cs-sa07-24019
John_Mbithi_Mutave

Report on Malware Introductory

Task 1: What is the Purpose of Malware Analysis?

Malware analysis is crucial for understanding the behavior, functionality, and impact of malicious software (malware). Its primary purposes include:

- **Detection and Classification**: Identifying the type of malware (e.g., virus, worm, trojan) to develop appropriate defenses.
- **Behavioral Analysis**: Understanding what actions the malware performs on infected systems.
- **Reverse Engineering**: Deconstructing malware to uncover its algorithms, protocols, and communication methods.
- **Attribution**: Determining the origin or authorship of the malware.
- **Defensive Measures**: Developing countermeasures and mitigations against current and future malware threats.

Task 2: Understanding Malware Campaigns

Malware campaigns refer to coordinated efforts by threat actors to distribute and execute malicious software across multiple targets. Key aspects include:

- **Attack Vectors**: How malware spreads (e.g., phishing emails, exploit kits, malicious websites).
- **Targets**: Types of systems or networks vulnerable to the malware.
- **Goals**: Objectives of the malware campaign (e.g., data theft, system disruption, espionage).
- **Lifecycle**: Phases from initial infection to execution and persistence.
- **Attribution**: Linking campaigns to specific threat actors or groups.

Task 3: Identifying if a Malware Attack has Happened

Signs of a malware attack include:

- Unexplained system slowdowns or crashes.
- Unexpected network activity or outgoing connections.
- Changes in system settings or files.
- Anti-virus alerts or warnings.
- Unauthorized access or data breaches.

Task 4: Static Vs. Dynamic Analysis

- **Static Analysis**: Examines the malware without executing it. Involves examining code, file structure, and metadata.
- **Dynamic Analysis**: Involves executing the malware in a controlled environment (sandbox) to observe behavior, interactions, and network activity.

Task 5: Discussion of Provided Tools & Their Uses

Common tools for malware analysis include:

- **Static Analysis Tools**: IDA Pro, Ghidra, PE Explorer.
- **Dynamic Analysis Tools**: Cuckoo Sandbox, Hybrid Analysis.
- **Utilities**: Wireshark for network traffic analysis, Process Monitor for system activity monitoring.

Task 6: Connecting to the Windows Analysis Environment (Deploy)

Setting up a Windows analysis environment involves:

- Using virtualization software like VMware or VirtualBox.
- Installing a clean, isolated instance of Windows for testing malware safely.

Task 7: Obtaining MD5 Checksums of Provided Files

MD5 checksums are obtained to verify file integrity and detect changes or tampering.

Task 8: Checking if MD5 Checksums have been analyzed before

Comparison of MD5 checksums against databases or online repositories (e.g., VirusTotal) to determine if the file has been previously analyzed or identified as malware.

Task 9: Identifying if the Executables are obfuscated / packed

Detection of obfuscation or packing techniques used to conceal the true purpose of executables.

Task 10: What is Obfuscation / Packing?

- **Obfuscation**: Techniques to make code difficult to understand or analyze.

- **Packing**: Compression and encryption methods used to reduce file size and hinder analysis.

Task 11: Visualising the Differences Between Packed & Non-Packed Code

Packed code appears as compressed or encrypted blocks, while non-packed code is more readable and structured.

Task 12: Introduction to Strings

Strings are sequences of characters within executable files that can reveal important information about functionality, behavior, or embedded resources.

Task 13: Introduction to Imports

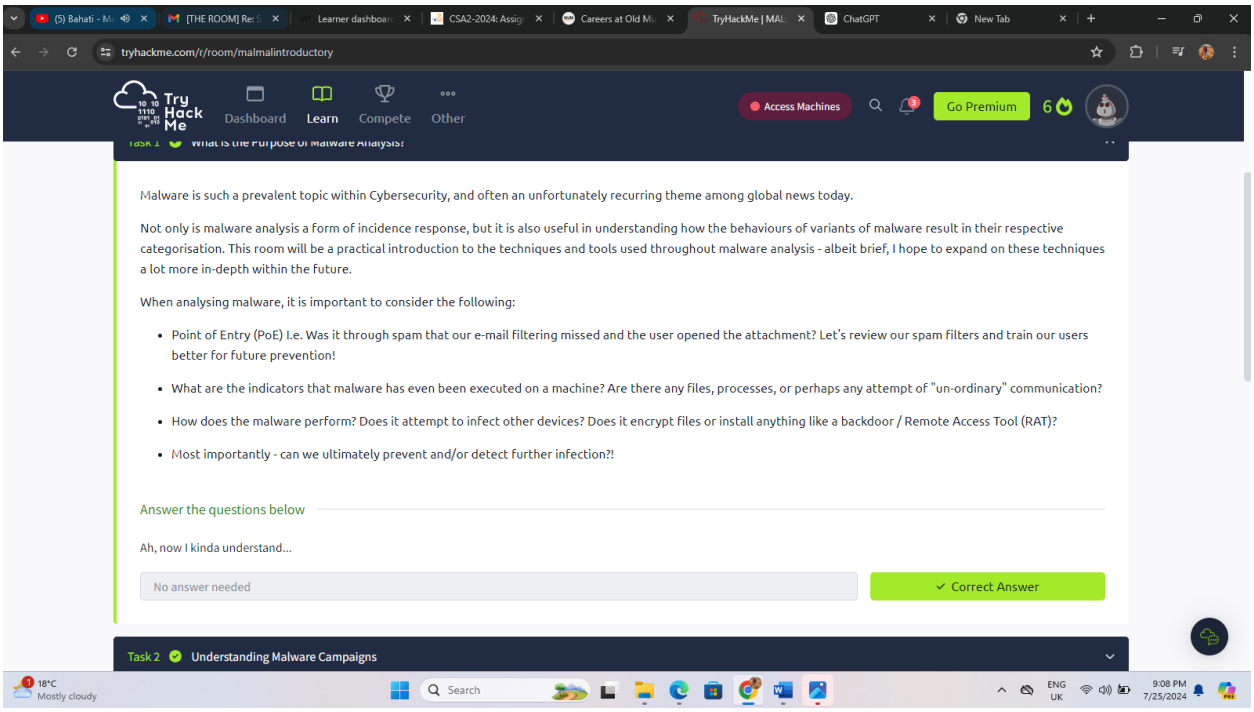
Imports refer to external functions or libraries called by executable files, providing insights into dependencies and functionality.

Task 14: Practical Summary

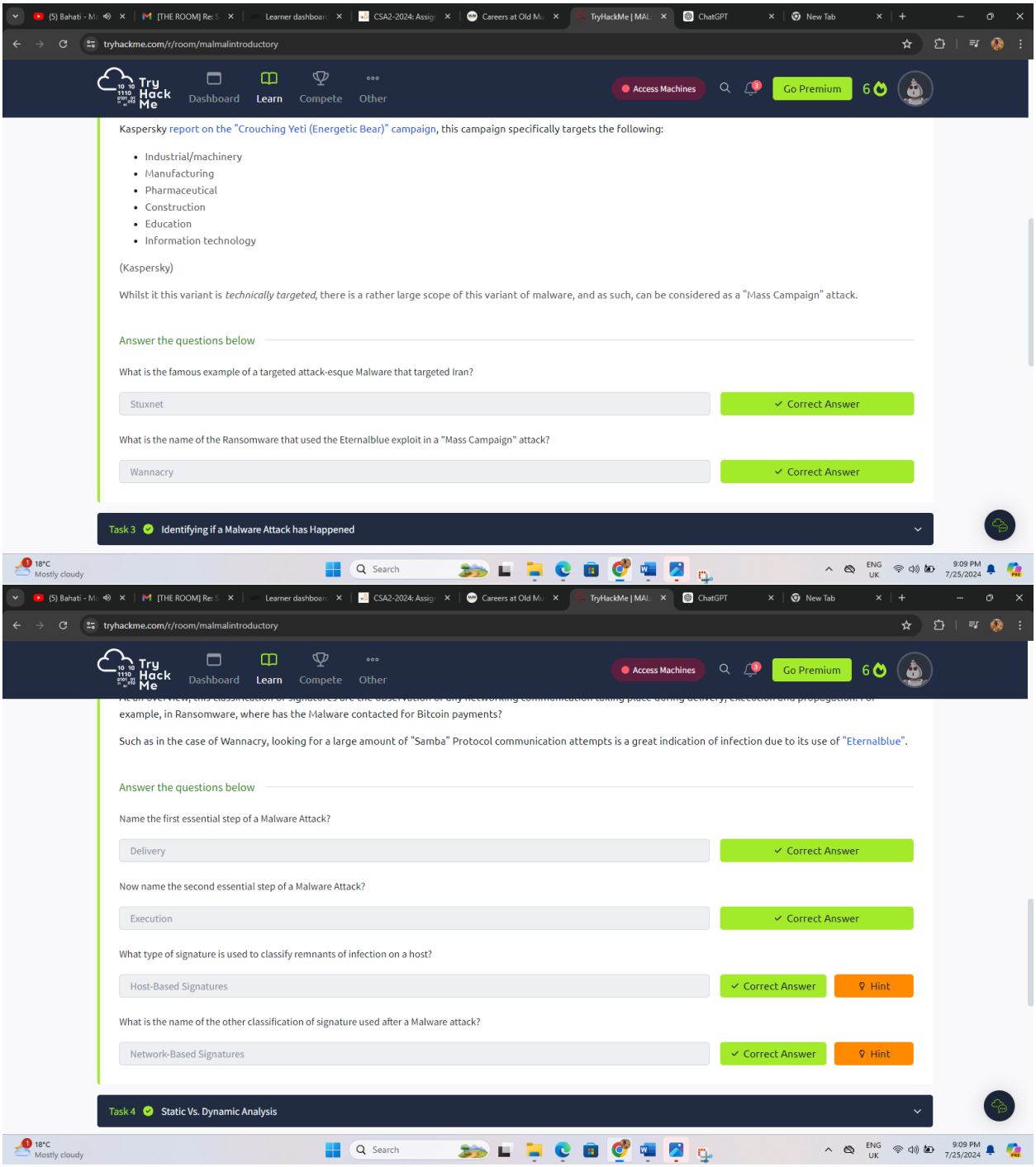
Malware analysis is essential for cybersecurity to understand, detect, and mitigate the impact of malicious software. It involves static and dynamic analysis techniques, the use of specialized tools, and understanding malware behaviors and campaign strategies. By deploying analysis environments and utilizing tools effectively, security professionals can better defend against evolving threats.

