Wireless Network Security

The main objective of this project is to showcase the effective implementation of wireless network security practices. Through a series of tasks, I performed comprehensive assessments of encrypted network traffic, decrypting files using various techniques to identify potential vulnerabilities.

Key Project Tasks:

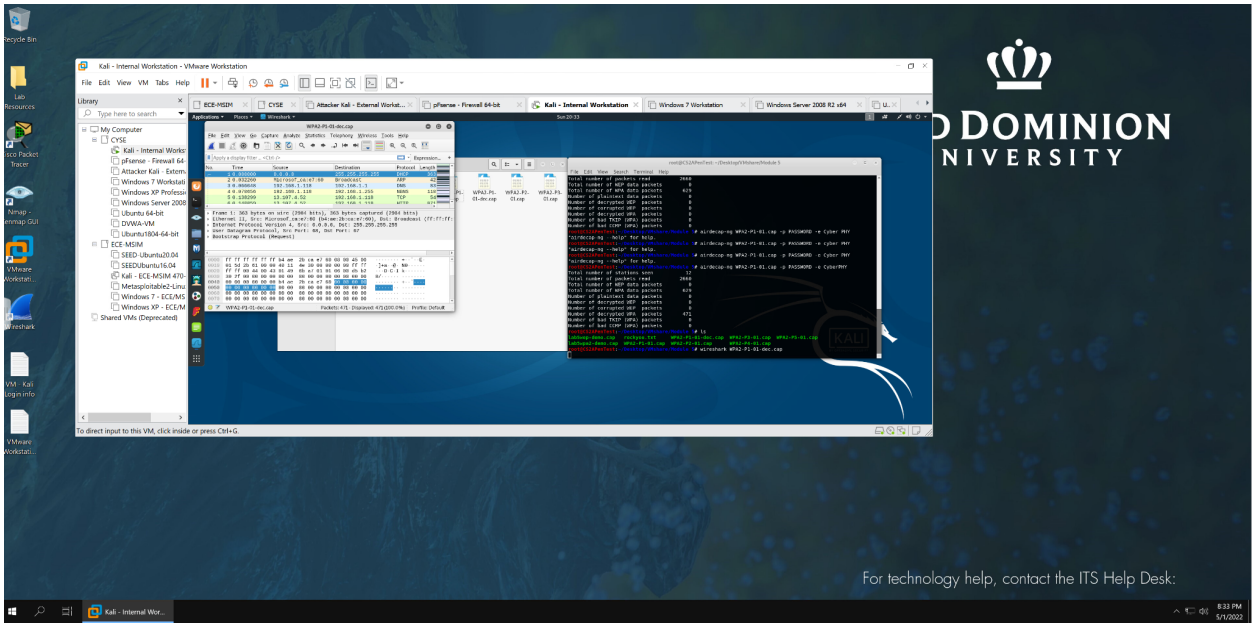
1. WEP File Decryption: Utilizing Wireshark, I accessed the password and successfully decrypted the WEP file, demonstrating the importance of robust security measures for wireless networks.
2. Aircrack Packet Analysis: Using Aircrack, I examined the list of packets within the file, laying the groundwork for subsequent decryption steps.
3. Key Identification: Employing Aircrack, I successfully found the key required to decrypt the traffic file, highlighting the significance of identifying and addressing potential security loopholes.
4. Traffic Encryption Break: With the identified key, I proceeded to break the encryption of the traffic, emphasizing the need for strong encryption protocols to safeguard sensitive data.
5. WPA File Decryption: Continuing with Wireshark, I employed the key to successfully decrypt the WPA file, further emphasizing the importance of robust security practices for wireless networks.
6. Data Encryption: As part of the project, I encrypted data in the file to demonstrate proactive security measures for protecting network communications.
7. Dictionary Attack: Utilizing a wordlist, I conducted a dictionary attack to evaluate the network's susceptibility to common password-based attacks.
8. Successful Decryption: Through a combination of the password and SSID, I successfully decrypted the traffic file, reinforcing the significance of strong passwords and secure network configurations.

