**Performance Assessment: Wireless Network Hacking**

In this Performance Assessment, you will perform the tasks you have been taught in the Guided Practices (iLabs content from EC-Council).  You may use the book and any notes you have. You may look at your prior labs. You may not give or receive help from other students. You may ask your instructor for assistance, but it is likely to cost points.

How does this practical lab apply in the real world?

Securing the enterprise and the small business is key to remaining compliant with industry regulations. Retail Technology Review suggests that 72% of business breaches in various forms originate through unsecured wireless. A research study of 1,075 participants indicated that wireless devices such as scanners, printers, and mobile phones contributed directly or indirectly to network infiltration, resulting in a data breach in the last 12 months. How does this apply to me at home or the organization I work for? Wireless security is key to maintaining a secure network and protecting proprietary data.

Resources Needed

This lab assessment covers Modules 16 from your EC-council lab content. Thus, all resources you will need will be from your labs, your text, and any research that you might have.

* ParrotOS (only)
* Aircrack-ng
* Rockyou.txt (Dictionary)
* Wireshark (locate BSSID) Mac address

Level of Difficulty

Moderate

*Important*

***Please note the following guidance****: This Assessment should be performed in the VCastle POD using the Parrot Linux virtual machine.*

*All screenshots should reflect your own work and should have the date, time and user information (name, student ID) clearly displayed*

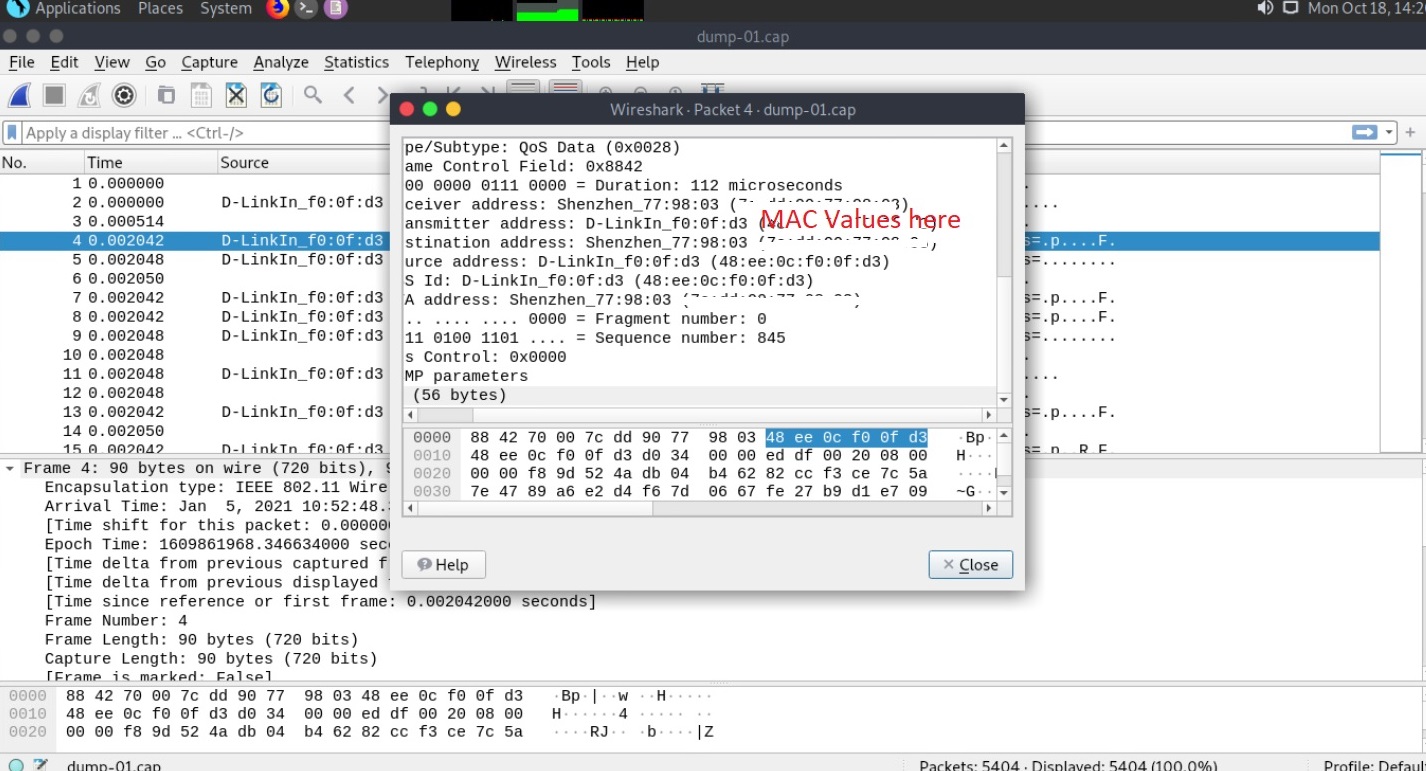
*All takeaways/inferences you can make about your target based on the password hash should be clearly expressed (full sentences without excessive use of bullet points) and should be in your own words and result from you doing the work.*

Instructions

***Tasks:***

1. Using any of the tools available on the Parrot OS virtual machine, perform a password crack using the appropriate tools from Parrot OS (**Note**: You will use the ParrotOS box only). You will use a capture file that is located on the desktop of the Parrot OS machine. The file will be labeled psk-01.cap as found on the desktop.
2. You will need to document all commands used to load the password and crack it using “Rockyou.txt” Will be. This file will also be located on the desktop with the .cap files. Also, please remember you must view the .cap file with Wireshark first to identify the BSSID (Mac Address Access Point). You will then use the mac address with the aircrack-ng to crack to capture. (This may require a google search)

*Example of Wireshark open to obtain MAC address of target SSID*



1. A screenshot of the process being run as well as the final password that has a hash value equivalent.

*\*Special note(Make sure you are in the correct directory when running Aircrack-ng)\**

1. Explain in a narrative the overall process of how you used the resources and tools to crack the hash value in a paragraph or more.