

Shariful Islam

ID: 2111252

21 Sep 2024

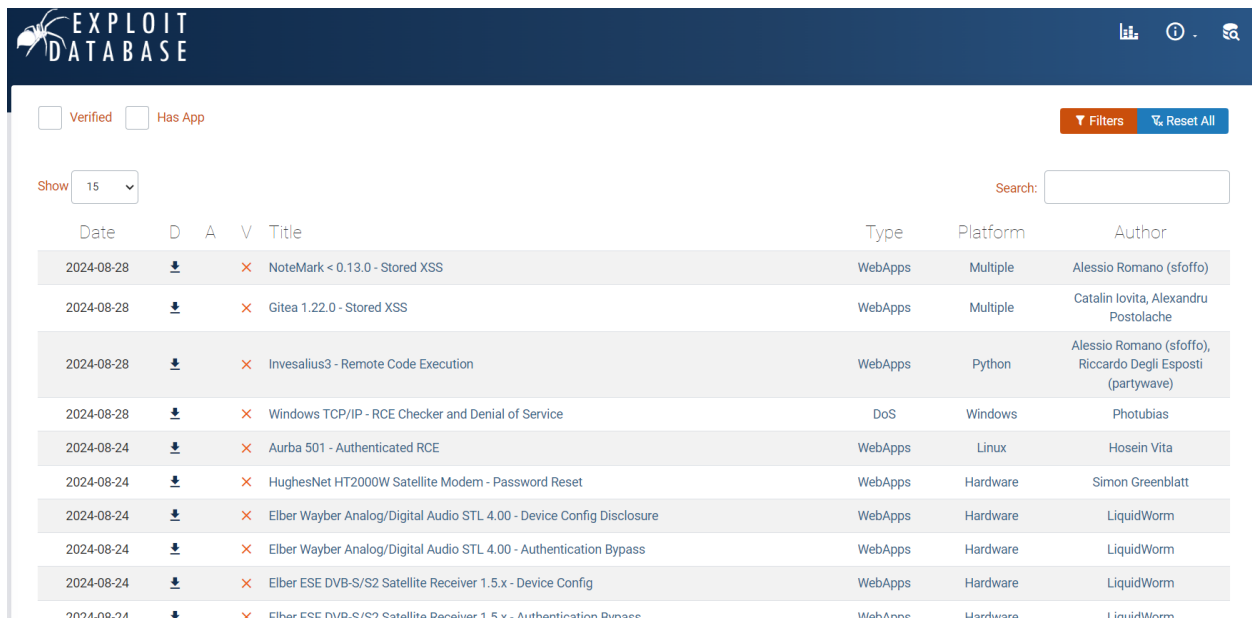
## Assignment no 2: OSINT Framework

### Three (3) Topic about Threat Intelligence:

#### 1. Threat Intelligence → TTPs → 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.



The screenshot shows the Exploit Database website interface. At the top, there's a dark blue header with the 'EXPLOIT DATABASE' logo and navigation icons. Below the header, there are filters for 'Verified' and 'Has App', a 'Show' dropdown set to '15', and a search bar. The main content is a table of exploits with columns for Date, D (download), A (add), V (verified), Title, Type, Platform, and Author. The table lists several exploits, including NoteMark < 0.13.0 - Stored XSS, Gitea 1.22.0 - Stored XSS, Invesalius3 - Remote Code Execution, Windows TCP/IP - RCE Checker and Denial of Service, Aurba 501 - Authenticated RCE, HughesNet HT2000W Satellite Modem - Password Reset, Elber Wayber Analog/Digital Audio STL 4.00 - Device Config Disclosure, Elber Wayber Analog/Digital Audio STL 4.00 - Authentication Bypass, and Elber ESE DVB-S/S2 Satellite Receiver 1.5.x - Device Config.

Date	D	A	V	Title	Type	Platform	Author
2024-08-28				NoteMark < 0.13.0 - Stored XSS	WebApps	Multiple	Alessio Romano (sfoffo)
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 (sfoffo), 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		Resource Development		Initial Access		Execution		Persistence		Privilege Escalation		Defense Evasion		Credential Access		Discovery		Lateral Movement		Collection		Command and Control											
10 techniques		8 techniques		10 techniques		14 techniques		20 techniques		14 techniques		43 techniques		17 techniques		32 techniques		9 techniques		17 techniques		18 techniques											
Active Scanning (0/2)	Scanning IP Blocks	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol																					
	Vulnerability Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media																					
Gather Victim Host Information (0/4)	Wordlist Scanning	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Access Token Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection																					
		Compromise Infrastructure	External Remote Services	Container Administration Command	Boot or Logon Initialization Scripts	Access Token Manipulation	Build Image on Host	Debugger Evasion	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding																					
Gather Victim Identity Information (0/3)		Develop Capabilities	Hardware Additions	Deploy Container	Browser Extensions	Boot or Logon Autostart Execution	Deobfuscate/Decode Files or Information	Exploitation for Credential Access	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation																					
		Establish Accounts	Phishing	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Autostart Execution	Deploy Container	Forced Authentication	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution																					
Gather Victim Network Information (0/6)		Obtain Capabilities	Replication Through Removable	Inter-Process Communication	Create Account	Access Token Manipulation	Domain or Tenant Policy Modification	Forge Web Credentials	Cloud Storage Object Discovery	Container and Resource Discovery	Data from Cloud Storage	Encrypted Channel																					
		Phishing for Information				Input Capture		Input Capture																									

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

## 2. Threat Intelligence → Malware Information Sharing Platform:

The Malware Information Sharing Platform (MISP) is an open-source threat intelligence platform that facilitates the sharing, storing, and correlation of indicators of compromise (IOCs) related to malware, cybersecurity threats, and vulnerability information.

### Key Features of MISP:

- Threat Intelligence Sharing
- Automation and Integration
- Correlation Engine
- Taxonomy and Tagging
- Community-Driven

### Use Case:

- Reverse Engineering

## 3. Threat Intelligence → Malware Patrol:

Malware Patrol is a cybersecurity service provider that specializes in malware intelligence, threat feeds, and cybersecurity solutions to help organizations protect themselves from cyber threats.

### Key Services Offered by Malware Patrol:

- Threat Data Feeds
- Malware Analysis
- Phishing Detection

**Use Cases:**

- Enterprises
- Researchers

**Malware Patrol's evaluation portal provides:**

- Anti-Cryptomining
- Bitcoin Block chain Strings
- Bitcoin Transactions
- C2 Addresses
- Domain Names Generated via DGAs
- DNS-over-HTTPS (DoH) Servers
- DNS RPZ Firewall
- Integration Feeds: Fortinet / MISP / PAN-OS
- Intrusion Insights
- Malicious IPs
- Malware & Ransomware URLs
- Malware Hashes
- Malware Samples (Binaries)
- Newly Registered Domains
- Phishing
- Phishing Screenshots and Raw HTML
- Scam Domains