cs-sa07-24019
John_Mbithi_Mutave

WiFi Hacking 101

Task 1: The Basics - An Intro to WPA

Objectives:

- Understand the fundamental concepts of WPA (Wi-Fi Protected Access) and WPA2.
- Learn about the differences between WEP, WPA, and WPA2 encryption standards.

Key Takeaways:

- **WPA and WPA2**: Both provide strong security for wireless networks, with WPA2 being an improved version of WPA, using AES for encryption.
- **WEP vs. WPA/WPA2**: WEP is outdated and less secure compared to WPA/WPA2. WPA2 is currently the most secure standard.

Task 2: You're Being Watched - Capturing Packets to Attack

Objectives:

- Learn how to capture wireless data packets.
- Understand the importance of packet capturing in the context of wireless security.
- Use tools to capture packets for further analysis.

Key Takeaways:

- **Packet Capturing**: This process involves intercepting and logging traffic that passes over a wireless network.
- **Tools Used**: Tools like airodump-ng are essential for capturing data packets. These tools can capture the handshake packets required for WPA/WPA2 attacks.

Steps:

1. **Setting Up**: Prepare the environment by configuring the wireless network interface card (NIC) to monitor mode.

2. **Capturing Packets**: Use airodump-ng to capture packets from the target network. Look for handshake packets which are critical for cracking WPA/WPA2 encryption.

Task 3: Aircrack-ng - Let's Get Cracking

Objectives:

- Use captured packets to attempt decryption.
- Understand how to use aircrack-ng to crack WPA/WPA2 passwords.

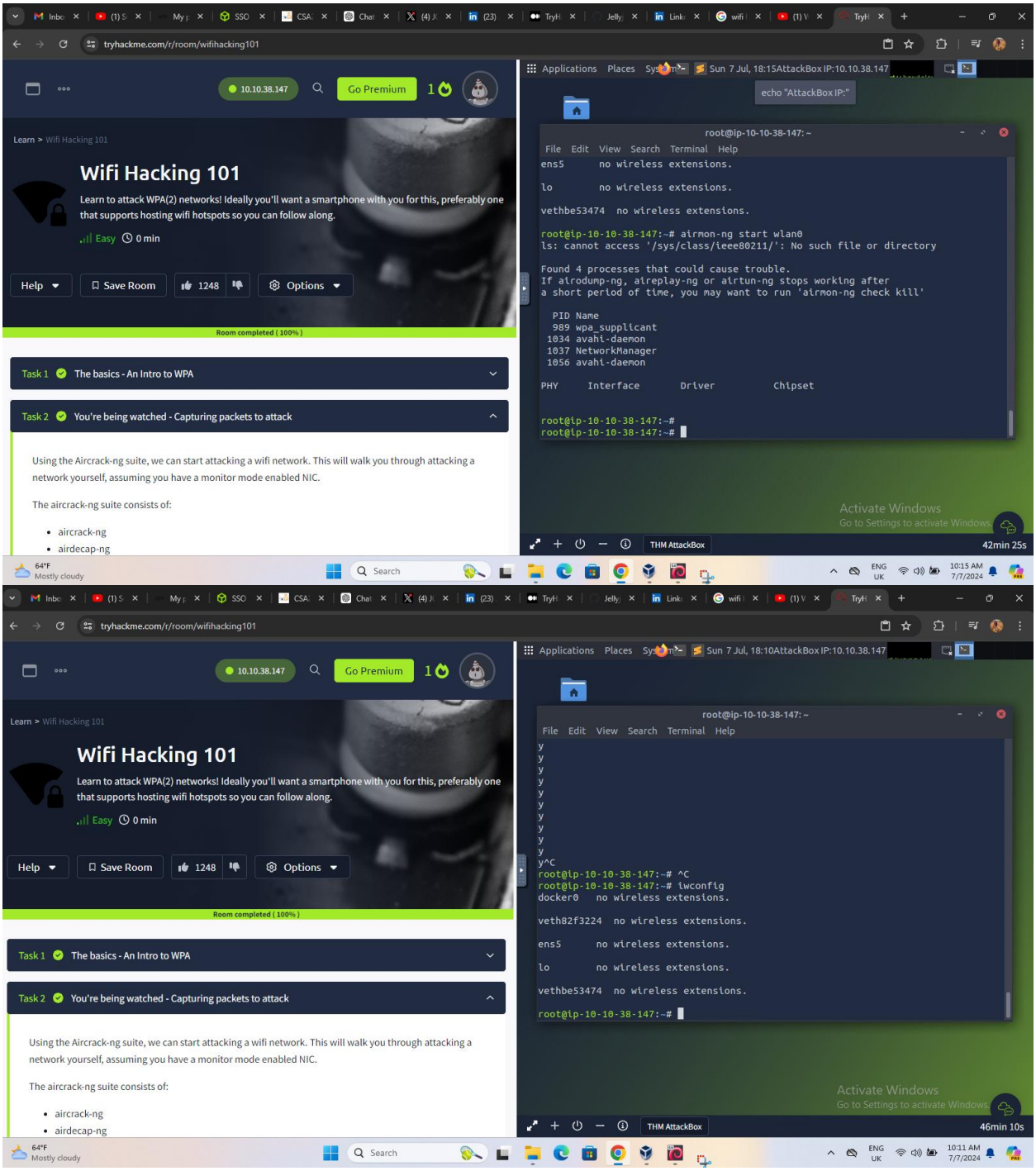
Key Takeaways:

