2022

Lab 8 – Deauth using Sparrow-Wifi and MITM using Wifiphisher and Airgeddon

Lab Requirements:

Kali VM running Wireshark.
Compatible USB Wi-Fi Adapter attached to Kali VM

Resources:

Read this document in full before you begin

Part 1: Deauth using Sparrow-WiFi

1) Sparrow-WiFi is a GUI Wi-Fi Analyzer that runs on Linux. What makes it special is its ability to perform Deauth attacks. This can be done simultaneously on multiple BSSIDs. This tool is effective in both the 2.4 GHz and 5 GHz bands.
   You can read about its full set of features here: https://github.com/ghostop14/sparrow-wifi
2) Install the tool using: **sudo apt install sparrow-wifi**
3) Run the tool using: **sudo sparrow-wifi**
   Note: Make sure your Kali rep lists are up-to-date first using: **sudo apt update**
4) Select the local interface and click scan to see APs in the area.
5) For the Deauth attack, in the Menu bar, click on Falcon > Advanced Scan. Select your Local Wireless interface and if not already in monitor mode, click on “Create Monitoring interface”. This will cause the interface to show up as a “Local Monitoring interface”. Click Scan.

6) Once you've detected your target APs, stop the scan.

7) Right-click on your target AP. You should see the following options:

Deauth Broadcast – Single : Send a single Deauth frame to the AP.
Deauth Broadcast – Continuous : Send continuous Deauth frames to the AP.

Capture WPA keys : Capture the 4-way handshake. On successful capture, a dialog box is displayed to prompt user for a location to save the capture file.

Test each one of these.

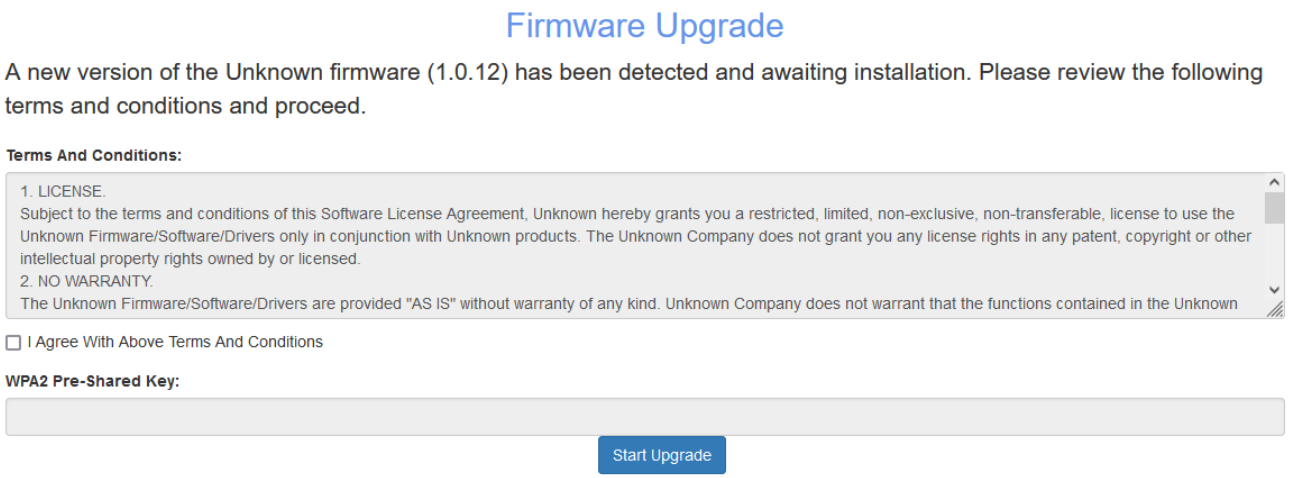
Successful completion will earn you 3 points.

Part 2: Evil Twin attack using Wifiphisher

A captive portal is a web page that is provided to a Wi-Fi client user when the user attempts to connect the client to the Wi-Fi network. The captive portal web page may have the user agree to terms or enter a username and password prior to permitting access to the Internet. The captive portal feature may be supported on SOHO (Small Office Home Office) wireless routers in addition to Enterprise APs.
The attack we're going to perform in this part involves using a captive portal page that tricks a victim into entering the network password.
Wifiphisher only works in the 2.4 Ghz band.

