

MITRE

Introduction

This section Covers US-based non-profit MITRE Corporation which has created for the cybersecurity community numerous frameworks. These frameworks are:

- ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework
- CAR (Cyber Analytics Repository) Knowledge Base
- ENGAGE
- D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)
- AEP (ATT&CK Emulation Plans)

MITRE is greatly associated with Common Threat Vulnerabilities and Exposures – resource the learner searches for an exploit for a given vulnerability.

The weekly task/assignment is divided into 9 sub-tasks that covers introduction to MITRE, basic terminology, ATT&K Framework, CAR Knowledge base, MITRE Engage, MITRE D3FEND, ATT&CK Emulation Plans, ATT&CK and Threat Intelligence and course conclusion on MITRE.

Activity

Lessons/Work for this module is about learning MITRE as outlined in the introduction.

Task 1: Introduction

This section introduces the learner by familiarizing them the foundations in MITRE and its application areas.

The screenshot shows a web browser window displaying a TryHackMe room page. The browser's address bar shows 'tryhackme.com/room/mitre'. The room title is 'Task 1 Introduction to MITRE'. The page content includes an illustration of a clipboard with a checklist and a pencil. Below the illustration, there is a paragraph of text explaining MITRE's role in cybersecurity and its various research areas. A bulleted list follows, detailing the frameworks created by MITRE: ATT&CK, CAR, ENGAGE, D3FEND, and AEP. The page also mentions the room's update date as July 1st, 2022, and prompts the user to answer questions below.

tryhackme.com/room/mitre

2693 MITRE MITRE This room will discuss the various resources MITRE has made available for the cybersecurity community.

Task 1 Introduction to MITRE

For those that are new to the cybersecurity field, you probably never heard of MITRE. Those of us that have been around might only associate MITRE with CVEs (Common Vulnerabilities and Exposures) list, which is one resource you'll probably check when searching for an exploit for a given vulnerability. But MITRE researches in many areas, outside of cybersecurity, for the 'safety, stability, and well-being of our nation.' These areas include artificial intelligence, health informatics, space security, to name a few.

From [MITRE.org](#): "At MITRE, we solve problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation."

In this room, we will focus on other projects/research that the US-based non-profit MITRE Corporation has created for the cybersecurity community, specifically:

- ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) Framework
- CAR (Cyber Analytics Repository) Knowledge Base
- ENGAGE (sorry, not a fancy acronym)
- D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense)
- AEP (ATT&CK Emulation Plans)

Let's dive in, shall we...

Room updated: July 1st, 2022

Answer the questions below

Read the above

28°C Partly sunny 4:02 PM 9/26/2023

Task 2: Basic terminology

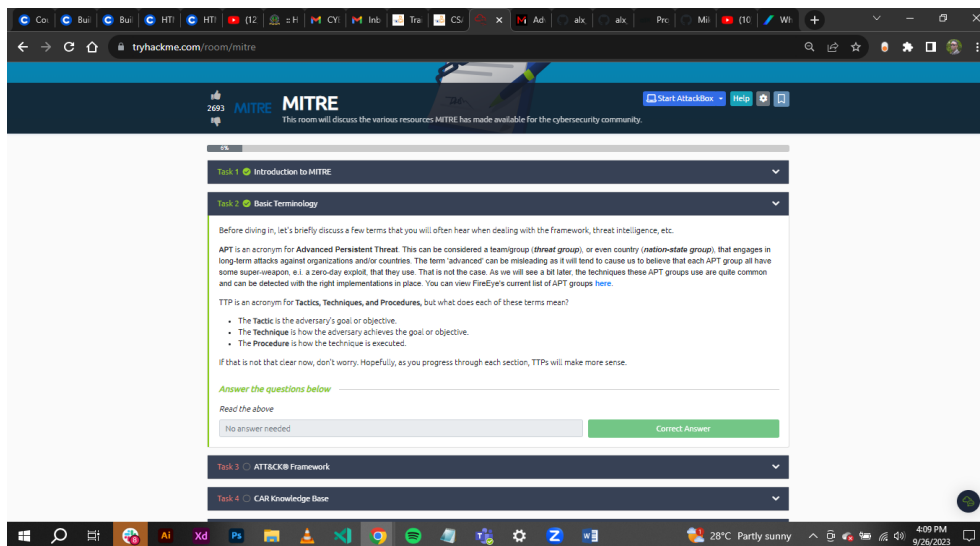
This part introduces more on APT (Advance Persistence Threat) which can be considered a team/group, or even country engaging in long-term attacks against organization and /or countries.

Managed to cover **TTP - Tactics, Techniques and Procedures**

Tactic – the goal or objective of the adversary.

Technique – the means adversary uses to achieve the goal or objective.

Procedure – how the technique is executed.