- **Aircrack-ng**: A powerful suite of tools used for auditing wireless networks. It is particularly useful for cracking WEP and WPA/WPA2-PSK keys.
- **Decryption Process**: Once the handshake packets are captured, aircrack-ng can be used to perform a dictionary attack on the captured data to find the network key.

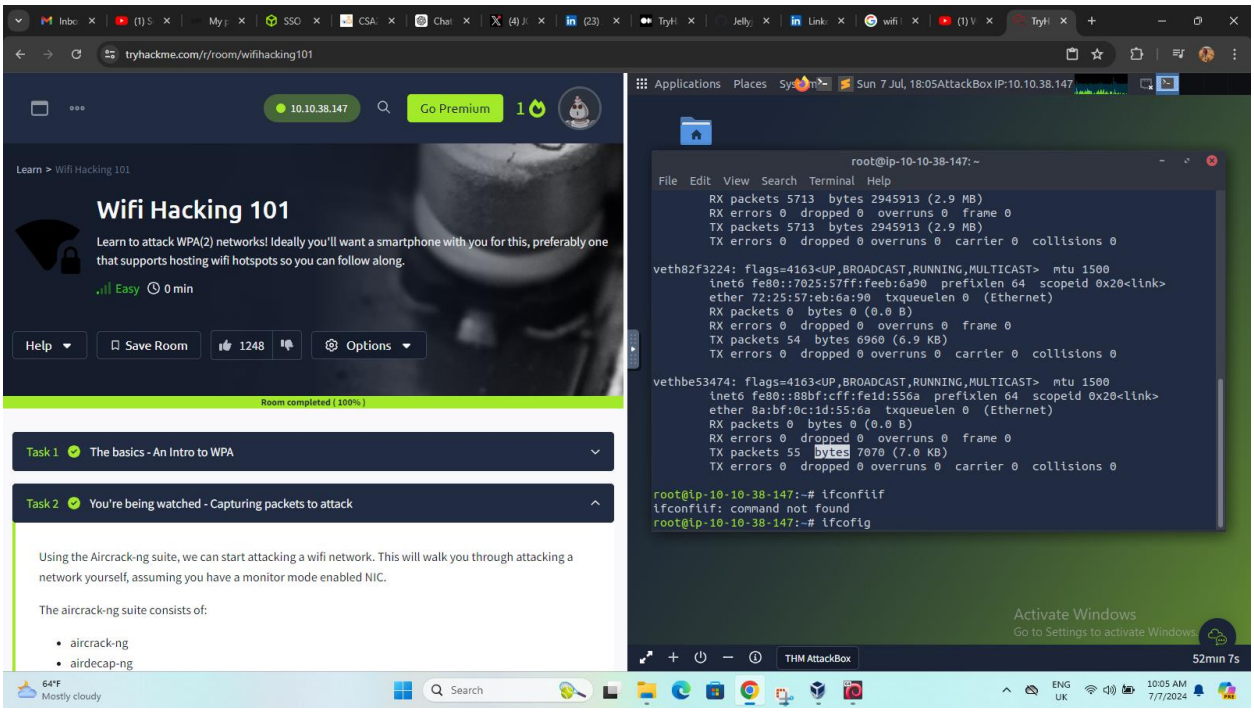
Steps:

1. **Using Aircrack-ng**: Run aircrack-ng with the captured handshake file and a wordlist to attempt to crack the WPA/WPA2 password.
2. **Successful Decryption**: If the correct password is in the wordlist, aircrack-ng will find it and display the WPA/WPA2 key.

cs-sa07-24019
John_Mbithi_Mutave

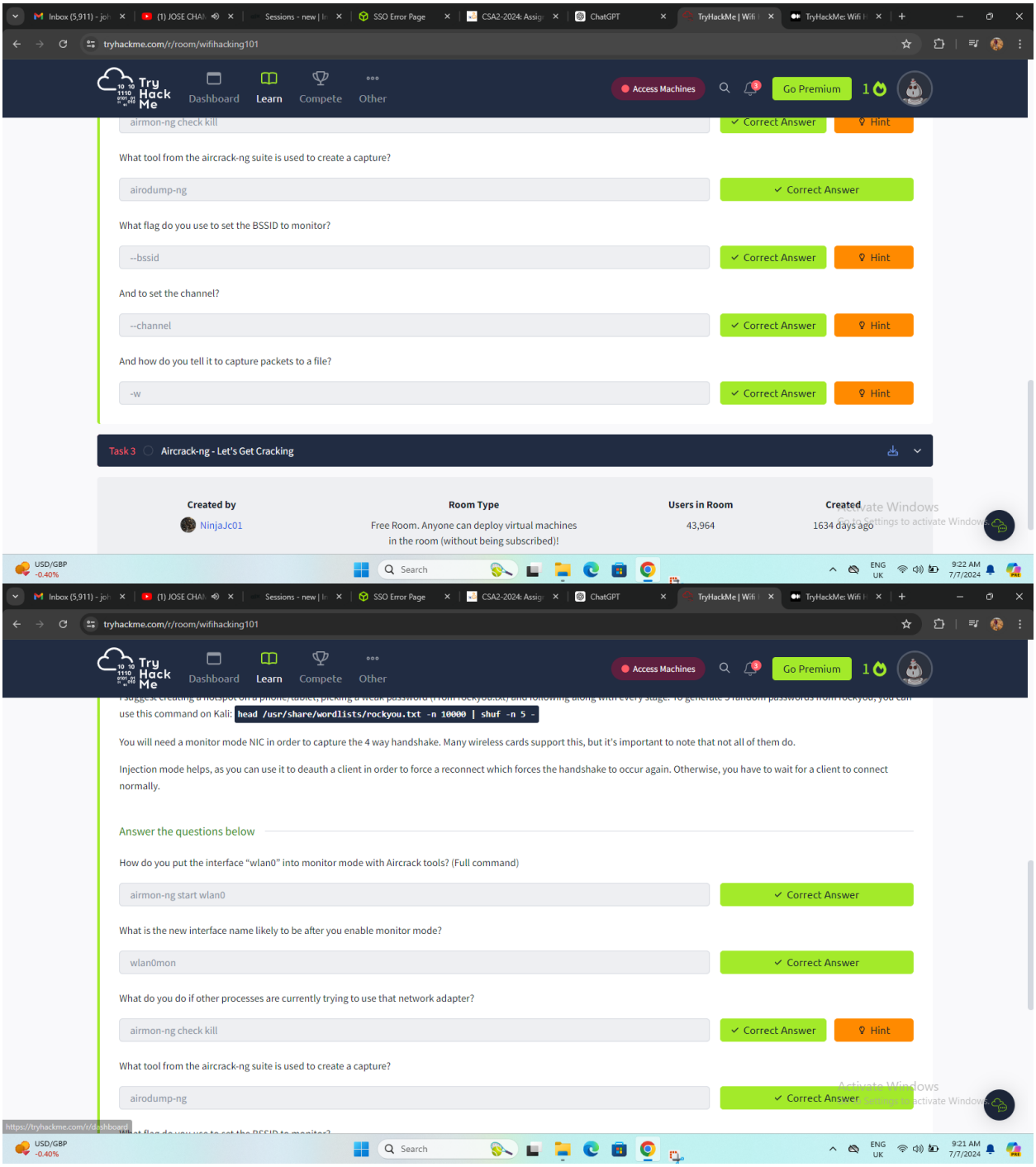


cs-sa07-24019
John_Mbithi_Mutave