Screenshot Overview of the Task

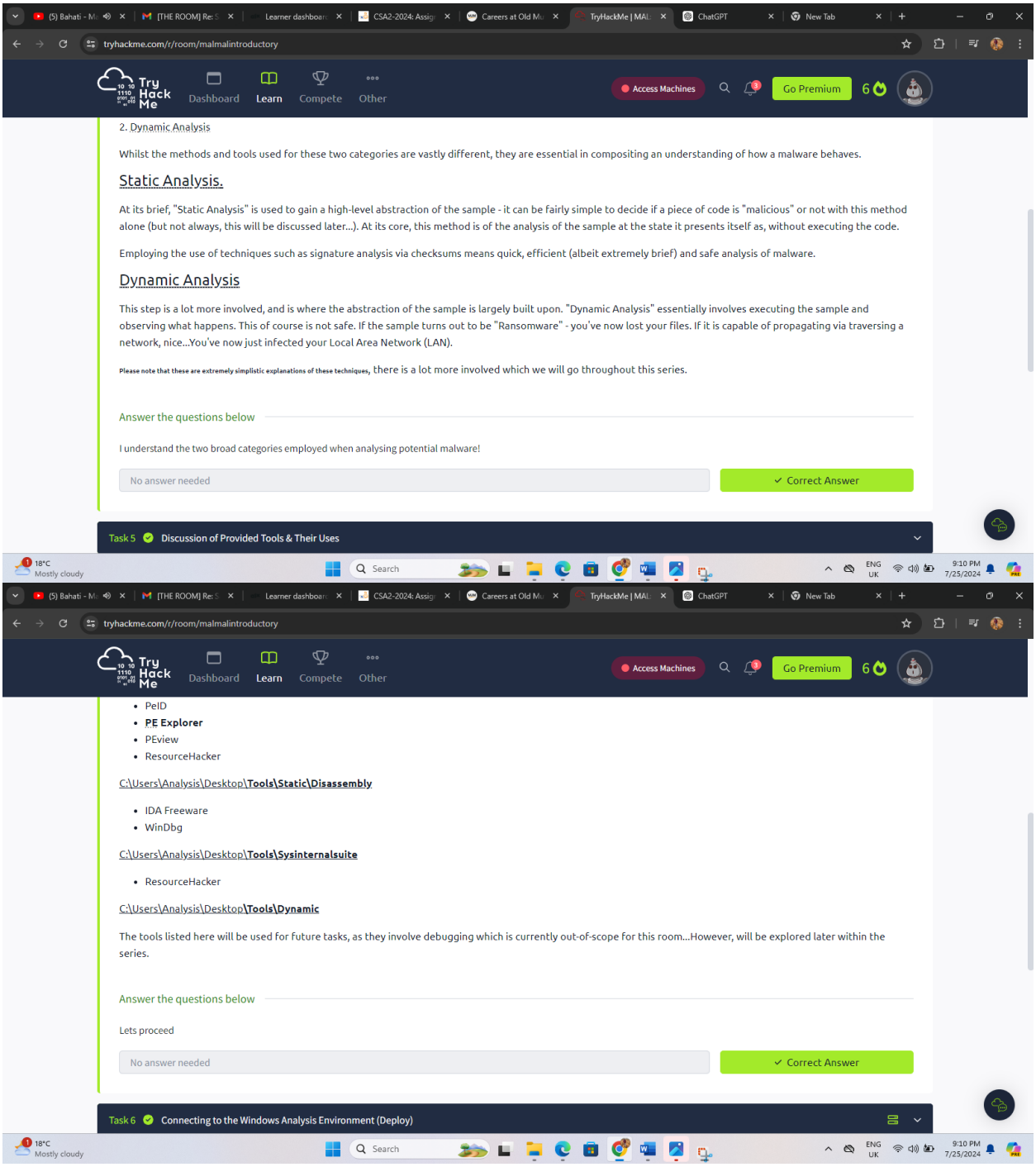
cs-sa07-24019
John_Mbithi_Mutave



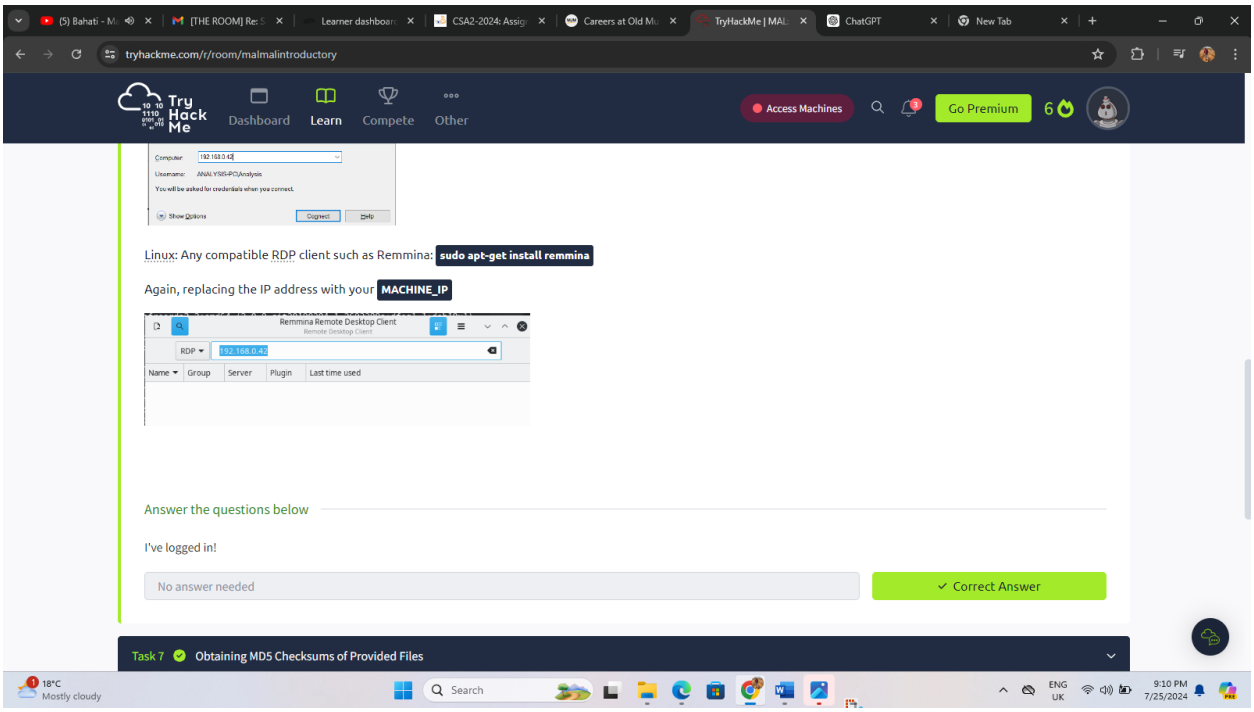
cs-sa07-24019
John_Mbithi_Mutave



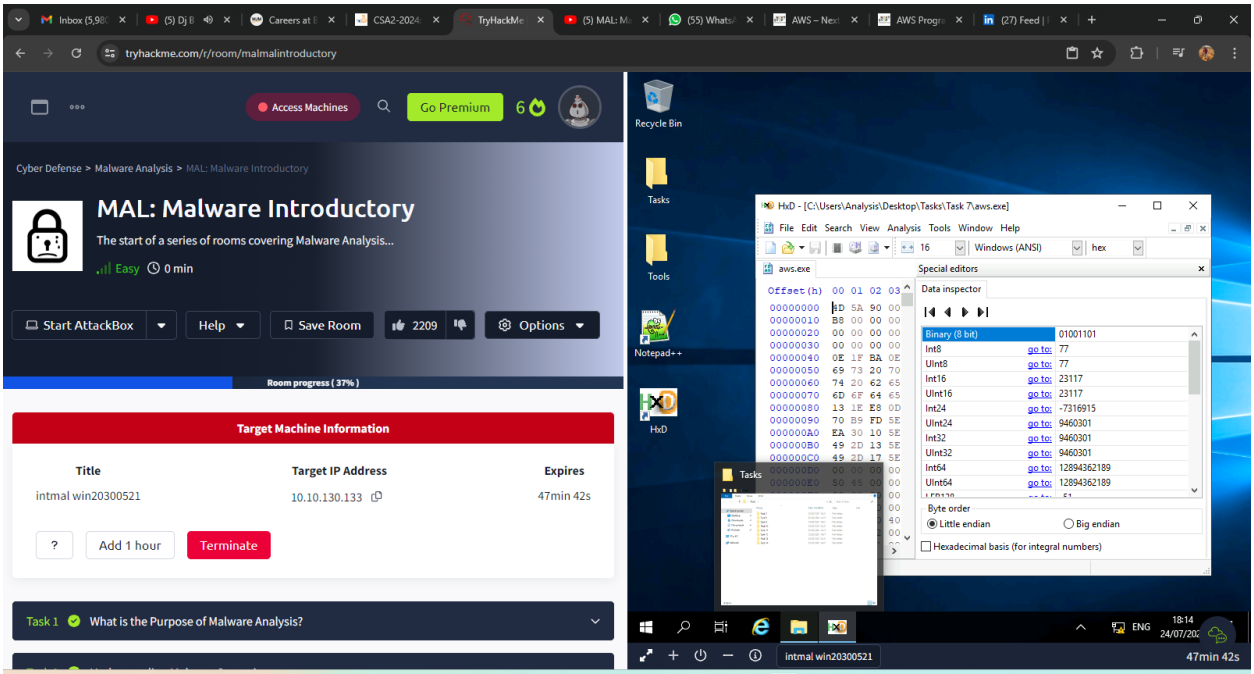
cs-sa07-24019