The screenshot shows a web browser window displaying the MITRE TryHackMe interface. The URL is tryhackme.com/room/mitre. The page features a dark blue header with the MITRE logo and a navigation bar. The main content area is titled 'Task 2: Basic terminology' and contains the following text:

Before diving in, let's briefly discuss a few terms that you will often hear when dealing with the framework, threat intelligence, etc.

APT is an acronym for **Advanced Persistent Threat**. This can be considered a team/group (threat group), or even country (nation-state group), that engages in long-term attacks against organizations and/or countries. The term 'advanced' can be misleading as it will tend to cause us to believe that each APT group all have some super-weapon, e.i. a zero-day exploit, that they use. That is not the case. As we will see a bit later, the techniques these APT groups use are quite common and can be detected with the right implementations in place. You can view FireEye's current list of APT groups [here](#).

TTP is an acronym for **Tactics, Techniques, and Procedures**, but what does each of these terms mean?

- The **Tactic** is the adversary's goal or objective.
- The **Technique** is how the adversary achieves the goal or objective.
- The **Procedure** is how the technique is executed.

If that is not clear now, don't worry. Hopefully, as you progress through each section, TTPs will make more sense.

Answer the questions below

Read the above

No answer needed

The screenshot also shows a task list on the left side of the interface with the following items:

- Task 1: Introduction to MITRE
- Task 2: Basic terminology
- Task 3: ATT&CK Framework
- Task 4: CAR Knowledge Base

The bottom of the screenshot shows a Windows taskbar with various application icons and a system tray displaying the date and time as 4:09 PM on 9/26/2023.

Task 3: ATT&K Framework

This refers to a globally-accessible knowledge base of adversary tactics and techniques based on real-world observation. This framework at most pays much concentration on Windows platform conducted through TTPs against a network and data collection of the same network for analysis. A very useful tool for the red team.

that this link is for version 8 of the ATT&CK Matrix.

Answer the questions below

Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purple Teamers, SOC Managers?)

Red Teamers Correct Answer

What is the ID for this technique?

T1566 Correct Answer Hint

Based on this technique, what mitigation covers identifying social engineering techniques?

User Training Correct Answer

What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)

Application Log,File,Network Traffic Correct Answer

What groups have used spear-phishing in their campaigns? (format: group1,group2)

Axiom,GOLD SOUTHFIELD Correct Answer

Based on the information for the first group, what are their associated groups?

Group 72 Correct Answer

What software is associated with this group that lists phishing as a technique?

HIKIT Correct Answer

What is the description for this software?

Hikit is malware that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise. Correct Answer

This group overlaps (slightly) with which other group?

Winnti Group Correct Answer

How many techniques are attributed to this group?

15 Correct Answer Hint

6:03 PM 27°C Partly sunny 9/26/2023

Task 4: CAR Knowledge base

The official definition of **CAR** is "The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics defining a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regards to their operating theory and rationale."

The screenshot shows a web browser window at tryhackme.com/room/mitre. The page content includes:

- A header with navigation links: Pre-OS Root, Scheduled Task/Job, Server Software Component, Masquerading, Mimicry, Authentication Process, Velocity Registry, and Unsecured Credentials.
- A note: "(The techniques highlighted in purple are the analytics currently in CAR)".
- Text: "Let's look at another analytic to see a different implementation, [CAR-2014-11-004: Remote PowerShell Sessions](#)."
- Text: "Under Implementations, a pseudocode is provided and an EQL version of the pseudocode. EQL (pronounced as 'equal'), and it's an acronym for Event Query Language. EQL can be utilized to query, parse, and organize Sysmon event data. You can read more about this [here](#)."
- Section: "Eql, EQL native"
- Text: "EQL version of the above pseudocode."
- Code block:

```
process where subtype.create and
(process_name == "wsmprovhost.exe" and parent_process_name == "svchost.exe")
```
- Text: "To summarize, CAR is a great place for finding analytics that takes us further than the Mitigation and Detection summaries in the ATT&CK® framework. This tool is not a replacement for ATT&CK® but an added resource."
- Section: "Answer the questions below"
- Question 1: "What tactic has an ID of TA0003?"
Answer: Persistence (Correct Answer button, Hint button)
- Question 2: "What is the name of the library that is a collection of Zeek (BRO) scripts?"
Answer: BZAR (Correct Answer button, Hint button)
- Question 3: "What is the name of the **technique** for running executables with the same hash and different names?"
Answer: Masquerading (Correct Answer button, Hint button)
- Question 4: "Examine CAR-2013-05-004, besides **implementations**, what additional information is provided to analysts to ensure coverage for this technique?"
Answer: Unit Tests (Correct Answer button, Hint button)
- Footer: "Task 5 MITRE Engage"

The Windows taskbar at the bottom shows the time as 6:08 PM on 9/26/2023, with a temperature of 27°C and weather "Partly sunny".

