cs-sa07-24019
John Mutave

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

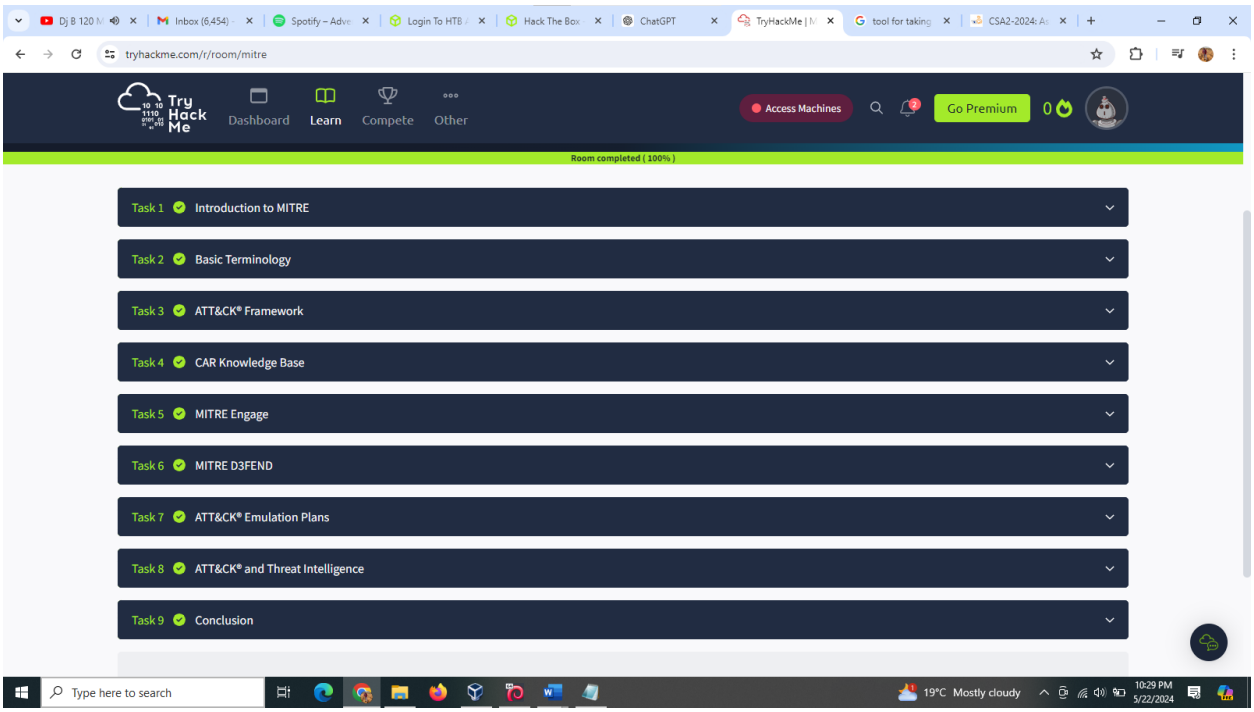
Structured Learning: Provides a clear, structured pathway for learning about cyber threats and defenses.

