Ahmed Kasteer

20F-0336  BCS-7C

Information security

**Metasploit**

**INTRODUCTION:**

• One popular cybersecurity tool is Metasploit, which is a valuable resource for hackers at different phases of finding and fixing security flaws in computer systems.

There are two versions of Metasploit available: Metasploit Framework, which is free and runs on commands, and Metasploit Pro, which is a paid edition with an intuitive interface.

• It helps with data collection, vulnerability identification, and the development of novel system access techniques.

• "Msfconsole," or the command center; "Modules," or tools; and "Tools," or programs, are its main constituents.

•'msfvenom' is a useful tool for creating unique attacks.

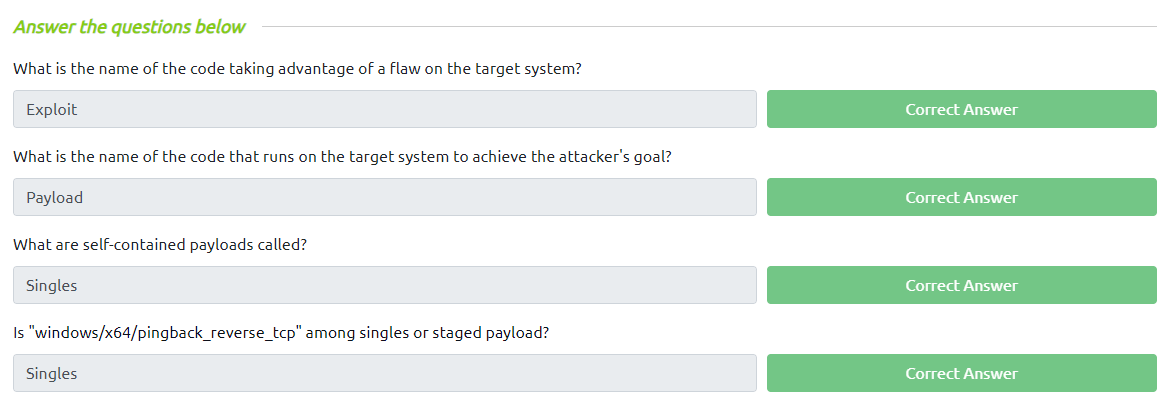
**TASK DESCRIPTION:**

* In the provided Metasploit room on TryHackMe, participants engage in different learning tasks focused on core Metasploit concepts and its key components.
* Metasploit is integral to every stage of penetration testing, and the components aiding in these phases include auxiliary, encoders, evasion, exploits, payloads, and posts.

**INSIGHTS:**

* Metasploit offers a range of functionalities through its command-line interface, known as 'msfconsole.' When launching 'msfconsole,' users enter a context-specific environment that allows them to execute various commands like 'ls' and 'ping,' conduct searches, and interact with modules such as exploits, payloads, and auxiliary tools.
* Each module operates within its specified parameters. The 'search' command is invaluable, enabling users to find relevant modules based on keywords, CVE numbers, or target systems. The framework's module ranking system provides insights into exploit reliability.