Project Significance:
This project is a practical demonstration of wireless network security assessment and showcases the critical role of encryption and password management in safeguarding network communications. By effectively decrypting and securing network traffic, I aimed to raise awareness about potential vulnerabilities and the importance of robust security practices.

Wireless Network Security

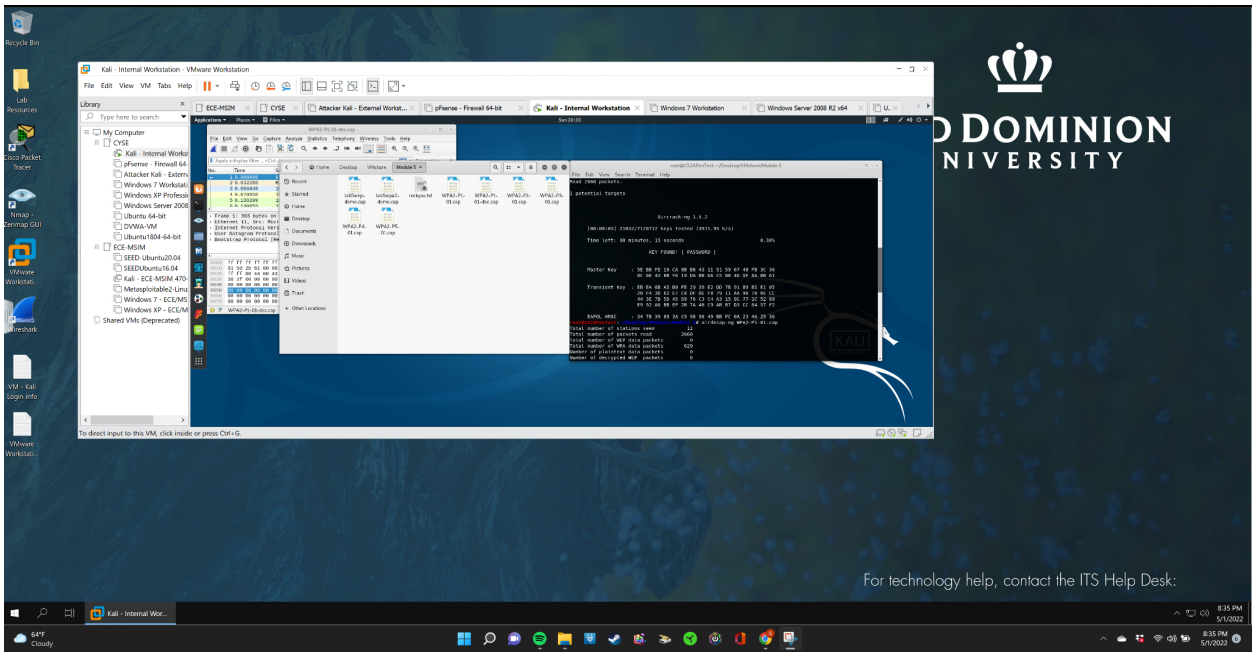
Step One

Decrypt the WEP file in Wireshark by accessing the password:



Step Two

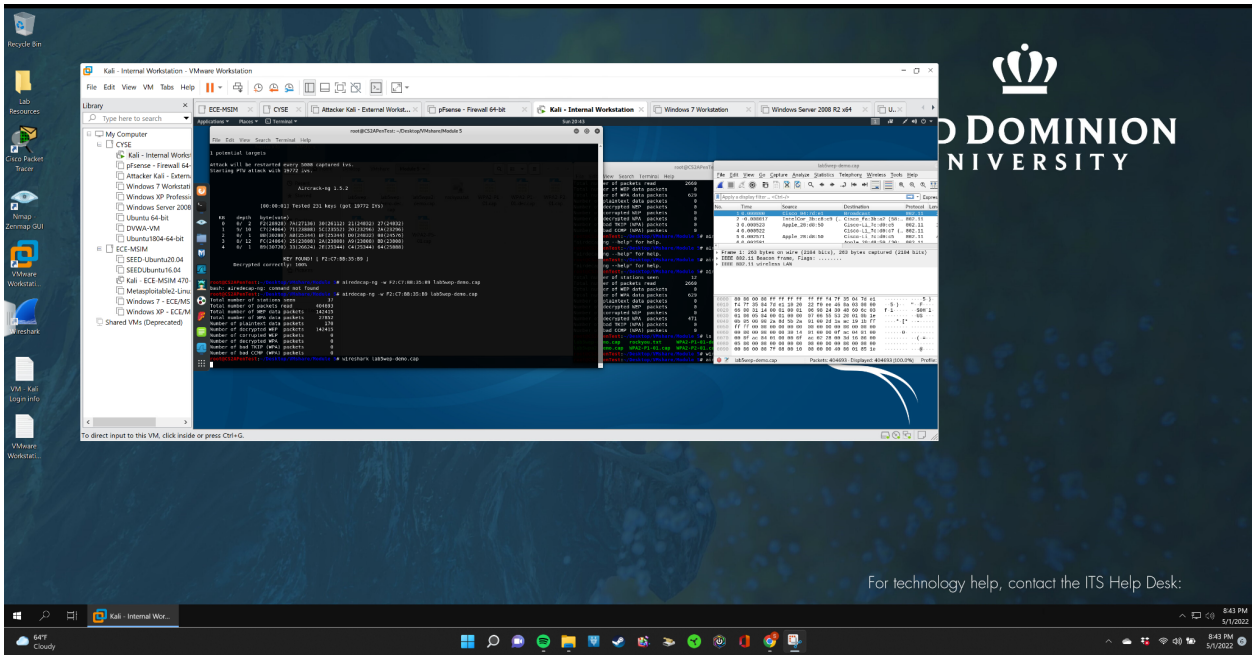
The image displays the use of aircrack to open the list of packets within the file and from here we can find the target by locating the WEP encryption:



