Scientific Journal Impact Factor (SJIF): 5.278

IJMTER International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

# REAL TIME HONEYNET FOR INTRUSION DETECTION AND PREVENTION

**Divyendu Shekhar[1], Abhijeet Chauhan[2], Abhinandan[3], Narendra Kumar[4]**

[1]*Information Science & Engineering, The National Institute of Engineering Mysore*
[2,3,4]*Computer Science & Engineering, The National Institute of Engineering Mysore*

**Abstract** — Attacks on the internet are increasing rapidly and causing harm to our security systems. For minimizing these threats, it is necessary to have a system that has ability to detect and block them. A honeypot is a deception technology, designed to create a virtual trap to lure attackers to compromise the computer systems of an organization.

A Honeynet is a group of high interaction honeypots on a highly monitored network. A honeypot can serve as an advanced security intelligence tool. Honeypots can also be used to analyze the type of attacks tried to compromise an information system to understand attacker behavior patterns and to improve the security policies. This paper proposes real-time honeynet intrusion detection system to investigate cybersecurity breaches to collect intel on how cybercriminals operate. The effectiveness of the existing methodologies was investigated to detect and prevent attacks. The study used open-source technologies which allows hackers to dynamically add or modify hacking incidences in a high-interaction honeynet system. It makes honeypots more attractive for hackers to spend more time on the intentionally compromised computer system to provide hacking evidence. Simulations showed the efficiency of the presented approach in collecting the information about the IP address, location and time of the attacks using centralized logging system.

**Keywords** — Honeypot, Honeynet, Puppet Management Server, HonSSH

## I. INTRODUCTION

The number of computers connected to a network and the internet is increasing rapidly. Intrusion detection and protection for network systems is becoming very challenging these days due to high network speed. Network systems contain data that must be protected from intruders. Traditionally firewalls and host-based detection system were used to detect attacks. Problems with this system is that they are running on the computers which are used on daily basis. The continuous usage of the system produces large log files and also makes it difficult to differentiate between the attacks and normal traffic. Honeypots can dramatically reduce these problems by tracking only illegal attacks which makes it extremely efficient.

A Honeypot is a system or program put on a network to have the system probed, attacked, and potentially exploited. Honeypots and honeynets are used to protect network systems. Honeypots are generally virtual machines similar to the real machines with some loopholes to attract intruders to spend their time trying to exploit the system. These activities are logged and monitored to study new hacking techniques from intruders and also to find the vulnerabilities in the system. Honeypots are used to collect, manage and analyze attack data efficiently.

## II. PROPOSED METHOD

A real-time honeypot system for intrusion detection system to investigate cybersecurity breaches to collect intel on how cybercriminals operate. The aim of the paper is to reduce manual interventions required for

DOI:10.21884/IJMTER.2021.8007.HANRB

adding and modifying a high interaction honeypot system and to detect the attacker behavior patterns and come up with the solution to mitigate the attacks in real time.

