Lab 5: Secure Implementation of Wireless Networking

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will view files and clear text traffic from an unsecured wireless capture file. Students will also obtain a WEP key and a WPA passphrase using the aircrack-ng utility. After obtaining the WEP key and WPA passphrase, students will decrypt the traffic using airdecap-ng. By completing these exercises, students will become more cognizant of the dangers involved in using unsecure wireless network, wireless networks with WEP, and wireless networks using WPA or WPA2 with a weak passphrase that is in the dictionary.

**Materials**

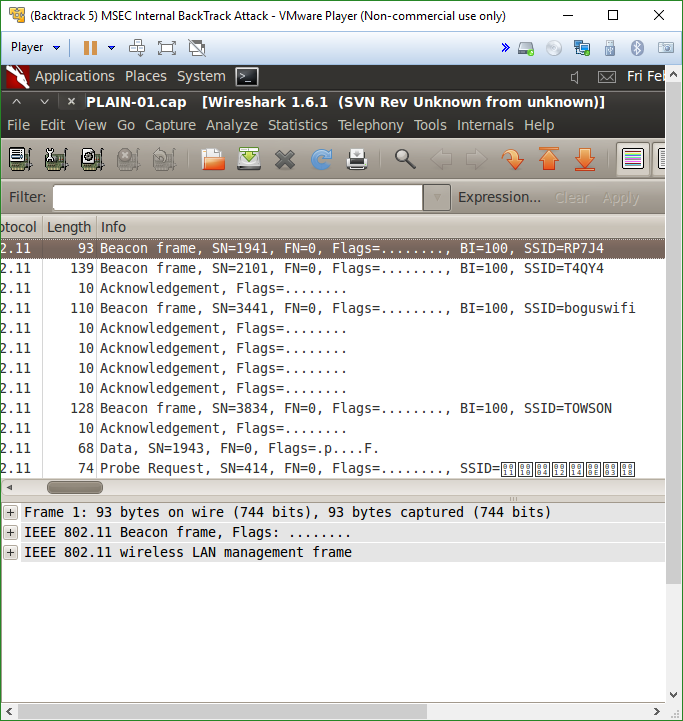
1. Backtrack 5

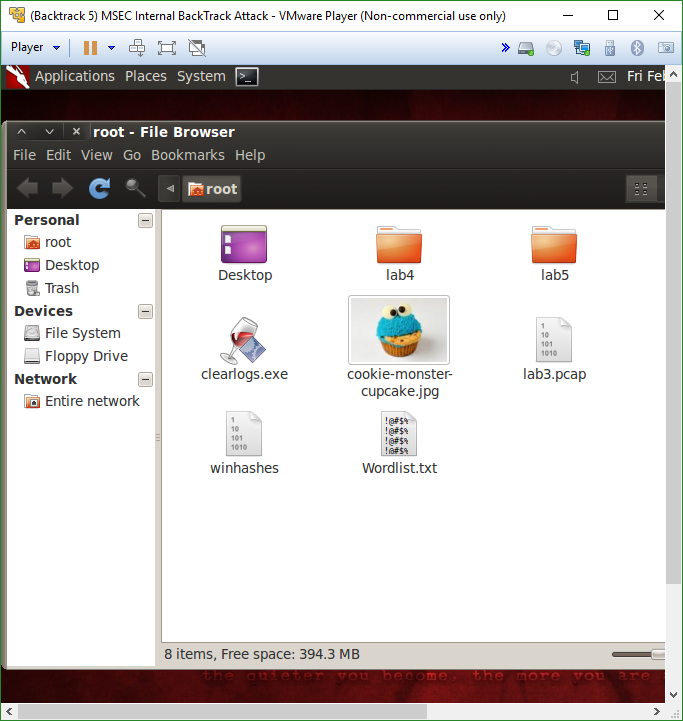
**Methodology**

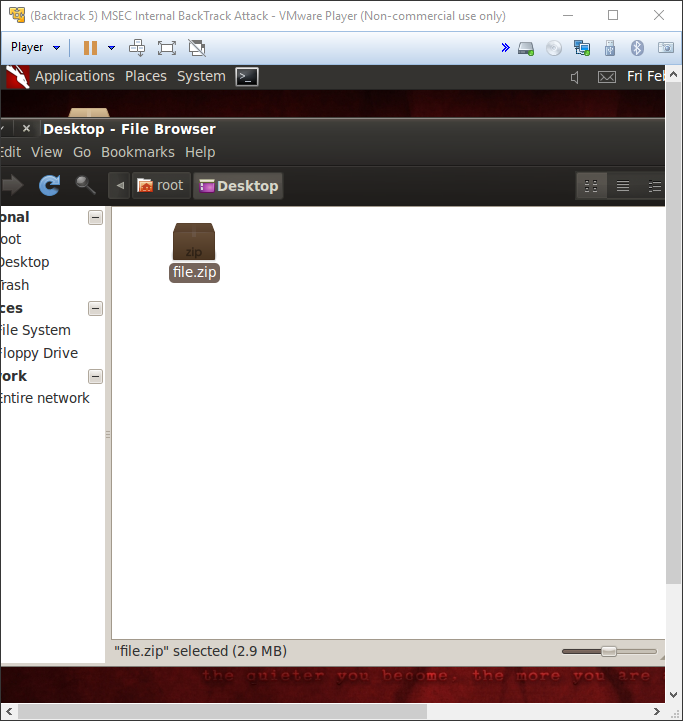
By using the aircrack-ng utility to obtain the passphrase and airdecap-ng to decrypt the traffic

**Lab**

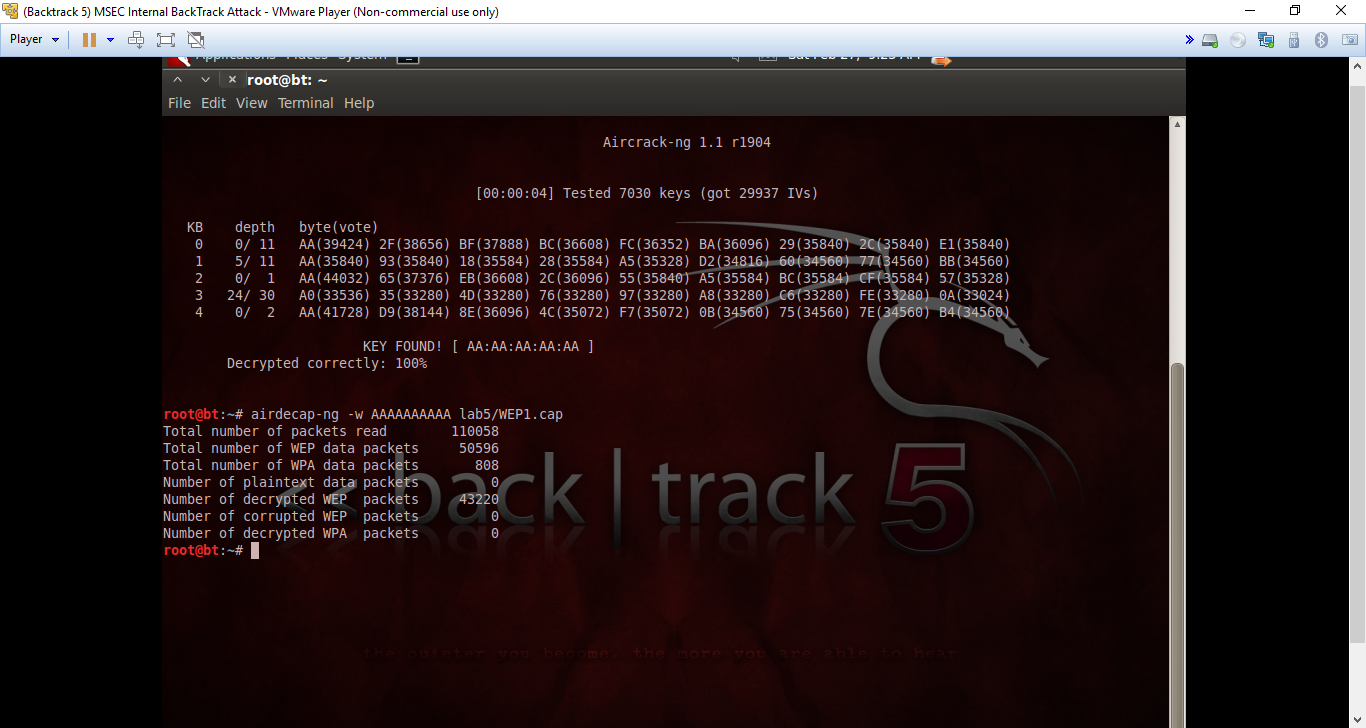
Task 1:

