If not, the server receives the packets.

4 .We'll discuss PentBox for the honeypot in this section:

4.1 PentBox (Penetration Testing Tool)

The pentbox is categorised as a security kit that

comes with many tools to let an ethical hacker or penetration tester do their job without any problems. PentBox is an application written in Ruby that runs on MacOS, Windows, GNU/Linux, and any other operating system that supports Java, Ruby, or Python. It is open source and free.

4.2 Tools

Network-tools, cryptography tools; web Honeypot ,Ip-grabber Mass attack , as well as License and contact.

4.3 Pentbox Target:

PentBox is intended to make clear how to set up a honeypot using Linux. It does this by tricking the attacker by predicting open ports that are associated to my IP address. The message that appears contains information about the attacker that is displayed in the honeypot, allowing us to view the attacker's IP address.

4.4 The work requirements:

- Linux (Here we have used aws linux instance)
- PentBox tool and install honeypot.

4.5 The steps for work:

We have implemented honeypot infrastructure as shown in below figure,

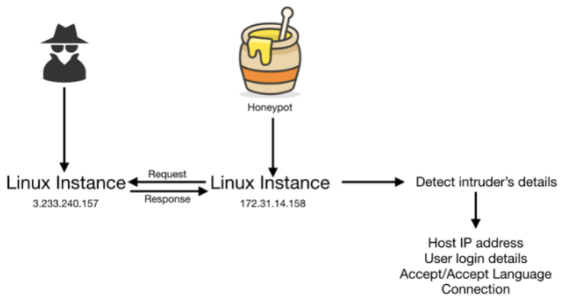

Figure2 : Honeypot working

Have created two instances, on which one instance is accessible to world and other is having honeypot installed. Here we have used both cloud instances. When user/intruder trying access website than honeypot will detects that and gather information about that user/intruder which will further help to decide if this is normal user or intruder.

Below listed steps are of how to use honeypot :

- To obtain the PentBox tool, use the following line in the Kali Linux terminal: git clone https://github.com/technicaldada/pentbox.
- Select Network Tools when all the tools on Pentbox have been downloaded and shown.

```
root@ip-172-31-14-158:/home/ubuntu/pentbox/pentbox-1.
8#./pentbox.rb
Pentbox 1.8
————————Menu ruby2.7.0 x86_64-linux-gnu
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8-Exit
 ->
```

Table 2 : Input panel while running pent box

```
- Exit

 -> 2
1- Net Dos Tester
2- TCP port scanner
3- Honeypet
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl) e-Back
0 - Back
// Honeypot //
You must run Pen Box with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration (Advanced Users, more options]
   ->
```

Table 3 : Network tool selection

- Once you choose network tools, choose Honeypot.
- After choose Honeypot; there are 2 types of options are available as listed below.
- we have chosen Auto Configuration, which makes use of the Web Service port 80, which is also used by the honeypot service.
- In order to complete this stage, I must use the command "ifconfing" to find the IP address of Linux, enter it into a web page (http://localhost), and display this message to the attacker.
- Simultaneously, but on a different side of the honeypot to display the attacker's warning message and record it's data.
- What the user is attempting to extract during the request is specified in the get statement.

- Host is the IP address

```
—> 3

// Honeypot //

You must run PenTBox with root privileges.

Select option.

1- Fast Auto Configuration

2- Manual Configuration [Advanced Users, more options]

-> 1

HONEYPOT ACTIVATED ON PORT 80 (2822-04-19
12:45:49 +0000)
```

Table 4 :Selection of pent box configuration

```
Access Denied!
```

Table 5 : Output while hitting URL

- Host is the IP address
- User-Agent: crome/5.0
- Accept: The kind of data that the user desires to obtain.
- Accept language: The language used to receive the data.
- Connection: Type of connection. Irregular or Continuous. In the event if persistent, the connection is maintained between requests.

```
// Honeypot //
You must run PenTBox with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
→1
HONEYPOT ACTIVATED ON PORT 80 (2822-04-20
08:50:39+0000)
INTRUSION ATTEMPT DETECTED! from
3.239.181.114:41222 (2022-04-20 08:50:58 +0000)
GET/ HTTP/1.1
Host: 3.239.181.114
User-Agent: crome/5.0 (X11; Linux x86_64; rv: 60.0)
Gecko/20100101 Google/60.0 Accept:
text/html,application/xhtml+xml,application/xml;q=8.9,*/*
;q=0.8 Accept-Language: en-US, en;q=0.5
Accept-Encoding: gzip,deflate
Connection: keep-alive.
```

Table 6 : Alert Generated and Intrusion Detected

5. Conclusion

It is advised that any organisation or business that has access to external resources, areas, or cloud administration implement cloud-based honeypots. The IT team needs to set up honeypots, but the real strategy should come from security units keeping an eye out for retaliatory actions. Associations handling sensitive data in the cloud will need to select Honeypots and hire experienced system managers to monitor logs and address information.