cs-sa07-24019
John Mutave

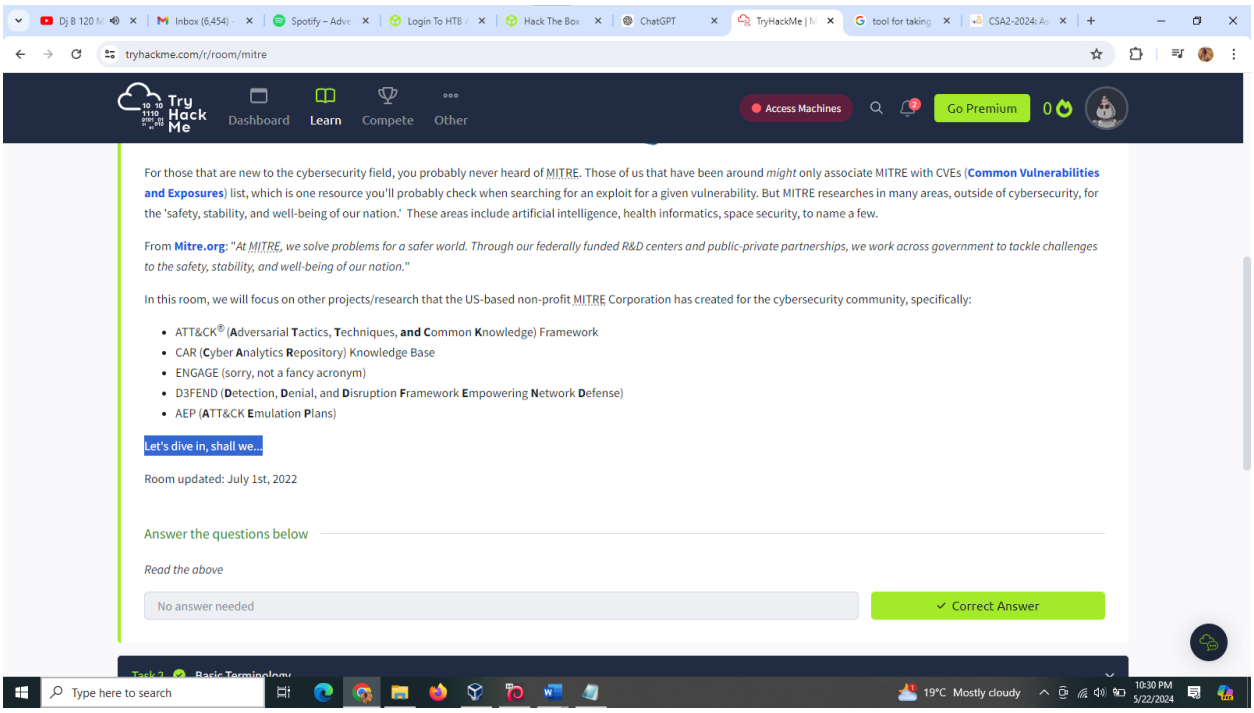
Real-World Relevance: Aligns training with real-world scenarios, ensuring learners are prepared for actual cybersecurity challenges.

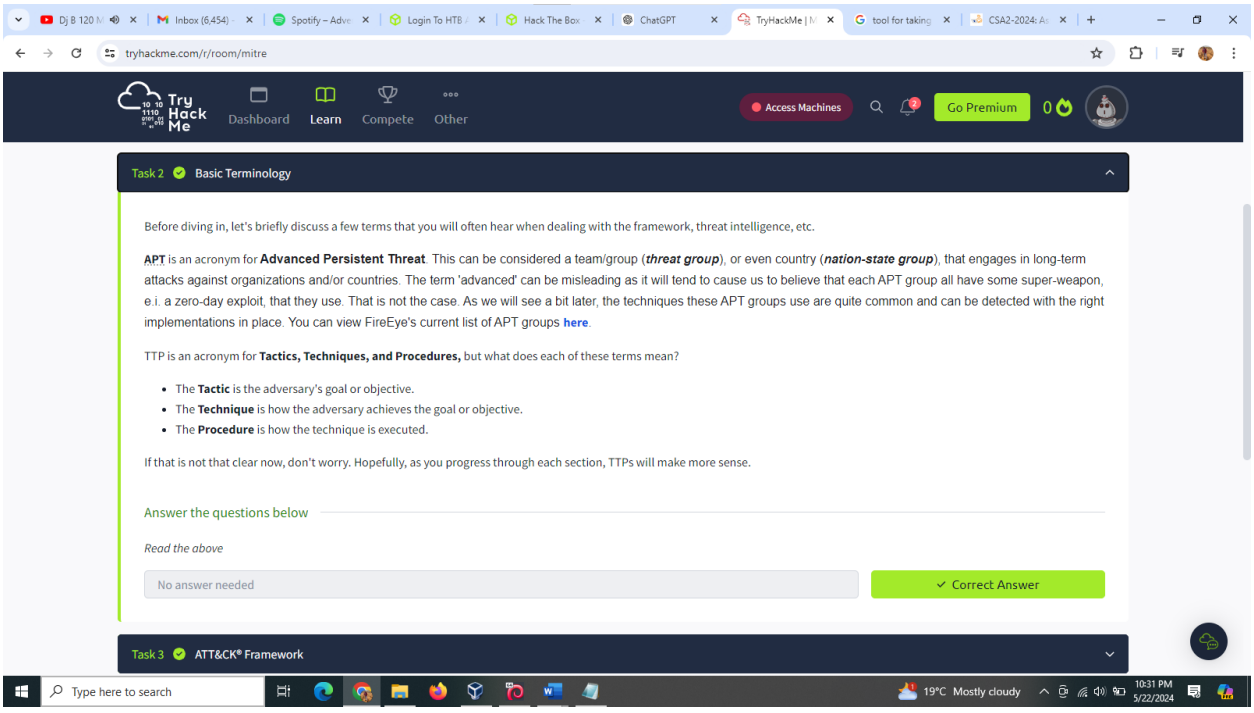
Enhanced Understanding: Helps learners understand the full scope of adversary tactics and techniques, improving their ability to detect and respond to threats.