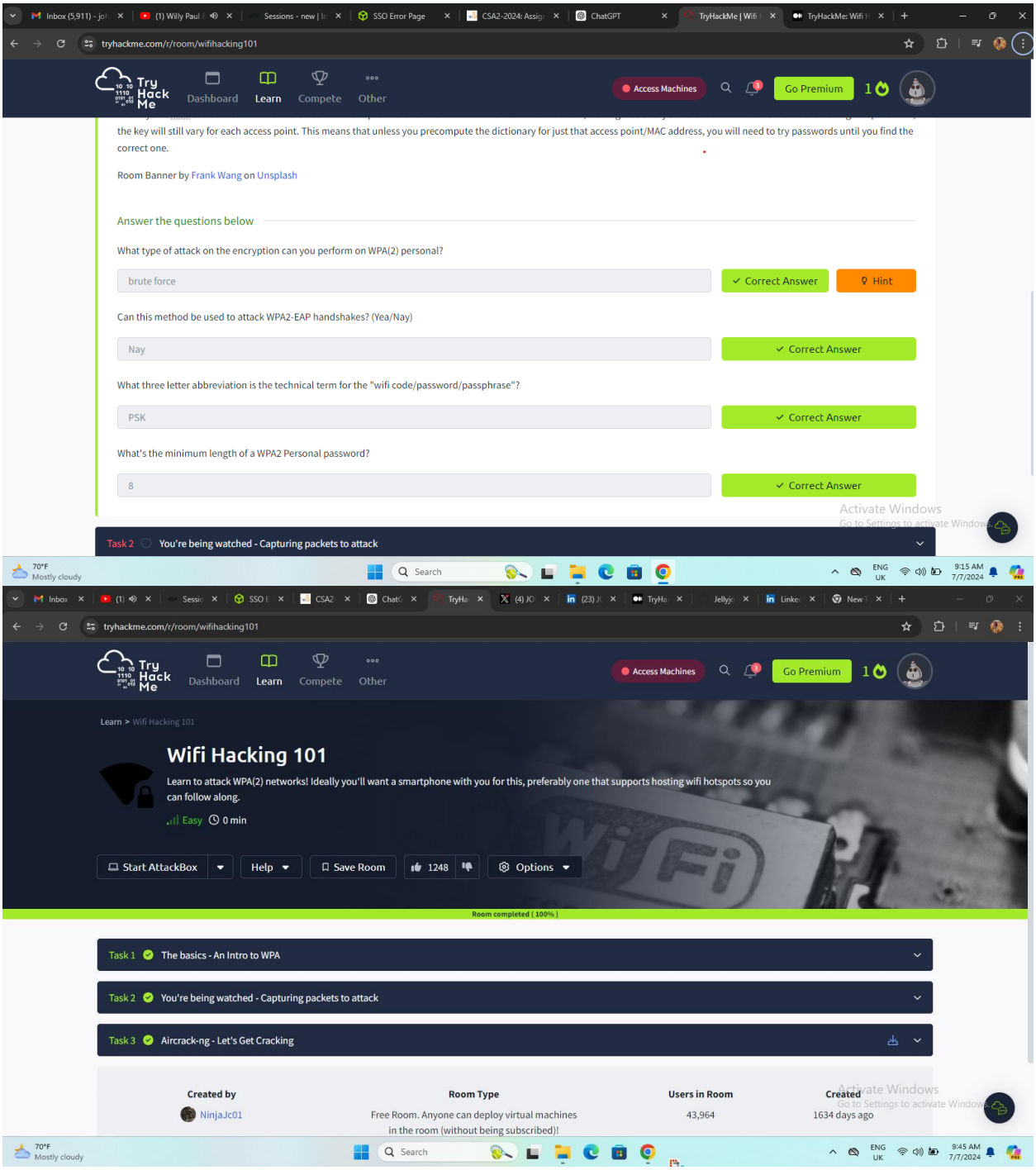


cs-sa07-24019

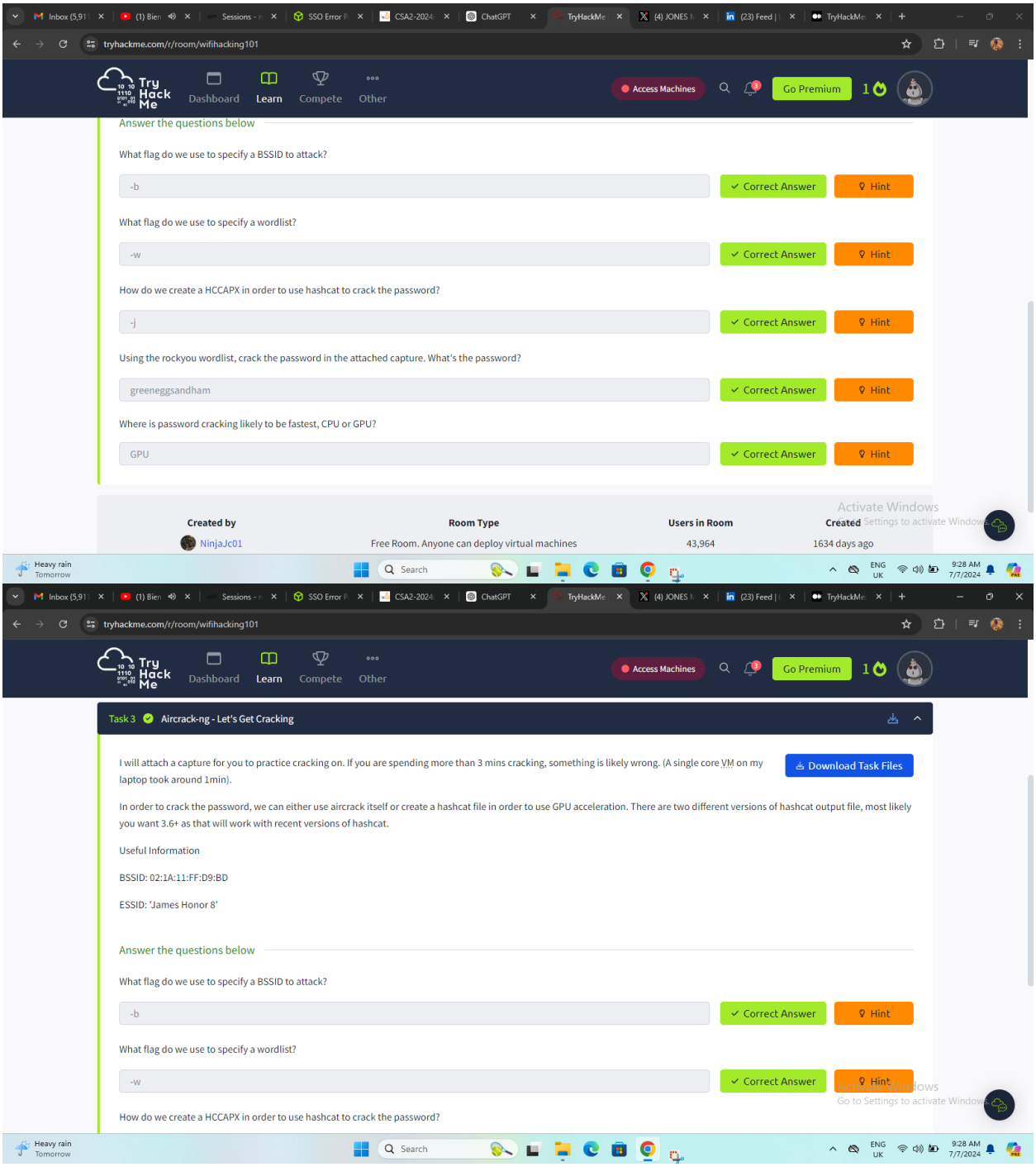
John_Mbithi_Mutave



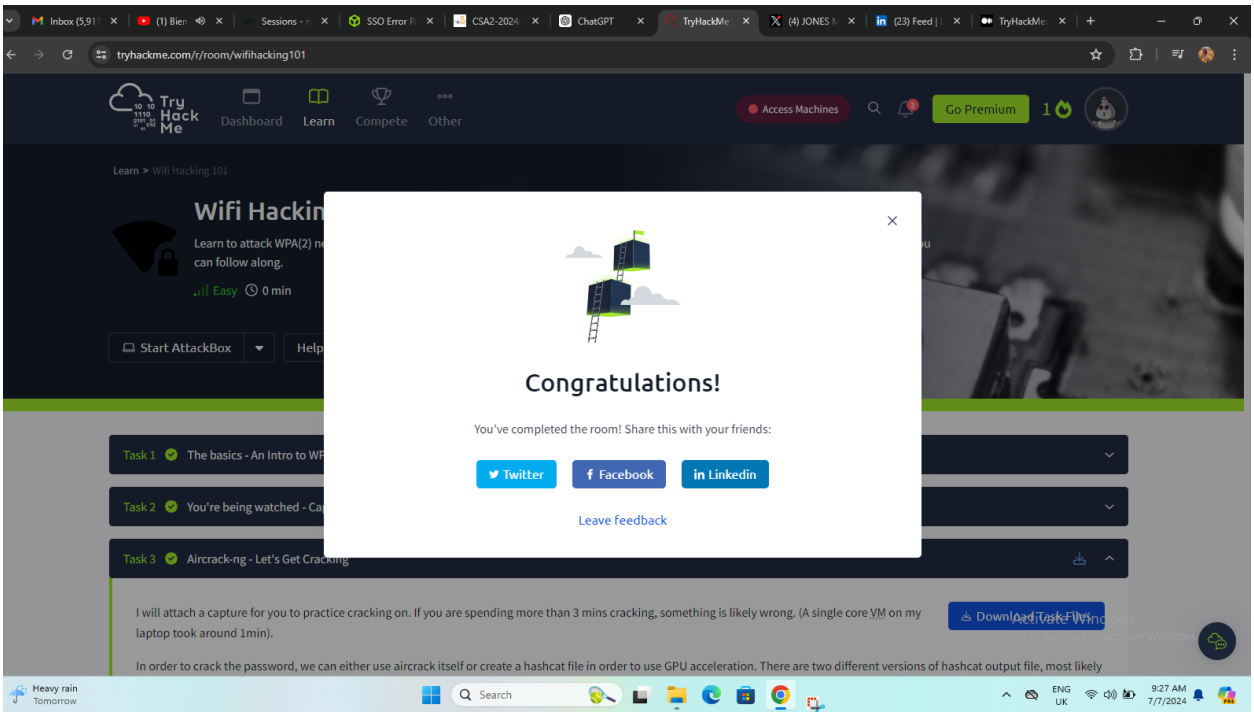
cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



cs-sa07-24019
John_Mbithi_Mutave



Shareable Link - https://tryhackme.com/r/room/wifihacking101

Conclusion

The WiFi Hacking 101 module on TryHackMe provided a comprehensive introduction to attacking WPA(2) networks. The tasks covered the essential steps from understanding the basics of WPA, capturing data packets, and using aircrack-ng to crack the encryption. This hands-on experience is invaluable for understanding wireless security vulnerabilities and the importance of using strong, complex passwords and updated encryption standards to protect wireless networks.

Recommendations

1. **Use WPA3**: Upgrade to WPA3 where possible for enhanced security.
2. **Strong Passwords**: Use complex and lengthy passwords to make dictionary attacks less effective.
3. **Regular Monitoring**: Continuously monitor wireless network traffic for unusual activities that might indicate an attack.