Bryant Watkins

4/9/26

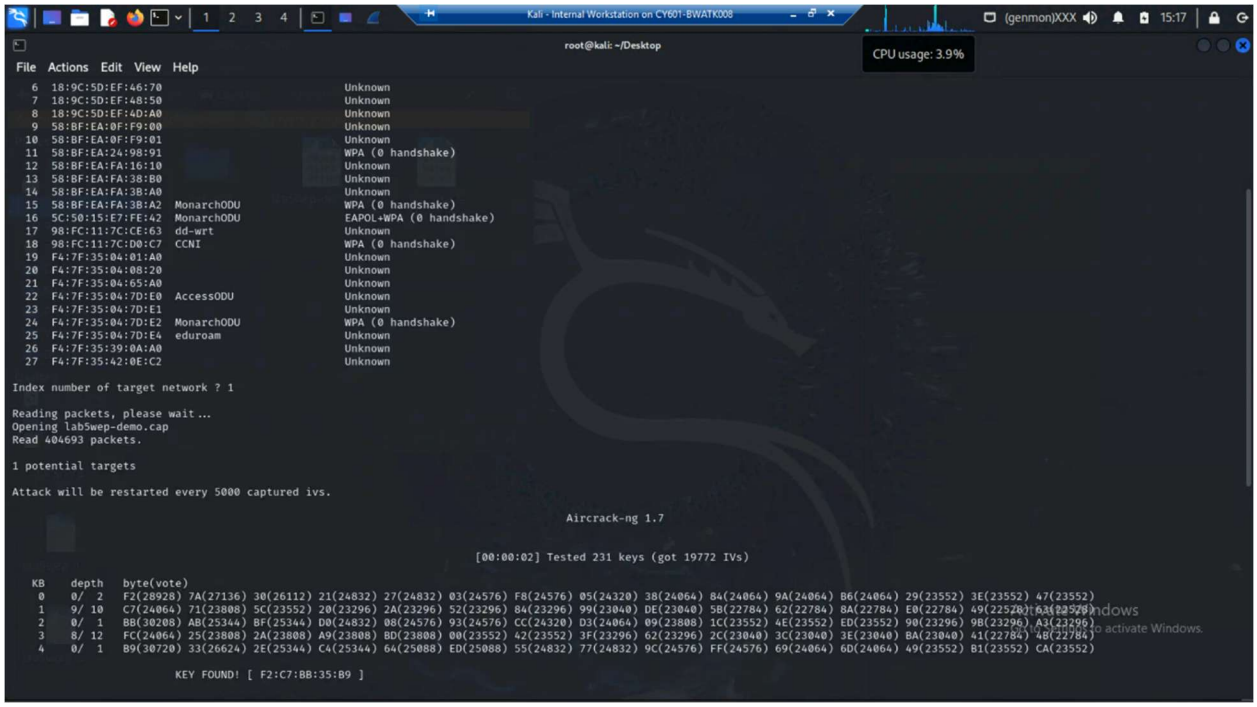
Wi-Fi Password Cracking LAB REPORT

CYSE 601

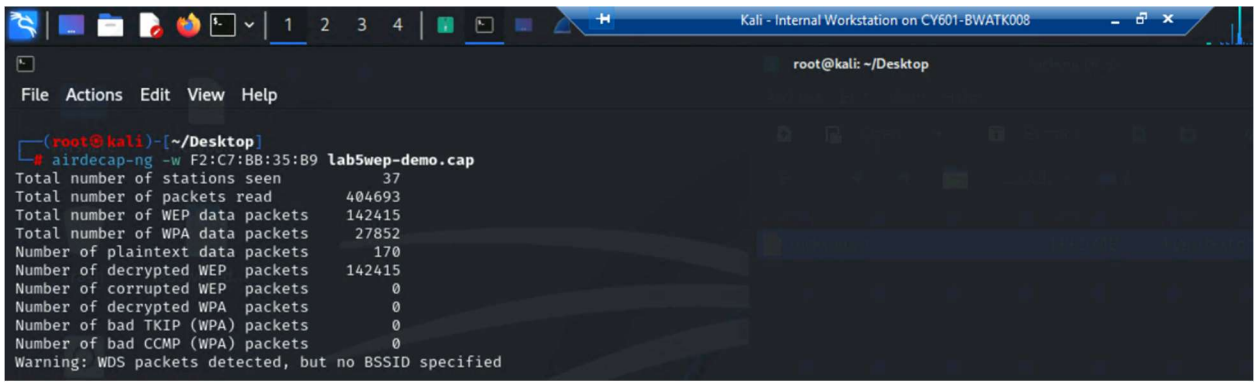
Relevant Systems

- pfSense firewall VM (IP: 192.168.10.2)
- Internal Kali Linux machine (IP: 192.168.10.13)

