Training Course on Attacker Tactics, Techniques, and Procedures Analysis

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's volatile digital landscape, understanding **adversary behavior** is paramount to effective cybersecurity. Training Course on Attacker Tactics, Techniques, and Procedures Analysis is meticulously designed to equip cybersecurity professionals with the advanced knowledge and practical skills required to dissect, analyze, and anticipate the actions of sophisticated threat actors. By deeply comprehending the *TTPs* employed in real-world **cyberattacks**, organizations can shift from a reactive defense posture to a proactive and intelligent security strategy, significantly enhancing their resilience against emerging and persistent threats. This course will delve into frameworks like **MITRE ATT&CK**, emphasizing the practical application of TTP analysis for enhanced **threat detection**, **incident response**, and **proactive defense**.

This intensive program goes beyond merely identifying indicators of compromise (IOCs); it focuses on the "how" and "why" behind attacks. Participants will learn to leverage **cyber threat intelligence (CTI)** to understand the full lifecycle of an attack, from initial reconnaissance to data exfiltration. Through hands-on labs and real-world **case studies**, attendees will gain proficiency in techniques such as **behavioral analysis**, **threat hunting**, and **security automation**, ultimately empowering them to build more robust and adaptive security defenses that can withstand the constantly evolving **cyber threat landscape**.

Programme Curriculum

Training Course on Attacker Tactics, Techniques, and Procedures Analysis

Introduction

In today's volatile digital landscape, understanding **adversary behavior** is paramount to effective cybersecurity. Training Course on Attacker Tactics, Techniques, and Procedures Analysis is meticulously designed to equip cybersecurity professionals with the advanced knowledge and

practical skills required to dissect, analyze, and anticipate the actions of sophisticated threat actors. By deeply comprehending the *TTPs* employed in real-world **cyberattacks**, organizations can shift from a reactive defense posture to a proactive and intelligent security strategy, significantly enhancing their resilience against emerging and persistent threats. This course will delve into frameworks like **MITRE ATT&CK**, emphasizing the practical application of TTP analysis for enhanced **threat detection**, **incident response**, and **proactive defense**.

This intensive program goes beyond merely identifying indicators of compromise (IOCs); it focuses on the "how" and "why" behind attacks. Participants will learn to leverage **cyber threat intelligence (CTI)** to understand the full lifecycle of an attack, from initial reconnaissance to data exfiltration. Through hands-on labs and real-world **case studies**, attendees will gain proficiency in techniques such as **behavioral analysis**, **threat hunting**, and **security automation**, ultimately empowering them to build more robust and adaptive security defenses that can withstand the constantly evolving **cyber threat landscape**.

Course Duration

5 days

Course Objectives

1. Master the **MITRE ATT&CK Framework** for comprehensive adversary emulation and defensive mapping.
2. Analyze **Advanced Persistent Threats (APTs)** and their evolving TTPs in real-world scenarios.
3. Develop robust **threat intelligence capabilities** to inform proactive security measures.
4. Implement **behavioral analytics** to detect anomalous activities indicative of sophisticated attacks.
5. Perform effective **threat hunting** using TTP-based methodologies and advanced tools.
6. Enhance **incident response** processes by integrating TTP analysis for faster containment and eradication.
7. Understand **red teaming** and **blue teaming** strategies for validating defensive controls against known TTPs.
8. Identify and track **emerging TTPs** employed by prevalent cybercriminal groups and nation-state actors.
9. Leverage **OSINT (Open-Source Intelligence)** for gathering actionable threat intelligence on adversary TTPs.
10. Apply **digital forensics** techniques to uncover TTPs during post-incident investigations.
11. Design and implement **security automation** workflows based on identified TTPs for rapid response.
12. Conduct **vulnerability analysis** and prioritize patching based on common attacker exploitation TTPs.
13. Foster a **threat-informed defense** mindset across the organization, aligning security operations with adversary behavior.

Organizational Benefits

- Proactive identification of sophisticated attacks before they cause significant damage.
- Faster and more effective containment, eradication, and recovery from cyber incidents.
- Development of adaptive defenses tailored to real-world adversary behavior.
- Prioritization of security controls and technologies based on intelligence-driven insights.
- Minimization of an organization's attack surface and overall cyber risk.

- Ability to transform raw threat data into actionable intelligence.
- Improved adherence to cybersecurity frameworks and regulatory requirements.
- Upskilling of security teams in advanced threat analysis and defense strategies.

Target Audience

1. Security Analysts (Tier 2/3)
2. Threat Intelligence Analysts
3. Incident Response Team Members
4. SOC Analysts
5. Cybersecurity Engineers
6. Security Architects
7. Penetration Testers (ethical hackers)
8. IT Security Managers

Course Outline

Module 1: Introduction to Attacker TTPs and Frameworks

- Defining Tactics, Techniques, and Procedures (TTPs)
- Overview of the Cyber Kill Chain and its relation to TTPs
- Deep Dive into the MITRE ATT&CK Framework: Enterprise, Mobile, ICS
- Understanding the importance of behavioral analysis over IOCs
- **Case Study:** Analyzing a recent ransomware attack (e.g., LockBit 3.0) through the lens of the Cyber Kill Chain and MITRE ATT&CK.

