2023

# Report on Honeypot 3

HONEYPOT OVERVIEW

PRASHANJIT BASU

INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY | Shibpur

## About Honeypot 3:

This honeypot contains the necessary libraries socketserver, httpserver and os. The PORT variable is set to 80 which is a default port for HTTP traffic. FILE variable is set to the directory path where the fake directory system is created (the fake directory may contain different files faking importance like a transaction csv file, bank log file, password pdf, etc. for a wide range analysis on the attack). http.server is a module which handles HTTP requests. The translate_path method is overridden in the FakeFileHandler class. This method is called by the server to translate the requested path into a valid file path on the server's filesystem. An instance of 'socketserver.TCPServer' is created, passing an empty string as the host (indicating the server will listen on all available network interfaces) and the PORT variable. The FakeFileHandler is specified as the request handler for the server. A message is printed to indicate that the fake file honeypot is running and listening on the specified port. http.serve_forever() function is called which starts the server and makes it run indefinitely, handling incoming HTTP requests. If the attacker tries to access any of the file within the fake directory it will capture the behaviour and show it in the system terminal (can also be shown in a log file). Such type of honeypot makes an unsecure overlay on the network which attracts attackers to exploit it, noting all their actions and behaviours.

## Mechanism of Honeypot:

1. PORT and fake file path are set.
2. A fakefilehandler instance is created on a port as network overlay.
3. After the honeypot is initiated, it captures all the HTTP requests.
4. If an attacker tries to interfere with the fake directory their behaviour and information is noted.
5. Whole HTTP request alongside the service exploited is noted with time in terminal/log file.

## Use-case and speciality:

- This is a web-based honeypot deployed outside the system firewall to deal with the problems like anonymous attackers, personal data exploitation etc.
- With few modifications in this concept of web-honeypot, it can be used to secure cloud data and data from databases.
- It can alert us before an attack is initiated to the system or the honeypot, since it detects the connection/interaction itself.
- It can mimic from small files to large databases the main concept this honeypot works on is deception and tarpitting (slowing down and delaying the process of attackers).
- Since it is deployed outside the system that is on the network it can secure us from external threats.
- It provides us the actions and behaviour of attackers, which is an important information about their objective, tools, advancements, resources; moreover, it provides us some information about the attacker as well.

## Disadvantages:

- Since this honeypot is a direct connection from the network to system, if not implemented properly professional hackers can get a hand-made path to enter the system and exploit sensitive data.
- Maintaing a fake directory consumes an amount of memory on the device, the larger the database the more amount of memory it consumes.
- It is vulnerable to the manual unauthorised access to the system directly.