**SCREENSHOTS**



A screenshot of a chat

Description automatically generated

A white rectangular object with black lines

Description automatically generated with medium confidence

**Wireshark**

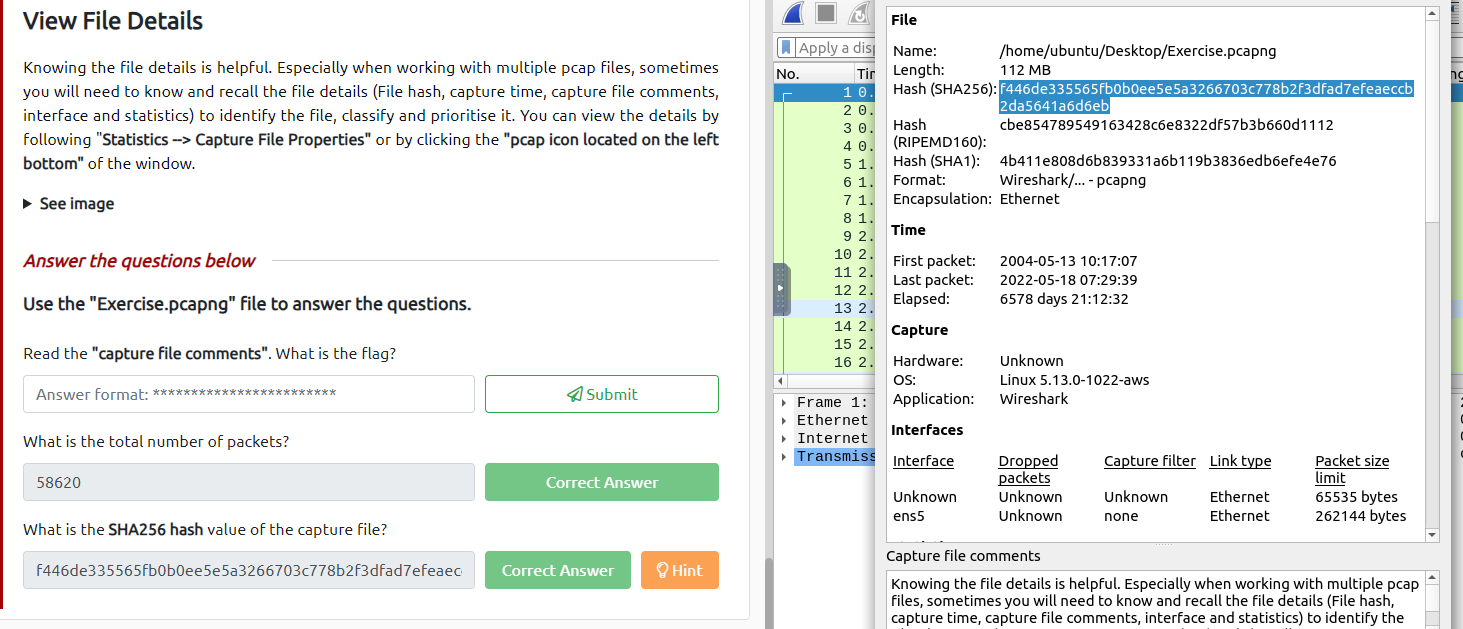
**INTRODUCTION:**

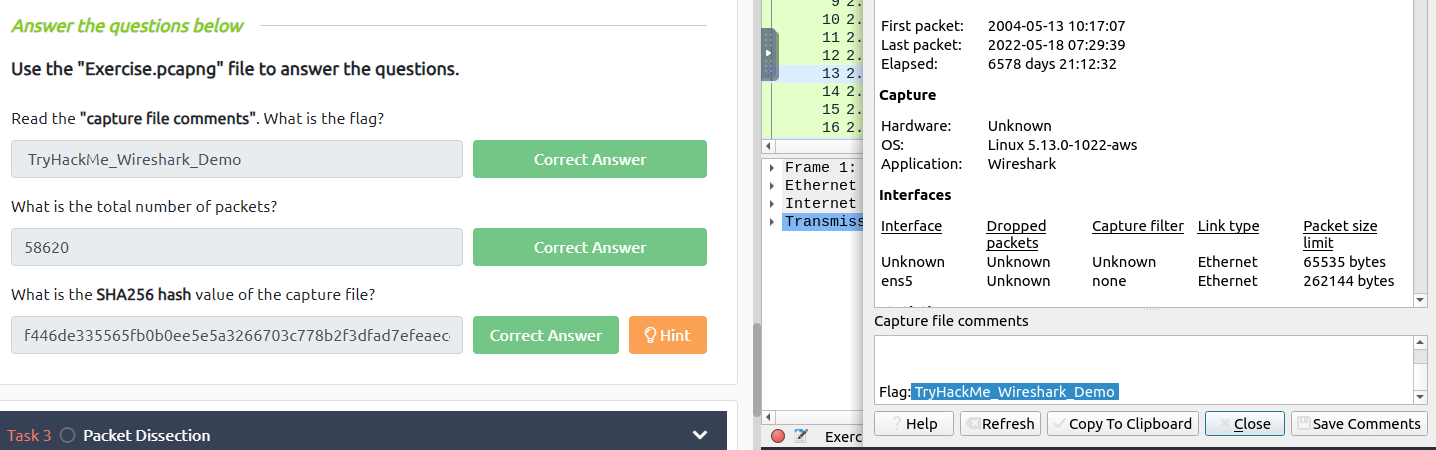
• One powerful tool for analyzing network protocols is Wireshark, which allows users to record and analyze data as it moves through a computer network in real time.This adaptable software offers comprehensive insights into network traffic, enabling users to examine data packets closely, identify possible security threats, fix network-related problems, and improve performance overall.For network administrators, cybersecurity specialists, and developers alike, Wireshark is an invaluable tool because of its user-friendly interface and extensive feature set.