John_Mbithi_Mutave

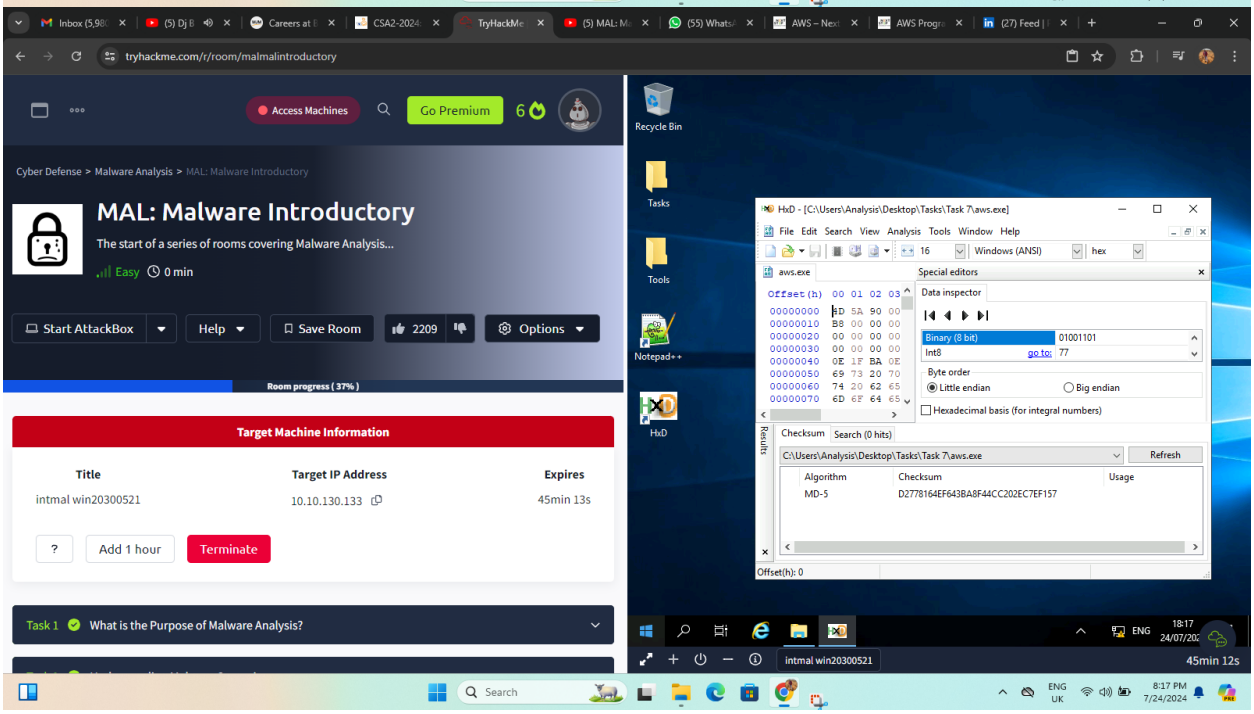


cs-sa07-24019
John_Mbithi_Mutave

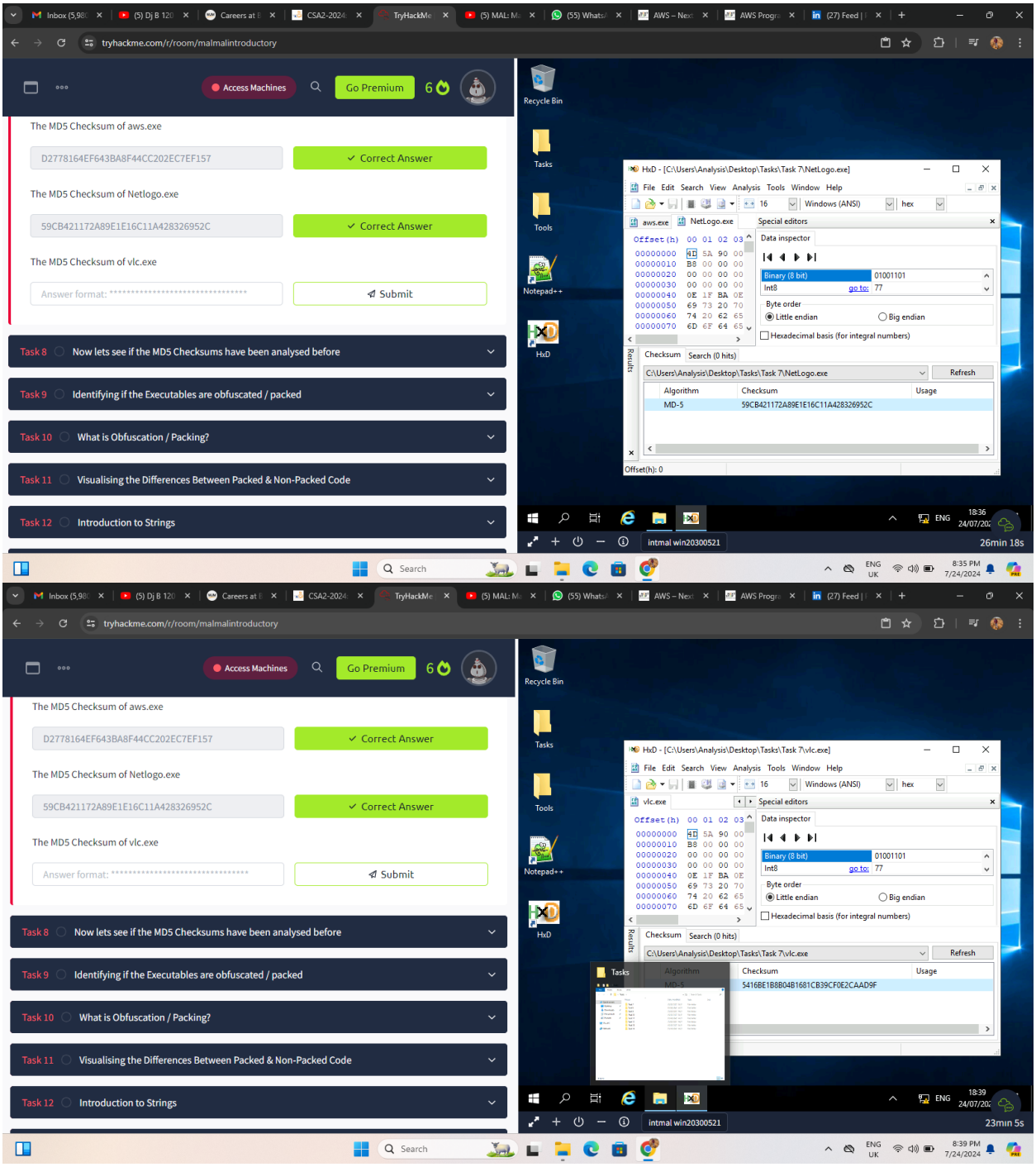


cs-sa07-24019
John_Mbithi_Mutave

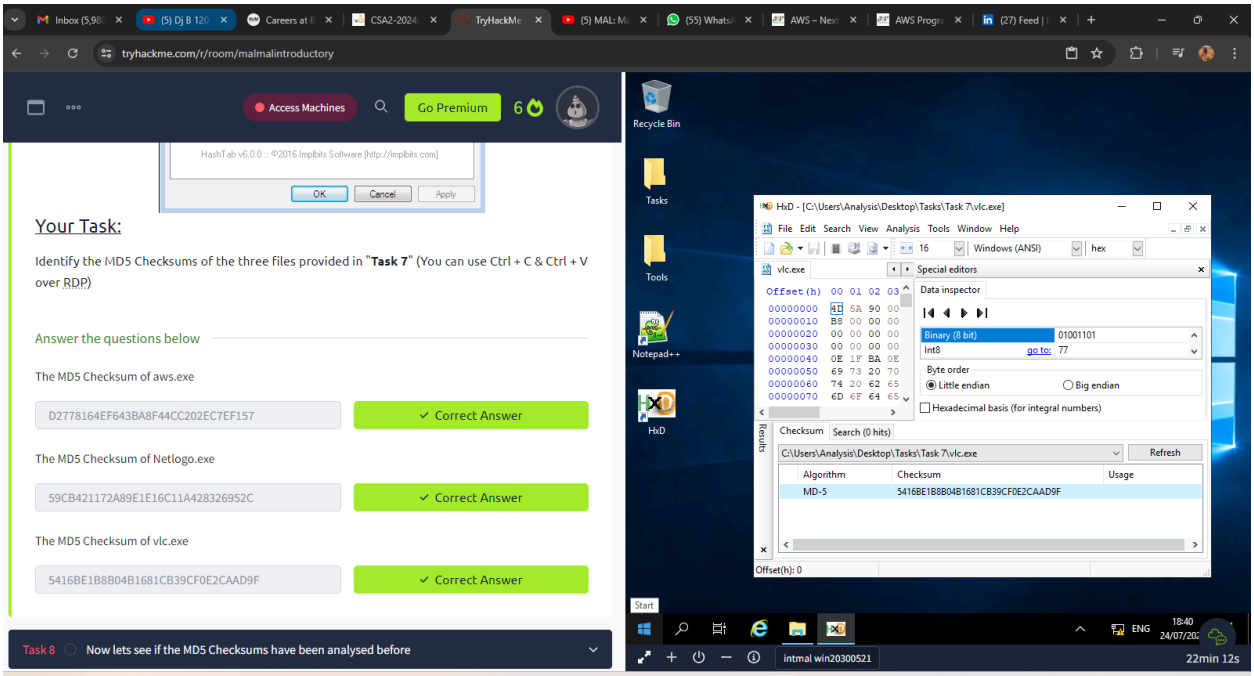