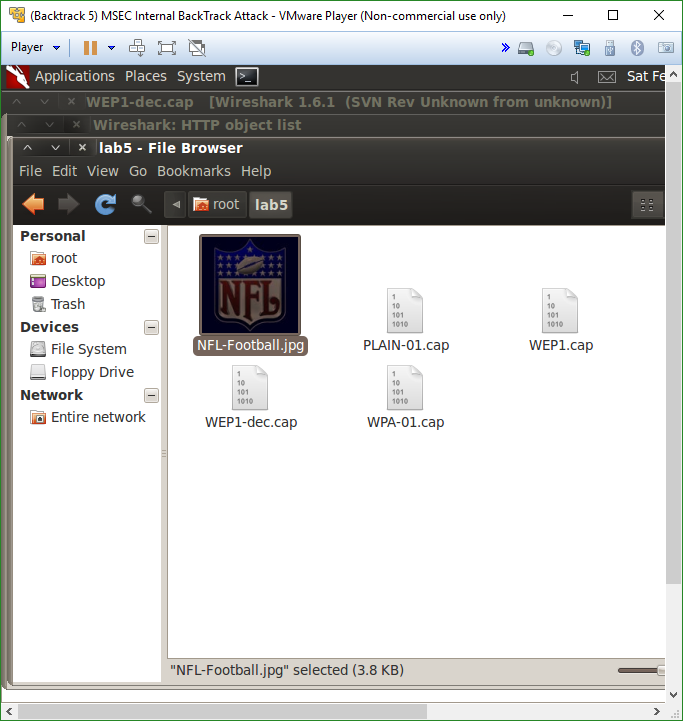
1. 