Module 2: Cyber Threat Intelligence (CTI) Fundamentals for TTP Analysis

- The CTI Lifecycle: Planning, Collection, Analysis, Production, Dissemination
- Sources of Threat Intelligence: OSINT, HUMINT, TECHINT, FININT
- Evaluating Threat Intelligence Feeds and Platforms (TIPs)
- Integrating CTI into Security Operations and Decision-Making
- **Case Study:** Utilizing OSINT tools and threat intelligence platforms to gather TTPs of a specific nation-state actor group (e.g., APT28/Fancy Bear).

Module 3: Initial Access and Execution TTPs

- Common Initial Access Techniques: Phishing, Exploiting Public-Facing Applications, Valid Accounts, External Remote Services
- Execution TTPs: Command and Scripting Interpreter, PowerShell, Scheduled Task/Job
- Analyzing email headers and malicious documents for initial access indicators
- Understanding social engineering tactics for initial compromise
- **Case Study:** Dissecting a spear-phishing campaign that led to a successful breach, mapping its initial access and execution TTPs to MITRE ATT&CK.

Module 4: Persistence, Privilege Escalation, and Defense Evasion TTPs

- Persistence Mechanisms: Registry Run Keys, Boot or Logon Autostart Execution, Scheduled Tasks
- Privilege Escalation Techniques: Exploiting Vulnerabilities, Process Injection, Credential Dumping
- Defense Evasion Strategies: Obfuscated Files or Information, Masquerading, Indicator Removal

- Identifying and mitigating common persistence and privilege escalation methods
- **Case Study:** Investigating a simulated scenario where an attacker achieved persistence and escalated privileges, detailing the forensic artifacts left behind and the TTPs used.

Module 5: Credential Access, Discovery, and Lateral Movement TTPs

- Credential Access Techniques: OS Credential Dumping (e.g., Mimikatz), Brute Force, Keylogging
- Discovery TTPs: Network Service Discovery, System Information Discovery, Account Discovery
- Lateral Movement Methods: Remote Services, Pass the Hash, SSH Hijacking
- Detecting lateral movement through network traffic analysis and endpoint logs
- **Case Study:** Tracing an attacker's lateral movement path within a compromised network using SIEM logs and network forensic tools, identifying specific credential access and discovery TTPs.

Module 6: Collection, Exfiltration, and Command and Control (C2) TTPs

- Collection Techniques: Data from Local System, Archive Collected Data, Screen Capture
- Exfiltration Methods: Exfiltration Over C2 Channel, Data Compressed, Encrypted, or Obfuscated
- C2 Communication Channels: Standard Application Layer Protocol, Custom C2 Protocol, Web Services
- Analyzing network telemetry for C2 beaconing and data exfiltration patterns
- **Case Study:** Analyzing a malware sample's C2 communication and data exfiltration TTPs, identifying indicators of compromise (IOCs) for detection.

Module 7: Adversary Emulation, Threat Hunting, and Detection Engineering

- Introduction to Adversary Emulation and Red Teaming exercises
- Developing threat hunting hypotheses based on TTPs
- Utilizing EDR and SIEM for proactive threat hunting
- Crafting detection rules and analytics based on observed TTPs (e.g., YARA rules, Sigma rules)
- **Case Study:** Conducting a simulated threat hunt for a specific APT's TTPs within a lab environment, demonstrating the process from hypothesis generation to detection rule creation.

Module 8: Advanced TTPs and Future Trends in Cyber Warfare

- Understanding TTPs in Cloud Environments (e.g., Cloud Attack Matrix)
- The rise of AI-driven TTPs and countermeasures
- TTPs in Supply Chain Attacks and IoT environments
- The role of Purple Teaming in validating and improving defenses
- **Case Study:** Analyzing the TTPs observed in a major supply chain attack (e.g., SolarWinds), discussing the implications for future security strategies and the role of advanced TTP analysis.

Training Methodology

This course employs a highly interactive and practical training methodology designed for maximum knowledge retention and skill development. It combines:

- **Instructor-Led Sessions:** Engaging lectures, discussions, and expert insights.

- **Hands-on Labs:** Practical exercises and simulations in a controlled environment using industry-standard tools and frameworks.
- **Real-World Case Studies:** In-depth analysis of actual cyber incidents to illustrate TTPs and their implications.
- **Interactive Demonstrations:** Live walkthroughs of attack techniques and defensive strategies.
- **Group Activities and Discussions:** Collaborative problem-solving and knowledge sharing among participants.
- **CTF (Capture The Flag) Challenges:** Reinforce learning through competitive, scenario-based exercises.
- **Q&A Sessions:** Opportunities for participants to clarify doubts and engage with instructors.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price

23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com