**Design**:

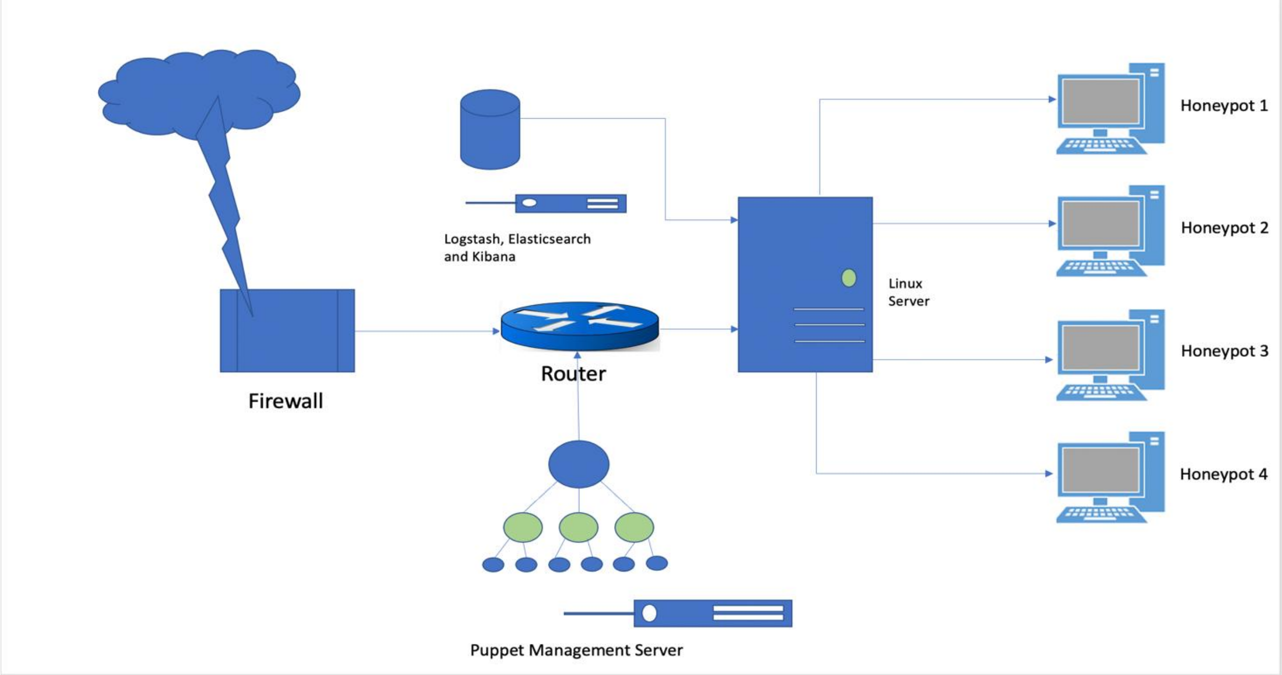

Figure 1 : Network Design Diagram

Figure 1 shows the configurations used to detect and prevent attacks on honeypots.

**Tools** :

1. Puppet : used to automate repetitive tasks (app installation, patch managements etc.)
2. Elasticsearch : used for achieving fast search responses as it does index search instead of text search
3. Kibana : used to visualise captured logs from compromised honeypots
4. HonSSH : open source high interaction honeypot software

**Hardware and Software Requirements**:

- VM running on VMware Workstation
- CPU : i7 or newer
- RAM : 12 Gb or more
- Storage : 500 Gb or more
- VM based honeynet having 4 honeypot systems

## III. SYSTEM IMPLEMENTATION

Puppet management server configure and automate on all honeypots, Hostname of the master node was set as puppetserver.com and each of the other nodes was set to point to proper IP addresses (192.168.1.10, 192.168.1.12 … ). Each of the puppet enterprise agents or honeypots were installed with the same OS and config as master node. Puppet agent packages were installed on each node. Each agent or honeypot was configured as per the below table :

| Agent | Configuration |
|---|---|
| Honeypot 1 | Apache Webserver, NTP Server, SSH server |
| Honeypot 2 | MYSQL server, NTP server, SSH server |
| Honeypot 3 | FTP server, NTP server, SSH server |
| Honeypot 4 | SMTP server, NTP server, SSH server |

Table 1 : Honeypots(agents) and their configurations

HonSSH (a high interaction Honeypot solution) was configured to sit between multiple honeypots and the attacker creating two separate SSH connections. It uses the following python script to select one of the four honeypots which were configured using puppet automation management tool:

```
import sys
from random import randint

if len(sys.argv) > 5
   sys.exit(1)

honeypots = ['node1, 192.168.1.3, 22', 'node2, 192.168.1.7, 22', 'node3,192.168.1.9,22', 'node4, 192.168.1.13,22']

honeypot = honeypots[randint(0,len(honeypots)-1]

print honeypot
sys.exit(0)
```

Elasticsearch, Logstash and Kibana, Nginx and Filebeat package was installed and set up as per the flow : User <-Nginx <- Kibana < - Elasticsearch <- Logstash <- Filebeat < -HonSSH. Using Filebeat SSL certificate and key pair was created to ship logs from HonSSH server. This was used to verify ELK server by filebeat. Logs were transported from HonSSH server to Logstash server by Filebeat.