1) Install Wifiphisher using: **sudo apt install wifiphisher**
2) Run it using: **sudo wifiphisher -i wlan0**
3) A scan will begin. Use the up and down arrow keys to pick your target AP. Press ENTER to select.
4) Next, use the up and down arrow keys to pick your phishing scenario based off which your captive portal web page will differ. Press ENTER to select.
5) Wifiphisher will now setup the Evil Twin AP which will have the same SSID as the target.

6) Connect your client (preferably phone) to the Evil Twin AP's SSID. The captive portal should pop up prompting for the network password (WPA2 Pre-shared Key). Below is the captive portal page when the "Firmware Upgrade" option is selected.



7) Enter the password and observe the Wifiphisher terminal. Notice anything interesting?

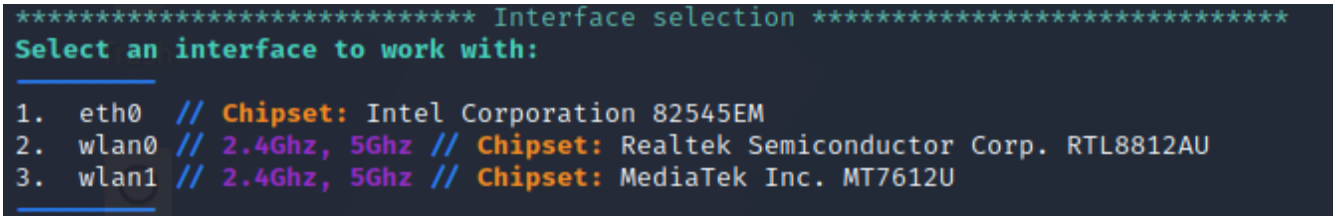
Successful completion will earn you 3 points.

Part 3: Evil Twin attack using airgeddon

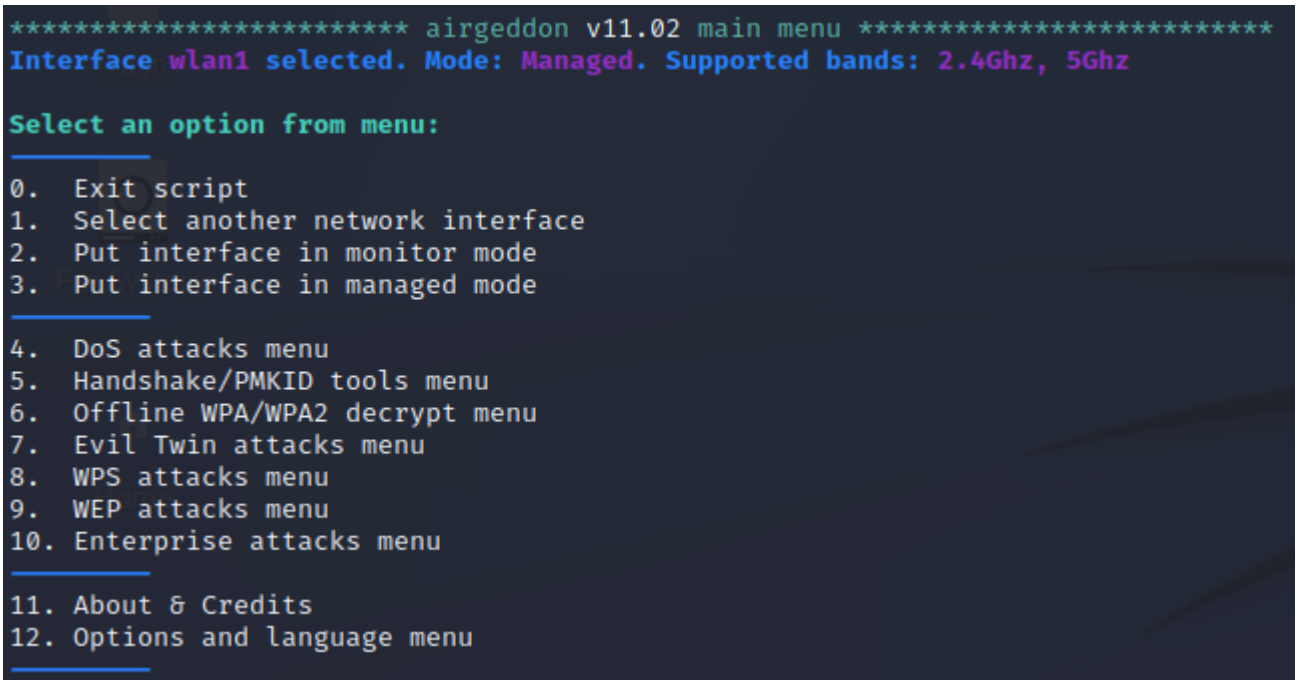
The airgeddon tool will perform a deauth attack in an attempt to get the client to reconnect to the network during which the 4-way handshake will be captured. Next the Evil Twin AP will be created, and the client will be deauthenticated again. This time the user may choose the Evil Twin AP. At this stage the client will be provided with a captive portal page prompting for the network password. Once entered, this password along with the 4-way capture will be used in a bruteforcing attack to verify if the password was entered correctly. If the password is entered incorrectly, the client will be prompted for the password again via the captive portal page. If entered correctly, the client will be displayed a message saying the password was correct and internet access will be provided shortly. However, the client is never connected to the Internet.