Wireless Network Security

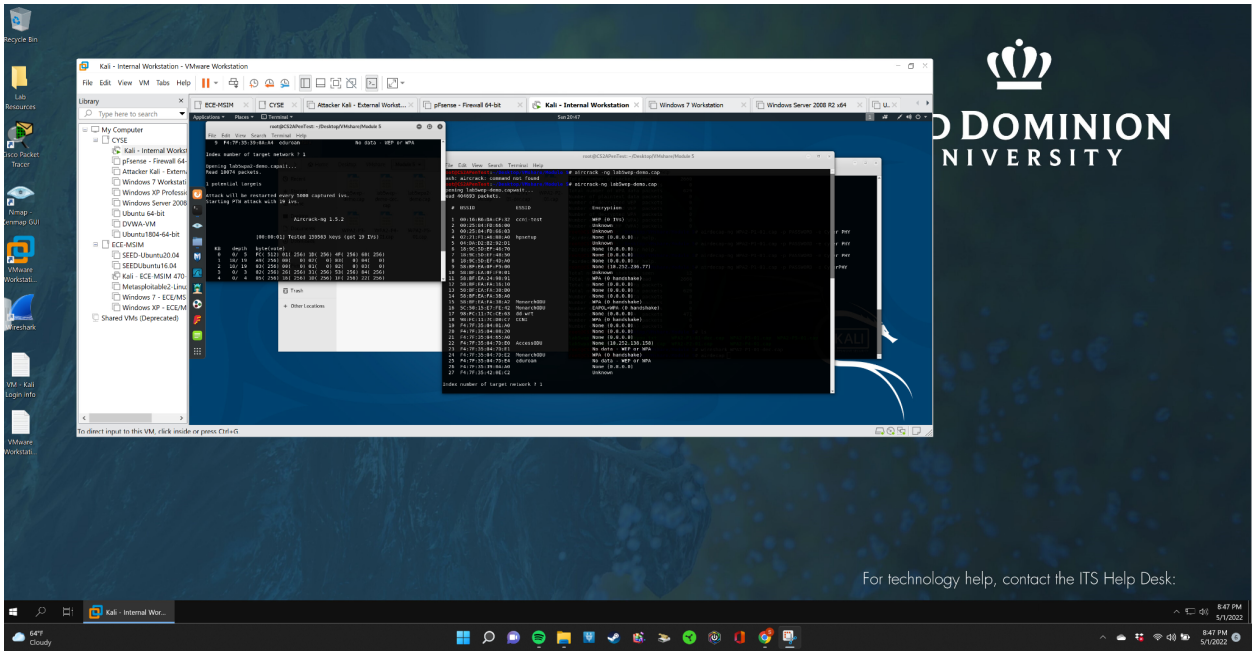
Step Three

Display using aircrack to successfully find the key needed to decrypt the traffic file

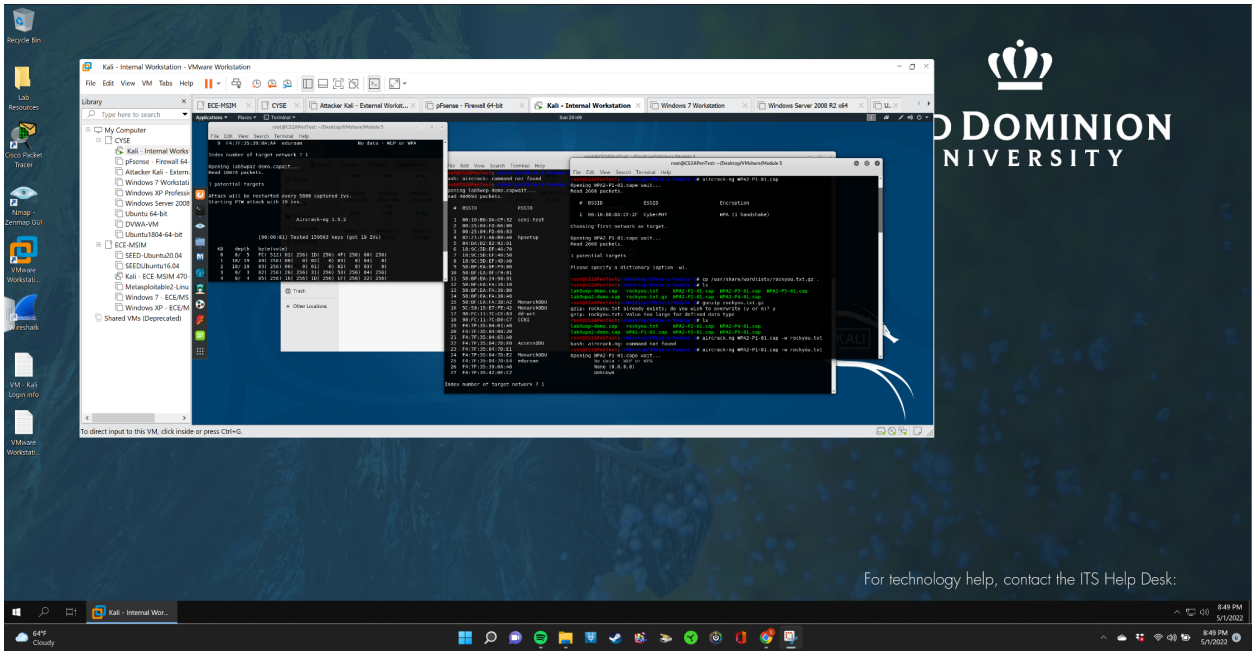


Step Four

Using the key to break the encryption of the traffic



Wireless Network Security

Step Five

By plugging in the password and the SSID we can successfully decrypt the traffic file