SSH Honeypot Abstract

*Team members:-*

*Tanumay Ghosh (RA2011027010101)*

*Omisha Singal (RA2011027010103)*

*Yashas Dewan (RA2011027010105)*

*Akaash Ram J (RA2011027010126)*

*Daily we face thousands of server attacks by hackers. Hackers are constantly trying to attack servers by applying various methods like Dos attacks Website Defacement, Directory Traversal, Misconfiguration attacks Phishing Attack, etc.*

*To prevent such attacks we want to implement a* ***SSH Honeypot****.*

*A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers usually, a server or other high-value asset and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.*

*Generally, a honeypot operation consists of a computer, applications, and data that simulate the behavior of a natural system that would be attractive to attackers, such as a financial system, internet of things (IoT) devices, or a public utility or transportation network. It appears as part of a network but is actually isolated and closely monitored. Because there is no reason for legitimate users to access a honeypot, any attempts to communicate with it are considered hostile. The exact placement of the honeypot varies depending on how elaborate it is, the traffic it aims to attract. We will also be showing the attackers IP and other info in a frontend UI.*

*Large enterprises and companies involved in cybersecurity research are common users of honeypots to identify and defend against attacks from advanced persistent threat (APT) actors. Honeypots are an important tool that large organizations use to mount an active defense against attackers or for cybersecurity researchers who want to learn more about the tools and techniques attackers use.*

*The cost of maintaining a honeypot can be high, in part because of the specialized skills required to implement and administer a system that appears* *to expose an organization's network resources, while still preventing attackers from gaining access to any production systems.*