**Filebeat configuration**:

```
filebeat:
  prospectors:
    -
      paths:
            - /usr/lib/honssh/logs/*.log
        document_type: log
     registry_file: /var/lib/filebeat/registry

     output:
        logstash:
            hosts: ["192.168.1.13:5044"]
            bulk_max_size: 1024
            tls:
               certificate_authorities: ["/etc/pki/tls/certs/logstash-forwarder.crt"]
         shipper:
         logging:
            files:
```

**Logstash server configuration** :

```
input {
    beats {
        port => 5044
        ssl => true
        ssl_certificate => "/etc/pki/tls/certs/logstash-forwarder.crt"
        ssl_key => "/etc/pki/tls/private/logstash-forwarder.key"
    }
}

filter {
    grok {
        match => {
            "message" => "%{TIMESTAMP_ISO8601:timestamp\[%{WORD:text},$
    }
    mutate {
        gsub => ["rest", "'", ""]
        gsub => ["rest", "False", "false"]
    }
    json {
        source => "rest"
    }
    mutate {
        remove_field => ["rest", "message"]
    }
}

output {
    elasticsearch {
        host => ["localhost:9200"]
        protocol => http
        manage_template => false
        index => "%{[@metadata][beat]}-%{+YYYY.MM.dd}"
        document_type => "%{[@metadata][type]}"
    }
    stdout {
        codec => rubydebug
    }
}
```

## IV. DATA ANALYSIS AND RESULT

Investigation on these systems were performed for 10 days. 100000 attacks were captured during this time. The experimental setup was similar to real world as it has Webserver, MYSQL server, FTP server and SMTP server installed on the honeypots. Below tables show the Source IPs and frequencies of them.

| Top Source IP | Frequency |
|---|---|
| 218.25.205.122 | 834 |
| 224.176.24.221 | 365 |
| 119.12.127.92 | 277 |
| 59.49.5.225 | 140 |
| 119.143.223.65 | 30 |
| Total | 1646 |

Table 2 : Attacks frequencies on Honeypot 1

| Top Source IP | Frequency |
|---|---|
| 218.25.205.122 | 855 |
| 224.176.24.221 | 389 |
| 119.12.127.92 | 278 |
| 59.49.5.225 | 108 |
| 119.143.223.65 | 31 |
| Total | 1661 |

Table 3 : Attacks frequencies on Honeypot 2

| Top Source IP | Frequency |
|---|---|
| 218.25.205.122 | 849 |
| 224.176.24.221 | 372 |
| 119.12.127.92 | 317 |
| 59.49.5.225 | 124 |
| 119.143.223.65 | 33 |
| Total | 1695 |

Table 4 : Attacks frequencies on Honeypot 3

| Top Source IP | Frequency |
|---|---|
| 218.25.205.122 | 859 |
| 224.176.24.221 | 311 |
| 119.12.127.92 | 309 |
| 59.49.5.225 | 107 |
| 119.143.223.65 | 34 |
| Total | 1620 |

Table 5 : Attacks frequencies on Honeypot 4

## V. CONCLUSION AND FUTURE WORK

The research designed and implemented the real time honeypot system for intrusion detection and prevention. System services on MYSQL server, FTP server, SMTP server and Apache Webserver were used to attract attackers. The experiment was done for 10 days and Almost 100000 attacks were logged. The result shows the IP addresses, location and usernames and passwords and ports of the attacks. This research also shows the reduction in manual efforts to add or modify honeynet systems.

In future Ansible can be used to capture and record activities of honeypots. Also, the system can be enhanced as a Honeymap to give more information about the type of attacks.

## REFERENCES

[1] Honeypot based Secure Network System, Yogendra Kumar Jain et al. / International Journal on Computer Science and Engineering (IJCSE)

[2] Honey Pot Intrusion Detection System http://www.ijeijournal.com/papers/Vol.4-Iss.5/E04_05-2841.pdf

[3]Honeydoop - A System for Creating Virtual Honeypots Using Hadoop http://ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503127.pdf

[4] How To Install Elasticsearch, Logstash, and Kibana https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04

[5] How To Install Nginx https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-ubuntu-18-04

[6] A software implementation of a genetic algorithm based approach to network intrusion detection https://ieeexplore.ieee.org/document/1434896

[7] Investigation and analysis of malware on websites
https://ieeexplore.ieee.org/document/5623567/citations?tabFilter=papers#citations

[8] Honeypot-based intrusion detection system: A performance analysis https://ieeexplore.ieee.org/document/7724682

[9] https://www.sciencedirect.com/topics/computer-science/honeynets

[10] Krawetz, N. (2004). Anti-honeypot technology. IEEE Security & Privacy, pp. 76-79. Liston, T. (2002, February 12). Tom Liston talks about LaBrea. Retrieved from http://labrea.sourceforge.net/Intro-History.html.

[11] Stiawan, D., Abdullah, A. H., & Idris, M. Y. (2011). Characterizing network intrusion prevention system. International Journal of Computer Applications (0975–8887).