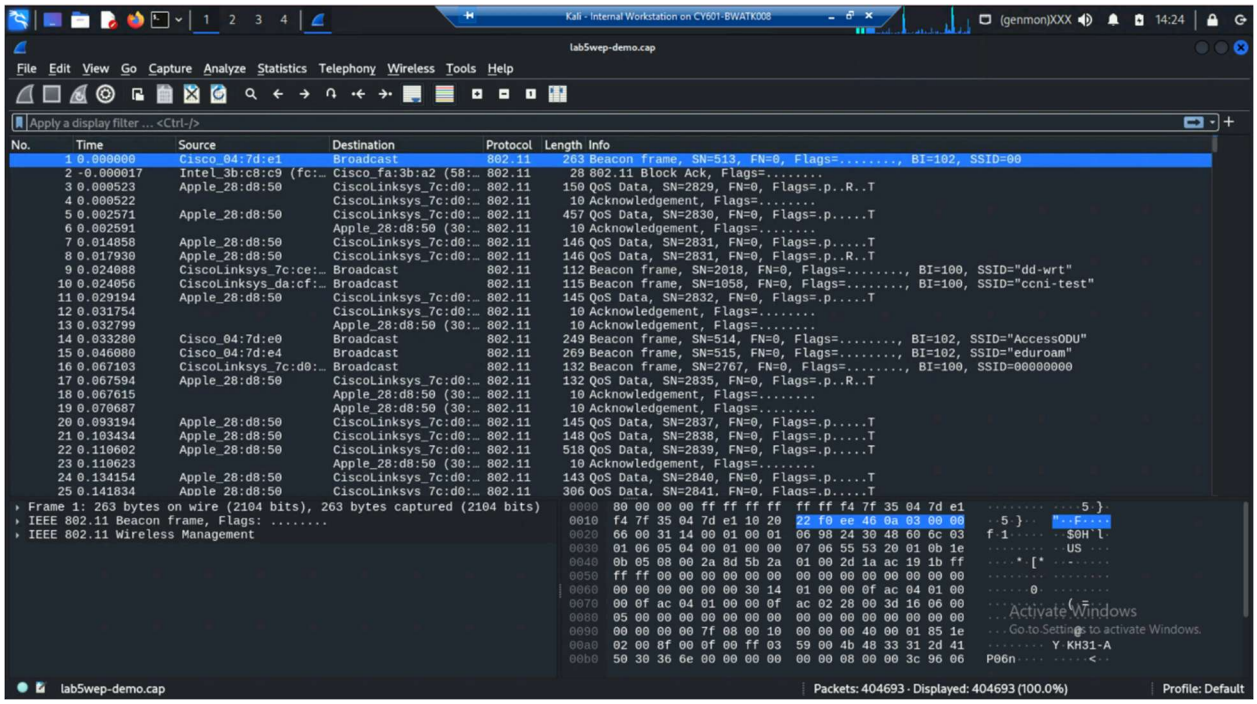
WEP Password Cracking



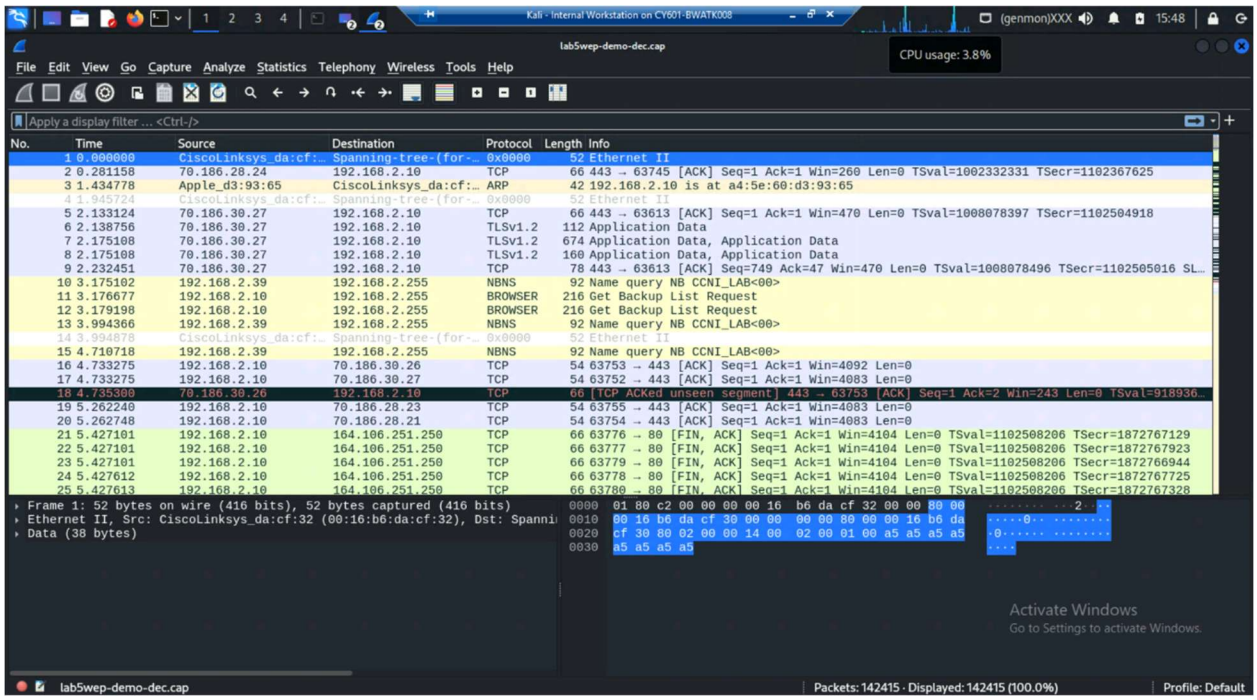
Aircrack-ng Command



Airdecap-ng Command



Encrypted Traffic



Decrypted Traffic

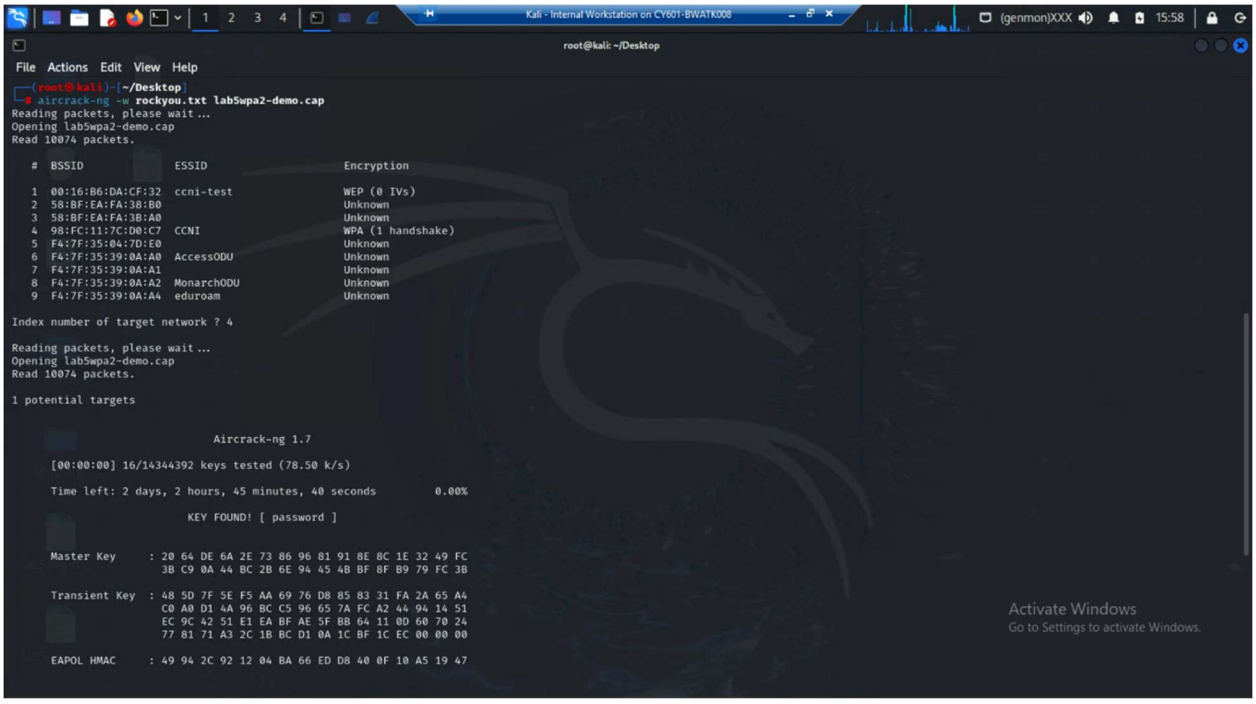
Analysis

The first step in the WEP Wi-Fi password cracking process entails changing the current working directory to the location of the encrypted Wireshark traffic data. The command to examine this traffic is *aircrack-ng "file name"*, this command will display any Wi-Fi networks within the captured packet traffic file. The administrator will then be prompted to select the "index number of target network", this simply requires the administrator to enter the number corresponding to the