Task 5: MITRE Engage

This is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals. It is considered an Adversary Engagement Approach. This is accomplished by the implementation of Cyber Denial and Cyber Deception.

The screenshot displays a web browser window at tryhackme.com/room/mitre. The page content includes a 'View settings' button, a 'FULL DEFINITION' button, and a section titled 'PLAN' with the sub-header 'Identify and align an operation with a desired end-state.' Below this, a paragraph explains the purpose of planning in engagement operations. A small diagram is visible below the text. The page then states: 'That should be enough of an overview. We'll leave it to you to explore the resources provided to you on this website. Before moving on, let's practice using this resource by answering the questions below.' A section titled 'Answer the questions below' follows, containing four quiz questions with input fields and 'Correct Answer' buttons:

- Question: 'Under Prepare, what is ID SAC0002?'
Answer: PERSONA CREATION
- Question: 'What is the name of the resource to aid you with the engagement activity from the previous question?'
Answer: PERSONA PROFILE WORKSHEET
- Question: 'Which engagement activity balts a specific response from the adversary?'
Answer: Lures
- Question: 'What is the definition of Threat Model?'
Answer: A risk assessment that models organizational strengths and weaknesses

The bottom of the browser window shows a task bar with 'Task 6 MITRE D3FEND' and a system tray with the date and time '6:12 PM 9/26/2023'.

Task 6: MITRE D3FEND

This resource is A knowledge graph of cybersecurity countermeasures.

D3FEND is still in beta and is funded by the Cybersecurity Directorate of the NSA.

D3FEND stands for **D**etection, **D**enial, and **D**isruption Framework Empowering Network Defense.

The screenshot shows a web browser window with the URL `tryhackme.com/room/mitre`. The page title is "Decoy File" and the subtitle is "D3.F". The content is organized into sections: "Definition", "How it works", "Considerations", "Example", and "Digital Artifact Relationships". Below these sections, there is a paragraph explaining the purpose of the resource and a section titled "Answer the questions below". The first question asks for the first MITRE ATT&CK technique listed in the "ATT&CK Lookup" dropdown, with the answer "Data Obfuscation" entered in a text box. The second question asks for the ATT&CK technique from the previous question's "D3FEND Inferred Relationships", with the answer "Outbound Internet Network Traffic" entered. The page also features a "Task 7" dropdown menu at the bottom, currently set to "ATT&CK Emulation Plans". The browser's taskbar at the bottom shows various application icons and the system clock indicating 6:36 PM on 9/26/2023.

Decoy File
D3.F

Definition
A file created for the purposes of deceiving an adversary.

How it works
The decoy file is made available as a local or network resource. Accesses to the file may be monitored. The files may be configurations, documents, executables, or other file types.

Considerations
Properties of the file such as cryptographic checksums, file creation date, file modified date, file size, file owner etc. may be modified to improve the credibility of the file.

Example
A CSV file with decoy user credentials is placed on a system. The system or network is then monitored to detect any accesses to the decoy files.

Digital Artifact Relationships:
This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

As you can see, you're provided with information on what is the technique (**definition**), how the technique works (**how it works**), things to think about when implementing the technique (**considerations**), and how to utilize the technique (**example**).

Note, as with other MITRE resources, you can filter based on the ATT&CK matrix.

Since this resource is in beta and will change significantly in future releases, we won't spend that much time on D3FEND.

The objective of this task is to make you aware of this MITRE resource and hopefully you'll keep an eye on it as it matures in the future.

We will still encourage you to navigate the website a bit by answering the questions below.

Answer the questions below

What is the First MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown?

Data Obfuscation Correct Answer

In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produce?

Outbound Internet Network Traffic Correct Answer Hint

Task 7 ATT&CK Emulation Plans

Task 7: ATT&CK Emulation Plans

The Center of Threat-Informed Defense (CTID) is an organization consisting of various companies and vendors from around the globe. They have an objective of conducting research on cyber threats and their TTPs and share this research to improve cyber defense for all.

Some of the companies and vendors who are participants of CTID:

- AttackIQ (founder)
- Verizon
- Microsoft (founder)
- Red Canary (founder)
- Splunk

The screenshot shows a web browser window with the URL `tryhackme.com/room/mitre`. The page title is "Task 7: ATT&CK Emulation Plans". The content includes:

- CTID**
If these tools provided to us by MITRE are not enough, under MITRE **ENGenuity**, we have CTID, the Adversary Emulation Library, and ATT&CK Emulation Plans.
- CTID**
MITRE formed an organization named The **Center of Threat-Informed Defense (CTID)**. This organization consists of various companies and vendors from around the globe. Their objective is to conduct research on cyber threats and their TTPs and share this research to improve cyber defense for all.
- Some of the companies and vendors who are participants of CTID:**
 - AttackIQ (founder)
 - Verizon
 - Microsoft (founder)
 - Red Canary (founder)
 - Splunk
- Per the website, "Together with Participant organizations, we cultivate solutions for a safer world and advance threat-informed defense with open-source software, methodologies, and frameworks. By expanding upon the MITRE ATT&CK knowledge base, our work expands the global understanding of cyber adversaries and their tradecraft with the public release of data sets critical to better understanding adversary behavior and their movements."**
- Adversary Emulation Library & ATT&CK Emulation Plans**
The **Adversary Emulation Library** is a public library making adversary emulation plans a free resource for bluehired teamers. The library and the emulations are a contribution from CTID. There are several **ATT&CK Emulation Plans** currently available: **APT13**, **APT29**, and **IRIS**. The emulation plans are a step-by-step guide on how to mimic the specific threat group. If any of the CSuite were to ask, "how would we flare if APT29 hit us?" This can easily be answered by referring to the results of the execution of the emulation plan.
- Review the emulation plans to answer the questions below.**
- Answer the questions below**
- In Phase 1 for the APT13 Emulation Plan, what is listed first?**
C2 Setup
- Under Persistence, what binary was replaced with cmd.exe?**
sethc.exe
- Examining APT29, what C2 Frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)**
Pussy/Metasploit Framework
- What C2 Framework is listed in Scenario 2 Infrastructure?**
PocCatC2
- Examine the emulation plan for Sandworm. What webshell is used for Scenario 1? Check MITRE ATT&CK for the Software ID for the webshell. What is the id? (format: webshellID)**
P.A.S.S.0598

The bottom of the screenshot shows a Windows taskbar with various application icons and a system tray displaying the date and time as 8:48 PM on 9/26/2023.

Task 8: ATT&CK and Threat Intelligence

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy.

I worked on a scenario of using ATT&CK for threat intelligence. The goal of threat intelligence is to make the information actionable.

Task 7: ATT&CK Emulation Plans

Task 8: ATT&CK and Threat Intelligence

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy. Large corporations might have an in-house team whose primary objective is to gather threat intelligence for other teams within the organization, aside from using threat intel already readily available. Some of this threat intel can be open source or through a subscription with a vendor, such as [CrowdStrike](#). In contrast, many defenders wear multiple hats (roles) within some organizations, and they need to take time from their other tasks to focus on threat intelligence. To cater to the latter, we'll work on a scenario of using ATT&CK for threat intelligence. The goal of threat intelligence is to make the information actionable.

Scenario: You are a security analyst who works in the aviation sector. Your organization is moving their infrastructure to the cloud. Your goal is to use the ATT&CK Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques targeting your areas of concern. You are checking to see if there are any gaps in coverage. After selecting a group, look over the selected group's information and their tactics, techniques, etc.

Answer the questions below

What is a group that targets your sector who has been in operation since at least 2013?

APT33 Correct Answer

As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?

Cloud Accounts Correct Answer

What tool is associated with the technique from the previous question?

Ruler Correct Answer

Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation?

Multi-factor Authentication Correct Answer

What platforms does the technique from question #2 affect?

Azure AD, Google Workspace, IaaS, Office 365, SaaS Correct Answer

Task 9: Conclusion

Conclusion

In this room, I was able to explore resources that MITRE has provided to the security community. The room's goal was to expose me to these resources and give a foundational knowledge of their uses. Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these resources are a must to know.

The screenshot shows a web browser window with the URL `tryhackme.com/room/mitre`. The page displays a list of tasks on the left side, including Task 3 (ATT&CK Framework), Task 4 (CAR Knowledge Base), Task 5 (MITRE Engage), Task 6 (MITRE D3FEND), Task 7 (ATT&CK Emulation Plans), Task 8 (ATT&CK and Threat Intelligence), and Task 9 (Conclusion). The 'Conclusion' task is selected, showing a text area with the following content:

In this room, we explored tools/resources that MITRE has provided to the security community. The room's goal was to expose you to these resources and give you a foundational knowledge of their uses. Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Some of you might be looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these tools/resources are a must to know.

As mentioned before, though, this is not only for defenders. As red teamers, these tools/resources are useful as well. Your objective is to mimic the adversary and attempt to bypass all the controls in place within the environment. With these resources, as the red teamer, you can effectively mimic a true adversary and communicate your findings in a common language that both sides can understand. In a nutshell, this is known as **purple teaming**.

Below the text, there is a section titled 'Answer the questions below' with a 'Read the above' button and a 'Correct Answer' button. The 'Correct Answer' button is highlighted in green.

At the bottom of the page, there is a note: 'Created by tryhackme and Dex01'. Below this, it says: 'This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 60867 users are in here and this room is 1049 days old.'

The browser's taskbar at the bottom shows various applications and the system clock, indicating the time is 8:56 PM on 9/26/2023.