



INSTITUTE OF INFORMATION TECHNOLOGY JAHANGIRNAGAR UNIVERSITY

Number of Assignment : 02

Name of Assignment : OSINT Framework

Course Title : Cyber Security

Submission Date : 25/09/2024

Submitted To

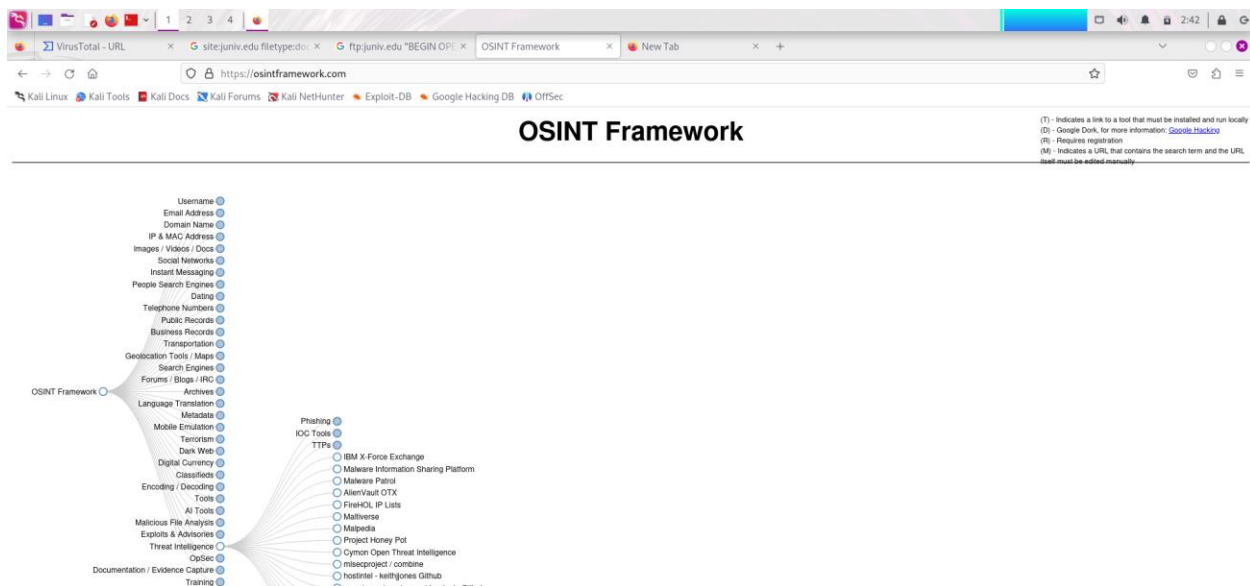
Moinoddeen Quader Al Arabi

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

Submitted By

Md. Shakil Hossain

ID: 2111258

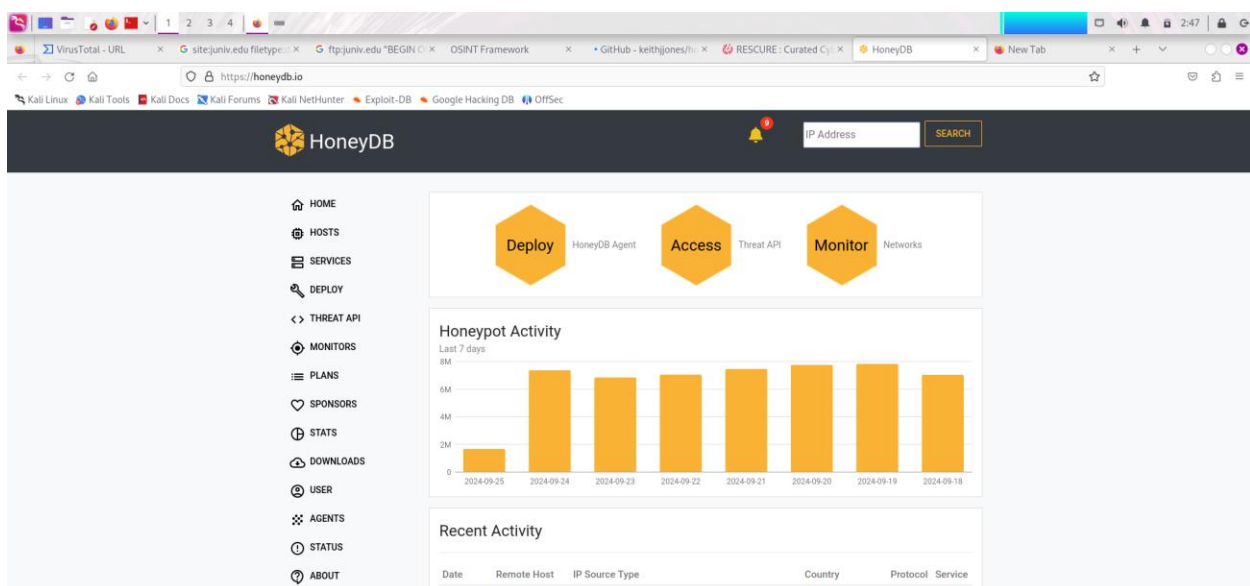


Threat Intelligence:

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

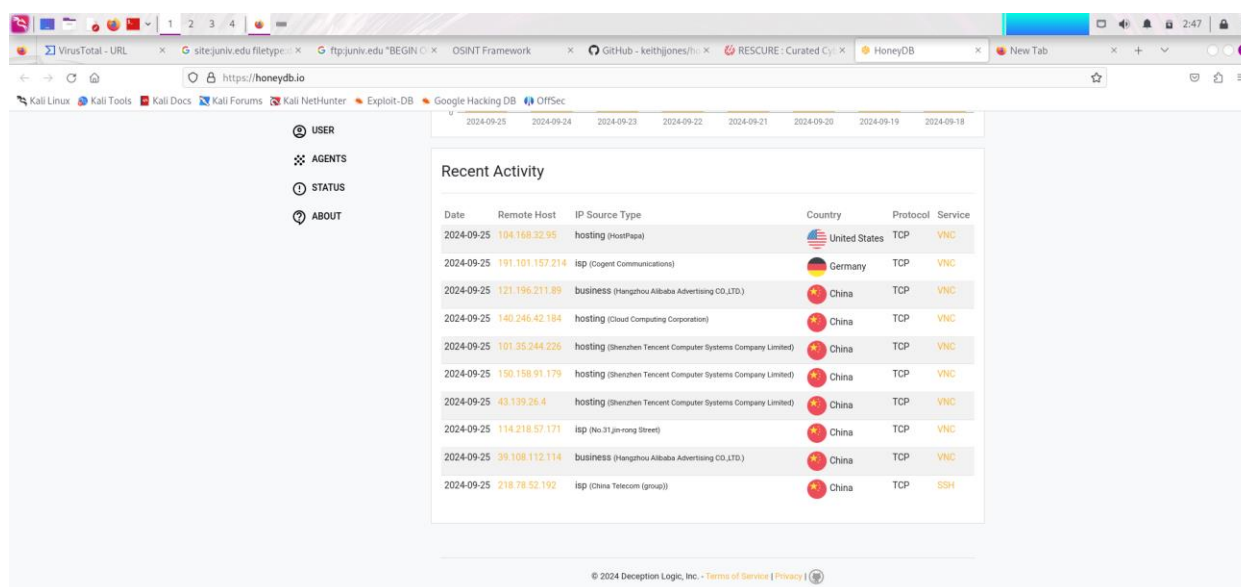
HoneyDB

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.



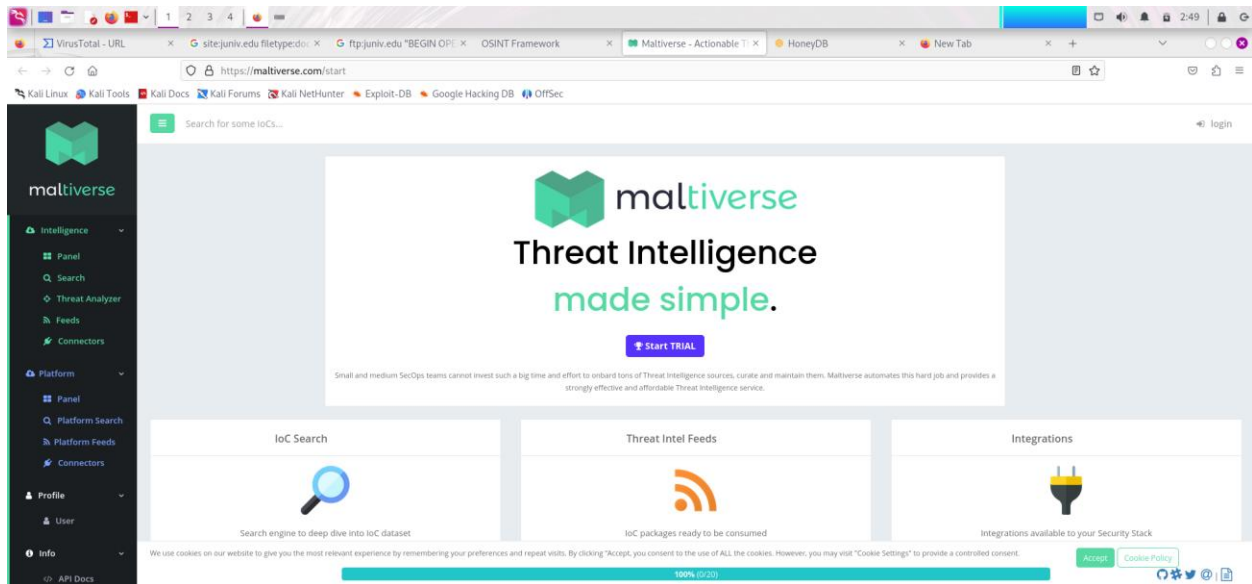
The screenshot shows the HoneyDB web interface. On the left is a sidebar with navigation links: USER, AGENTS, STATUS, and ABOUT. The main content area is titled 'Recent Activity' and displays a table of recent connections. The table has columns for Date, Remote Host, IP Source Type, Country, Protocol, and Service. The data shows various connections from different countries, including the United States, Germany, and China, with protocols like TCP and services like VNC and SSH.