Two adapters are required to perform this part so you may work in pairs.

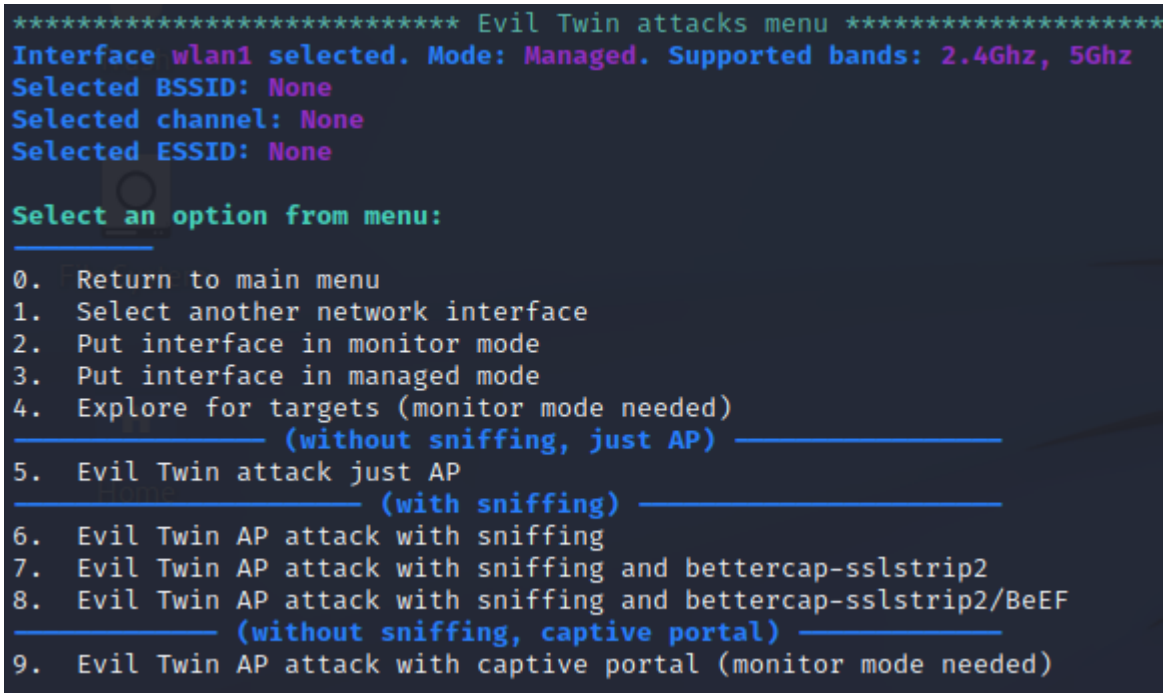
1) Install the airgeddon tool using command: **sudo apt install airgeddon**
   Note: Make sure your Kali rep lists are up-to-date first using: **sudo apt update**
2) Run the tool using: **sudo airgeddon**
   Pay attention to the Essential tools and Optional tools and install the ones that are missing. Then restart the tool.
3) You will be prompted to select an interface to use.