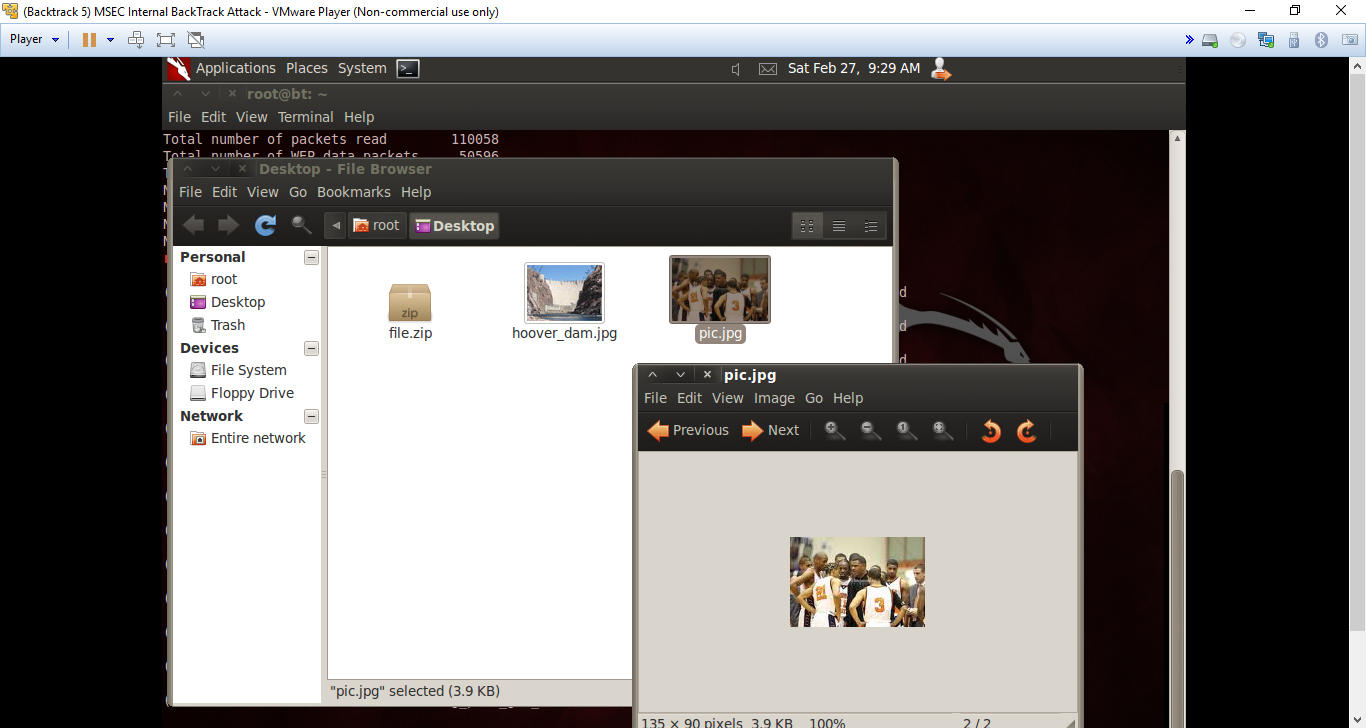
2, 

3. 

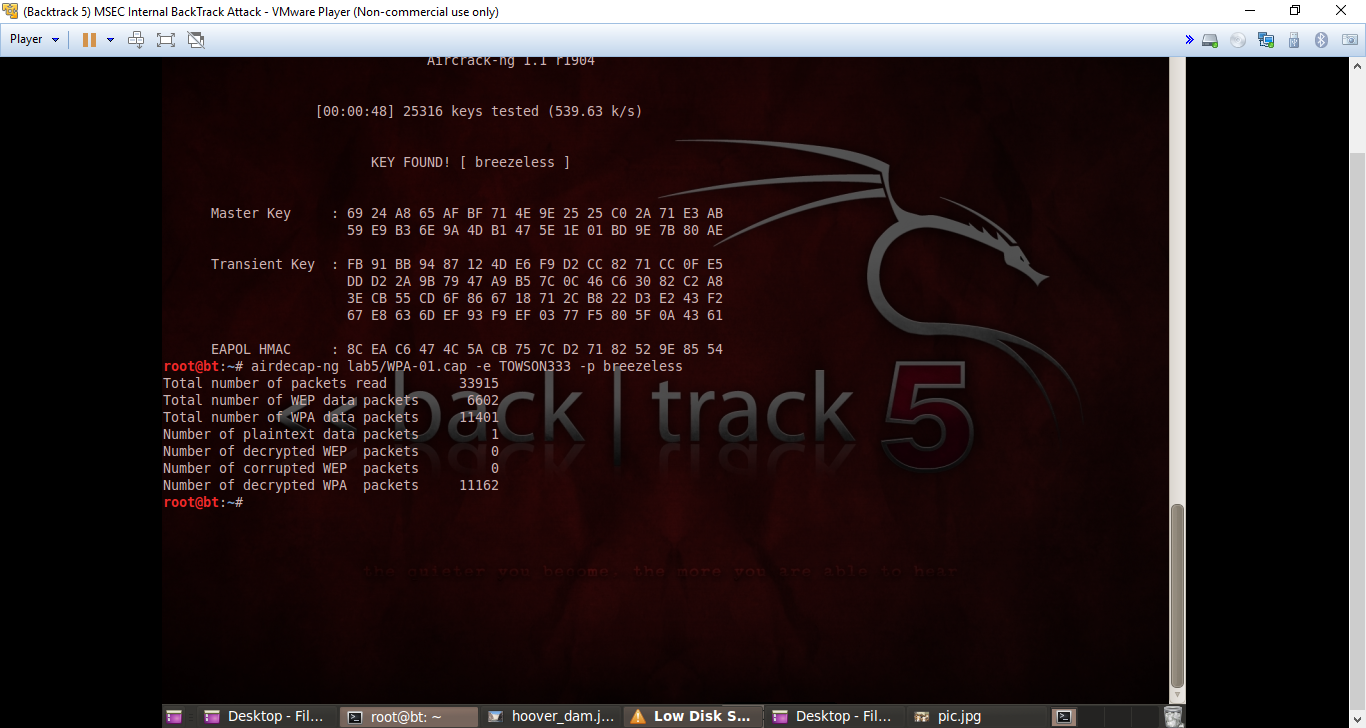
Task 2:

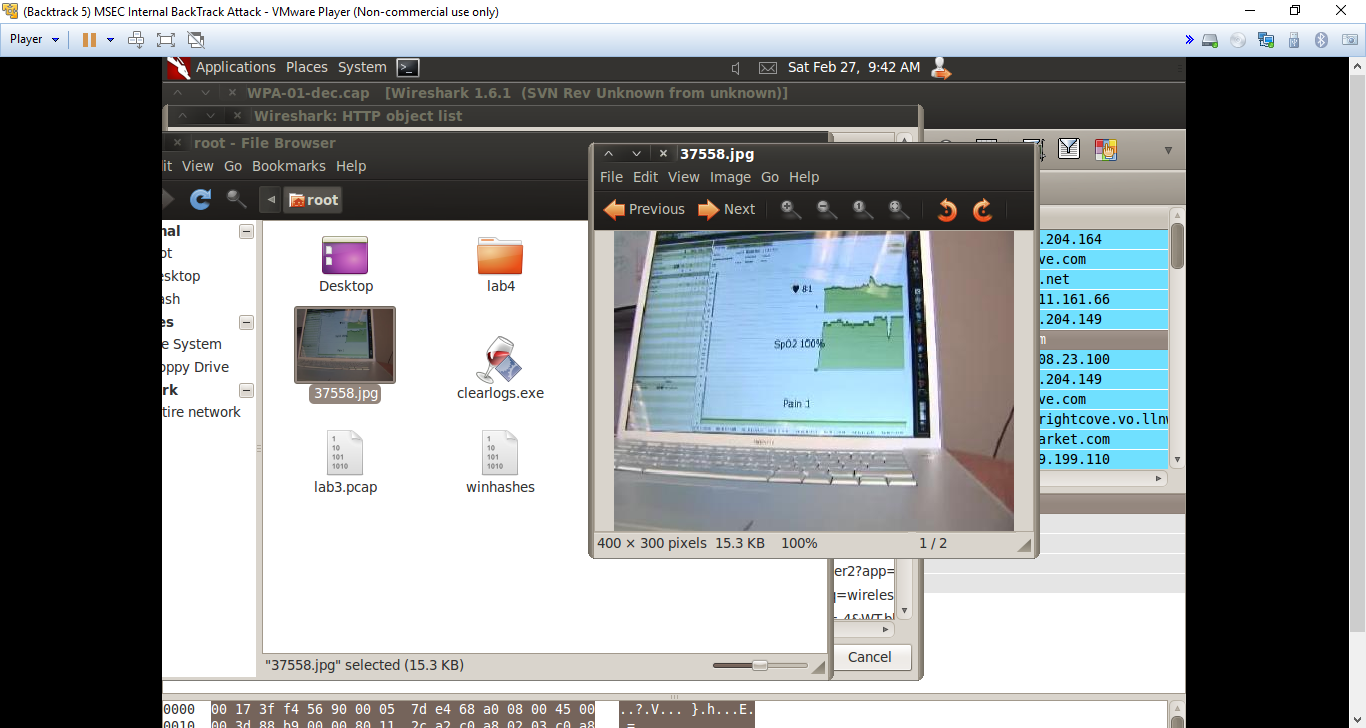
1. 