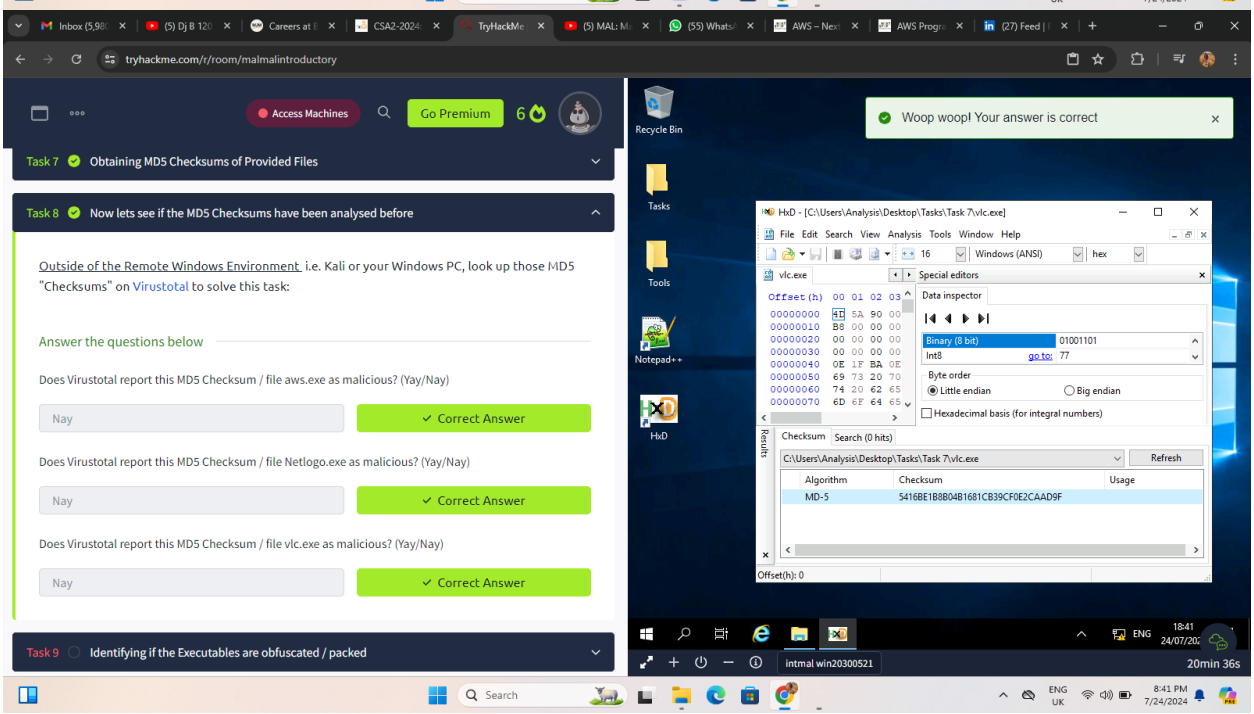


cs-sa07-24019
John_Mbithi_Mutave

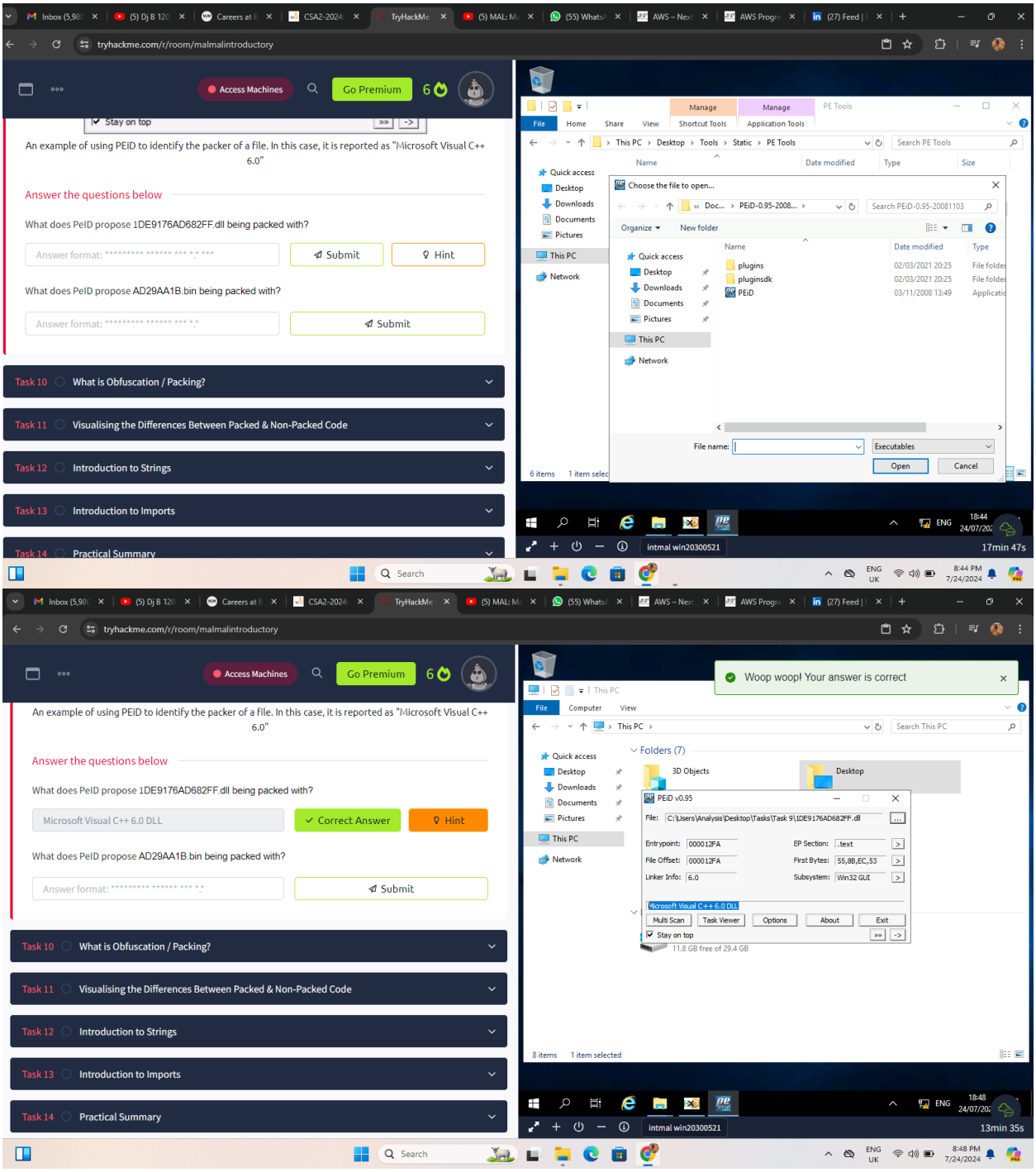


cs-sa07-24019
John_Mbithi_Mutave

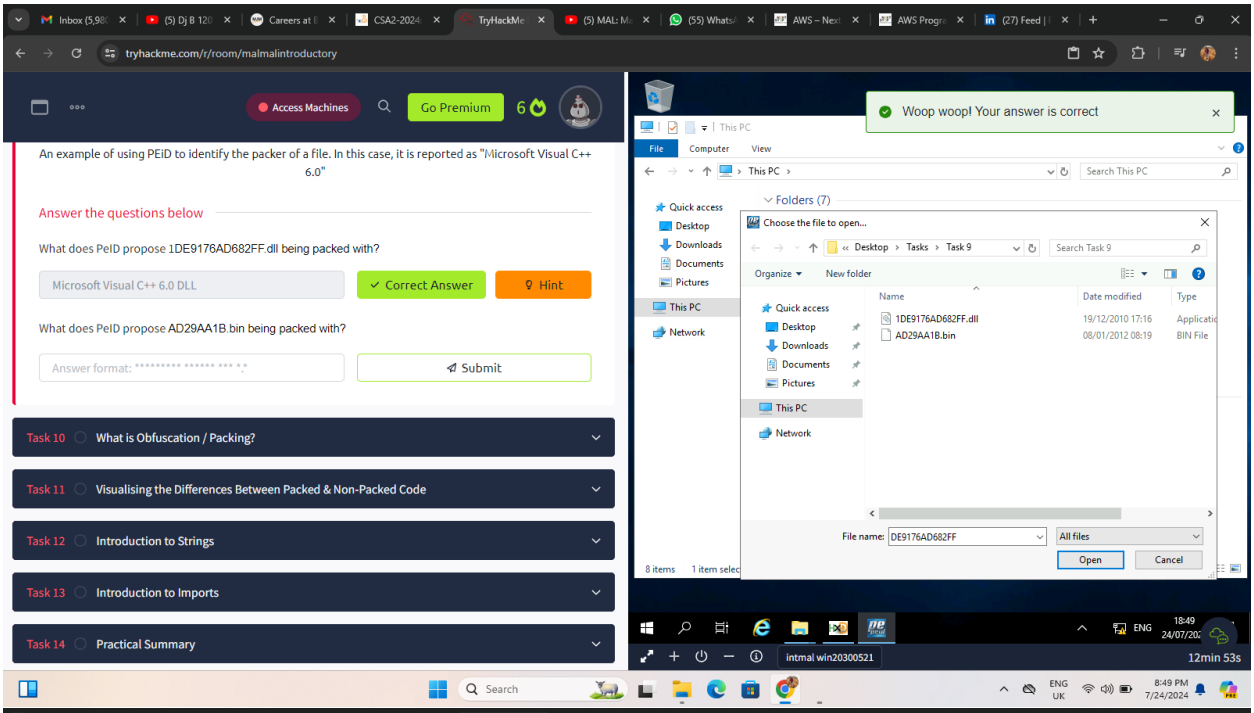


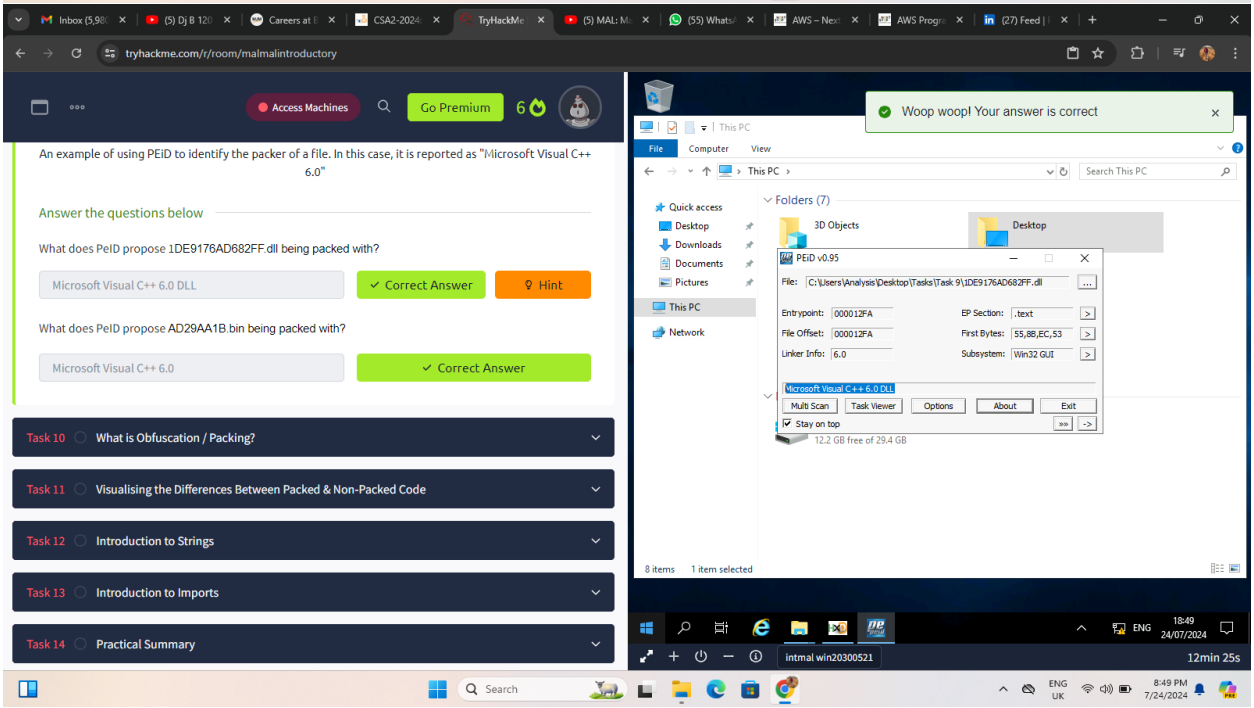


cs-sa07-24019
