

MITRE

The MITRE ATT&CK Framework is a comprehensive matrix of tactics and techniques used by cyber adversaries. It provides a detailed and systematic approach to understanding and combating various cyber threats. TryHackMe, an online platform offering cybersecurity training, integrates the MITRE ATT&CK Framework into its learning modules to enhance the educational experience for aspiring security professionals.

MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used by cybersecurity professionals to develop threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. The framework is organized into several matrices, with the Enterprise matrix being the most commonly used. This matrix is divided into tactics and techniques:

Tactics: The "why" of an attack, representing the adversary's goals, such as initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, exfiltration, and impact.

Techniques: The "how" of an attack, detailing the methods adversaries use to achieve their goals, such as phishing, command-line interface, process injection, and credential dumping.

TryHackMe and MITRE ATT&CK

TryHackMe uses the MITRE ATT&CK Framework to structure its training modules and labs, providing a practical and interactive way to learn about the various tactics and techniques used by attackers. By aligning its content with the framework, TryHackMe ensures that learners can:

Understand Adversary Behavior: Gain insights into how attackers operate and the methods they use, making it easier to anticipate and defend against real-world attacks.

Map Learning to Real-World Scenarios: Relate exercises and challenges to actual tactics and techniques used in the industry, enhancing the relevance and applicability of the training.

Develop Comprehensive Defense Strategies: Learn how to detect, prevent, and respond to attacks using a structured approach, improving overall cybersecurity posture.

Key Modules on TryHackMe

Several key modules on TryHackMe are built around the MITRE ATT&CK Framework, providing hands-on experience with specific tactics and techniques. These modules cover various aspects of cybersecurity, including:

Initial Access: Techniques such as phishing and exploiting public-facing applications.

Execution: Methods like command-line interface usage and script execution.

Persistence: Techniques including scheduled tasks and account manipulation.

Privilege Escalation: Methods such as exploiting vulnerabilities and bypassing access controls.

Defense Evasion: Techniques like obfuscation and disabling security tools.

Credential Access: Methods including keylogging and credential dumping.

Discovery: Techniques such as network scanning and account discovery.

Lateral Movement: Methods like remote services exploitation and internal spear-phishing.

Collection: Techniques for gathering data, including data from local systems and removable media.

Exfiltration: Methods like automated exfiltration and data compression.

Impact: Techniques such as data destruction and service stop.

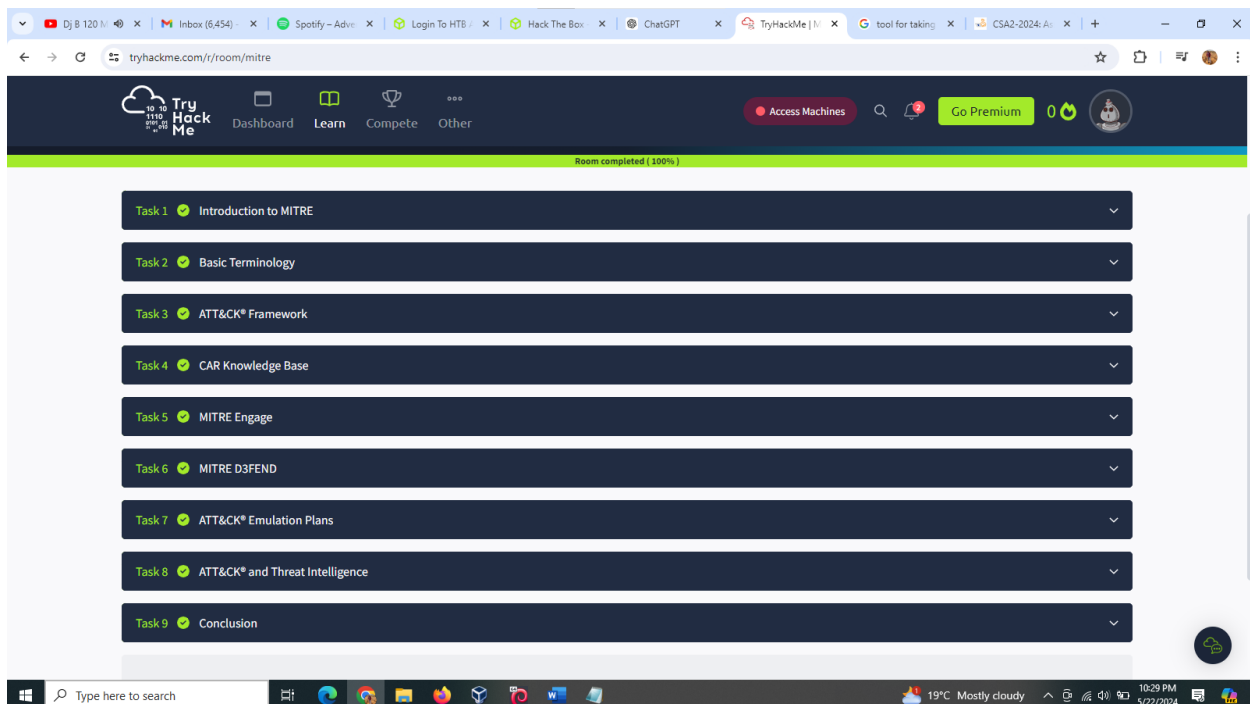
Benefits of MITRE ATT&CK in TryHackMe

Structured Learning: Provides a clear, structured pathway for learning about cyber threats and defenses.

Real-World Relevance: Aligns training with real-world scenarios, ensuring learners are prepared for actual cybersecurity challenges.

