Classroom Lab: Introduction to MITRE ATT&CK Framework

Title: "Mapping Cyber Attacks with MITRE ATT&CK using Windows Server & Cisco Devices"

Duration: 4 hours  
Target Audience: Beginner cybersecurity students  
Lab Objective: Understand and simulate key MITRE ATT&CK tactics using real-world tools on Windows Server and Cisco devices.

# Lab Requirements

* Windows Server 2022 or Windows 10/11
* Two Windows clients (for attacker/victim simulation)
* Cisco switch (e.g. 2960 or Catalyst 3560)
* Cisco router (e.g. CSR1000v or ISR 4321)
* Wireshark or Sysmon
* PowerShell and Command Prompt
* Kali Linux VM (for attacker simulation)
* Remote desktop enabled on Windows
* Cisco IOS configured (basic connectivity)

# Part 1: Theory Intro

* Explain the MITRE ATT&CK matrix (Initial Access, Execution, etc.)
* Demonstrate usage on https://attack.mitre.org
* Discuss use cases for red/blue teams and SOC

# Lab 1 – Simulate Initial Access

* Enable RDP on Windows Server
* Login via RDP from Kali or another PC
* Monitor Event Viewer on Server (Event ID 4624)
* Map to MITRE ID T1021.001

# Lab 2 – Execution Technique

* Use PowerShell to initiate reverse shell
* Listener on Kali: nc -lvnp 4444
* Discuss usage and detection
* Map to MITRE ID T1059.001

# Lab 3 – Defense Evasion

* Encode PowerShell script in Base64
* Execute encoded command
* Map to MITRE ID T1027

# Lab 4 – Cisco Device Monitoring

* Enable logging on Cisco router
* Login via SSH from attacker machine
* Use show users and show logging
* Map to MITRE ID T1021.004

# Reflection & Mapping

* Use MITRE worksheet to map tactics and techniques
* Group discussion on real-world mitigations