Date	Remote Host	IP Source Type	Country	Protocol	Service
2024-09-25	104.168.32.95	hosting (HostPapa)	United States	TCP	VNC
2024-09-25	191.101.157.214	isp (Cogent Communications)	Germany	TCP	VNC
2024-09-25	121.196.211.89	business (Hangzhou Alibaba Advertising CO.,LTD.)	China	TCP	VNC
2024-09-25	140.246.42.184	hosting (Cloud Computing Corporation)	China	TCP	VNC
2024-09-25	101.35.244.226	hosting (Shenzhen Tencent Computer Systems Company Limited)	China	TCP	VNC
2024-09-25	150.158.91.179	hosting (Shenzhen Tencent Computer Systems Company Limited)	China	TCP	VNC
2024-09-25	43.139.26.4	hosting (Shenzhen Tencent Computer Systems Company Limited)	China	TCP	VNC
2024-09-25	114.218.57.171	isp (No.31 jin-rong Street)	China	TCP	VNC
2024-09-25	95.108.112.114	business (Hangzhou Alibaba Advertising CO.,LTD.)	China	TCP	VNC
2024-09-25	218.78.52.192	isp (China Telecom (group))	China	TCP	SSH

© 2024 Deception Logic, Inc. - [Terms of Service](#) | [Privacy](#) | 

Maltiverse

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.

EXPLOIT DATABASE

☐ Verified ☐ Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sffoffo)
2024-08-28				Gitea 1.22.0 - Stored XSS	WebApps	Multiple	Catalin Iovita, Alexandru Postolache
2024-08-28				Invesalius3 - Remote Code Execution	WebApps	Python	Alessio Romano (sffoffo), Riccardo Degli Esposti (partywave)
2024-08-28				Windows TCP/IP - RCE Checker and Denial of Service	DoS	Windows	Photubias
2024-08-24				Aurba 501 - Authenticated RCE	WebApps	Linux	Hosein Vita
2024-08-24				HughesNet HT2000W Satellite Modem - Password Reset	WebApps	Hardware	Simon Greenblatt
2024-08-24				Elber Wayber Analog/Digital Audio STL 4.00 - Device Config Disclosure	WebApps	Hardware	LiquidWorm
2024-08-24				Elber Wayber Analog/Digital Audio STL 4.00 - Authentication Bypass	WebApps	Hardware	LiquidWorm
2024-08-24				Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Device Config	WebApps	Hardware	LiquidWorm
2024-08-24				Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Authentication Bypass	WebApps	Hardware	LiquidWorm

Fig: Exploit TTP Database

layer X +

Selection Controls Layer Controls Technique Controls

Reconnaissance 10 techniques

Resource Development 8 techniques

Initial Access 10 techniques

Execution 14 techniques

Persistence 20 techniques

Privilege Escalation 14 techniques

Defense Evasion 43 techniques

Credential Access 17 techniques

Discovery 32 techniques

Lateral Movement 9 techniques

Collection 17 techniques

Command and Control 18 techniques

Active Scanning (0/3)	Scanning IP Blocks (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/3)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/3)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services (0/3)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)
Gather Victim Host Information (0/4)	Vulnerability Scanning (0/3)	Acquire Infrastructure (0/3)	Drive-by Compromise (0/10)	Command and Scripting Interpreter (0/10)	BITS Jobs (0/6)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/3)	Archive Collected Data (0/3)	Communication Through Removable Media (0/3)
Gather Victim Identity Information (0/3)	Wordlist Scanning (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application (0/3)	Container Administration Command (0/14)	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/6)	Browser Information Discovery (0/6)	Lateral Tool Transfer (0/2)	Audio Capture (0/3)	Content Injection (0/3)
Gather Victim Network Information (0/6)		Compromise Infrastructure (0/3)	External Remote Services (0/4)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/3)	Account Manipulation (0/6)	Debugger Evasion (0/6)	Cloud Infrastructure Discovery (0/6)	Remote Service Session Hijacking (0/2)	Automated Collection (0/3)	Data Encoding (0/3)
Gather Victim Org Information (0/4)		Develop Capabilities (0/4)	Hardware Additions (0/3)	Exploitation for Client Execution (0/3)	Browser Extensions (0/14)	Boot or Logon Autostart Execution (0/6)	Deobfuscate/Decode Files or Information (0/2)	Cloud Service Dashboard (0/6)	Remote Services (0/6)	Browser Session Hijacking (0/3)	Data Obfuscation (0/3)
Phishing for Information (0/4)		Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/3)	Direct Volume Access (0/2)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/3)	Clipboard Data (0/3)	Dynamic Resolution (0/3)
		Obtain Capabilities (0/3)	Replication Through Removable (0/3)	Inter-Process Communication (0/3)	Create Account (0/3)	Domain or Tenant Policy Modification (0/2)	Forge Web Credentials (0/2)	Container and Resource Discovery (0/2)	Software (0/3)	Data from Cloud Storage (0/3)	Encrypted Channel (0/3)

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

The End