INSTITUTE OF INFORMATION TECHNOLOGY
JAHANGIRNAGAR UNIVERSITY

Number of Assignment	**: 02**
Name of Assignment	**: OSINT Framework**
Course Tittle	**: Cyber Security**
Submission Date	**: 25/09/2024**

Submitted To

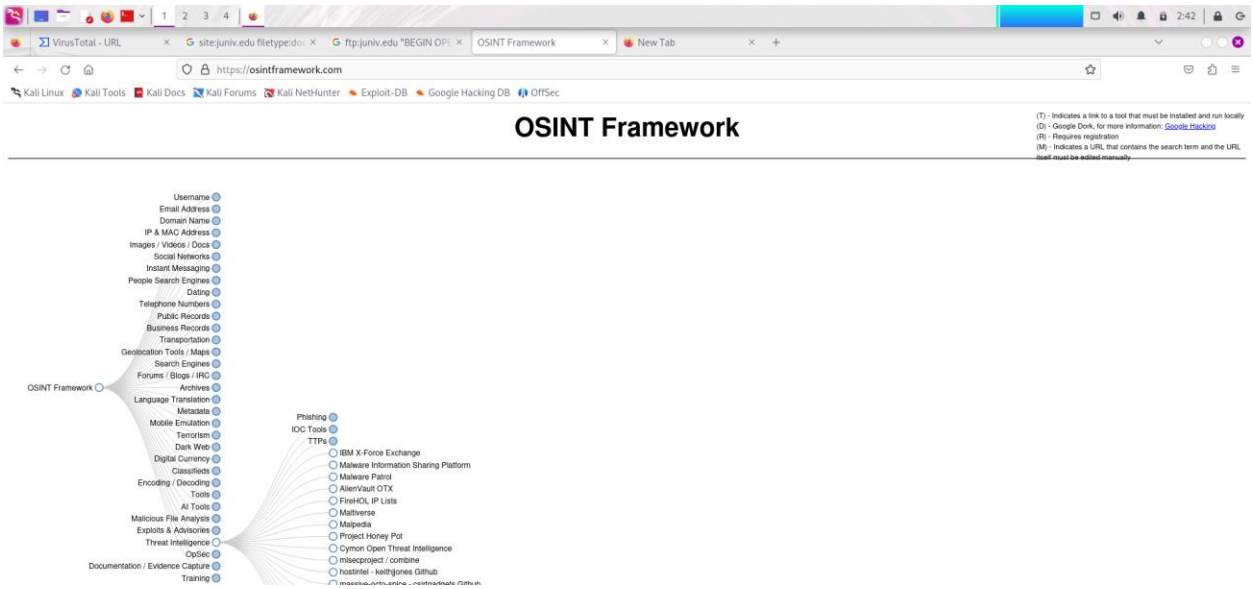
Moinoddeen Quader Al Arabi

Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber Security Consultant in Dhaka Division, Bangladesh.

Submitted By

Md. Shakil Hossain

ID: 2111258

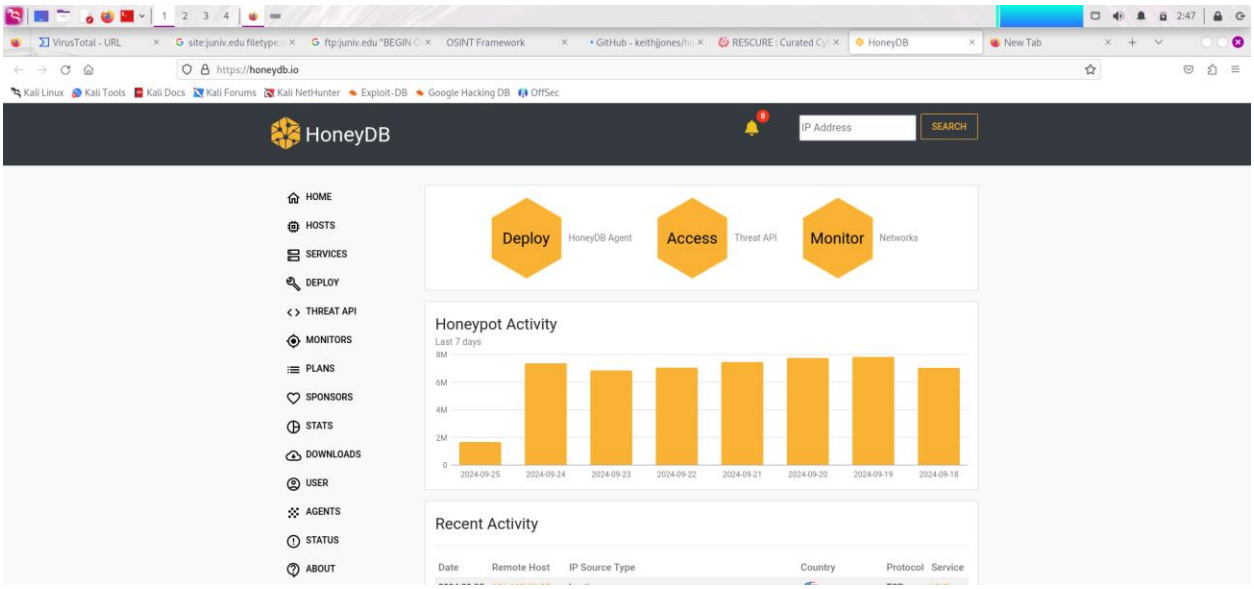


Threat Intelligence:

1. **HoneyDB**
2. **maltiverse**
3. **Malware Exploit TTP Database**

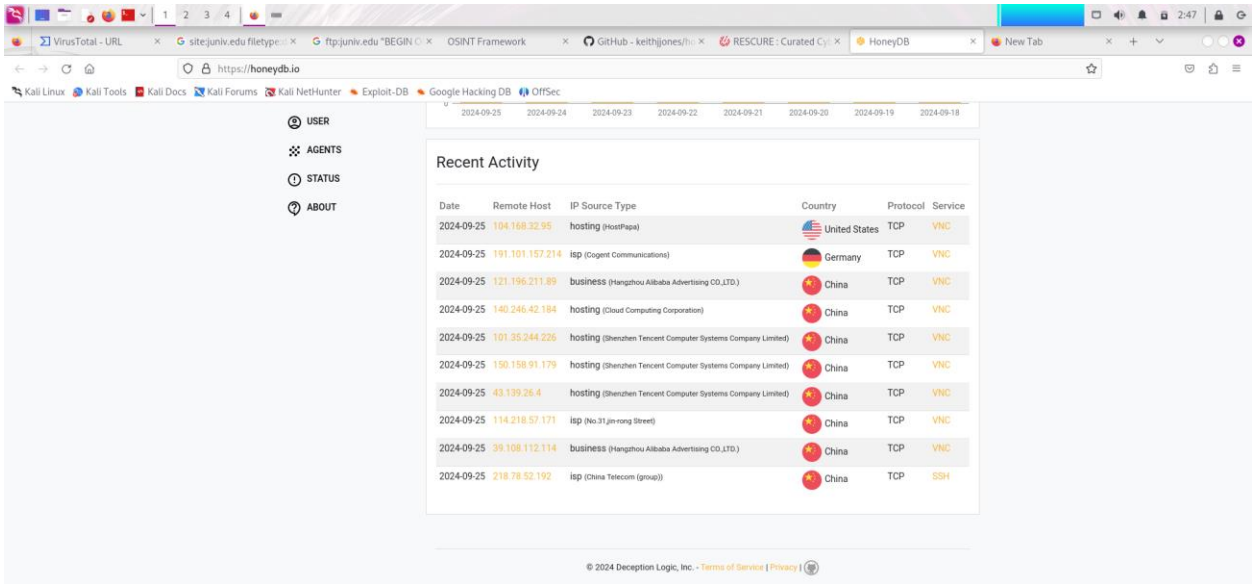
HoneyDB

HoneyDB is a platform that collects and analyzes information related to honeypots and other forms of threat intelligence. It aggregates data from various sources to provide insights into cyber threats, helping security professionals understand attack patterns and improve their defenses.



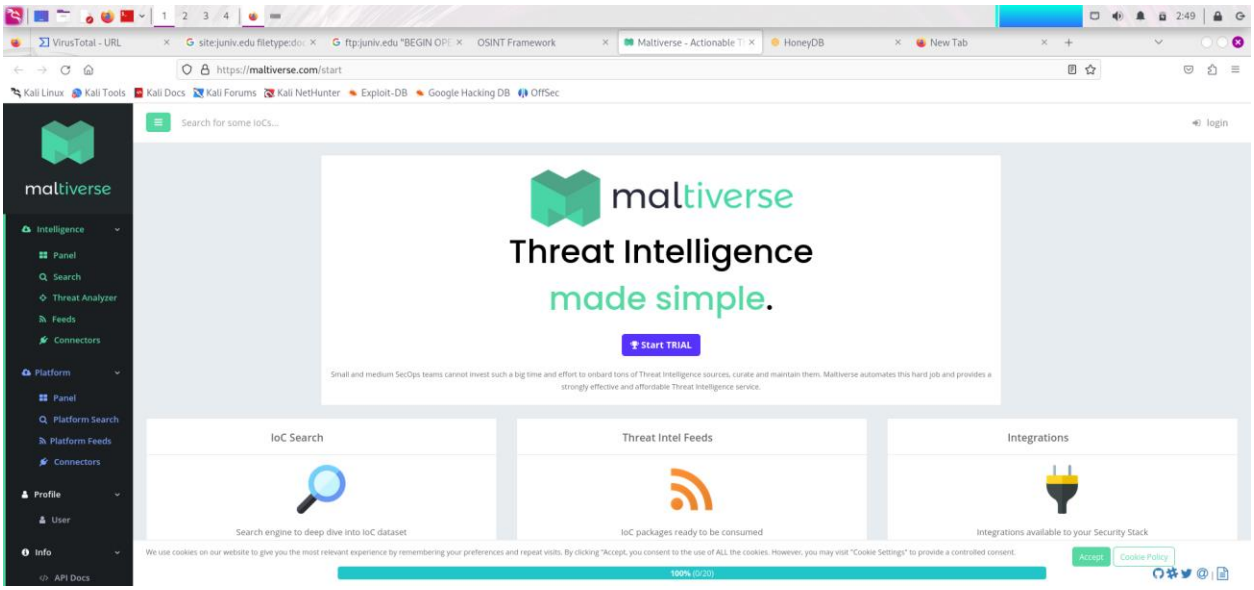
Key features of HoneyDB include:

- **Threat Intelligence:** Provides insights into emerging threats and attack vectors.
- **Data Aggregation:** Collects data from different honeypots and security researchers.
- **Community Contributions**: Users can share their findings and collaborate on threat analysis.
- **API Access:** Allows users to programmatically access threat data for integration into their own tools.



Multiverse

Maltiverse is a platform that provides threat intelligence and analysis services, focusing on malware and related threats. It aggregates data from various sources to help security professionals and organizations understand and mitigate risks associated with malware.



Key Features of Maltiverse:

- **Malware Analysis**: Offers detailed reports and analysis on various types of malware, including their behaviors and characteristics.
- **Threat Intelligence**: Provides insights into emerging threats and trends in the cyber threat landscape.
- **Community Contributions**: Users can contribute data and insights, fostering collaboration among cybersecurity professionals.
- **API Access**: Allows integration with other security tools and automated systems for streamlined threat detection and response.
- **Search Functionality**: Users can search for specific malware samples or related indicators of compromise (IoCs).

Malware Exploit TTP Database

The TTP (Tactics, Techniques, and Procedures) Database refers to a structured way to understand and classify the behavior of cyber adversaries. TTPs help cybersecurity teams to identify and respond to cyberattacks by analyzing the methods and patterns used by threat actors. These frameworks can be used for activities like threat hunting, malware detection, and exploit analysis.

For example, MITRE's ATT&CK Framework is widely recognized for its comprehensive collection of real-world attack techniques used by adversaries.

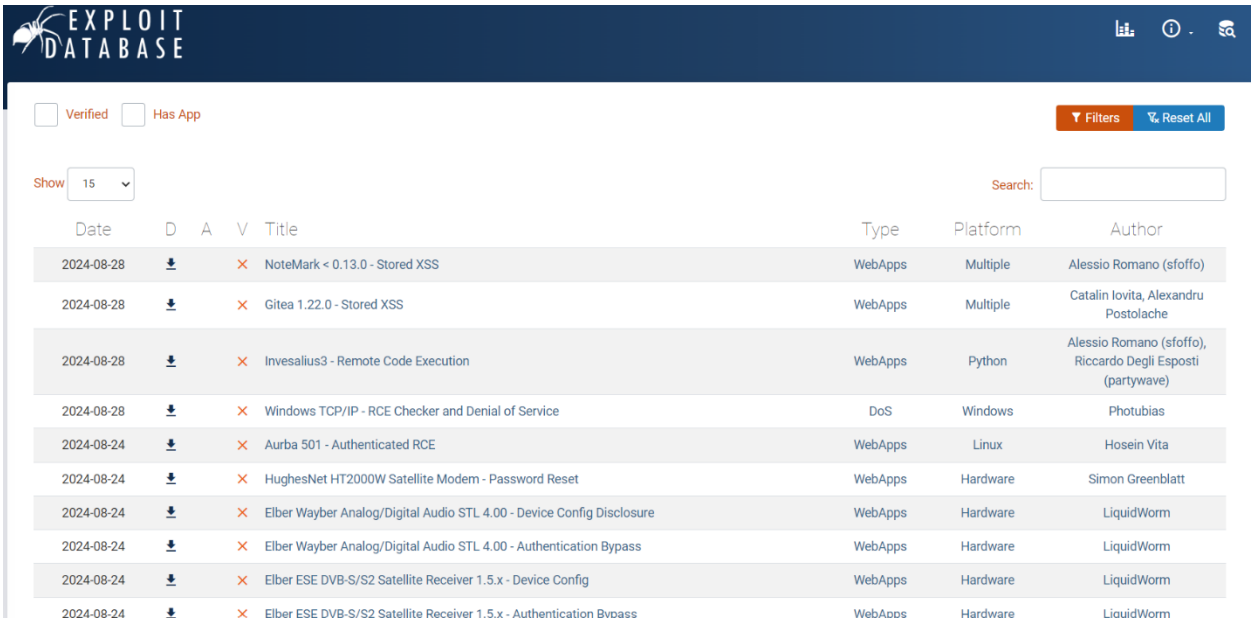


Fig: Exploit TTP Database

Fig: MITRE's ATT&CK: Real-world att&ck techniques

The End