**MITRE ATT&CK TTP Mapping – Week 1**

**Intern Name:** Tushar chaturkar

**Intern ID:** 116

**Internship Task:** Threat Intelligence Collection & Analysis

**Tools Used:** ThreatView.io, MISP, YARA Rules

**🔍 MITRE ATT&CK TTP Mapping**

**📌 What is MITRE ATT&CK?**

The [MITRE ATT&CK®](https://attack.mitre.org/) framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It’s used by cybersecurity professionals to:

* Understand attacker behavior
* Improve threat detection
* Design defensive strategies
* Perform threat modeling and red teaming

**🎯 What is TTP Mapping?**

**TTP** stands for **Tactics, Techniques, and Procedures**. In the context of MITRE ATT&CK:

* **Tactics**: The adversary's tactical goal (e.g., **Privilege Escalation**).
* **Techniques**: How the goal is achieved (e.g., **Exploitation for Privilege Escalation**).
* **Procedures**: Specific implementations (e.g., using a particular exploit tool).

**TTP Mapping** refers to aligning observed security incidents, threat intelligence, or detection rules with corresponding MITRE ATT&CK entries.

**🧠 Why Use ATT&CK TTP Mapping?**

Mapping to MITRE ATT&CK helps you:

* **Identify Gaps**: Understand what techniques you can or cannot detect.
* **Standardize Threat Intelligence**: Speak a common language across teams.
* **Enhance Incident Response**: Quickly identify what an attacker did and plan a response.
* **Build Detection Rules**: Link logs or behaviors to specific ATT&CK techniques.

**📘 Example: TTP Mapping in Practice**

| **Observed Behavior** | **ATT&CK Tactic** | **ATT&CK Technique** | **Technique ID** |
| --- | --- | --- | --- |
| PowerShell used to download payload | Execution | PowerShell | T1059.001 |
| User account creation | Persistence | Create Account | T1136 |
| Credential dumping via LSASS | Credential Access | OS Credential Dumping | T1003.001 |

**🛠️ How to Perform TTP Mapping**

1. **Collect Data**: Gather logs, threat reports, incident evidence.
2. **Analyze Behavior**: Look for patterns of malicious activity.
3. **Match to ATT&CK**: Use MITRE ATT&CK Navigator or threat intelligence tools.
4. **Document Mappings**: Create tables, charts, or JSON/YAML structures.

**🔗 Resources**

* [MITRE ATT&CK Navigator](https://mitre-attack.github.io/attack-navigator/)
* [ATT&CK Techniques](https://attack.mitre.org/techniques/)
* [ATT&CK on GitHub](https://github.com/mitre/attack)
* [Threat Intelligence Platform](https://threatconnect.com/)

**📁 Example Files**

You can include mappings as:

* ttp-mapping.csv
* ttp-mapping.json
* ttp-report.md