Name: Mst. Sumiya Siddika

ID:2111262

Assignment no: 3

Threat Intelligence tools:

1. **HoneyDB**: HoneyDB is a database and web site created to capture and display event data from HoneyPy sensors that are running on the Internet. At the highest conceptual level a honeypot is simply a computer that is configured to look and behave like any other computer you might find on any given network. A honeypot can be configured to offer various network services like HTTP, SSH, file sharing, etc. HoneyPy is a low to medium interaction honeypot, written in Python At a high various charts showing top traffic statistics. You can click on the pie charts to drill down into specific activity generated from an IP address. One main feature to highlight is the API. The API enables users to leverage the data HoneyDB is collecting as a threat information feed.

2. **APTnotes**: APT stands for advanced persistent threat. An advanced persistent threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period. APT attacks are initiated to steal highly sensitive data rather than cause damage to the target organization's network. The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible.

3. **Malpedia:** The primary goal of Malpedia is to provide a resource for rapid identification and actionable context when investigating malware. It is a collaboration platform for curating a malware corpus.