I. Airbender

Airbender is a WPA/WPA2 automated password cracker. Normally one would use the tools provided by the AirCrack suite to crack a WPA/WPA2 password. The down side to cracking the password by hand is that the process requires a variety of steps and at the end of each step the AirCrack tools return data that requires understanding and interpretation before the next step in the process can be started. Our tool simplifies the process by running the necessary commands for the user and parsing the data returned for each tool. Airbender takes four main steps to accomplish its job: Set up the correct environment to run Airbender, acquire a target access point, capture a four way handshake between the access point and a verified user, and crack the handshake to retrieve the password.

A. Environmental Setup

This section of Airbender ensures that no other processes will interfere with Airbender. The best solution to this is to use “airmon”, an AirCrack tool that kills any processes that may interfere with the suite, stop the “Avahi-daemon”, and bring down the eth0 connection. The following commands accomplish our initial setup:

```
Airmon-ng check kill

/etc/init.d.avahi-daemon stop

Ifconfig eth0 down
```

B. Scan For Target Access Point

After the environment has been set the next step is to scan for a target access point. At this point Airbender will prompt the user for a channel number to use. Airbender will then run one of two commands. Airbender will run the first command if provided with a channel to listen to where [channel] is the provided channel. If provided with a 0 for input Airbender will run the second command. The two commands are as follows:

```
Airodump-ng –c [channel] --output-format csv –w [packetPath]dump [interfaceName]
Or
Airodump-ng -- output-format csv –w [packetPath]dump [interfaceName]
```

After running for the amount of time that the user inputted prior to the scan, airmon terminates. The user is then presented with the available BSSID addresses for target Access Points. The user chooses one and the handshake capture is ready to begin.

C. Handshake Capture

In order to capture the handshake packet Airbender uses two tools: airodump and aireplay. Airodump works in the same ways as when Airbender uses it to scan for the target Access Point, only this time it only captures packets from the Target Access Point

as opposed to every all access points in the area. After airodump starts running Airbender automatically starts sending out deauthentication packets in order to force all the clients connected to the Access Point to disconnect and reconnect. The following commands are ran in order:

```
Airodump-ng -c [channel] --bssid [targetBSSID] --output-format cap -w [packetPath]packet [interfaceName]

Aireplay-ng -0 1 -a [targetBSSID] -c [clientMacAddress] [interfaceName]
```

D. Handshake Crack

Finally with the the reconnection packet we captured we can use aircrack to take the authentication packet and crack the password. The command used is:

```
Aircrack-ng -w [dictionaryPath] -b [targetBSSID] [packetPATH]packet-01.cap
```

This command executes a dictionary attack on the password within the captured authentication packet. Aircrack is limited by the dictionary list the user uses and the power of the system.

II. Obstacles

To use this tool you must have the necessary environment and tools installed. The first issue is you need to have AirCrack installed and be using an operating system that can utilize all of the AirCrack library. Certain operating systems can only use a subset of the AirCrack library (MacOS). Also due to the nature of the script the user must have a network card that can enter monitor mode. If a portable network card is used then one would need to also enable it if the OS does not do so automatically. These requirements in combination created a lot of frustrations when trying to setup and run the script for different members of the team.

III. Airbender 2.0

For Airbender 2.0 there are a few improvements we would love to make. First off some of the handshakes we intercepted took a significant amount of time to crack. Offloading the cracking to a distributed system would greatly improve performance. Another drawback of the current build is that it relies on the user already having the Aircrack Suite and a good dictionary of passwords. 2.0 would take care of this situation by checking the user's system for these two components, and if not found ask the user if they would like Airbender 2.0 to install them. At the same time if a password dictionary was found Airbender 2.0 would compare it to the default one it would have installed to see which is more robust. If the default one it would let the user know and ask if they would like to use the Airbender 2.0 default. Finally we would really like Airbender 2.0 to

be able to crack WPA/WPA2 enterprise networks. Airbender 2.0 would be able to mimic a target enterprise access point in order to capture authentication attempts.