IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADVANCE HONEYPOT SYSTEM

[1]Kavita Joshi, [2]Dhruv Patel, [3]Priyanka Bhoir, [4]Mohini Patel, [5]Yash Patel

[1]Assistant Professor Laxmi Institute Of Technology,Sarigam,
[2]Laxmi Institute Of Technology, Sarigam,
[3]Laxmi Institute Of Technology, Sarigam,
[4]Laxmi Institute Of Technology, Sarigam,
[5]Laxmi Institute Of Technology, Sarigam,
[1]Information Technology,
[1]Laxmi Institute Of Technology, Sarigam, Valsad, India

Abstract: Now a Days Industries are doing Great job but they forget about “security”, security of their products security of their companies. The purpose of this study is to keep intruders away from real system and to closely monitor the intruder to study the exploits which are used. Make use of the Vulnerability to trap intentional attackers and study attack.

Keywords— **Honeypot, Network Security, Network Attack, Network Threats, Darknet, Malicious Attack,**

I. INTRODUCTION

The paper is about the final year college project on advanced honeypot system which is an alert and logging unit of cowrie ssh honeypot [1]. Parsing the log file generated in json format by honeypot and showing it on an authorized user’s mobile device. These days web application is being extensively used over the internet which also indirectly gives the invitation to the attackers to hack the websites and retrieve confidential information and data. The vulnerabilities of the web application let the attackers intrude to servers or can even get inside the network environments. Attackers then can exploit the web sites with different attacks and can cause heavy damage to the owners of the website or the corporate holders. In this situation, the owners of the website have to stay updated all times so that they can fight against the vulnerabilities of the websites. However, it also gets very difficult to protect the websites against zero-day exploits which are newly developed and invented.

The goal of honey pot is to secure networks from such kind of security flaws. The Honey pot detects malicious packets in network and provides wrong information. When attacker tries to attack by sending malicious traffic to a server having a honey pot embedded into it. The server responds to attacker with miss information or wrong information and this can even use for capturing the attacker by forming a trap.

II. THEORETICAL FRAMEWORK

[1] Honeypot classification and mapping with attack process: we provide a detailed classification of current honeypot solutions and we link this classification with the different phases of attack collected. We outline the different properties and limitations of honeypots.

Hybrid architecture: we describe an innovative honeypot solution that provides both a high scalability and a high level of interaction. We also introduce the concept of an attack event, to differentiate network attacks worth of analysis from the noise of malicious traffic. Our architecture is designed to be able to harvest large IP spaces while actively filtering attack events from attack traffic for detailed focused analysis.

[2] **Botnet Abolish Using Honey pot:**

Honeypots are a modern approach to network security. Because “botnet” can be used for illicit financial gain they have become quite popular in internet attacks. ”Honeypot” have been successfully deployed in many defense systems. Thus attacker constructing and maintaining botnet will be forced to find a many way to avoid honeypot traps. Independent honeypot detection methodology based on following assumption : security professional deploying honeypot have liability constraints such that they can’t allow there honeypotto practice in real attacks. Based on this assumption ,attackers can’t detect honeypot in their botnet by checking whetherthe compromised machine in botnet can successfully send out unmodified malicious traffic to attackers sensor or whether the compromised machine in botnet can successfully send out unmodified malicious traffic to attacker.

III. RESEARCH METHODOLOGY

Here we have created a mobile app which work as alert and logging unit of a honeypot system. here the honeypot system is cowrie which generates the logfiles(at var/log/cowrie/log_<date>.json) day wise wich stores the attacks info.so at first we parsed the date wise different json files then seperated all parsed all the content of it. It contains session id, login id, password, Event, timestamp,sourceIp, message. the ip is mapped with GeoLite2-Country.mmdb[5]data base which is readly available which gives locations from ip whish is used to displays threatmaps, in mobile app using google maps API. All this parsed data is been sent to firebase from honeypot server. The attacker might upload some malicious content or payloads on attacking machine. Whoch is stored at(/home/cowrie/cowrie/var/lib/cowrie/downloads) location, which is pushed to firebase's storage section and from there it gets accessed on the mobile mobile phone according to type and size of file uploaded by attacker. On the basis of attack we have diiferentiated flags and most common attack to differentiate and mannage the attacks.