Amazing open-source tools have been developed to assist in monitoring and collecting logs from Honeypots. It obviously depends on the cloud platform itself. "The perfect Honeypot for Amazon EC2 will contrast from Microsoft's Azure or IBM's cloud" . The traditional Honeypots aren't perfect in every way because they often mirror the more traditional desktop and server operating systems. However, they are unquestionably best communicated in situations when appropriate security professionals are also examining and analysing every situation.

The added use of human cooperation adds another degree of protection, and the specialist can spot a possible or harmful attack that has never been witnessed, thus watching code would no longer be educational." Restarting from the beginning is one of the best pieces of best practice advice. Because honeypot invention is open source, the bad guys will be suspicious of default settings and will look for these telltale signals of an impending trap. These technologies need to be installed in a setting that values its clients and seeks to provide an additional layer of protection for its cloud-based platform.

6. Future Scope

Our work so far has revealed the advantages and functionality of honeypots in cloud environments. Our next task is to utilize honeypots to detect network intrusions in cloud environments. Investing in technology requires putting in more effort. Honeypots provide security and detection capabilities that can be upgraded as technology develops.

Author contributions

Himali Gajjar: Conceptualization, Methodology, Software, Field study **Dr. Zakiyabanu Malek:** Guidance

References

[1] P.aS.aNegi,aA. Garg and R. Lal, "IntrusionaDetectionaandaPreventionausing Honeypot Network for Cloud Security," 2020 10th International Conference onaCloud Computing, Data Science & Engineering (Confluence), 2020, pp. 129-132, doi: 10.1109/Confluence47617.2020.9057961.

[2] https://www.techtarget.com/whatis/feature/How-to-build-a-honeypot-to-increase-network-security

[3] Julian Jang-Jaccard,aSurya Nepal,A survey ofaemerging threats in cybersecurity,
[4] Journal of Computer and System Sciences,Volume 80, Issue 5,2014,Pages 973-993,
[5] ISSN 0022-0000, https://doi.org/10.1016/j.jcss.2014.02.005.
[6] J. Rosenberg, Chapter e6 -aEmbedded security, Editor(s): Augusto Vega, Pradip Bose, Alper Buyuktosunoglu,aRugged
Embedded Systems, Morgan Kaufmann,
[7] 2017, Pages e1-e74, ISBN 9780128024591, https://doi.org/10.1016/B978-0-12-802459-1.00011-7.
[8] https://www.sciencedirect.com/topics/computer-science/network-based-intrusion-detection-system#:~:text=A%20netwo rk%2Dbased%20intrusion%20detection,the%20traffi c%20they%20monitor%3B%20Fig.
[9] https://www.sciencedirect.com/science/article/pii/B97 80128024591000117)
[10] Sagala,a"Automatic SNORT IDS rule generation based on honeypot log," 2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE), 2015, pp.a576-580, doi:
[11] 10.1109/ICITEED.2015.7409013.
[12] S. Kulkarni, M.aMutalik, P. Kulkarni and T. Gupta, "Honeydoop - a system for on-demand virtual high interaction
honeypots," 2012 International Conference for Internet Technology and SecuredATransactions, 2012, pp. 743-747.
[13] H. Gajjar and Z. Malek, "A Survey of Intrusion Detection System (IDS) using Openstack Private Cloud," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 162-168, doi: 10.1109/WorldS450073.2020.9210313.
[14] YogeshaKumar, RajivaMunjal andaHarsh Sharma,".Comparisonaof Symmetric and AsymmetricaCryptographyAwithAExisting Vulnerabilitiesaand Countermeasures" IJCSMS International Journal of Computer Science and ManagementStudies, Vol. 11, Issue 03, Oct 2011.
[15] Mr. GurjeevanaSingh, Mr. AshwaniSingla and Mr. K S Sandha " Cryptography Algorithm Compaison ForSecurity
Enhancement In Wireless Intrusion Detection System" InternationalaJournal of Multidisciplinary ResearchVol.1 Issue 4,August 2011.
[16] BhaskarMandal,Tanupriya Choudhury,"aA Key Agreement Scheme for Smart Cards Using Biometrics.", IEEE InternationalaConference (Published in IEEE) ICCCA. 2016 ,Galgotias University,2016.
[17] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of SymmetricaEncryption Algorithms", Communications of the IBIMA Volume 8, 2009.
[18] Bhaskar Mandal ,Tanupriya, Choudhury, "AaSecure Biometric Image Encryption Scheme using Chaos and Wavelet Transformations", International Journal of Advanced Security in Data Analytics and Networks (Special Issue for Recent Advances inACommunications and Networking Technology),2016.
[19] "Honeypots: Catching the Insider Threat",aavailable at Lance Spitzner Honeypot Technologies Inc. lance@Honeypots.com.
[20] Karthik Sadasivam,aBanuprasad Samudrala, T. Andrew Yang.A"Design of Network Security Projects using Honeypots", University of Houston.