Senior Project Proposal

Date: [11.10.2021]

Project

Set-up and Maintenance of an SSH Honeypot

Website URL

https://ayse-nur-safak.github.io/HoneyTED/

Group Members:

Ayşe Nur ŞAFAK
Kayra Ege ARDA
Ebru KILIÇ
Baran AKIN

Supervisor: Emin KUĞU

Juries:
Venera ANDANOVA
Tolga Kurtuluş ÇAPIN

Abstract

Honeypots are counterfeit servers or systems that are placed near to real servers or systems that have the purpose of tricking hackers into compromising the counterfeit system. They use security vulnerabilities to attract attackers. So, they concentrate on detecting vulnerabilities in the internal network as well as deceiving the hackers. As the authors, we are attempting to further harden our systems and increase the barrier of entry further. Also, we can analyze the common people that are trying to enter to further broaden our insight on the malicious actors, thus allowing us to harden our system further.

Problem

As the number of ways and strategies used to attack networks increases, the objective of protecting a network must similarly increase. While existing approaches and many other techniques can help to build a secure network, it is important to expect that vulnerabilities will always exist and will be exploited eventually. As a result, we must always develop new ways to combat threats, and one major technique is to install honeypots. While the concept is not recent, we believe that it will give valuable insight into what is vulnerable on our system, and how can we fix these vulnerabilities.

Aim

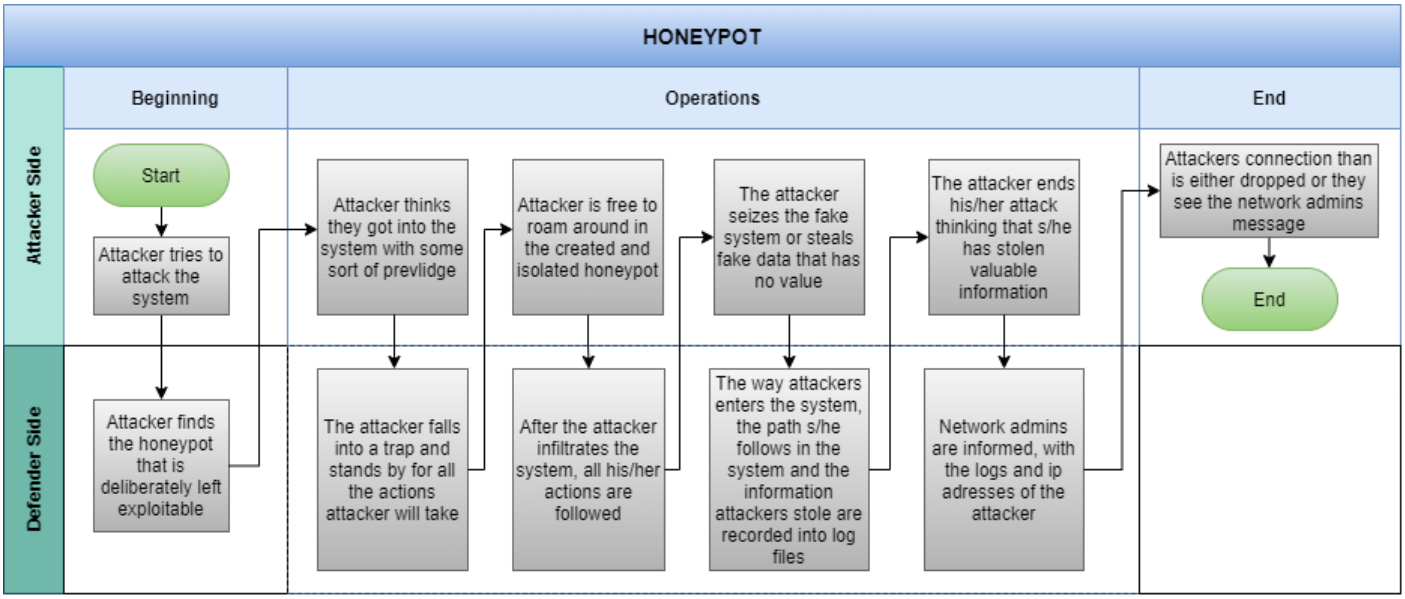
Our project's goal is to design a low-interaction, SSH honeypot. It will be installed on a public Linux server in order to investigate cyber-attack methods. The reason that we want to have our honeypot in the public is that we want to collect organic data about the attacks that may take place and further analyze this data.
Our major reason for pursuing this project derives from our curiosity about the cybersecurity, computer networks and cyberattacks.

Another one of our goals is that we would like to analyze and learn how the bad actors usually act, thus broadening our experience and views for both defending and pen testing in the future, in our careers.
We also plan to use the data that we collect to assist in the manifestation or improvement of some IDS and IPS systems. Furthermore, this attacker data will enable us to predict and learn the behaviors and steps of the bad actors.

Why a Honeypot May be Used?

1. Break The Kill Chain of Hackers: Hackers typically scan our network for vulnerabilities. They may interact with our honeypot as they lie in wait for attacking. By using honeypots, we may both capture the attacker inside and analyze its activities. Furthermore, honeypots break the kill chain of hackers by tempting attackers to spend their time pursuing worthless information in the honeypot rather than their targets.
2. Understand the attacker's techniques in order to better secure real-world systems and servers.
3. Assist in the testing of Detection and Response Processes
4. We may observe hackers at work and learn about their behaviors
5. We may collect the data on attack vectors, malware, and exploits and use it to teach us.
6. When a major attack is made on the system, it reduces the load of the attack. For example, if many attackers get into honeypot, the number of people attacking the real system decreases.
7. To further research hardening already common practices in the industry such as IPS(intrusion prevention system)
   and IDS(intrusion detection system)

Workflow


HONEYPOT
Attacker Side
Defender Side
Beginning
Operations
End
Start
Attacker tries to attack the system
Attacker finds the honeypot that is deliberately left exploitable
Attacker thinks they got into the system with some sort of prevlidge
The attacker falls into a trap and stands by for all the actions attacker will take
Attacker is free to roam around in the created and isolated honeypot
After the attacker infiltrates the system, all his/her actions are followed
The attacker seizes the fake system or steals fake data that has no value
The way attackers enters the system, the path s/he follows in the system and the information attackers stole are recorded into log files
The attacker ends his/her attack thinking that s/he has stolen valuable information
Network admins are informed, with the logs and ip adresses of the attacker
Attackers connection than is either dropped or they see the network admins message
End