John_Mbithi_Mutave

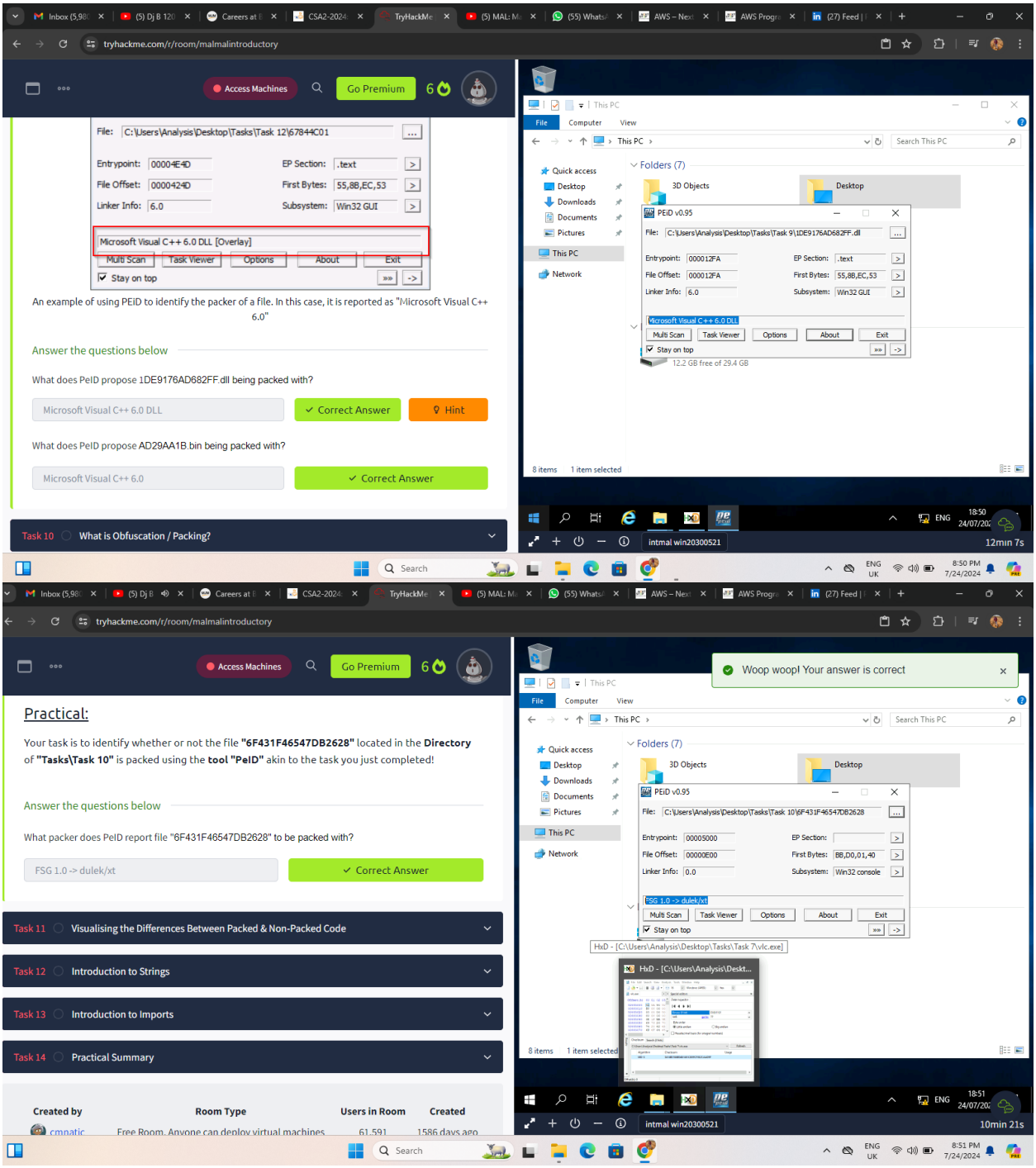


cs-sa07-24019
John_Mbithi_Mutave



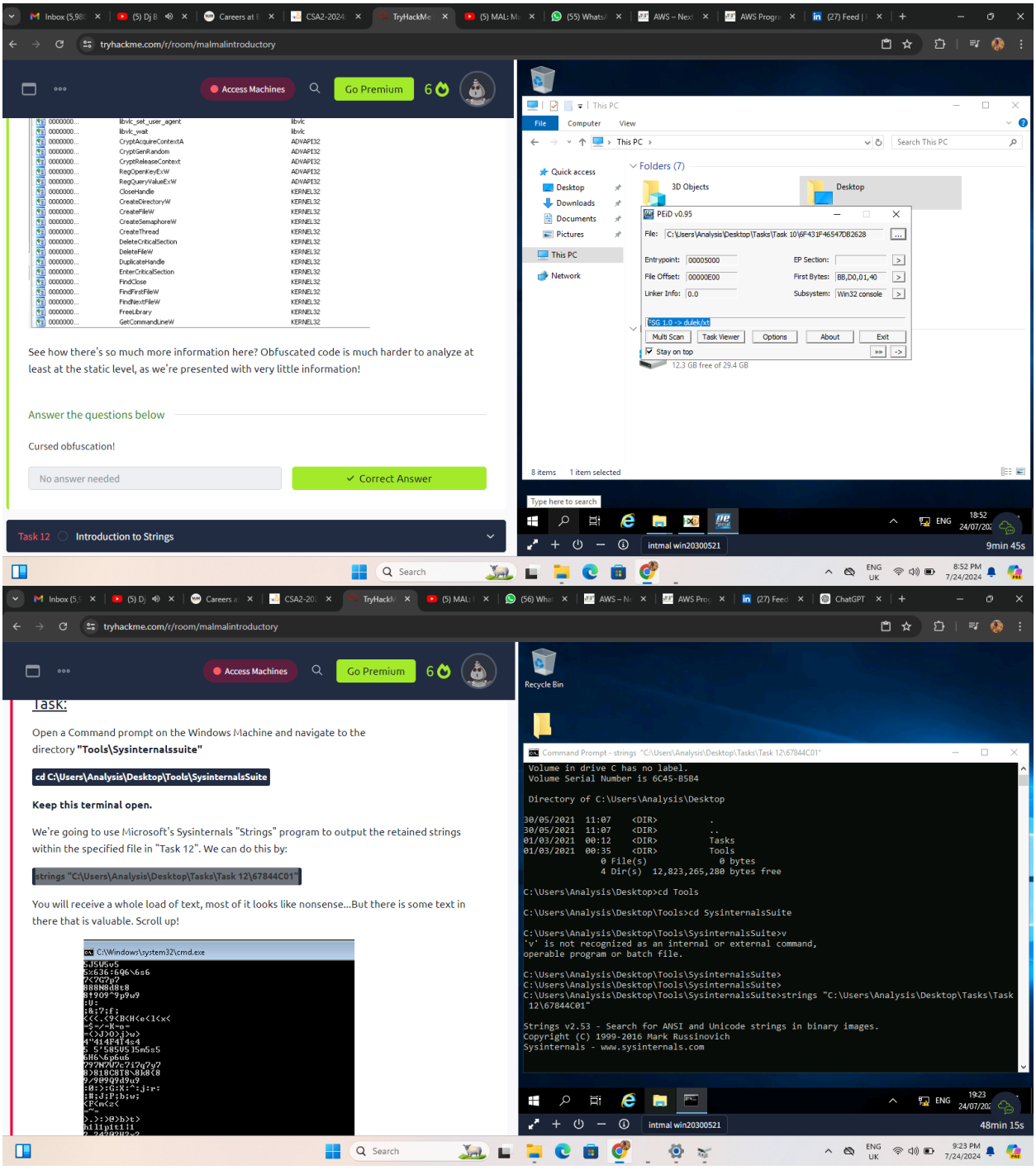


cs-sa07-24019
John_Mbithi_Mutave



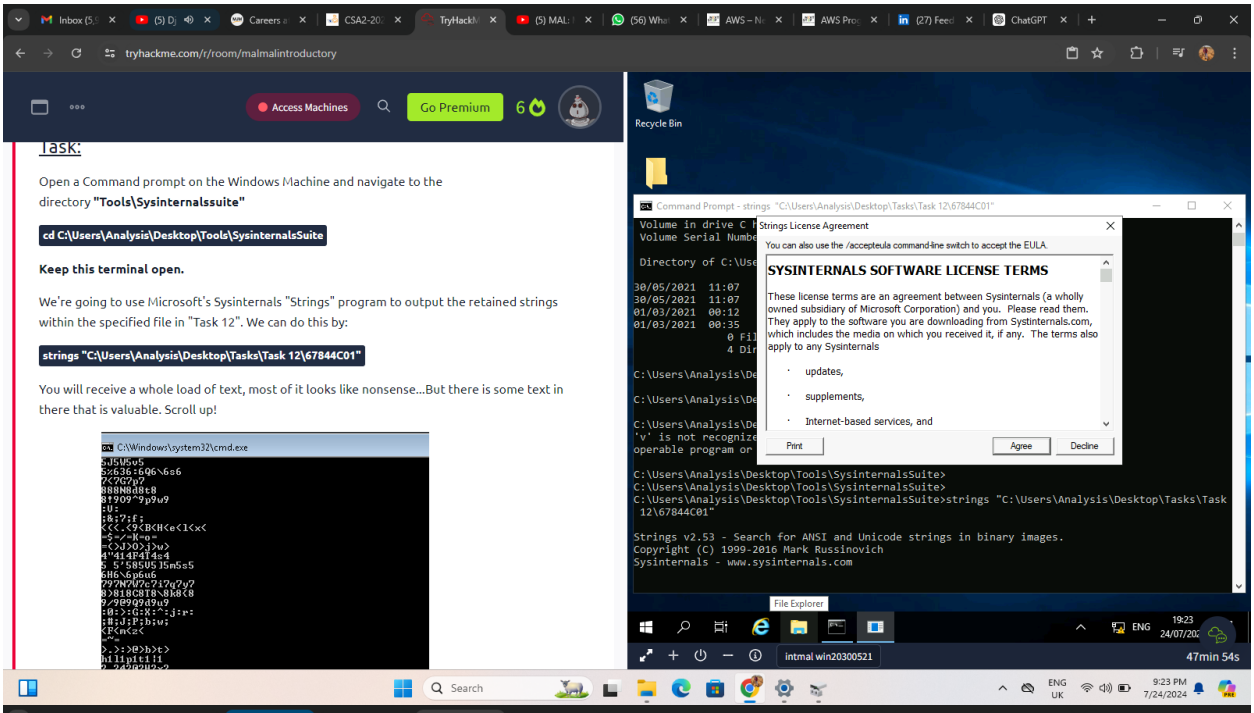
cs-sa07-24019

