EN.650.431 Ethical Hacking Home Work #1

Recent examples such as [1] remind us that knowledge of core computer science courses is not a requirement to become an expert hacker. The only real requirements are a tenacious spirit and an analytical mind. Given these facts, please use your available resources to perform the below tasks.

1. Given the Parrot Bebop 1, use available hacking tools to determine (show how you were able to determine this):
   a. The IP address for the Bebop
   b. The operating system used in the Bebop
   c. UDP & TCP ports open on the Bebop
2. Focusing on the wireless connection between the Bebop and its controller (smartphone running the FreeFlight Application), use Wireshark to analyze this interaction and technically document the ARDiscovery Process [2]:
   a. Which one initiates the connection, the controller or the drone?
   b. What information is sent to initiate the connection? (This information resides in the packets passed back and forward)
   c. How do you know if the drone has a connected user already ? (Document this response and how you got this)
   d. How many connections can exist via the ARDiscovery Process between the drone and the controller? How do you know? What happens if the number of allowed connections is violated?
3. How can you wage a denial of service (DoS) attack against the ARDiscovery Process?
   a. Find a weakness in the ARDiscovery Process that you documented in question #2, write code to exploit this weakness, then demonstrate that it works. You can use [2] as a guide to help with this.
      i. Note, DoS-ing the ARDiscovery Process will break the link between the controller and the Bebop. One side effect would be the streaming video sent from the Bebop to the smartphone stops.

In a 5-minute (or less) video, explain and illustrate the results from your work above. You can work in groups of no more than five. Please email to Lanier.Watkins@jhuapl.edu and put **EN.650.431 and** all student names and in subject

References:

[1] A. Greenberg. "iPhone Super-Hacker Comex, Let Go From Apple, Goes To Work For Google". Forbes Online Magazine, April 24, 2013. Available at: http://www.forbes.com/sites/andygreenberg/2013/04/24/iphone-super-hacker-comex-let-go-from-apple-goes-to-work-for-google/#fe1536a60528

[2] Michael Hooper , Yifan Tian, Runzuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, Wlajimir Alexis, "Securing Commercial WiFi-Based UAVs From Common Security Attacks," In IEEE MILCOM 2016, Baltimore, MD, November , 2016.