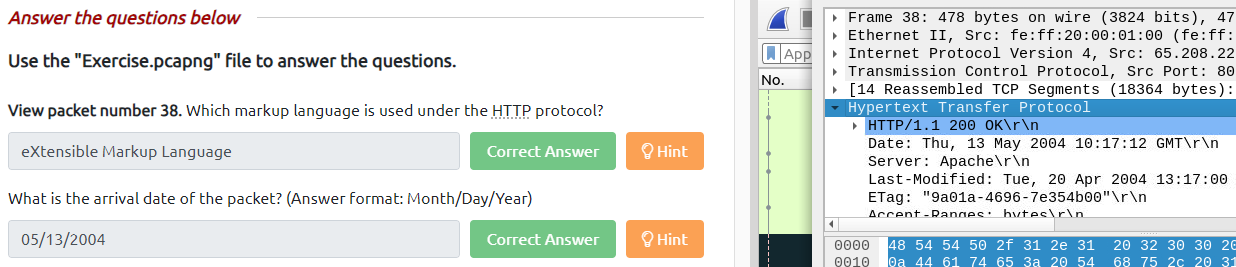
• It helps to ensure the efficiency and security of computer networks as well as to understand network behavior and diagnose network issues.

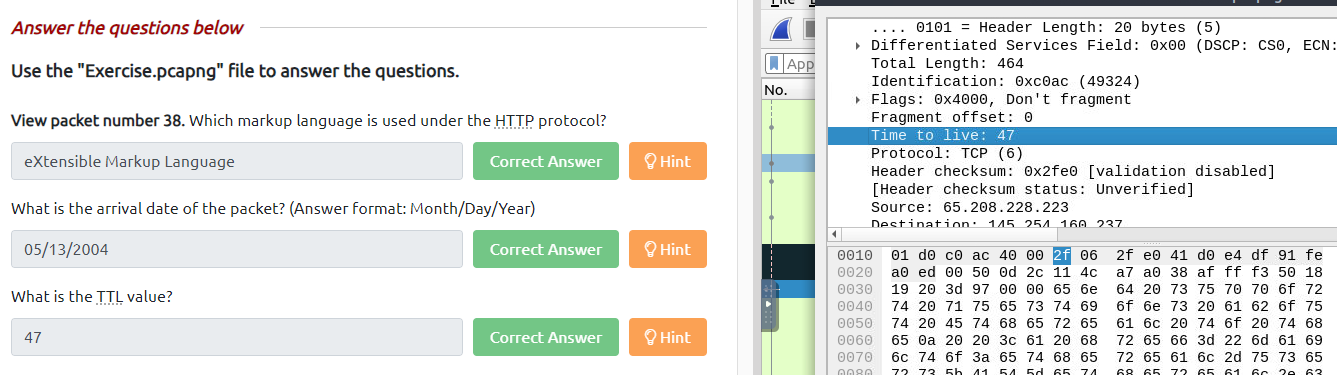
• In the fields of network forensics, protocol analysis, and network troubleshooting, Wireshark is a vital tool for anyone involved in the administration, security, or advancement of networked systems.

