TED University/ CMPE491

Senior Project

Project Specification Report

GROUP MEMBERS	SUPERVISOR
AYŞE NUR ŞAFAK	EMIN KUĞU
KAYRA EGE ARDA	
BARAN AKIN	JURIES
EBRU KILIÇ	VENERA ANDANOVA
	TOLGA KURTULUŞ ÇAPIN

Date
10-31-2021

PROJECT SPECIFICATION REPORT

Introduction

The rising vulnerabilities are one of the most regarding situation of the day. So every day, billions of attacks on small, medium, and large networks appear around the world[1]. Some detection tools have been developed to protect networks by gathering information from previous malicious attacks[1].A honeypot is one of these tools which traps attackers by using fake data that a hacker will attempt to steal from. In this project, we will design a low-interaction, SSH honeypot. It will be installed on a public server in order to investigate cyber-attack methods.

Decscription

Honeypots are fake servers or systems that are located near real servers or systems in order to manipulate hackers into compromising the fake system. They attract attackers by exploiting security vulnerabilities. As a result, they focus on detecting vulnerabilities in internal networks as well as trying to deceive hackers. The reason we want to have our honeypot open to the public is so that we can collect organic data about potential attacks and analyze it. Also, in this project, we want to analyze and learn how the bad actors usually act, thus broadening our experience and views for both defending and pen testing. Nevertheless, we plan to use the data that we collect to assist in the manifestation or improvement on some IDS and IPS systems. Furthermore, this attacker data will enable us to predict and learn the behaviors and steps of the bad actors.7

Requirements

Our requirements will be a VPS server to host our honeypot. While we do not plan to use any off the shelf or proprietary software if we do it will be arranged and disclosed in the related documents and development notes. We plan to use outside libraries to, (but may not be limited just for these actions), manage data, create a honeypot environment, configure such services, host these services, and maintenance of these services.

Functional Requirements

SSH honeypot shall perform as a server in a Linux environment.

The Honeypots that emulates a vulnerable web server shall catch up attacker activity.
The Honeypots shall take the log files which includes attacker’s information.

Non-Functional Requirements

The system shall be stable.

The system shall not be exploitable.

An attacker would only have limited access to the operating system. Because it is a much more static environment and 'low interaction' means that the attacker will not be able to interact with our fake system in any detail.

The honeypot needs to be reliable.

The honeypot should be secure (it cannot become or create a vulnerability to the host system).

The Honeypot does not use significant resources to maintain.

Project Constraints

PROJECT SPECIFICATION REPORT

Economic

They are, renting and maintaining a basic VPS, and we believe that this will not cost more than 200-300 Turkish liras per month.

Environmental

We will have no physical product and our only environmental impact would be hosting an server.

Social Constraints

We will be catching potentially malicious actors whom they also might be security resarchers like us, thus we plan to keep their information hidden and anonym unless they damage the system and try to harm the hosting services than we will have to legally disclose their information with the hosting company.

Political

We do not condone or support any political partys or groups, and with the nature of the project we believe that we will not have any part and issue regarding any political affairs, regarding health and safety, we will not have an pyhsical product at the end of this project, but our project is constructed such that we plan to use the data that we gather to further strenghten the safety of it systems. by analyzing the data that we gather which is attacker actions, by knowing the knowhow of the attackers we plan to further improve the security of the system's. a concern and constraint that we have is that we need to find a host that accepts to host a honeypot. with our research we have found that other security researchers have used amazon web services to rent a vps and host a honeypot on it, we contacted aws and are waiting for an positive reply.

Manufacturability Again

We will not have an pysical product and manifacturement of an pyhsical product falls outside the scope of this project.

Sustainibility

Our constraints would be the limited maintenance and updation of the service/s and the cost of renting a vps server.

Ethical

Honeypots can be used in unethical ways, although that is uncommon. In this project, there is no any piece of illegality. The reason is, the purpose of using honeypots is for doing analyze and research. Also, nay honeypots do not force an attacker to interact with them because they are machines that simulate specific services that the attacker have to choose to interact with.

Profesional and Ethical Responsibilities

Our profesional and ethical repsonsibilities for this project would be that our honeypot must not interfere with the hosting service's to insure that we need to monitor the activities that are happening on the honeypot and try our utmost best to isolate the actual server from the honeypot that we are developing.

Secondly, we must keep the identitites of the bad actors anonymous in our reports and analyisis, other than the cases that we are required to disclose their identity with the hosting provider, these cases include but are not limited to; trying to damage and or reverse engineer the actual hosting companies software, any and all ddos and dos attacks. Trying to collect data from our actual service that we are trying to keep anonym and discuss this with third parties. We also promise that if we encounter a situation that an attacker's information that needs to be disclosed, we will not disclose this information to any third party other than the authorities and the hosting company itself. Keep in mind that we do not and will not have any authority over what will the hosting company do with this information.

Thirdly as students and researches we pledge to not use the information that has been gathered for our own or for any groups or communities malicious activities.

References

- [1] S. Russell and P. Norvig, Virtual honeypots: from botnet tracking to intrusion detection, 3rd ed. Addison-Wesley Professional, 2007.
- ACM Code of Ethics and Professional Conduct
- The Software Engineering Code of Ethics, IEEE Computer Society
- IEEE Code of Ethics
- Computer and Information Ethics, Stanford Encyclopedia of Philosophy