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.

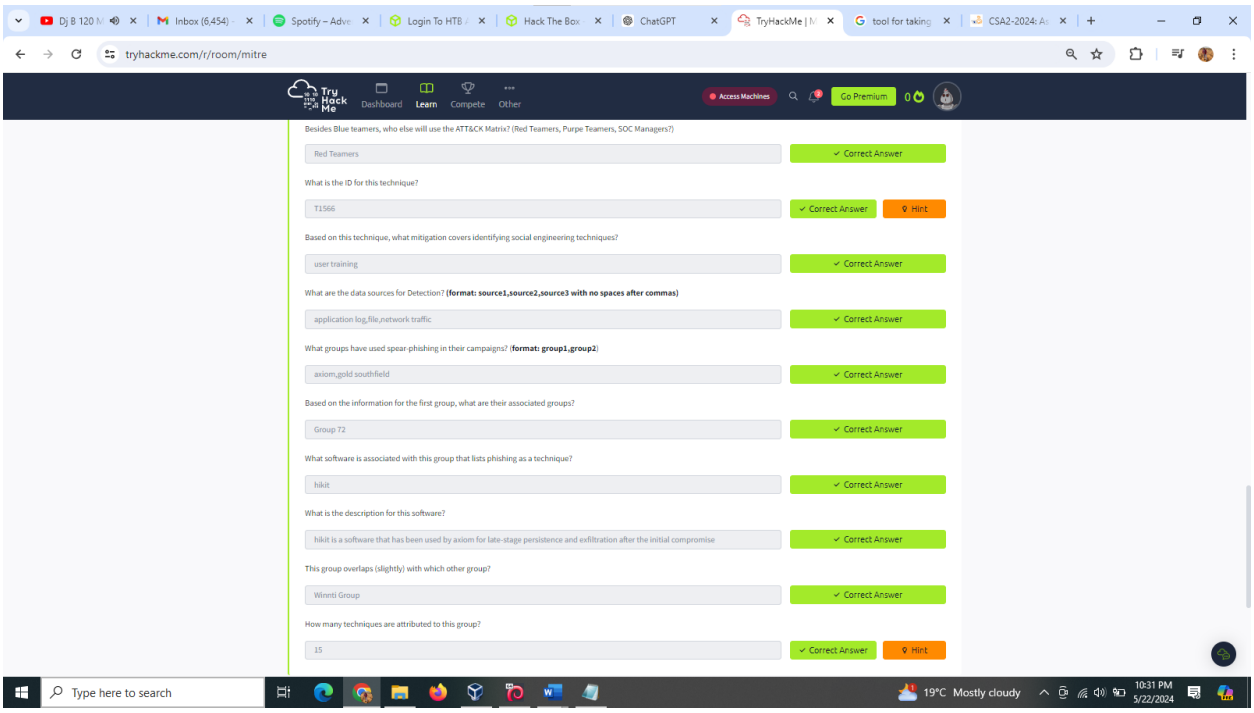


