Threat Prediction Using Honeypot and Machine Learning

SUBMITTED IN COMPLETE FULFILLMENT OF THE

REQUIREMENTS OF THE DEGREE OF

BACHELOR OF ENGINEERING

IN

INFORMATION TECHNOLOGY

BY

SACHIN MAURYA

MELVIN RAJU

CHANDRAKANT THAKUR

UNDER THE GUIDANCE OF

Prof. SUVARNA ARANJO

(Department of Information Technology)

INFORMATION TECHNOLOGY DEPARTMENT

XAVIER INSTITUTE OF ENGINEERING

UNIVERSITY OF MUMBAI

2021 – 2022

XAVIER INSTITUTE OF ENGINEERING

MAHIM CAUSEWAY, MAHIM,

MUMBAI - 400016

CERTIFICATE

This to certify that

SACHIN MAURYA	(30)
MELVIN RAJU	(31)
CHANDRAKANT THAKUR	(62)

Have satisfactorily carried out the PROJECT work titled "**Threat Prediction Using Honeypot and Machine Learning"** in complete fulfillment of the degree of Bachelor of Engineering as laid down by theUniversity of Mumbai during the academic year 2021-2022

Suvarna Aranjo
Supervisor/Guide

Prof. Meena Ugale
Head of Department

DR. Y.D Venkatesh
Principal

PROJECT REPORT APPROVAL FOR B.E.

This project report entitled "Threat Prediction Using Honeypot and Machine Learning "

By

SACHIN MAURYA (30)

MELVIN RAJU (31)

CHANDRAKANT THAKUR (62)

is approved for the degree of BACHELOR OF ENGINEERING.

Examiners

1. _____

2. _____

Supervisors

1. _____

2. _____

Date:

Place: MAHIM, MUMBAI

DECLARATION

I declare that this written submission represents my ideas in my own words and where others' Ideas or words have been included; I have adequately cited and referenced the original sources.

I also declare that I have adhered to all the principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which thus have not been properly cited or from whom proper permission have not been taken when needed.

Sachin Maurya (30) ----------

Melvin Raju (31) ----------

Chandrakant Thakur (62) ----------

Date:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

A honeypot is a deception tool, designed to entice an attacker compromise the electronic information systems of an organization. If deployed correctly, a honeypot can serve as an early-warning and an advanced security surveillance tool. It can be used to minimize the risks of attacks on IT systems and networks. Honeypots can also be used to analyze the ways attackers try to compromise an information system and to provide valuable insights into potential system loopholes. This research investigated the effectiveness of the existing methodologies that used honeynet to detect and prevent attacks. The study used centralized system management technologies called Puppet and Virtual Machines to implement automated honeypot solutions. A centralized logging system was used to collect information about the source IP address, country, and timestamp of attackers. In this paper, we detect a compromised SSH session that is carrying out malicious activities. We use flow-based approach and machine learning techniques to detect a compromised session. In a flow-based approach, individual packets are not scrutinised. Hence, it works better on a high-speed network. The data is extracted from a distributed honeypot. The paper also describes the machine learning techniques with appropriate parameters and feature selection technique..

Acknowledgement

We would like to thank Fr. (Dr). John Rose S.J. (Director of XIE) for providing us with such an environment so as to achieve goals of our project and supporting us constantly.

We express our sincere gratitude to our Honourable Principal Mr Y.D.Venkatesh for encouragement and facilities provided to us.

We would like to place on record our deep sense of gratitude to Prof Meena Ugale, Head of Dept. Of Information Technology, Xavier Institute of Engineering, Mahim, Mumbai, for her generous guidance help and useful suggestions.

With deep sense of gratitude we acknowledge the guidance of our project guide Prof Suvarna Aranjo. The time-to-time assistance and encouragement by her has played an important role in the development of our project.

We would also like to thank our entire Information Technology staff who have willingly co-operated with us in resolving our queries and providing us all the required facilities on time.

Sachin Maurya (30) ----------

Melvin Raju (31) ----------

Chandrakant Thakur(62) ----------