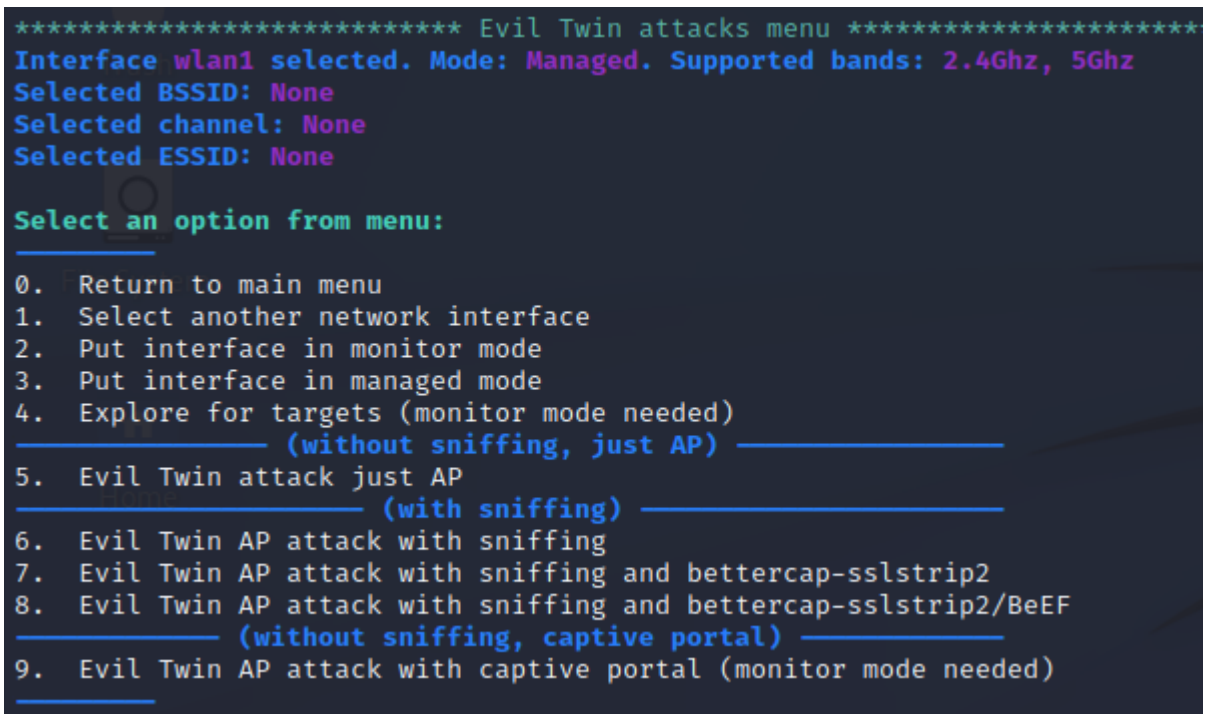
4) Next, you have to select an attack type to perform. We will select option 7 for “Evil Twin attacks menu”:



5) Next, select the specific attack. We will select option 9 for “Evil Twin AP attack with captive portal”.



6) Next, if your interface was not already in monitor mode, you will be prompted to put into into monitor mode which you can do using option 2 in the main menu as shown below:

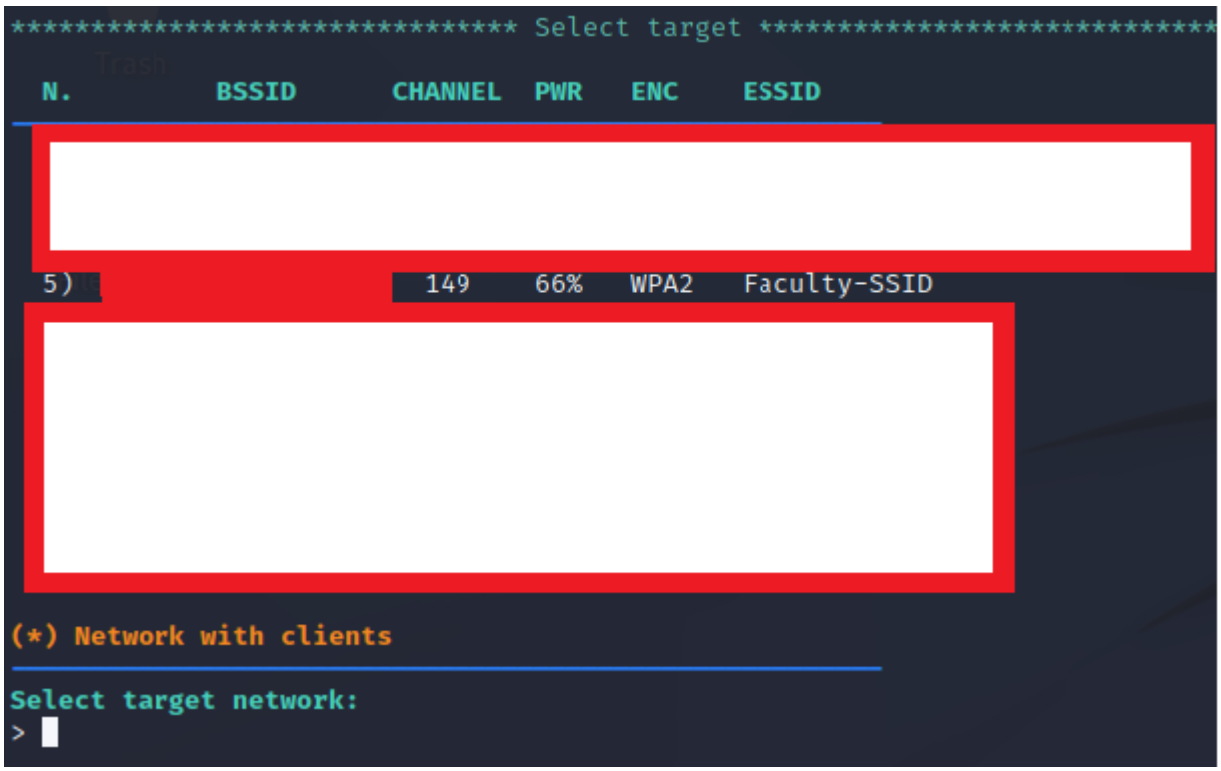


7) Notice a message that says:

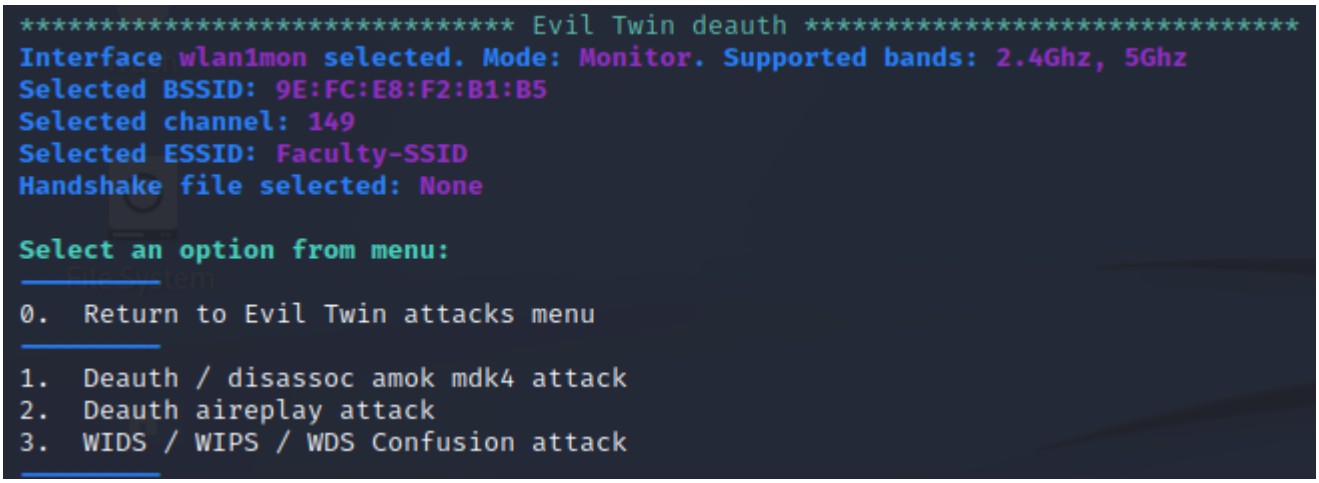
   Hint **The unique Evil Twin attack in which it's not necessary to have an additional interface with internet access is the captive portal attack**

   This indicates that a second interface is required. This is because one interface will be used to perform the deauth attack (monitor mode) while the other interface will be used to act as the Evil Twin AP (managed mode).

8) Next, there will be a scan of nearby APs and connected stations (clients) which will occur in a separate terminal. Use CTRL+C to stop the scan.
   You will then be provided with a dump of the scan in the main terminal.