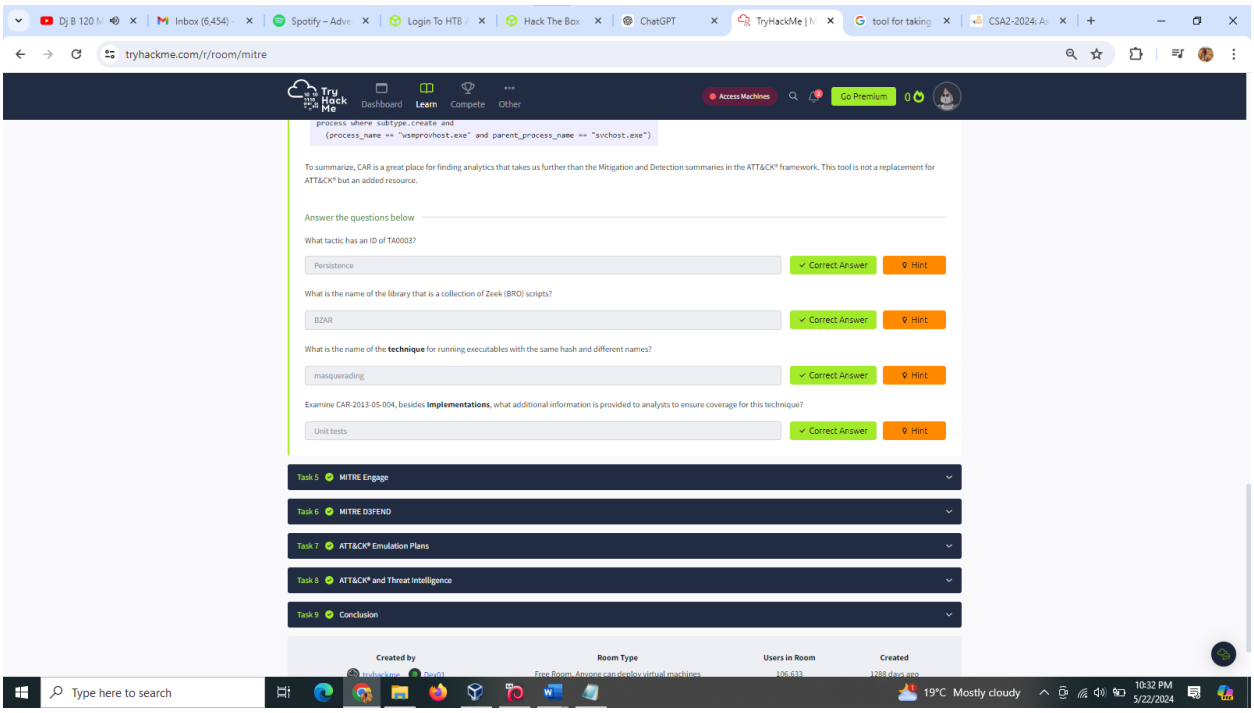
cs-sa07-24019
John Mutave



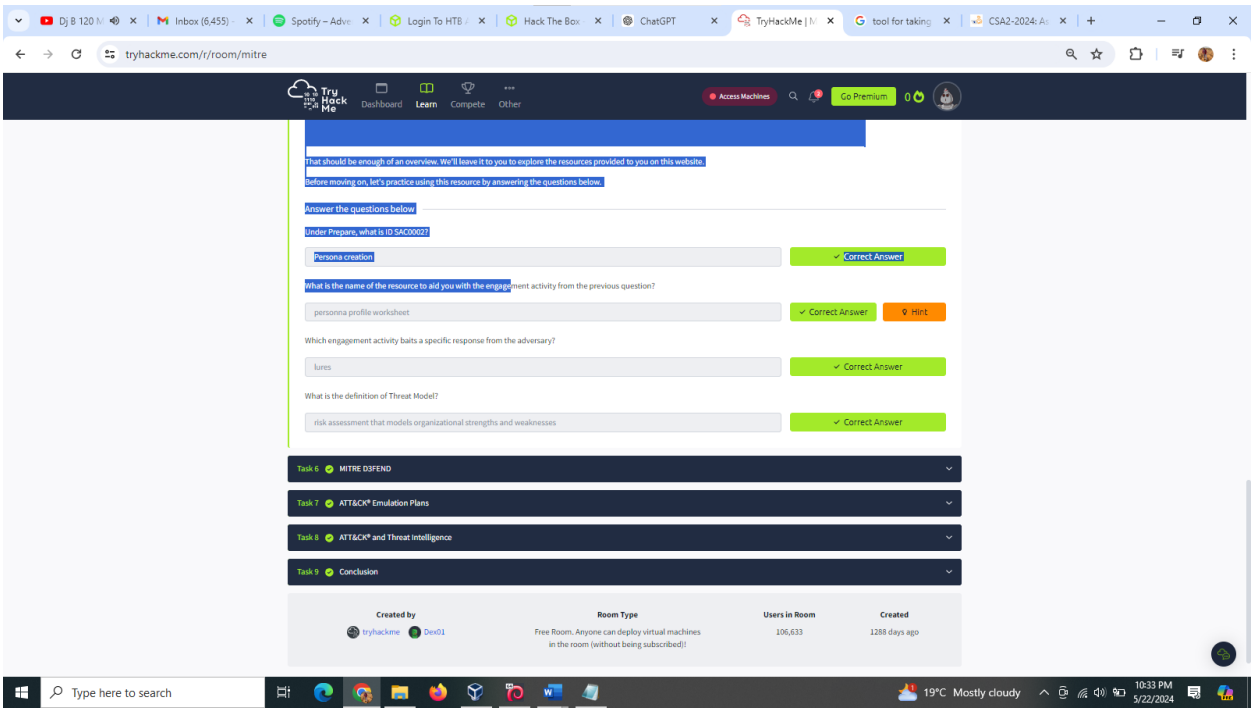


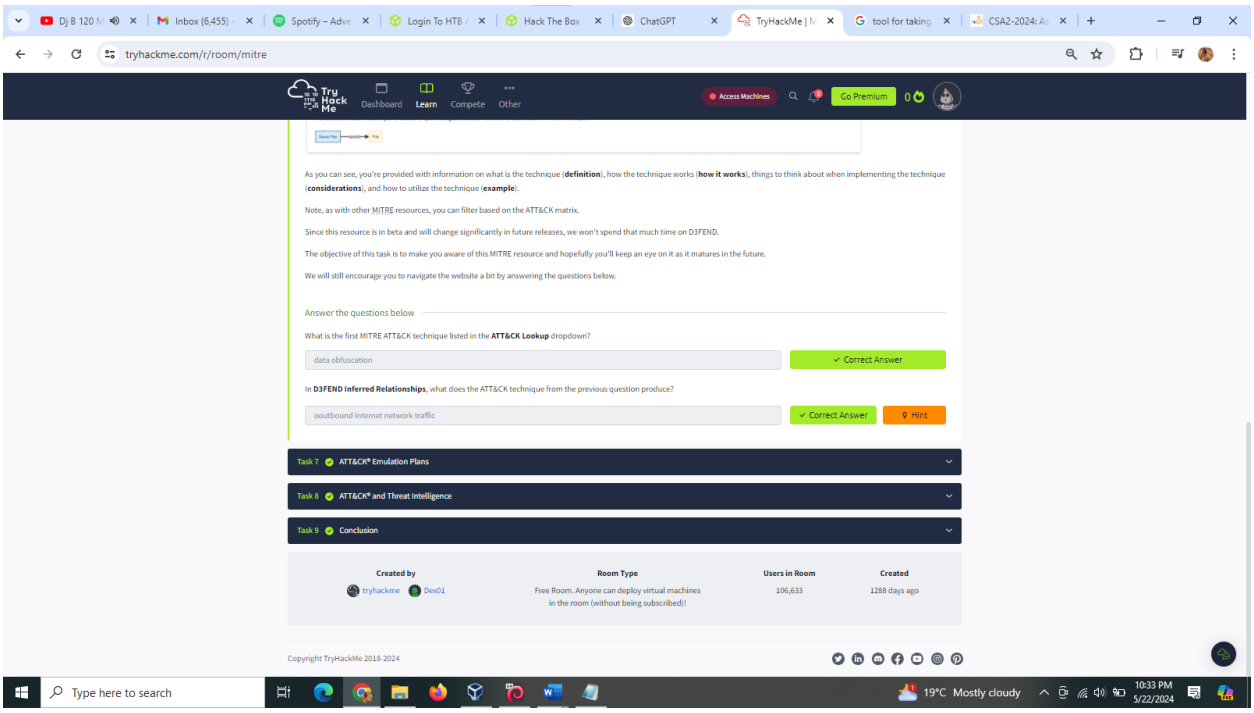
