**End semester report on R & D Project**

**Academic Year- 2020-21**

on

**FUZZING IN THE FACE OF THREAT HUNTING**

A dissertation

Submitted in partial fulfillment of the requirements for the award of the degree

Master of Technology

by

1. **Mahesh M MT20ACS516 Cyber Security**

Under supervision of

**Prof. Ashu Sharma**



NIIT University, Neemrana, Rajasthan-301705

Dec 2021

1. INTRODUCTION

FUZZING (known as fuzz testing) is “an automated testing method covering numerous boundary cases using fuzzed data (ranging from networking protocols, file types, API calls and other different types of targets) as an input to the target trying to find out vulnerabilities as well as robustness of the software and may even lead to DoS due to impact of Fuzzing.

It was first proposed by Miller et al. in 1988, and since then, it has developed into an effective, fast, and efficient way of finding bugs in the software.[1]

In general, Fuzzer (the system generating Fuzzed test cases) will feed those large number of test cases towards the Target (the system receiving Fuzzed test cases) aiming to activate software errors in the target. The usual mechanism to check if the system has passed the fuzzed test case is by sending out a valid packet to the target (within fraction of seconds sending fuzzed packet) and expecting the response from the target.

If the target didn’t respond, it is believed to be impacted by the Fuzzed test cases and it continues sending the valid test case till the target has responded. When the target responds back, it is assumed that the target is able to recover from the impact of fuzzed test cases and time taken to respond back is considered downtime for the target.

If the target did respond in the first time, it believes that the target is robust enough to tackle the fuzzed test case. With advancement in fuzzing methodologies, a modern Fuzzer has evolved itself to be one of the most important security techniques to improve the security of the software.

Threat Hunting is an approach to identify threats by proactively going through the networks, endpoints, or datasets which may have evaded detection by existing tools [2]

There are multiple tools used by hunters such as CyberChef[4], Yara[5], etc and there are multiple threats such as DoS attack, MITM attack, Phishing, SQL Injection.

The relationship between Threat Hunting and Fuzzing is that Fuzzing aims to perform DoS threat and identify which inputs are creating the DoS threat with the time involved which may or may not be created as a report depending upon the fuzzing the tool.

A. Motivation

The motivation for this research is over the last few decades, fuzzing has become a mainstay in Software Security and different varieties of Dos Threat. Thousands of threats in all kinds of software have been found using Fuzzing.[2]. It is able to find many unknown vulnerabilities/Zero-day vulnerabilities [6] which is necessary to stay securely in the current generation and our research hopes to bring more concise information on Fuzzing, art of Fuzzing and how Fuzzing can be better utilized for Threat Hunting especially DoS Threat.

1. CONCLUSION

REFERENCES

[1] Hongliang Liang; Xiaoxiao Pei; Xiaodong Jia; Wuwei Shen; Jian Zhang “1: State of the Art” IEEE Transactions on Reliability Vol 67 no:3, pp. 1-5, Sep. 2018.

[2]McAfee, <https://www.mcafee.com/enterprise/en-in/security-awareness/operations/what-is-cyber-threat-hunting.html>

[3] Cyborg Security, <https://www.cyborgsecurity.com/threat-hunting/>

[4] Crown Copyright, “<https://github.com/gchq/CyberChef>”

[5]Yara, <https://virustotal.github.io/yara/>

[6] Trend Micro, “<https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability>”