Extra Reading 09 – Introduction to the MITRE ATT&CK Framework (Red Team Series)

1. Why This Video?

- Previous videos introduced several red-team frameworks (Cyber Kill Chain, Unified Kill Chain, MITRE ATT&CK).
- This video provides a **proper, formal introduction** to the MITRE ATT&CK framework:
    - What it is
    - How it's used
    - Why it's important for red-team and blue-team operations

2. What is the MITRE ATT&CK Framework?

Definition

MITRE ATT&CK is a **globally accessible, free knowledge base** of adversary **tactics** and **techniques** derived from **real-world threat actors**, primarily APT groups.

Key Characteristics

- **Open and free** — no account or payment required.
- **Knowledge base** — think of it as a large, structured reference of:
    - Known adversary behaviours
    - Publicly documented attacks
    - TTPs mapped to real threat groups
- **Behavior-focused** — built from analysis of real attacks, not theoretical models.

3. ATT&CK as a Tool for Red and Blue Teams

Red Team Uses

- Provides a structured **baseline of adversary behaviour**.
- Helps plan and model red-team operations.
- Enables adversary emulation:
    - Selecting TTPs used by a specific APT group.
    - Building realistic scenarios based on those behaviours.
- Serves as planning guidance during:
    - Recon
    - Resource development

    - Initial access
    - C2 operations
    - Privilege escalation

Blue Team Uses

- Important misconception: ATT&CK is **not only for offensive roles**.
- Blue teams and SOC analysts use ATT&CK to:
    - Understand threat actor behaviour
    - Build detection logic
    - Implement mitigations
    - Map defensive coverage gaps
    - Generate threat intelligence
- Helps defenders communicate effectively using shared terminology.

4. Understanding TTPs: Tactics, Techniques & Procedures

Tactics (the *why*)

- Represent the **goal or objective** for the attacker.
- Examples: Initial Access, Privilege Escalation, Defense Evasion.

Techniques (the *how*)

- Describe **how** the attacker accomplishes a tactic.
- Example (under Initial Access): Phishing.

Sub-techniques

- Add specificity to a technique.
- Example: Phishing →
    - Spearphishing Attachment
    - Spearphishing Link
    - Spearphishing via Service

Procedures (the *what they did exactly*)

- Real-world examples of **how specific APT groups implemented the technique**.
- This is where MITRE becomes a "knowledge base" rather than just a model.

5. MITRE ATT&CK in Red Team Planning

When planning an operation, ATT&CK provides a structured guideline. For example:

- **Recon:** Information gathering, scanning

- **Resource Development:** Acquire C2 infrastructure, domains, malware
- **Initial Access:** Target misconfigured external services
- **Execution:** Use PowerShell or scripting interpreters
- **Privilege Escalation:** Choose applicable techniques based on target OS

This structure mirrors an adversary lifecycle and helps red teams design realistic engagements.

6. ATT&CK Matrices (Environments & Platforms)

MITRE ATT&CK provides matrices tailored to different environments:

Enterprise Matrix

- The default and most commonly used.
- Covers tactics and techniques for enterprise systems.

Platform-Specific Views

- Windows
- Linux
- macOS
- Cloud environments
- Network
- Containers

Mobile Matrix

- Android
- iOS

ICS (Industrial Control Systems) Matrix

- Techniques specific to OT/industrial environments.

These filters allow teams to narrow TTPs to the environment they're assessing.

7. Technique Structure in Detail

Each technique or sub-technique includes:

- **Technique ID** (e.g., T1548.002)
    - Standardized names enable clear communication between red/blue teams.
- **Applicable Platforms**
- **Permissions Required**
- **Mitigations**
- **Detection methods**

- **Procedure examples from real threat actors**

This is especially useful for:

- **Red teamers** learning real adversary tradecraft
- **Blue teamers** building detections and mitigation strategies

8. Example Covered in the Video: UAC Bypass (T1548 – Abuse Elevation Control)

- ATT&CK lists multiple UAC bypass techniques.
- Procedure examples show how APT29 and others bypassed UAC.
- Real-world references (e.g. Mandiant reports) illustrate:
    - Specific exploits used (e.g., UACMe, CVE-2018-8120)
    - Tools employed
    - Stages of the intrusion

This demonstrates how procedure examples provide **actionable threat intelligence**.

9. Benefits of Using ATT&CK

Why Red Teamers Should Use It

- Provides structure and realism
- Helps plan operations and choose techniques
- Allows communication with defenders using IDs (e.g., "We used T1059.001 during execution")

Why Blue Teamers Should Use It

- Helps identify coverage gaps
- Provides detection and mitigation guidance
- Supports CTI analysis and reporting
- Enables alignment with known adversary behaviours

Shared Language

Technique IDs create a **standardized nomenclature** that both teams understand instantly.

10. The MITRE ATT&CK Navigator (Preview)

- Will be covered in the next video.
- Used to visualize and operationalize ATT&CK for campaigns and assessments.
- Helps map:
    - Threat actor TTPs
    - Detection coverage

    - Red-team plans
    - Purple-team exercises

11. Summary

- MITRE ATT&CK is a free, globally accessible knowledge base of real adversary behaviour.
- Organizes threats into Tactics → Techniques → Sub-Techniques → Procedures.
- Provides value to both red and blue teams.
- Includes platform-specific matrices and detailed mitigation/detection guidance.
- Essential for adversary emulation, threat intelligence, and operational planning.