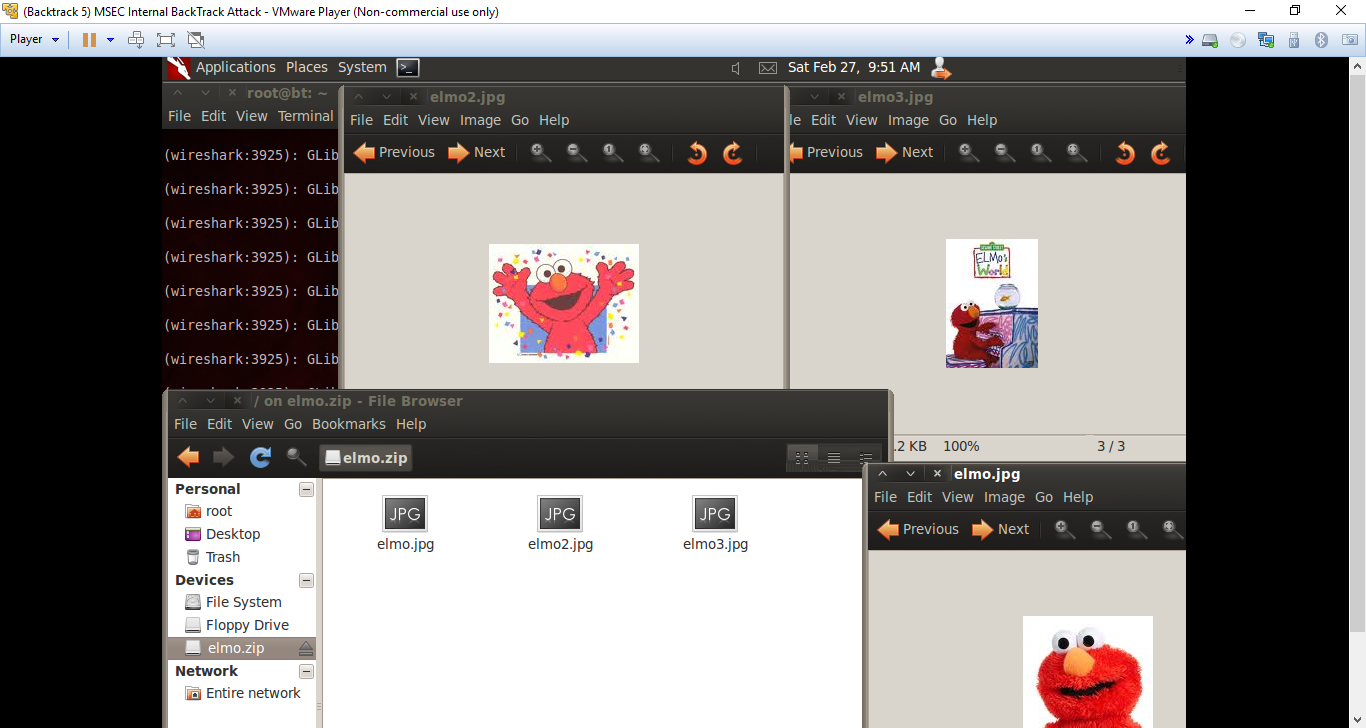
2.

3.

Task 3

1. 

