IC00AI83 Privacy and Social Engineering

Harsha Gunasekara

Study Right No. 2401908

Week 7: In Class Extras

Task 1: Lockpicking 1p

Required to pick open 2 locks of your choice. You may pick the others as well, but 2 are required for a point.

Start with the Padlock - The padlock is the easiest lock in the set, a good starting point for practicing lockpicking skills using the provided lockpicks and turning tools.

Move on to the Double-sided lock - This lock presents a slightly higher level of difficulty than the padlock, requiring practice to differentiate between feedback and conflict.

Experiment with the Small cylindrical lock - The lock presents challenges, particularly with its blocked view, so it's recommended to experiment with various picking styles and picks to find the best fit.

Attempt the Cruciform/Zeiss lock - The lock may be the toughest, but without discourage; experiment with different techniques to learn and improve own skills.

Pick 2 locks of own choice - Familiarize with the set of locks and focus on two to open. Apply learnings from other locks and experiment with different approaches if needed.

Seek help if needed - If stuck or unable to pick a lock, seek assistance from experienced individuals for fresh angles and guidance to overcome difficulties.

Task 2: Wi-Fi Deauthentication password attack 1p

Aircrack-ng, How to use a wordlist to perform the attack?

1. Prepare Linux environment with a monitor mode-capable HUAWEI WiFi AX2.
2. Capture Wi-Fi traffic, including deauthentication frames, using tools like ‘airodump-ng’.
3. Save captured traffic to a .pcap file.
4. Use aircrack-ng to perform a dictionary attack on the .pcap file.
5. Install wordlists using ‘wordlistctl’ and fetch popular wordlists like ‘rockyou’.
6. Use the fetched wordlist as input for the dictionary attack with ‘aircrack-ng’.

This process involves setting up the environment, capturing traffic, saving it to a file, and then using aircrack-ng with a wordlist to attempt to crack the Wi-Fi password.

Aireplay-ng, How to use the deauthentication attack with aireplay-ng?

1. Set the HUAWEI WiFi AX2 to monitor mode using ‘airmon-ng’.
2. Capture 802.11 frames using ‘airodump-ng’.
3. Use Wireshark to capture traffic.
4. Focus on capturing frames from the target access point (BSSID) using ‘airodump-ng’.
5. Send deauthentication frames to the target BSSID using ‘aireplay-ng’.
6. Monitor EAPOL authentication packets.
7. Stop and save the capture to a .pcap file.
8. Use aircrack-ng with a wordlist to perform a dictionary attack on the captured .pcap file.

This process allows to perform a Wi-Fi deauthentication attack and then attempt to crack the password of the target access point using captured traffic and a dictionary attack.

Airmon-ng, How to set an adapter to monitor mode?

To set an HUAWEI WiFi AX2 to monitor mode using ‘airmon-ng’:

1. Open a terminal.
2. Plug the monitor mode-capable Wi-Fi adapter.
3. Run ‘iwconfig’ to find the adapter name - HUAWEI WiFi AX2
4. Use ‘sudo airmon-ng start HUAWEI WiFi AX2 to start monitor mode.
5. Verify with ‘iwconfig’.

HUAWEI WiFi AX2 is in monitor mode and ready for use.

Wireshark, How to save a .pcap file?

1. Capture the desired traffic by starting a capture session in Wireshark.
2. Once captured the traffic, need to stop the capture session.
3. Go to "File" in the menu bar.
4. Select "Save As...”
5. Choose the location where want to save the .pcap file.
6. Enter a name for the file and make sure the file extension is .pcap.
7. Click "Save" to save the .pcap file to the specified location.