desired Wi-Fi network, which is *WEP* in this case. The *aircrack-ng* command will then produce an output displaying a 64-bit WEP key, which will be used for the next command.

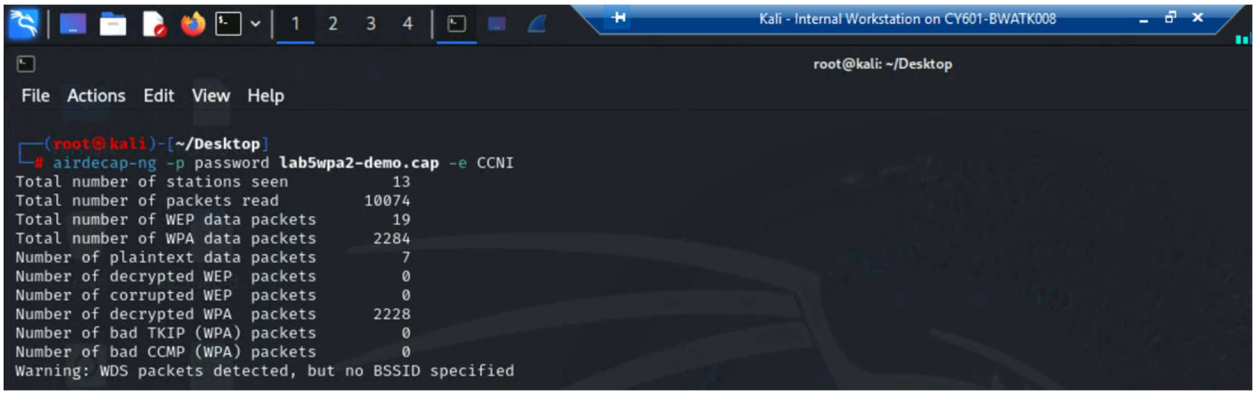
The next applicable command in the process is *airdecap-ng* to further decrypt the traffic file, and this command will require the inclusion of the newly acquired 64-bit WEP key along with file name. This will then produce a new decrypted packet file available for further analysis. Upon opening the newly created decrypted packet file, there will be a plethora of data fields to assess. Upon assessing the data, the administrator will be able to observe any distinctive patterns in traffic.

The decrypted Wi-Fi Wireshark traffic obtained provides us with a few data points of particular note. The packets' protocols are now visible, as they were initially illustrated as "802.11" initially. Critically, the newly decrypted traffic also now displays source and destination internet protocol addresses previously concealed, providing further information for potential escalatory attacks if desired. An incredibly high volume of ARP protocol packets is visible as well, indicating the immense scanning efforts taken in the decryption process. Analyzing data points such as these are critical in the understanding of the Wi-Fi password cracking process and can assist in exploring options for future incursions and vulnerability exploitation.