9) Once the network is selected, you will need to select the tool to be used for the Deauth attack. We will select option 1 “Deauth / disassoc amok mdk4 attack”.



10) You will next be prompted to select if you wish to use DoS pursuit mode. This is useful if an AP switches to another channel. You may select either yes or no.

11) You will also be prompted if you wish to spoof your interface MAC address. You may select yes or no.

12) You will then be asked if you have a previously saved capture file for the 4-way handshake. **Select No!**

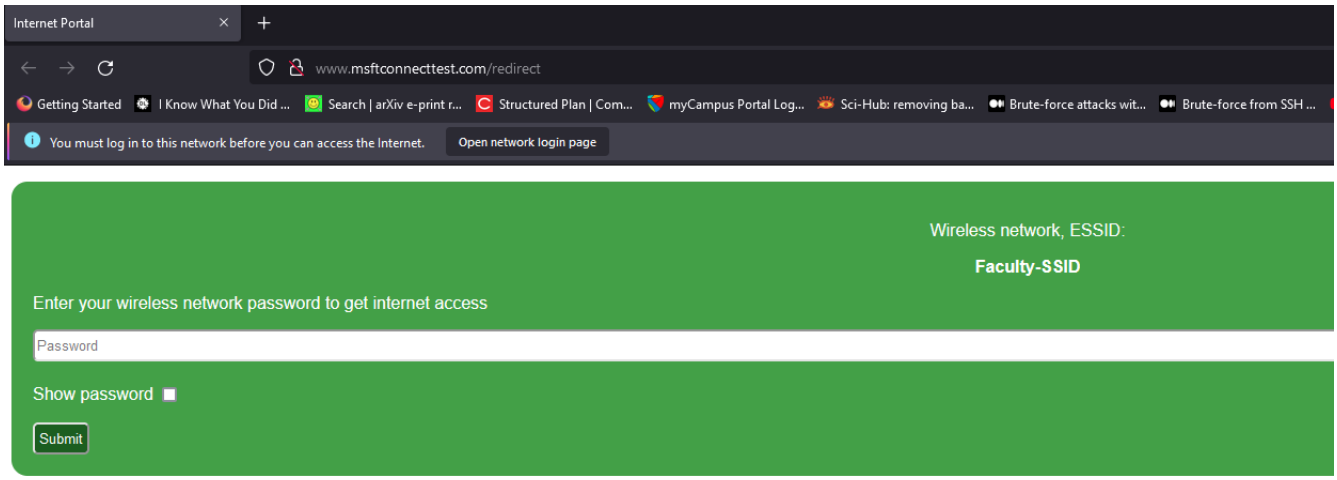
13) Then set the deauth timeout as you see fit. More the better.

14) If you already have a client connected to the AP, it will be deauthenticated. If not, attempt to connect a client. Your client will actively be deauthenticated and the 4-way handshake will be captured.

15) You will need to pick some file paths to save the handshake file, captured password and pick a language for the Captive Portal.

16) You will then be prompted to begin the Evil Twin attack. This will open a number of separate terminal windows.

17) The Evil Twin AP will show up with the same SSID as your legitimate Wi-Fi network but will be an open network i.e. it will not require a passphrase. Connect a client it and you will automatically be taken to the Captive Portal page.



18) Entered an incorrect password first and observe the message displayed in the Captive Portal. Also see the captured password in the “Control” terminal window.

19) Now try the correct password and observe the message displayed in the Captive Portal. Also see the captured password in the “Control” terminal window.

Successful completion will earn you 3 points.

Reflection Question:

1) What specifically can be done to protect against the DoS attacks used above? Explain (1 point).

Submission Requirements: You may work in groups of no more than 2 students and submit a single video link explaining the steps in the Kali VM and the wireless client. Ideally you can do this if you run the Kali VM and wireless client on the same PC. If your PC does not have a Wireless NIC, you may use one of your alfa adapters to act as client and the other in monitor mode.

Insert Video Link below:

2022

Grading Rationale:

1) Graded out of 10 points.
2) Not performing a step correctly or an incomplete step including not answering a question correctly results no points earned.
3) Deduction for poorly organized work including not using the lab document, poor/incorrect arrangement of answers, missing labels for each Part and Step. Depending upon severity, deduction of 1-10 points.
4) Incorrect/incomplete/incompetent work can result in zero if fundamental requirements are not met.