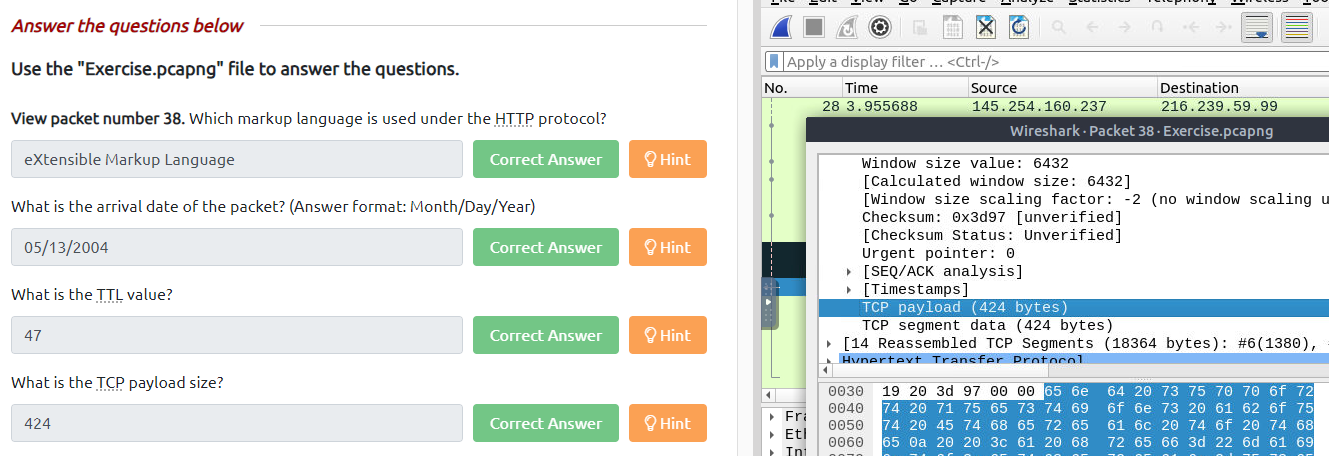
**SCREENSHOTS**

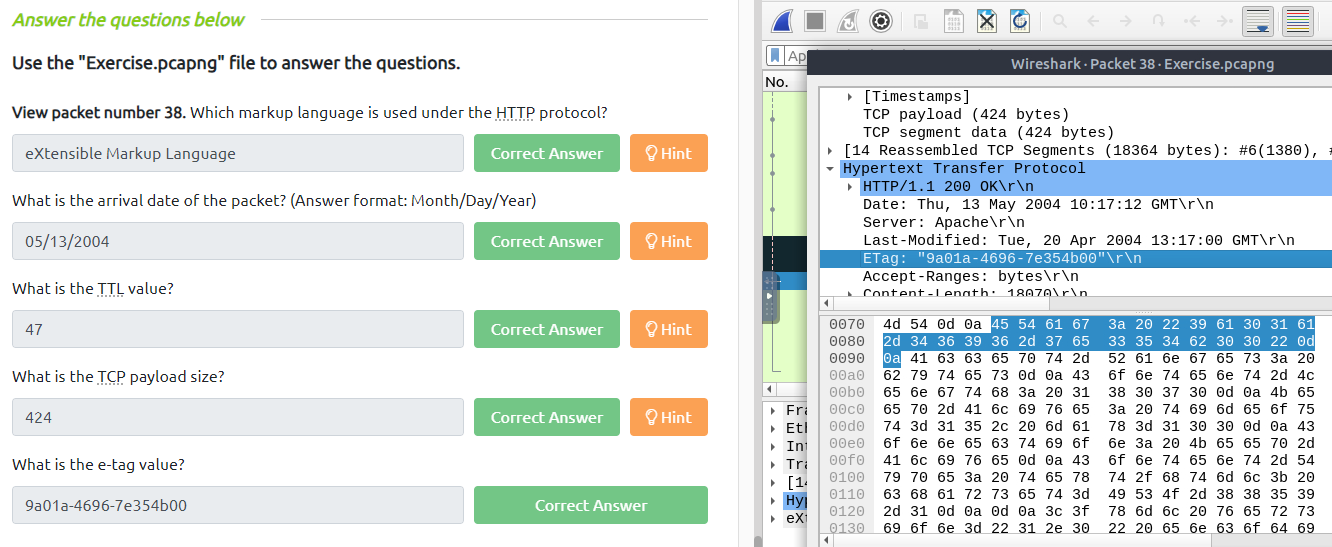


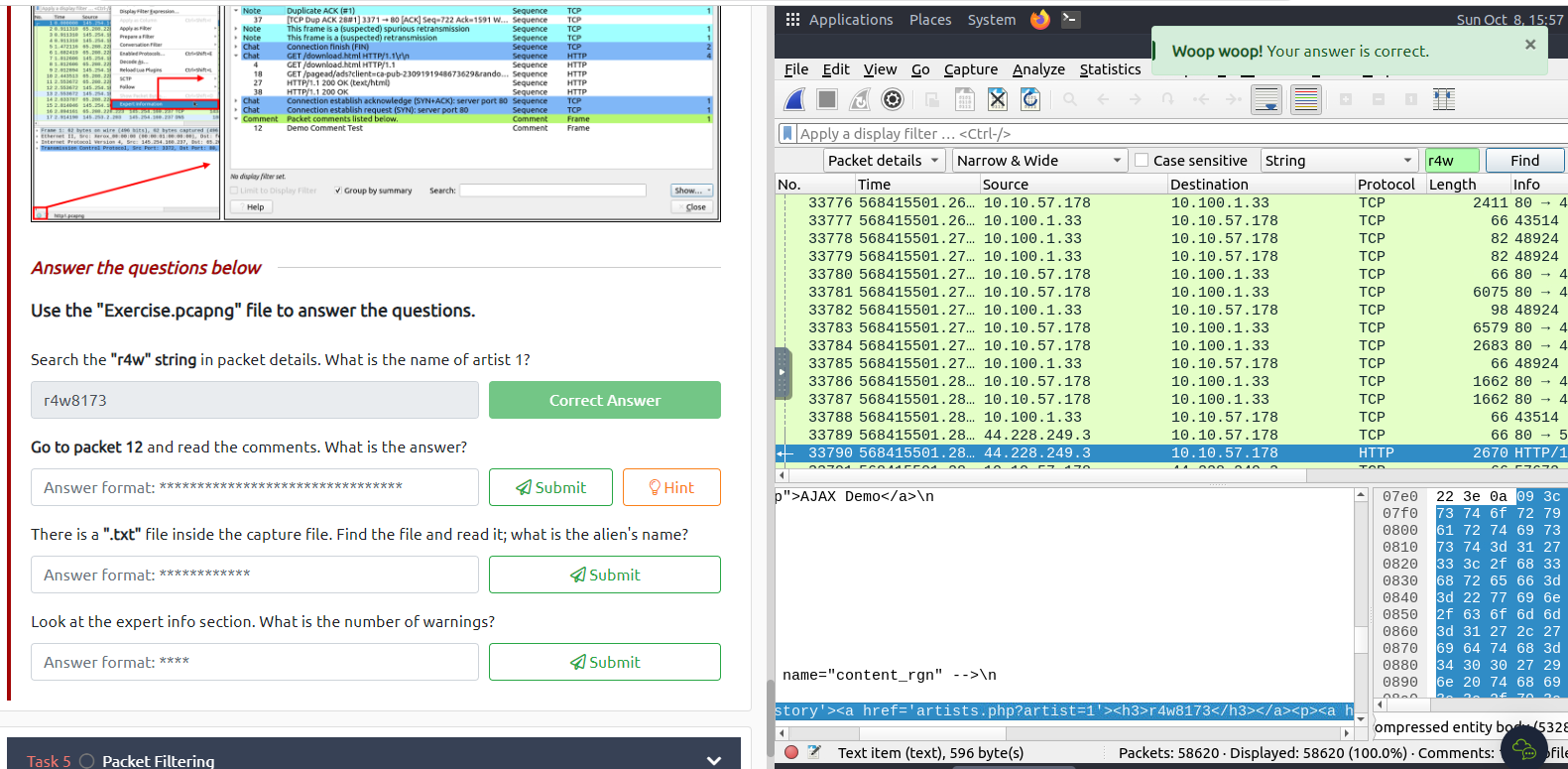


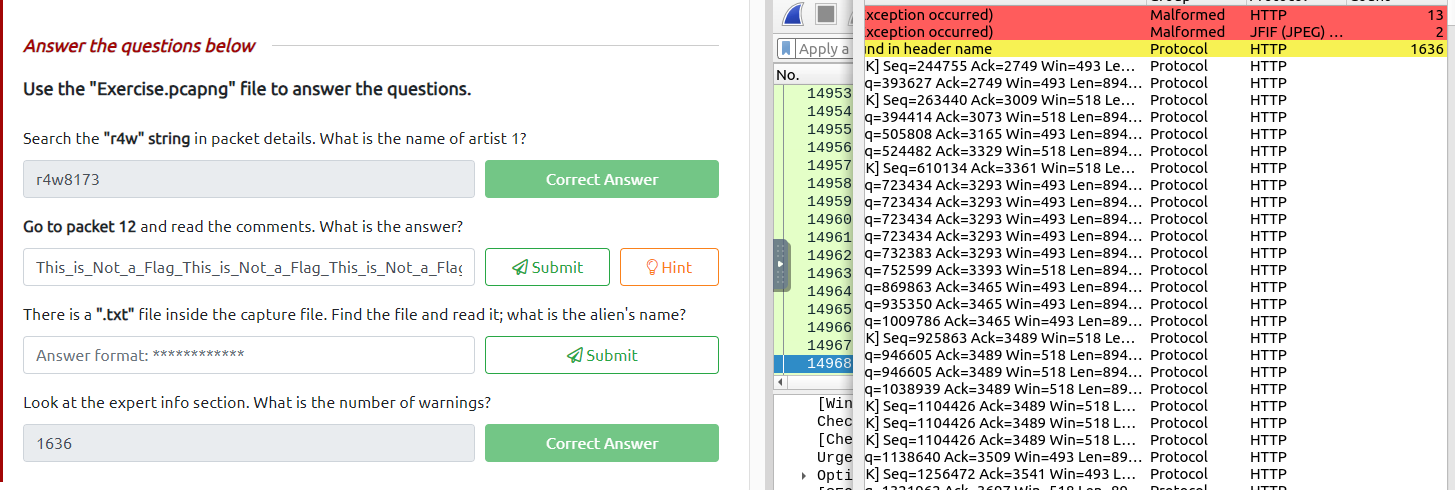


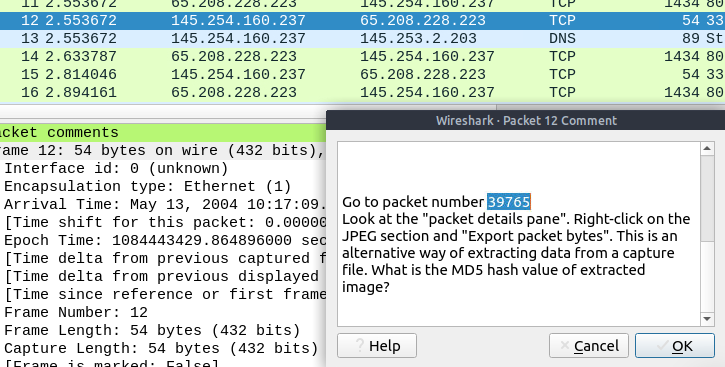


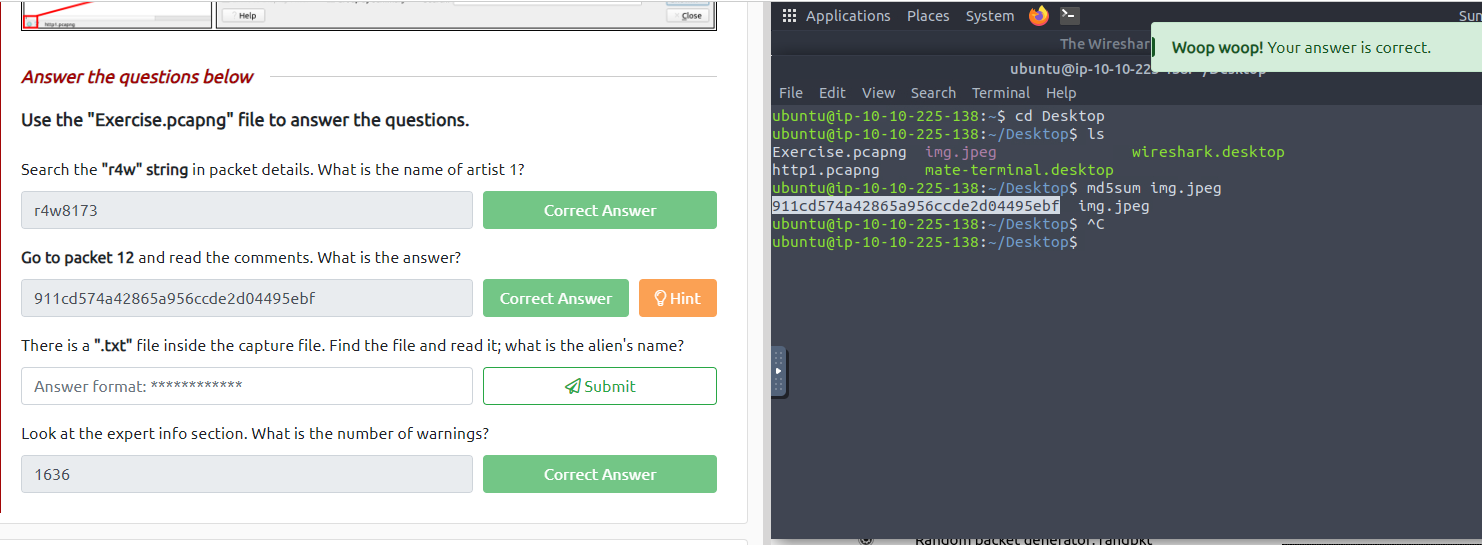


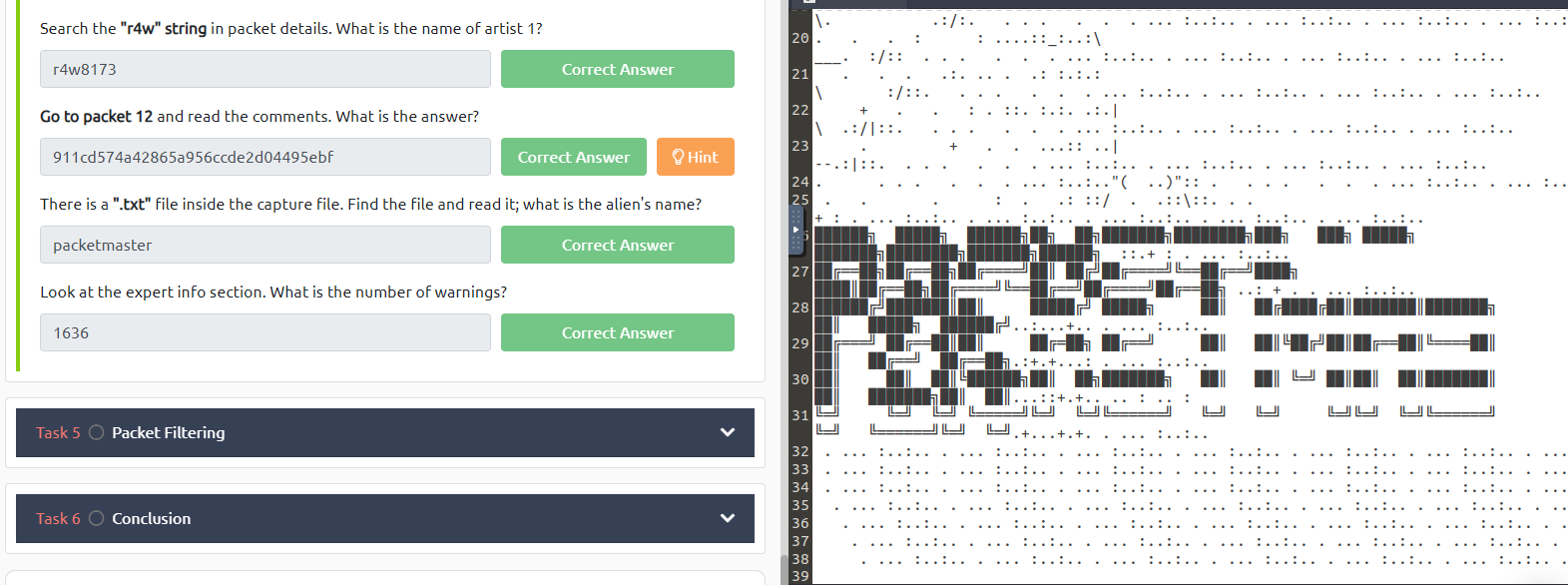


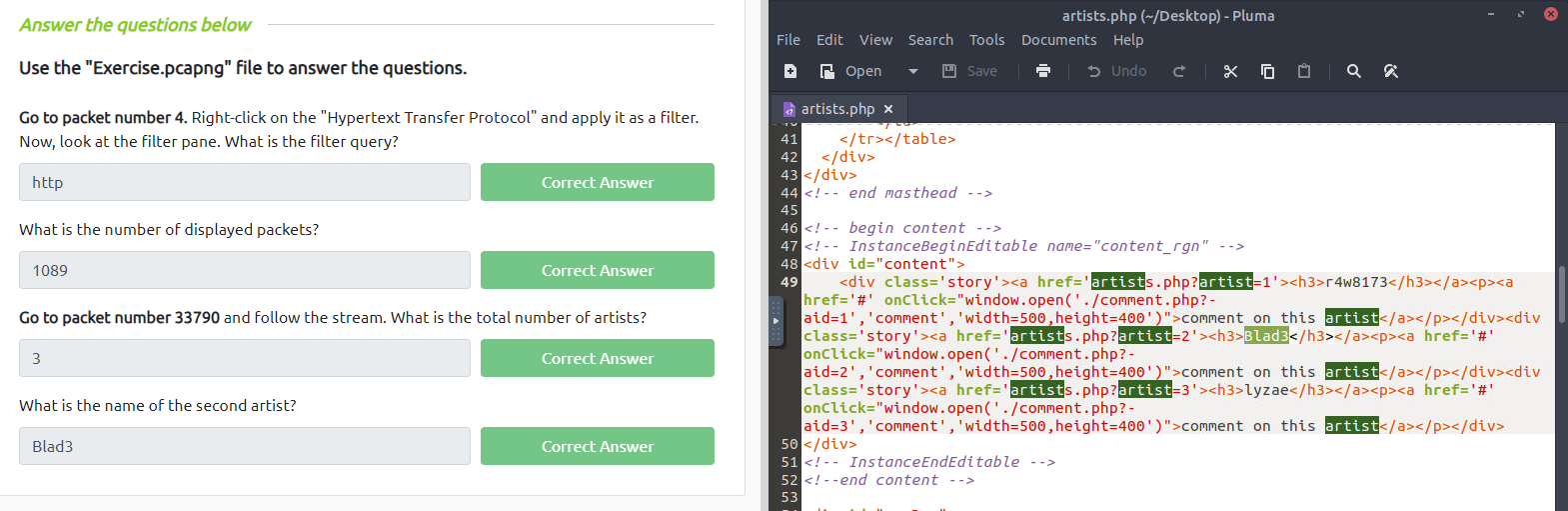












**Netcat**

**INTRODUCTION:**

Netcat is a powerful tool that is used by hackers, security