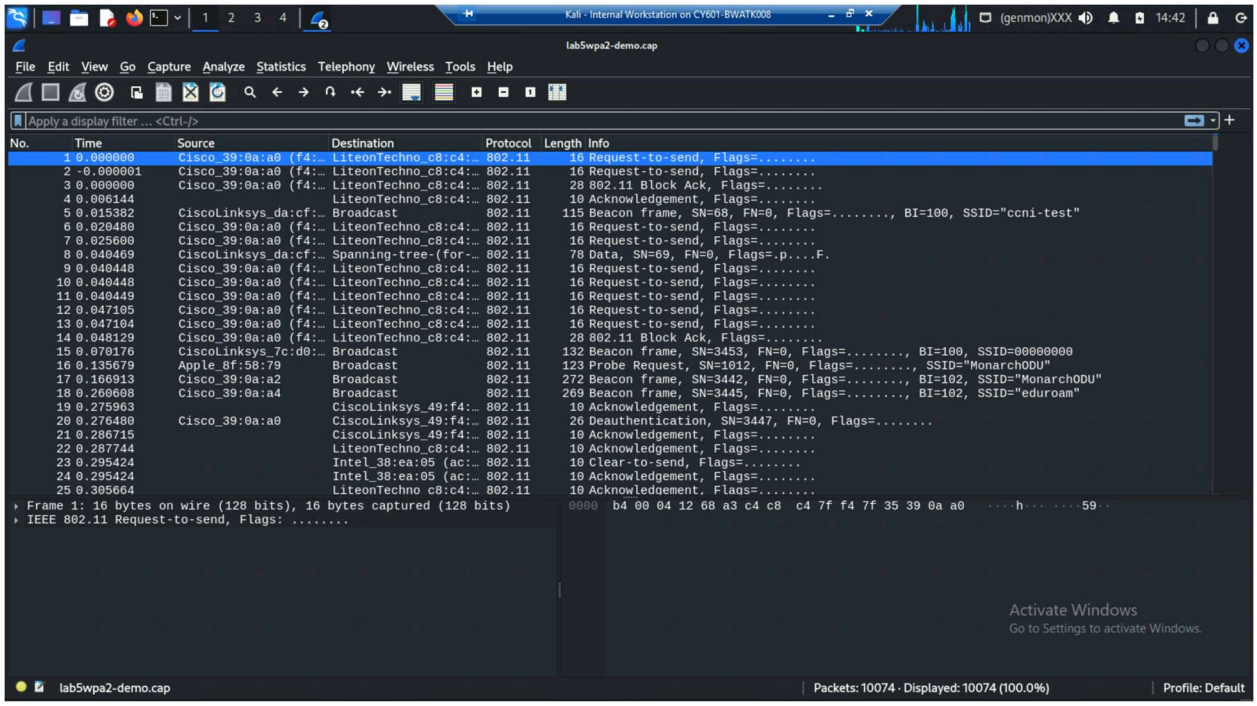
WPA2 Password Cracking



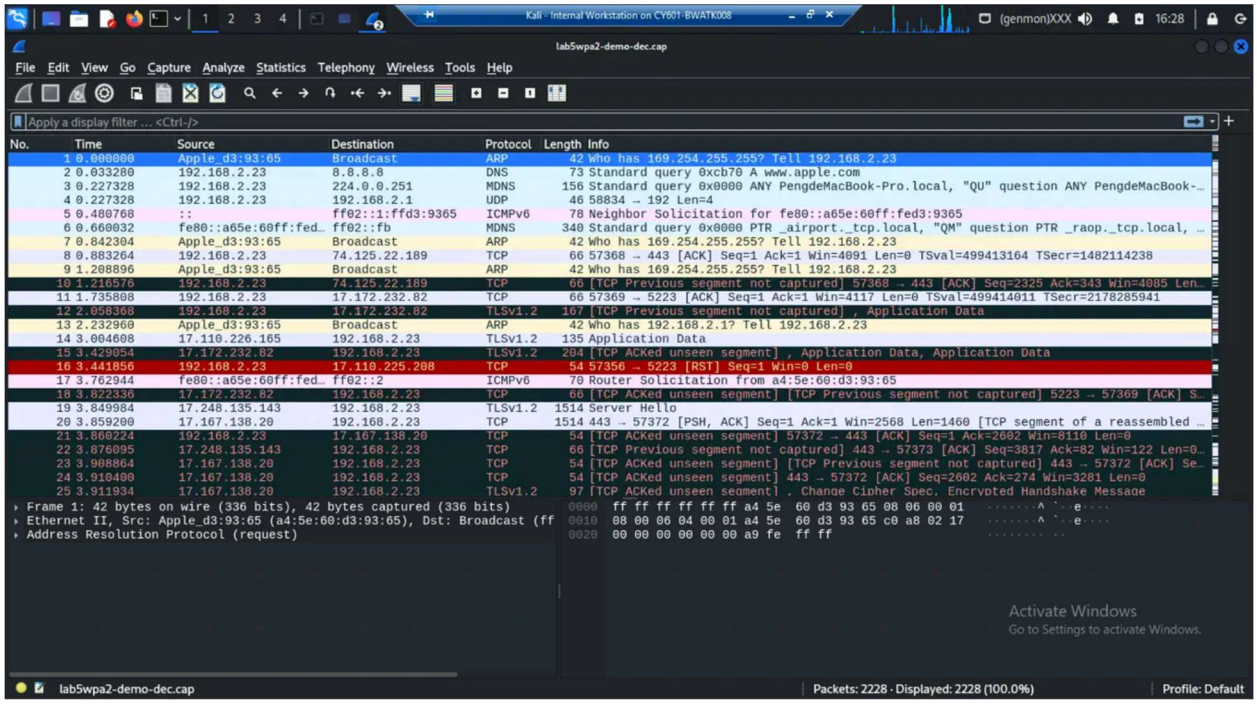
Aircrack-ng Command



Airdecap-ng Command



Encrypted Traffic



Decrypted Traffic

Analysis

The first step in the WPA2 Wi-Fi password cracking process entails changing the current working directory to the location of the encrypted Wireshark traffic data file. The command to examine this traffic file is *aircrack-ng "file name"*, this command will display any Wi-Fi networks within the captured packet traffic file. The administrator will then be prompted to select the "index number of target network", this simply requires the administrator to enter the number corresponding to the desired Wi-Fi network, which is *WPA* in this case. This is where the *WPA* password cracking process begins to differ from the *WEP* password cracking process. Not only are we looking for *WPA*, however, but we must also ensure the option selected has a four-way handshake. As opposed to the *aircrack-ng* command producing an output displaying a 64-bit WEP key, the output for *WPA* will further require the administrator to "Please specify a dictionary". After selecting the desired dictionary file, the administrator may now successfully obtain the password through a Dictionary attack (Syntax: *aircrack-ng "Traffic file name" -w "Dictionary file name"*).

The next applicable command in the process is *airdecap-ng* to further decrypt the traffic file, and this command will require the inclusion of the newly acquired password along with file name and ESSID (which can be obtained from the initial *aircrack-ng* command output). This will then produce a new decrypted packet file available for further analysis. Upon opening the newly created decrypted packet file, there will be a plethora of data fields to assess. Upon assessing the data, the administrator will be able to observe any distinctive patterns in traffic.

The decrypted Wi-Fi Wireshark traffic obtained provides us with a few data points of particular note. The obtained unencrypted data shares a few similarities with the *WEP* uncencrypted data. The packets' protocols are now visible, as they were initially illustrated as "802.11". Critically, the newly decrypted traffic also now displays source and destination internet protocol addresses previously concealed, providing further information for potential escalatory attacks if desired. As opposed to the patterns observed within the *WEP* traffic data, there is an incredibly high volume of TCP protocol packets that are visible. The high volume of TCP packets indicates a high level of network activity/traffic, which can also be indicated by the red TCP packet indicating network congestion and connection failure. As with *WEP traffic* data, analysis of data points such as these are integral in the understanding of the Wi-Fi password cracking process and could assist in exploring options for future incursions and vulnerability exploitation.