Lecture Notes: MITRE ATT&CK Framework

1. Introduction

- The **MITRE ATT&CK framework** is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- It is used by cybersecurity analysts to understand, detect, and respond to threats.
- The framework helps map attacks across the **entire attack lifecycle**, from initial access to objectives.

---

2. TTPS: Tactics, Techniques, and Procedures

- **Tactics (The "WHY")**
    - Define the **attacker's goal or motivation**.
    - Examples: Initial Access, Privilege Escalation, Exfiltration.
- **Techniques (The "HOW")**
    - Describe **how the attacker achieves a tactic**.
    - Examples: Phishing, Credential Dumping, Data Encrypted for Impact.
- **Procedures**
    - Step-by-step actions or **specific implementations of a technique**.
    - Example: Using PowerShell scripts to perform credential dumping for privilege escalation.

---

3. The Attack Lifecycle

- MITRE ATT&CK organizes attacks into a **lifecycle sequence**:

    1. **Reconnaissance:** Gathering information about the target.
    2. **Initial Access:** Gaining entry into the target system (e.g., phishing).
    3. **Execution:** Running malicious code.
    4. **Persistence:** Maintaining access across restarts or credentials.
    5. **Privilege Escalation:** Gaining higher-level permissions.
    6. **Defense Evasion:** Avoiding detection by security systems.
    7. **Credential Access:** Stealing account credentials.
    8. **Discovery:** Identifying systems and resources.
    9. **Lateral Movement:** Moving within the network.
    10. **Collection:** Gathering sensitive data.
    11. **Exfiltration:** Sending stolen data outside the network.
    12. **Impact:** Disrupting or damaging systems (e.g., ransomware).

---

4. Purpose and Use in Cybersecurity

- **Threat Analysis:** Understand attackers' goals and methods.
- **Detection & Monitoring:** Identify which techniques are being used in real time.
- **Incident Response:** Map observed behavior to tactics and techniques for faster mitigation.
- **Red Teaming & Blue Teaming:** Helps simulate realistic attacks and defenses.

---

5. Key Takeaways

- **Tactics** = WHY the attacker is acting.
- **Techniques** = HOW the attacker achieves their goal.
- **Procedures** = The exact steps used to implement a technique.
- Using MITRE ATT&CK, analysts can **systematically study attacks** and improve security posture.