Wireless Network Security

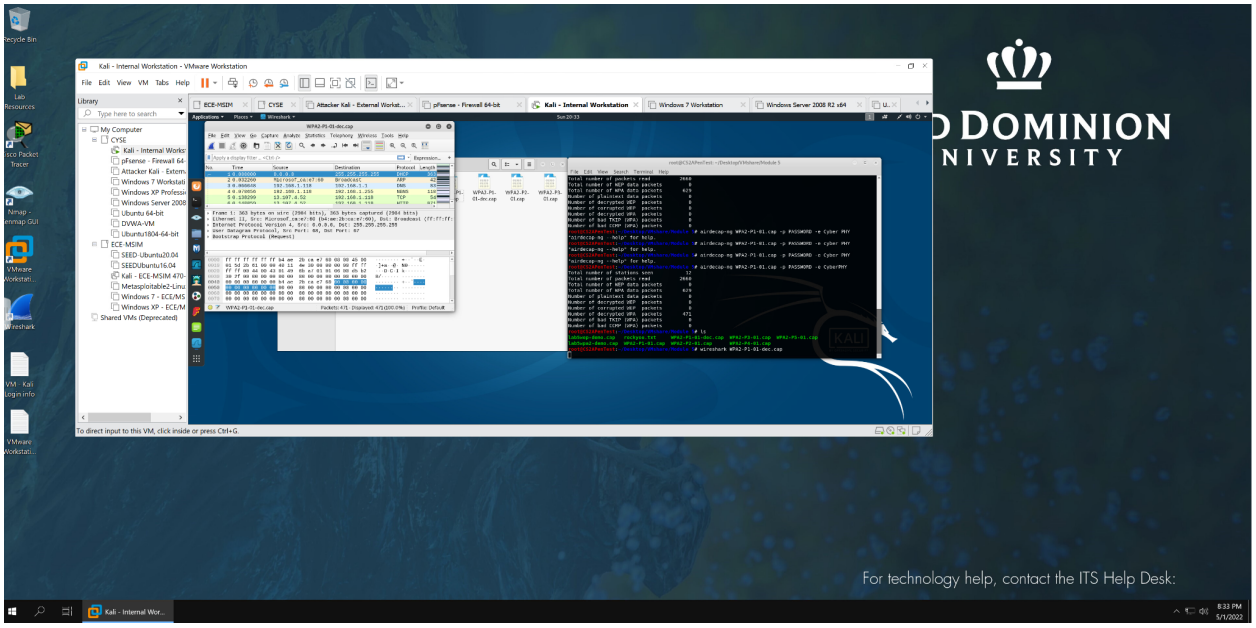
Kali Linux

Overview:

This project's purpose is to display the use of wireless network security practice. The tasks performed in this project are the following. Decrypting the WEP file in wireshark by accessing the password. The use of aircrack to open the list of packets within the file. The use of aircrack to successfully find the key needed to decrypt the traffic file. Using the key to break the encryption of the traffic. Use the key to successfully decrypt the WPA file in wireshark. Encrypting data in the file. The use of a dictionary attack using the wordlist. Lastly, by plugging in the password and the SSID we can successfully decrypt the traffic file

