**Seeramdas Pavan Raj**

**B00886940**

**Protecting Network Structures by Deploying Honeypots**

Network structures are arranged over an organization in such a way that it provides the better connectivity in transferring the information across the same network as well as the outside world. The attackers are possibly out there targeting these networks to form a session on the devices and extract the sensitive information stored over the same. Different network security mechanism out there for the security of the data where this report will focus on the honeypots as the device implanted on the network to divert the attacks onto this system and avoiding the loss of data from the original devices present on the network. These devices are deployed in such a way that it attracts the attackers as if some valuable information is residing over them having some vulnerable versions running and further analyze the different attacks performed by the attackers and processing the security of the original devices according to that.

The honeypots systems can be deployed in either of the way that is hardware-based honeypots or the software-based honeypots. In this report I will be discussing in detail about the two as well as the working of the same to understand the processes. I will also be learning about different levels of interaction-based honeypots working in detail. The deployment of these honeypots depends on the security risk to the network structure which will be discussed in my report as well. In this report I will be describing various other protection mechanisms with the various honeypots that can be deployed on the network such as the tools and the hardware involved.

For the implementation or the outcome part of my report I will be using a dedicated hardware system which can be a Raspberry Pi 3 or 4 model based on the availability as this will help me in understanding how honeypots in real world are deployed as an external entity on the network protecting from attacks. In my scenario my local network will have few devices such as laptop and mobile devices where this raspberry Pi microcomputer will be deployed, and all the attacks will be performed on this honeypot as this will be visible as an easy to attack device on the network. In the implementation section I will be describing in detail about the scripts, or the tools used over this raspberry Pi system such as DShield or HoneyPi including the installation steps involved and further upon successful installation of the honeypot system on this micro board I will be analyzing the packets received from the attacker as in my case will be my local laptop which will be try to connect to the majority of the ports such as SSH, RDP, or SMB which are majority ports used by the attackers to access the target systems and all the data received of a possible connection will be recorded using tools such as Tcpdump, etc. All the steps that are involved in the setting up of the access on the Raspberry PI honeypot to capturing the packets and displaying the results will be described in detail in this part of my report. The network capture will help as an owner to restrict access to these services by applying strong security measures. In this report I will be also discussing about various other possible options and tools that can be deployed in the achievement of deploying a honeypot on the network. This will cover the working of how the software-based honeypots work and how they can help in protecting the original system from being compromised.