cs-sa07-24019
John Mutave



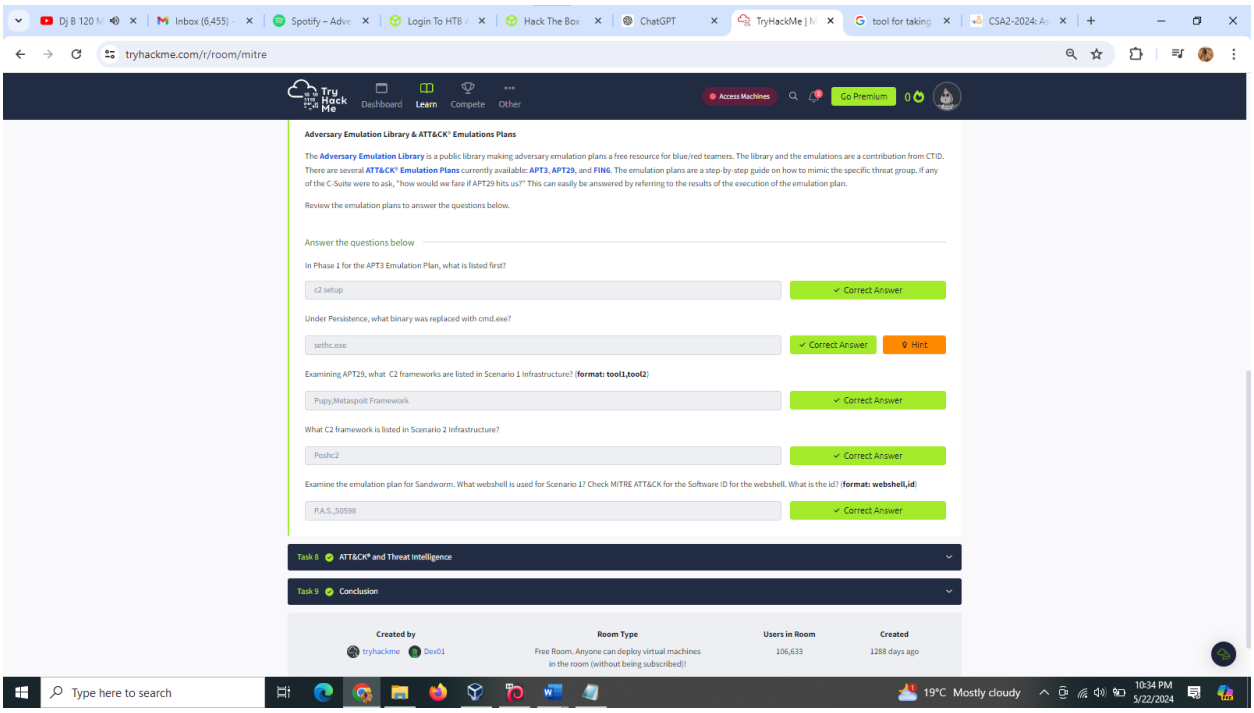


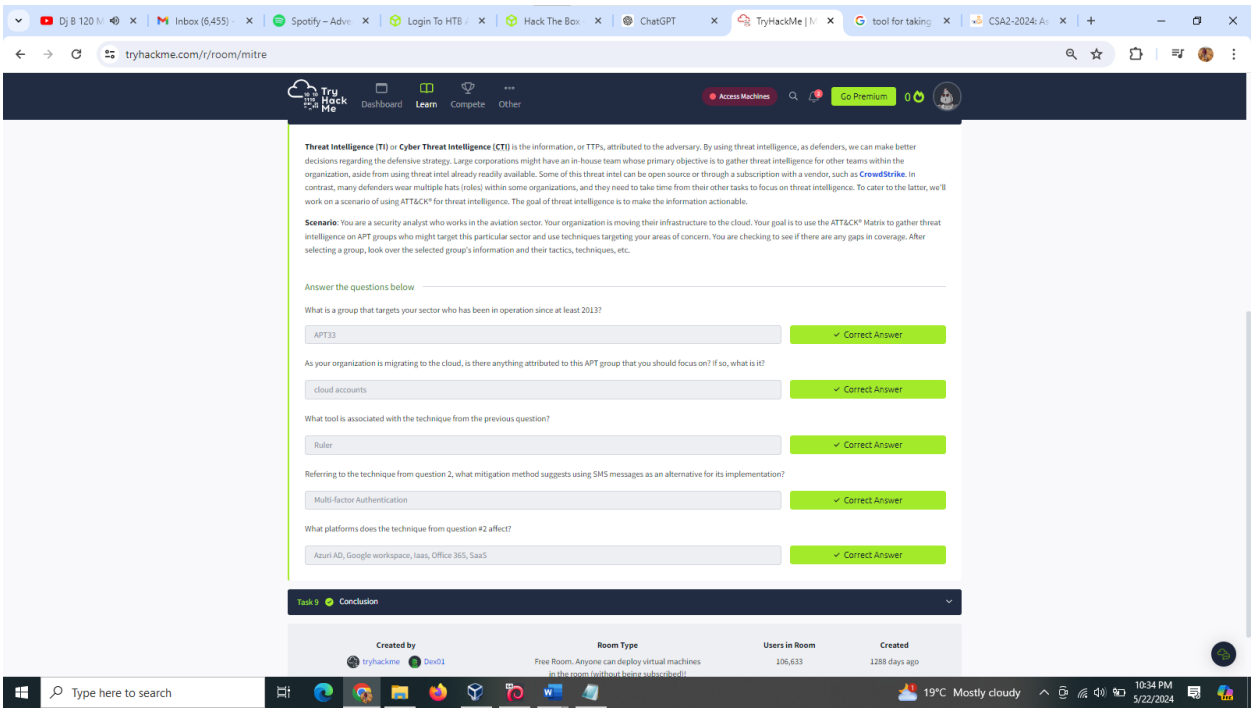
cs-sa07-24019
John Mutave





cs-sa07-24019
John Mutave





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

Username mbithi.bloggs

cs-sa07-24019
John Mutave

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**.