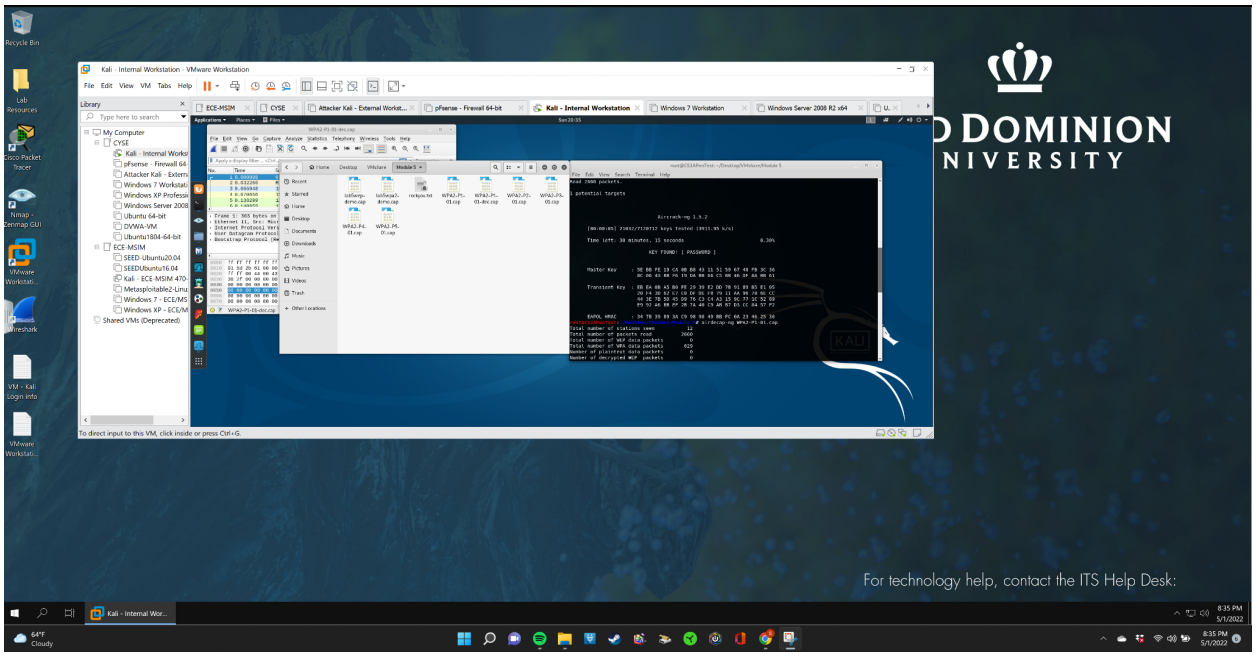
Step One

Decrypt the WEP file in wireshark by accessing the password:



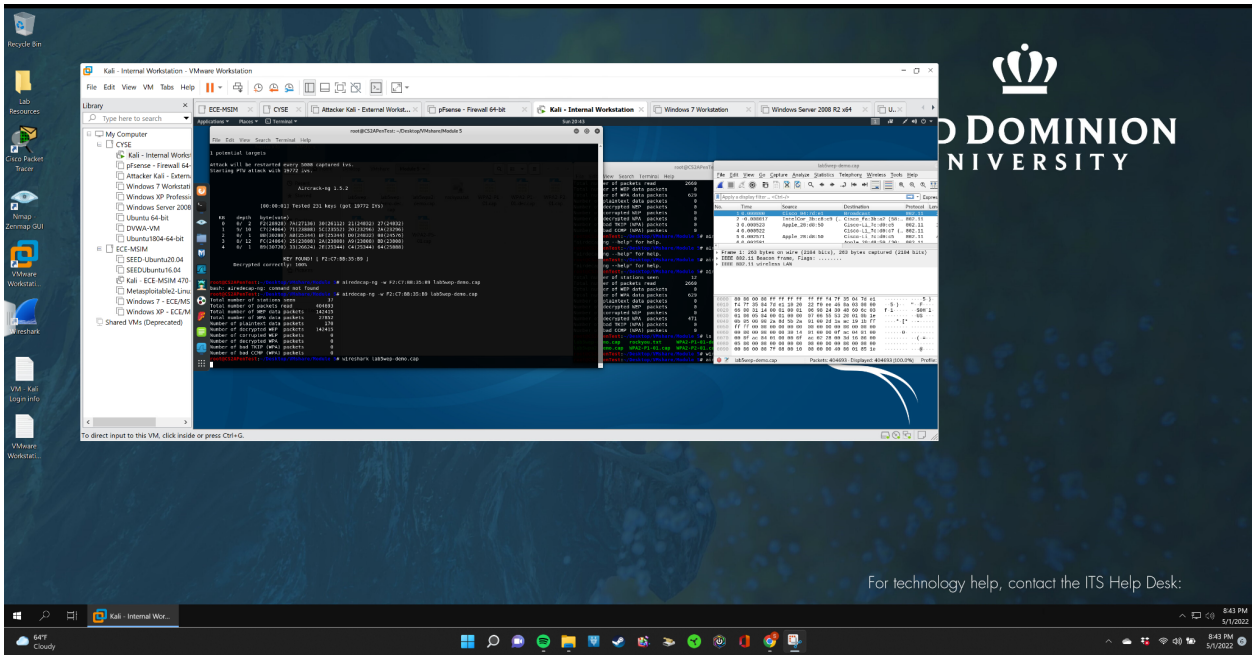
Step Two

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:



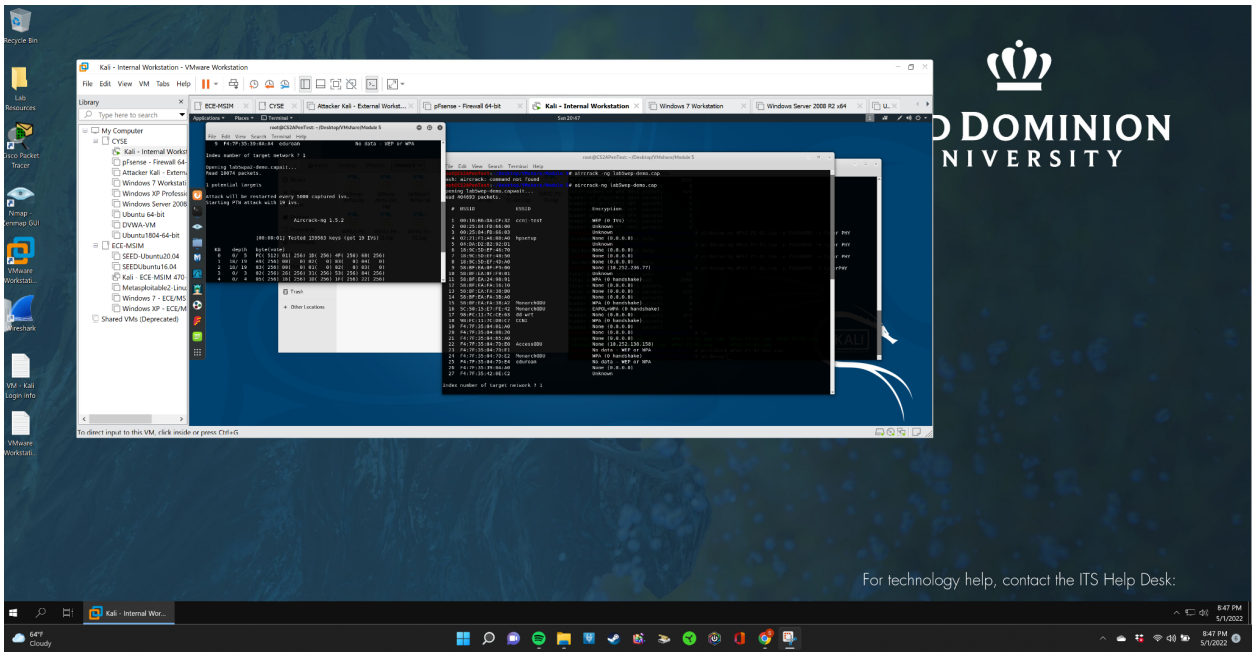
Step Three

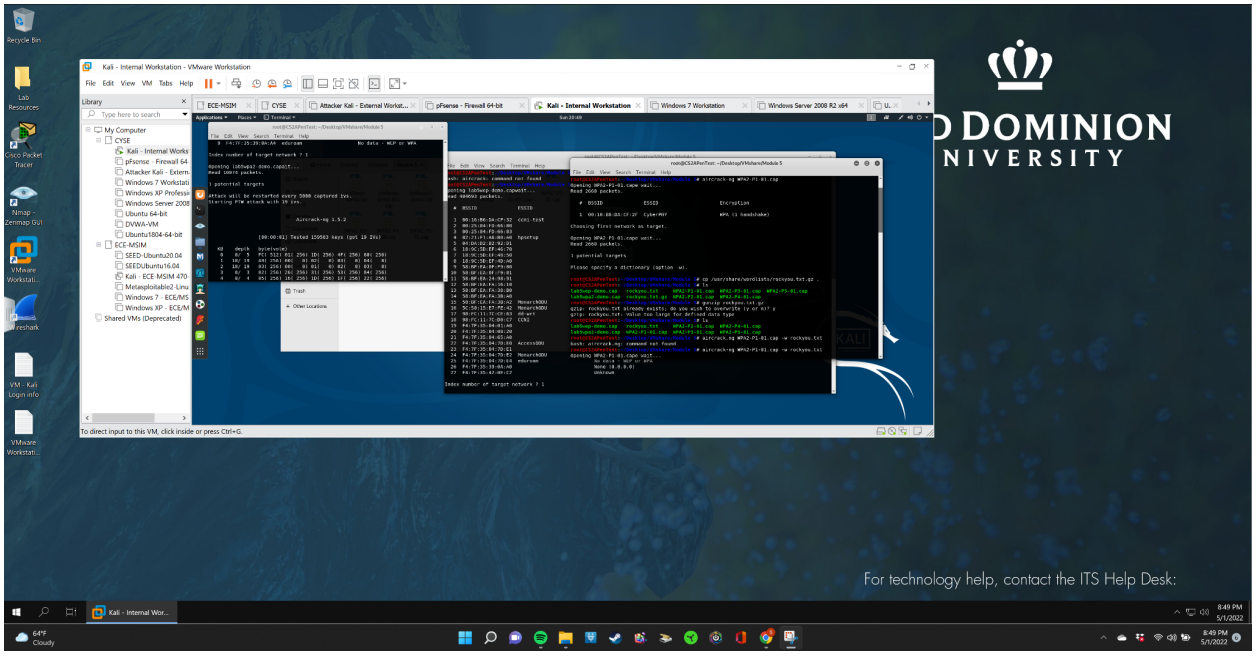
Display using aircrack to successfully find the key needed to decrypt the traffic file



Step Four-

Using the key to break the encryption of the traffic



Step Five

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