Lab 5 – Wireless Attack Lab

Task 1.1

1. What is the source name for the AP?
    a. AmpedWir_44
2. What is the MAC address for the AP?
    a. F8:7B:8C:44:6B:18
3. What channel was the AP using?
    a. 5
4. Who is the vendor/manufacturer for the AP?
    a. RealtekS
5. What is the source name for the device that sent the most data to the AP?
    a. Apple_1a
6. What is the MAC address for the device that sent the most data to the AP?
    a. 1C:BF:CE:55:A2:71
7. Who is the vendor/manufacturer for the device that sent the most data to the AP?
    a. Apple
8. What is the password for the AP?
    a. ABCDE

Task 1.2

1. What is the source name for the AP?
    a. AmpedWir_44
2. What is the MAC address for the AP?

    a. F8:7B:8C:44:6B:1D

3. What channel was the AP using?
    a. Unknown
4. Who is the vendor/manufacturer for the AP?
    a. Epigram
5. Where did you get your password dictionary?
    a. Rockyou.txt built into Kali Linux image.
6. What is the password for the AP?
    a. wireless
7. What command did you issue to find the password of the AP?
    a. aircrack-ng -w rockyou.txt catalyst-01.pcap
8. Was your password dictionary sufficient or did you have to download other password dictionaries? How many dictionaries did you need?
    a. The rockyou.txt dictionary was sufficient.
9. How many entries in your password dictionary?
    a. 9822768, according to the aircrack-ng command process
10. Since CATALYST is on a 5 GHz network, what command would you have used to scan the network specifically searching for CATALYST on a specific channel?

Task 1.3

1. What is the source name for the AP?
    a. Netgear_a0
2. What is the MAC address for the AP?
    a. DC:EF:09:A0:DE:DE

3. What channel was the AP using?
    a. 7
4. Where did you get your password dictionary?
    a. https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm
    b. (smaller wordlist)
5. Who is the vendor/manufacturer for the AP?
    a. Epigram
6. What is the password for the AP?
    a. Cyberspace
7. Was your password dictionary sufficient or did you have to download other password dictionaries? How many dictionaries did you need?
    a. Rockyou.txt was not sufficient, tried many other dictionaries found on stackexchange, skullsecurity, Kali's provided lists, but only the crackstation dictionary worked.
8. How many entries in your password dictionary?
    a. After using grep ^C wordlist.txt > captialC.txt to filter out passwords starting with a capital C, as per the hint on Canvas, the total entries was 1506814