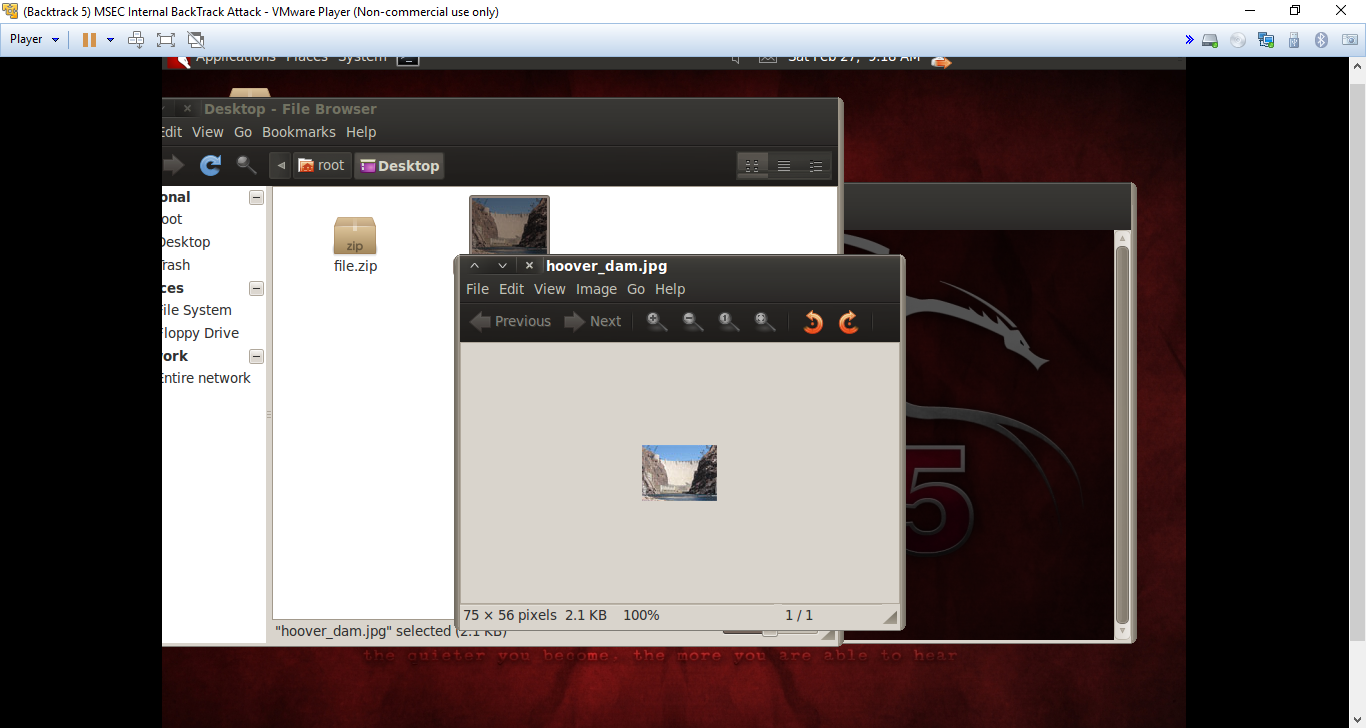
2.

3.

**Questions:**

Task 1

1. What is the type or router (name of company) being used on the wireless network with the Service Set Identifier (SSID) of *boguswifi*? **Microsoft WPA**
2. See if you can locate the channel that the TOWSON wireless network is using. **Channel 1, with a DS parameter set of 3**
3. From the Wireshark menu, select File, Export, Objects, HTTP. Find the Hoover\_dam.jpg picture and save it to your home folder. View the picture.



Task 2

1. Provide the name of at least one file that was transferred during the FTP session. **pic.jpg**
2. What is the name of the tool that can be totalized to decrypt WEP traffic? What must you do in conjunction with the tool for the traffic to be decrypted? **The aircrack-ng utility; pick the target network (in this case it’s #5 on the list)**
3. Which 2 IP Addresses were involved in the transfer of data via the FTP protocol? **192.168.2.3 and 192.168.2.4**

Task 3

1. Find the names of at least 2 picture files that were transferred. **Elmo.jpg and elmo2.jpg**
2. Using the same ftp filter in Wireshark, and find the name of the 2 executable files that were transferred. **putty.exe and WinPcap\_4\_1\_2.exe**
3. What was the password used to log on to the FTP site? **hfgfh**

**Conclusion**

This lab was a bit tricky because of the difficulty in finding specific files was rather time consuming. However, besides that the lab was relatively self-explanatory, walking you through different attacks like the dictionary attack in particular. Also, even though it was a bit annoying, it was helpful to figure out where certain things are located in wireshark, and constantly having to search for different files was in the end beneficial. Lastly, it is clear now that WEP is way easier to hack into because I’ve now experienced the difference in WPA and WEP which I found very insightful.

**Grading Rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement | **Points Allowed** | **Points Actual** | **Comments** |
|  |  |  |  |
| **Title page** | **5** |  |  |
| **Screen shots** | **5** |  |  |
| **Questions** | **10** |  |  |
| **Conclusion** | **5** |  |  |
|  |  |  |  |
| **Extra Credit** |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Total Points** | **25** |  |  |