**Hands-on 6C**

Course: CIS 3347-1

Submitted to University of Houston

College of Technology

Information and Logistics Technology

by

John Smith

Cell Phone: xxx-xxx-xxxx

October 1, 2017

Instructor: Dr. Ron Viseh

# Capture a snapshot for the screen having all the information related to the various network connections that you collected during your warwalking.

Figure 1 shows the list of active Wireless Local Area Networks (WLANs) using the NetSpot software (NetSpot, 2017) from the Example subdivision/place/library in Houston, Texas on October 1, 2017.



*Figure 1.* The NetSpot software output screen shot of active WLANs

# How many networks kept the original/default SSID? Why could this be a security problem?

According to figure 1, the NetSpot software (NetSpot, 2017) discovered total of 22 WLANs includes….

Here is the list;

* 2WIR446
* ….

# What is your overall assessment of the WLAN usage with respect to security?

The overall assessment according to figure 1, this area WLANs mostly except Xfinity WLAN networks are using WPA2 that is the newest, most secure type of WLAN security (FitzGerald et al., 2012) because of using the advanced encryption standard (AES).

In conclusion, the possible recommendations include: change the router default password, change the default service set identifier (SSID), restrict the WLAN access by using media access control (MAC) address filtering, and disable the broadcast SSID option that the NetSpot software (NetSpot, 2017) unable to discover the WLAN as a visual examination revealed this result by the researcher.

# References

FitzGerald, J., & Dennis, A., Durcikova, A. (2012). *Business Data Communications and Networking* (11ed.). Hoboken, NJ: Wiley.

Kennedy, S. (2017). *Best Practices for Wireless Network Security.* Retrieved from https://www.computerworld.com/article/2573986/mobile-wireless/best-practices-for-wireless-network-security.html

NetSpot (2017). *Wi-Fi Site Surveys, Analysis, Troubleshooting*. Retrieved from https://www.netspotapp.com/