IMPLEMENTATION OF ATTACK DATA COLLECTION INCORPORATING MULTI LEVEL DETECTION CAPABILITIES USING LOW INTERACTION HONEYPOT

RUBY KAMBOJ & VANITA RANA

Department of Computer Science, Indo Global College of Engineering, Punjab Technical University

Begowal, Punjab, India

ABSTRACT

Nowadays, security system is very important to any organization to protect their data or any information kept in their computer from the intruders to access. A honeypot is a type of information system that is used to obtain information on intruders in a network. This paper proposes a methodology for establishing a virtual Honeypot on a Virtualbox Server running dionaea. The implementation is specific to a Linux based host having a single physical network interface card. An effort has been made to ensure that all the software (both the OS and associated tools) used for the project are either free or Open Source. Special techniques were implemented in order to enhance the data capture mechanisms on the Linux-based Honeypot to efficiently generate reports. The ultimate goal of Attack Data Collection system is to detect and identify any malicious activity coming from the Internet. This system incorporates multi level detection by using vulnerabilities based attack data collection and network intrusion detection based attack data collection. Our system is tested by visiting of various malicious websites and detection of malwares dropped on the system is detected and logged in the system database.

KEYWORDS: Study of Network Security, Interaction, Honeypot, Attack, Level