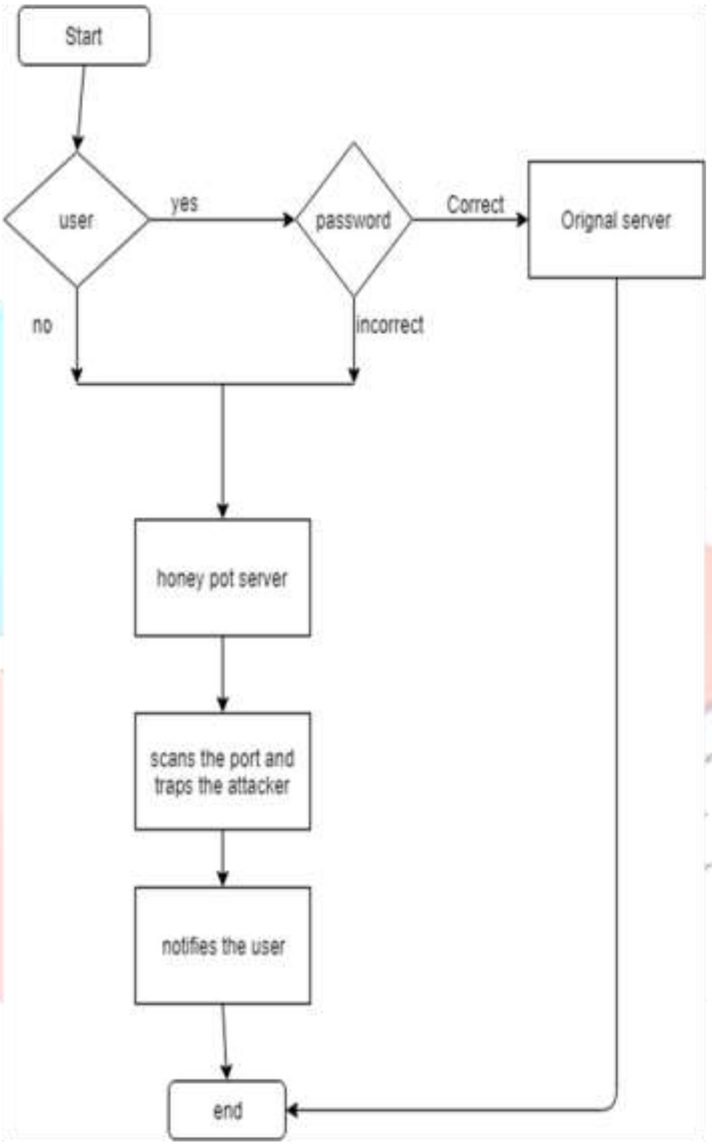
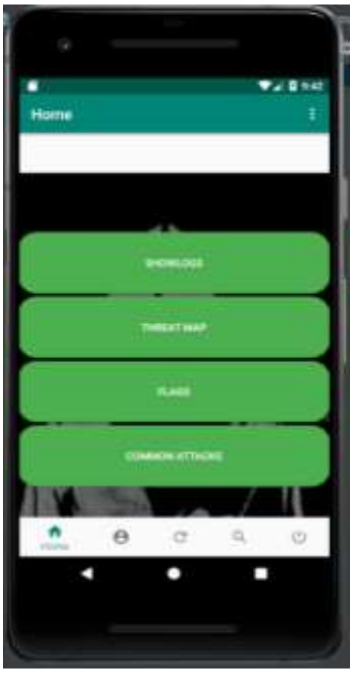
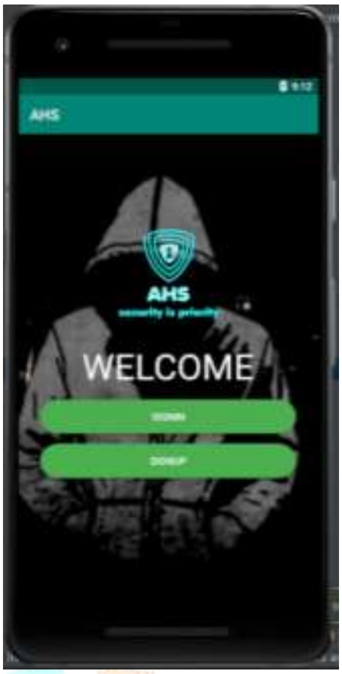
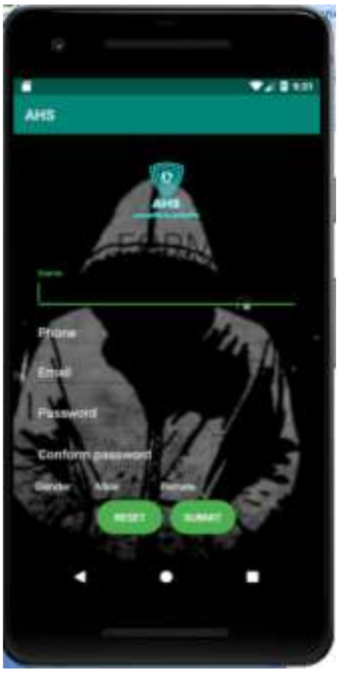


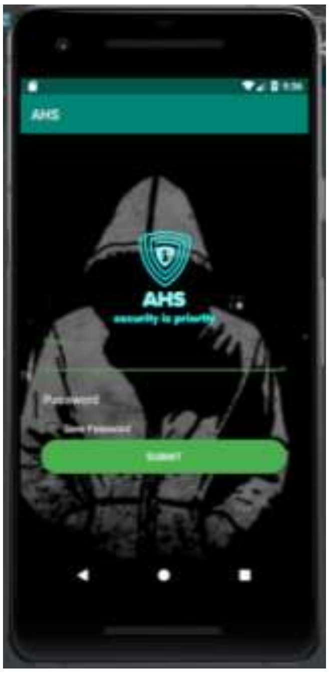
Fig. System flowchart

IV. IMPLEMENTATION









Home page Registration Page Login page

V. RESULTS AND DISCUSSION

In this semester we have successfully completed the documentation of our project.Adopting a spiral model approach is a fundamental change in working practices for the management team and everyone else involved in this project. Successful iterative and incremental developments require a progressive and adaptive approach to be taken to the management of the project and require the whole team to embrace change and the continual improvement that this change will help to produce exponential height in project. The logs generated by honeypot can be help to detect web application attacks against the web servers in the production network and help gather information like IP address, tools, techniques etc. related to those attacks. This information can be used to further secure the web application servers and can also detect coordinate attacks against web servers. For the next part of our project, we are going to create a virtual files system which is known as honeyfs which will give fake info to an attacker who has unauthorized access to our server and we are developing a threat map for the visual representation of attacks and an alert the unit which will give notifications to users about the attack.

REFERENCES

[1] https://cowrie.readthedocs.io/en/latest/README.html#
[2] https://firebase.google.com/docs/firestore/quickstart
[3] https://firebase.google.com/docs/firestore
[4] https://developer.android.com/docs
[5] https://developers.google.com/maps/documentation