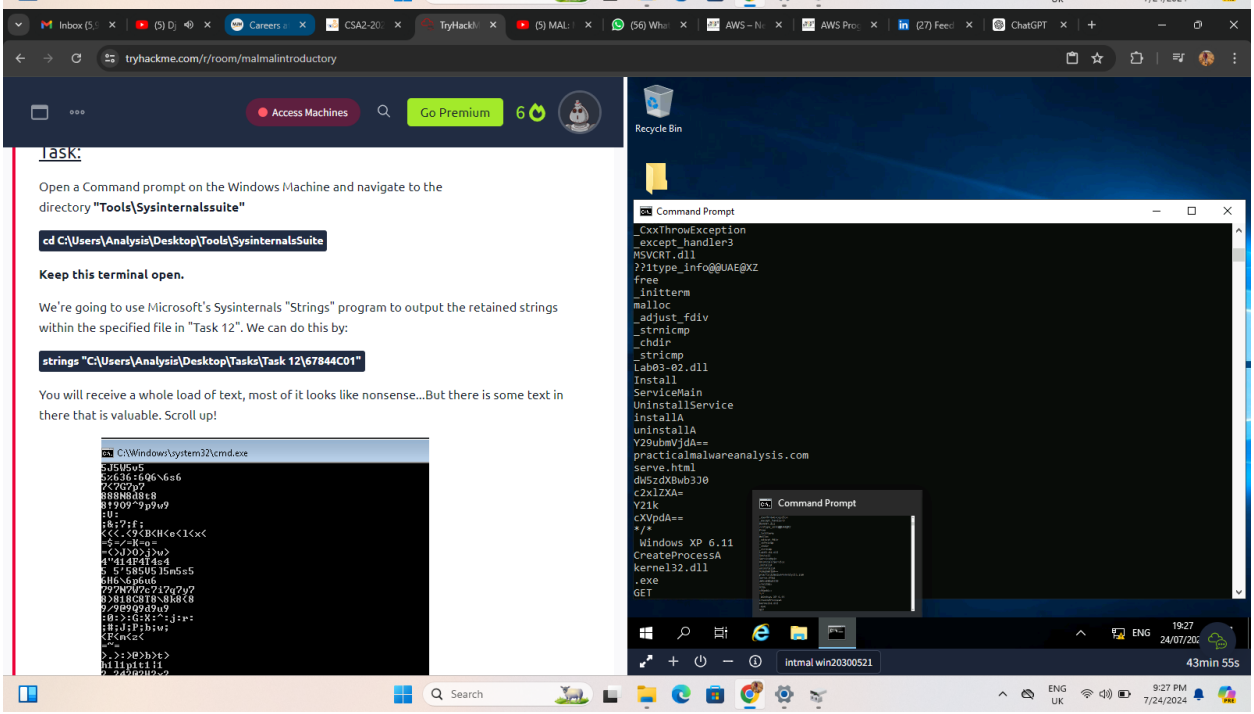
John_Mbithi_Mutave



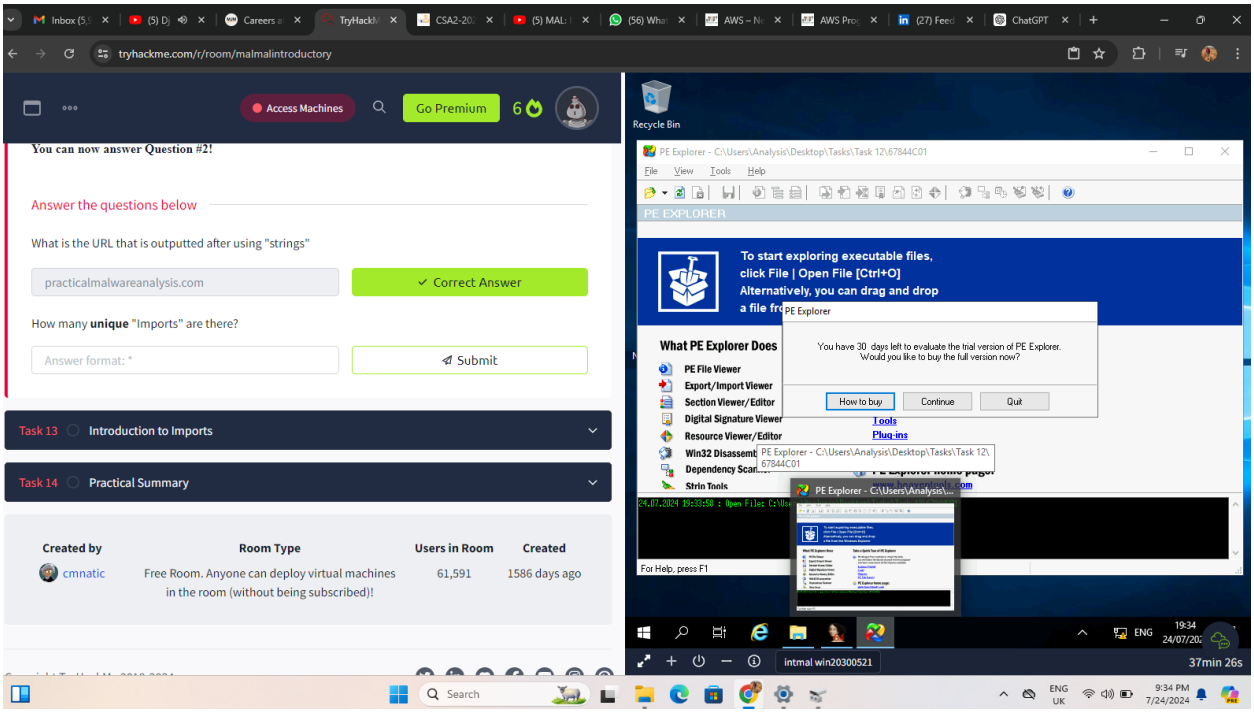
cs-sa07-24019

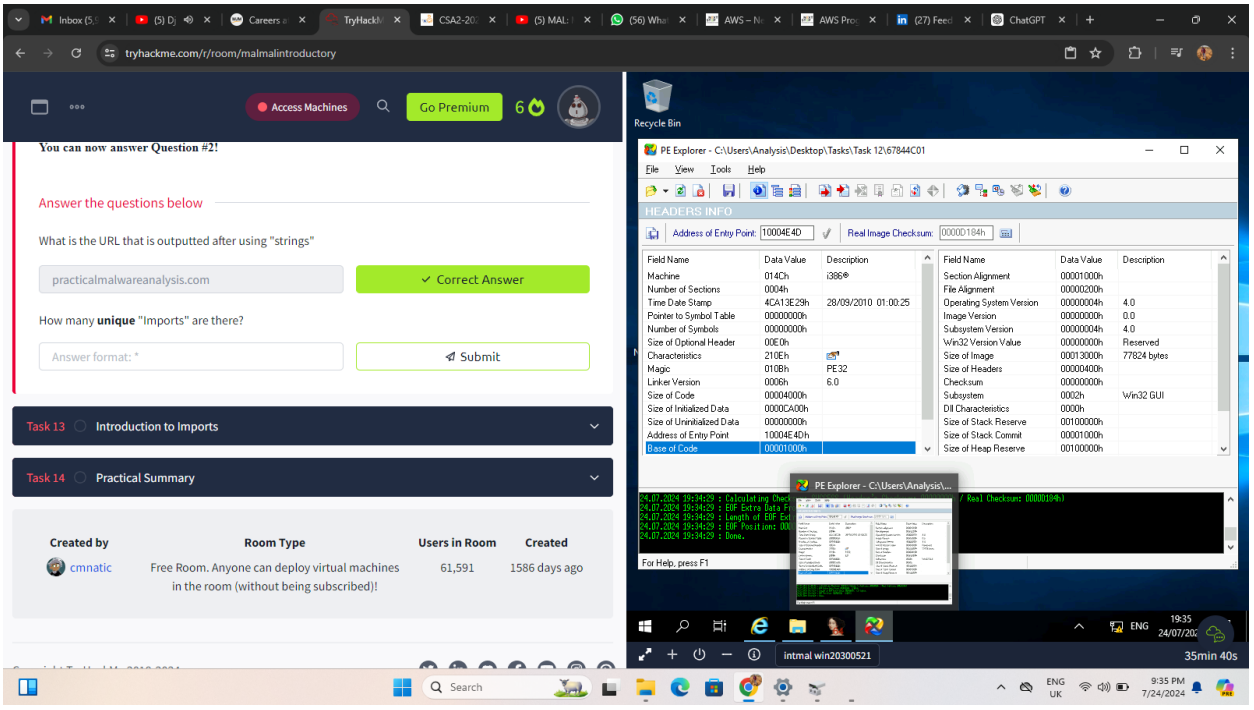
John_Mbithi_Mutave



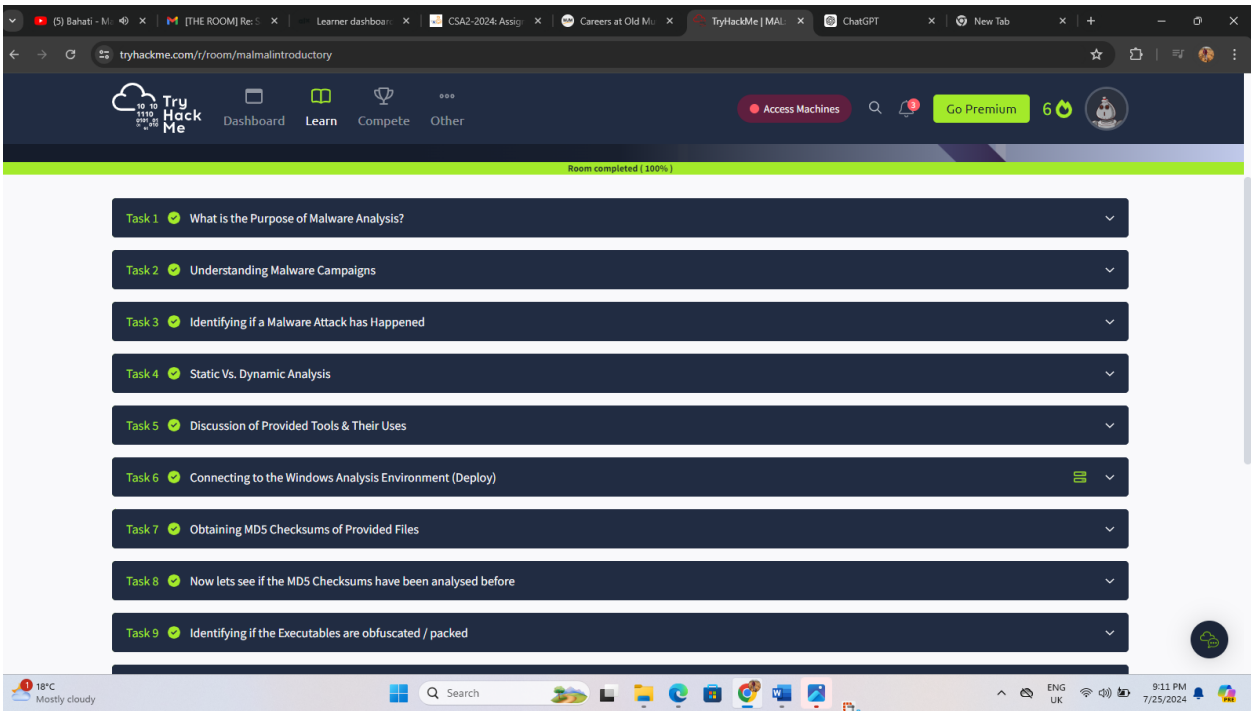


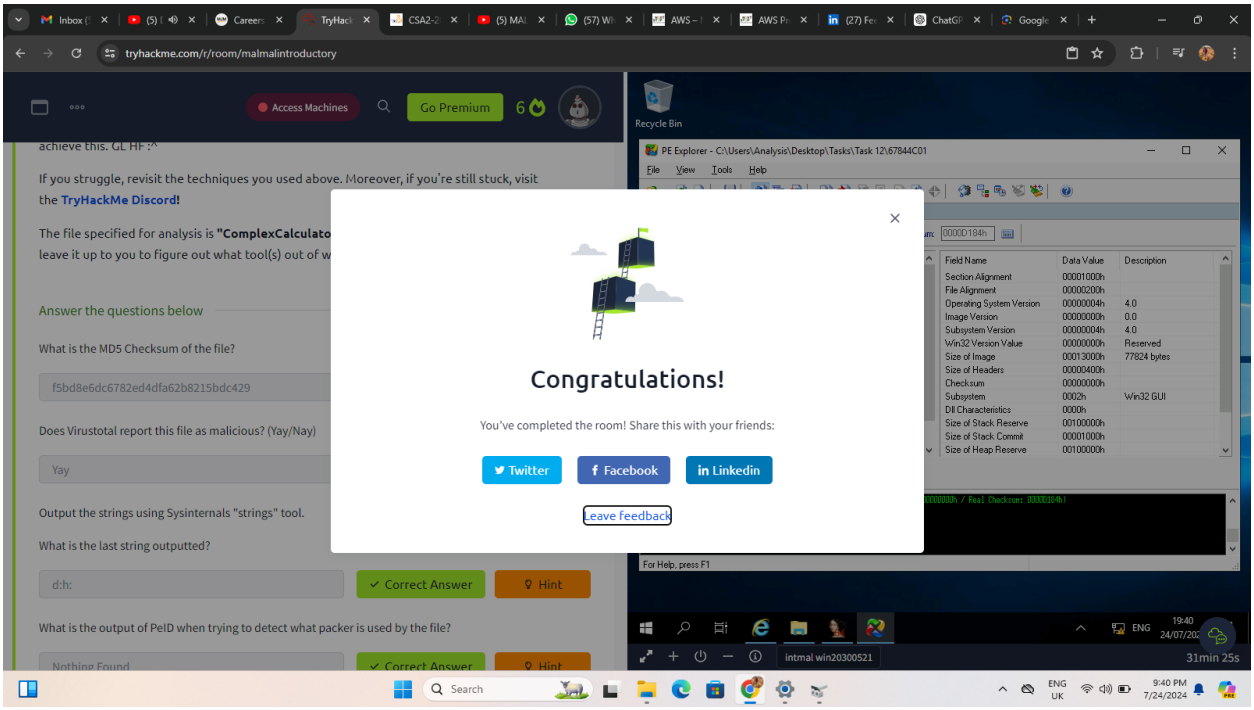
cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave





cs-sa07-24019
John_Mbithi_Mutave

Shareable Link - https://tryhackme.com/r/room/malmalintroductory

Conclusion

This comprehensive report provides an overview of key aspects related to malware analysis, from its purpose and techniques to practical considerations and tools used in the field. Each task addresses essential components necessary for understanding and combating malware threats effectively.