professionals, and network administrators alike. This multipurpose tool is well known for its ability to create and manage network connections in a variety of ways. Netcat clarifies the use of essential networking tools such as ping, traceroute, telnet, and its own features. It also highlights the importance of reconnaissance during the early phases of penetration testing. It accomplishes this by using networking commands, developer tools, and useful browser extensions.

**TASK DESCRIPTION:**

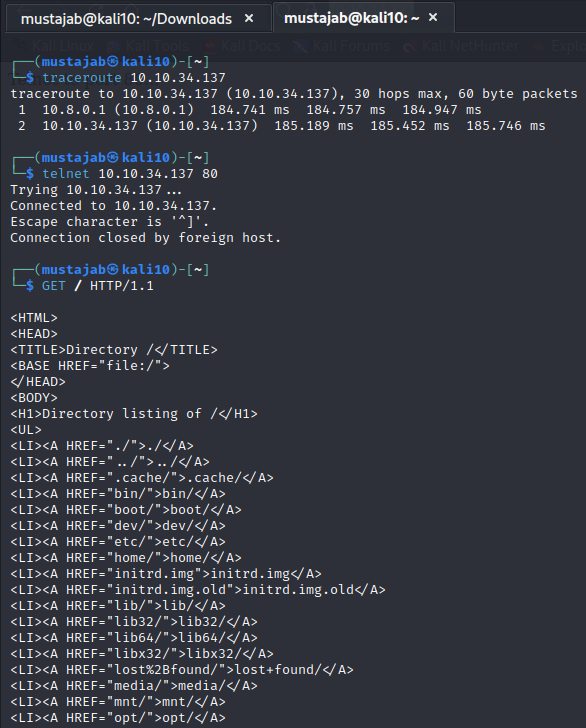
In the TryHackMe Netcat room, users are presented with a variety of educational tasks that center on using developer tools and commands in a real-world setting. The space is intended to support a thorough grasp of web development tools as well as the capabilities and applications of different networking commands, including Netcat, ping, telnet, and traceroute.

**INSIGHTS:**

The Netcat room provides an invaluable window into the world of active cybersecurity reconnaissance. It gives participants the know-how of fundamental enumeration and scanning methods for evaluating network security. Moreover, it raises awareness about potential security flaws in web services and applications.

**LIMITATIONS OR CONSIDERATIONS:**

Although active reconnaissance is very important in cybersecurity, there are some restrictions and moral issues to take into account. First and foremost, active reconnaissance must be carried out within the law and with the necessary authorizations. Active reconnaissance techniques come in a variety of resource-intensive forms that may interfere with network operations. Additionally, it's crucial to use caution because active reconnaissance tools occasionally deliver false information that could waste time.



A screenshot of a computer program

Description automatically generated