Enhanced Understanding: Helps learners understand the full scope of adversary tactics and techniques, improving their ability to detect and respond to threats.

Integrating the MITRE ATT&CK Framework into TryHackMe's training modules provides a robust and practical approach to cybersecurity education. It helps learners understand and mitigate cyber threats by providing detailed insights into adversary tactics and techniques, ensuring they are well-prepared to handle real-world cybersecurity challenges.



cs-sa07-24019

John Mutave

TryHackMe

Dashboard Learn Compete Other

Access Machines

Go Premium

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

No answer needed

Correct Answer

TryHackMe

Dashboard Learn Compete Other

Access Machines

Go Premium

Task 2 Basic Terminology

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 that 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

Correct Answer

Task 3 ATT&CK® Framework

cs-sa07-24019

John Mutave

tryhackme.com/r/room/mitre

tryHackMe Dashboard Learn Compete Other Access Machines Go Premium 0

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 T2 ✓ 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 a software 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?

Wineltd Group ✓ Correct Answer

How many techniques are attributed to this group?

15 ✓ Correct Answer Hint

tryhackme.com/r/room/mitre

tryHackMe Dashboard Learn Compete Other Access Machines Go Premium 0

```
process.where ruletype:create and
(process_name == "usaspnhost.exe" and parent_process_name == "svchost.exe")
```

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.

Answer the questions below

What tactic has an ID of TA0003?

Persistence ✓ Correct Answer Hint

What is the name of the library that is a collection of Zeek (BRO) scripts?

BZAR ✓ Correct Answer Hint

What is the name of the **technique** for running executables with the same hash and different names?

masquerading ✓ Correct Answer Hint

Examine CAR-2013-05-004, besides **implementations**, what additional information is provided to analysts to ensure coverage for this technique?

Unit tests ✓ Correct Answer Hint

Task 5 MITRE Engage

Task 6 MITRE DEFEND

Task 7 ATT&CK Emulation Plans

Task 8 ATT&CK and Threat Intelligence

Task 9 Conclusion

Created by	Room Type	Users in Room	Created
tryhackme	Free Room- Anyone can deploy virtual machines	106/513	1288 days ago

cs-sa07-24019

John Mutave

tryhackme.com/r/room/mitre

tryHackMe Dashboard Learn Compete Other Access Machines Go Premium 0 0

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.

Answer the questions below

Under Prepare, what is ID SAC0002?

Persona creation ✓ Correct Answer

What is the name of the resource to aid you with the engagement activity from the previous question?

persona profile worksheet ✓ Correct Answer Hint

Which engagement activity baits a specific response from the adversary?

lures ✓ Correct Answer

What is the definition of Threat Model?

risk assessment that models organizational strengths and weaknesses ✓ Correct Answer

Task 6 MITRE D3FEND

Task 7 ATT&CK Emulation Plans

Task 8 ATT&CK and Threat Intelligence

Task 9 Conclusion

Created by	Room Type	Users in Room	Created
tryhackme Dev01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	106,633	1288 days ago

tryhackme.com/r/room/mitre

tryHackMe Dashboard Learn Compete Other Access Machines Go Premium 0 0

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 8 ATT&CK and Threat Intelligence

Task 9 Conclusion

Created by	Room Type	Users in Room	Created
tryhackme Dev01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	106,633	1288 days ago

Copyright TryHackMe 2018-2024

cs-sa07-24019

John Mutave

The screenshot shows the TryHackMe interface for the room 'Adversary Emulation Library & ATT&CK'. The page title is 'Adversary Emulation Library & ATT&CK' Emulations Plans'. The content describes the library as a public resource for blue/red teamers, mentioning several emulation plans: APT3, APT29, and FIN6. It provides a step-by-step guide on how to mimic specific threat groups. Below the text, there are several questions and answers related to the emulation plans. The questions are: 'In Phase 1 for the APT3 Emulation Plan, what is listed first?', 'Under Persistence, what binary was replaced with cmd.exe?', 'Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)', 'What C2 framework is listed in Scenario 2 Infrastructure?', and '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: webshell_id)'. The answers are: 'C2 setup', 'sethc.exe', 'Pupy, Metasploit Framework', 'Powershell', and 'PA.S_S0598'. At the bottom, there is a table with room statistics: Created by (tryhackme, Dev01), Room Type (Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)), Users in Room (106,633), and Created (1288 days ago).

The screenshot shows the TryHackMe interface for the room 'Threat Intelligence (TI) or Cyber Threat Intelligence (CTI)'. The page title is 'Threat Intelligence (TI) or Cyber Threat Intelligence (CTI)'. The content describes threat intelligence as information or TTPs attributed to the adversary, used by defenders to make better decisions regarding defensive strategy. It mentions that 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. Below the text, there is a 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.' Below the scenario, there are several questions and answers related to threat intelligence. The questions are: 'What is a group that targets your sector who has been in operation since at least 2013?', '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?', 'What tool is associated with the technique from the previous question?', 'Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation?', and 'What platforms does the technique from question 4 affect?'. The answers are: 'APT33', 'cloud accounts', 'Ruler', 'Multi-factor Authentication', and 'Azure AD, Google workspace, iaaS, Office 365, SaaS'. At the bottom, there is a table with room statistics: Created by (tryhackme, Dev01), Room Type (Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)), Users in Room (106,633), and Created (1288 days ago).

Shareable link - <https://tryhackme.com/dashboard>

Username mbithi.bloggs

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**.