Lab 3: Protocols and Default Network Ports – Transferring Data Using TCP/IP

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

By the end of this lab, students will be able to transfer files using the ftp, http, and scp protocols. Protocols like HTTP, FTP, and SCP can be used to transfer files from one computer to another. File transfers are unencrypted by default when the FTP or HTTP protocols are used. File transfers will be encrypted if SCP is used. In this lab, the student will have the opportunity to configure servers and utilize file transfer client utilities.

**Materials**

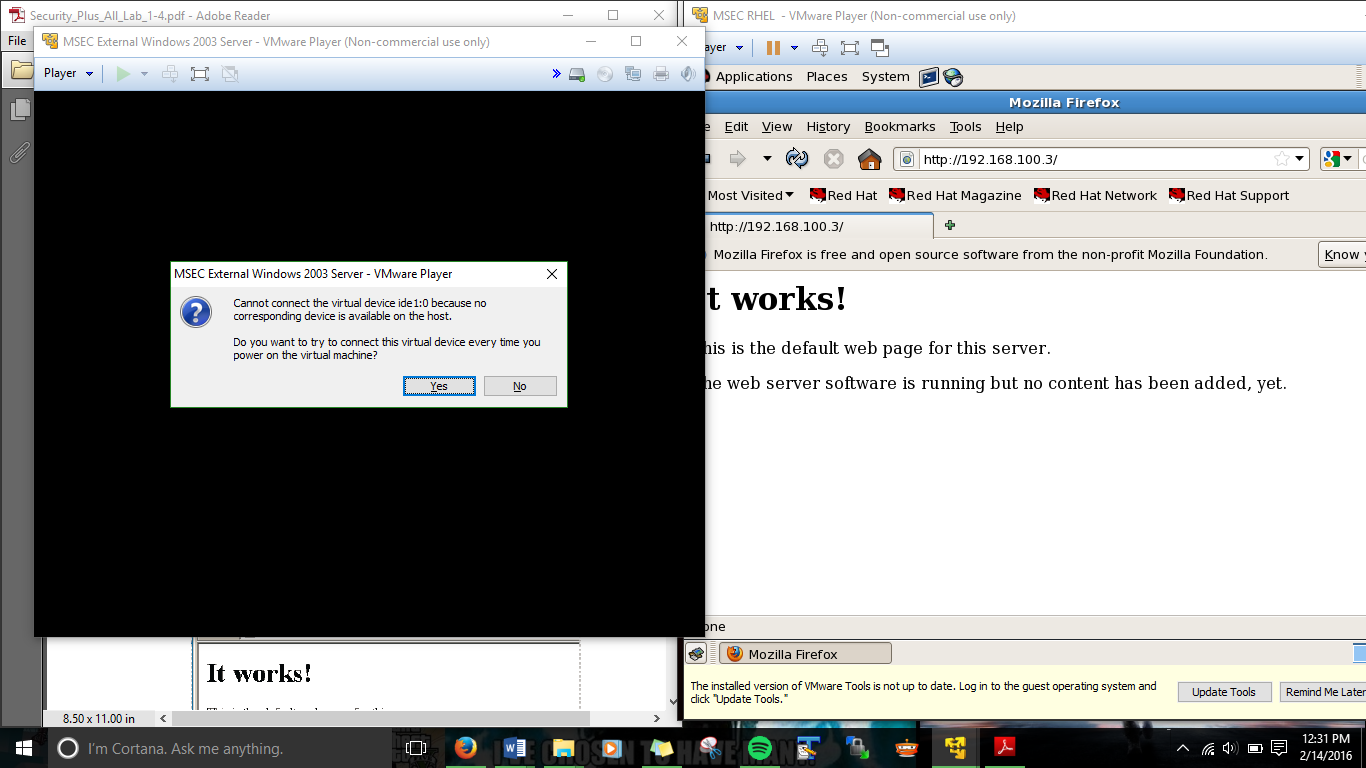
1. Backtrack 5
2. Red Hat Linux
3. Windows 2003 **INTERNAL** server

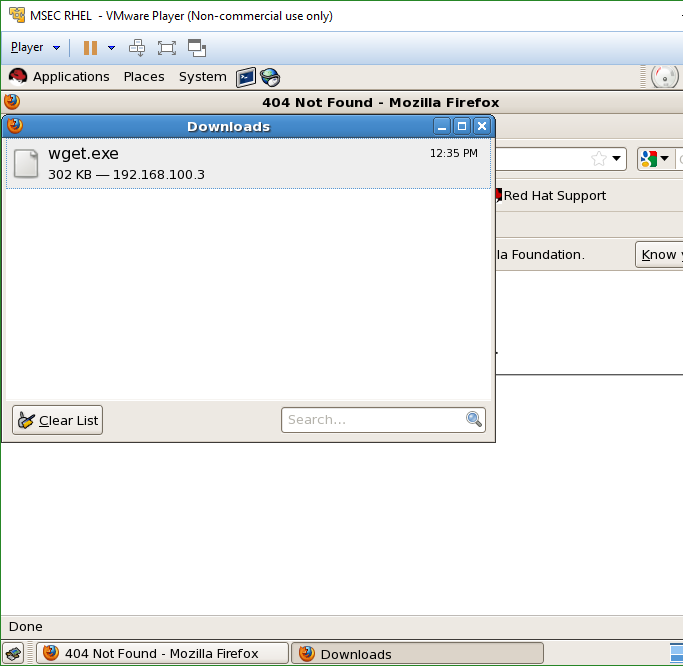
**Methodology**

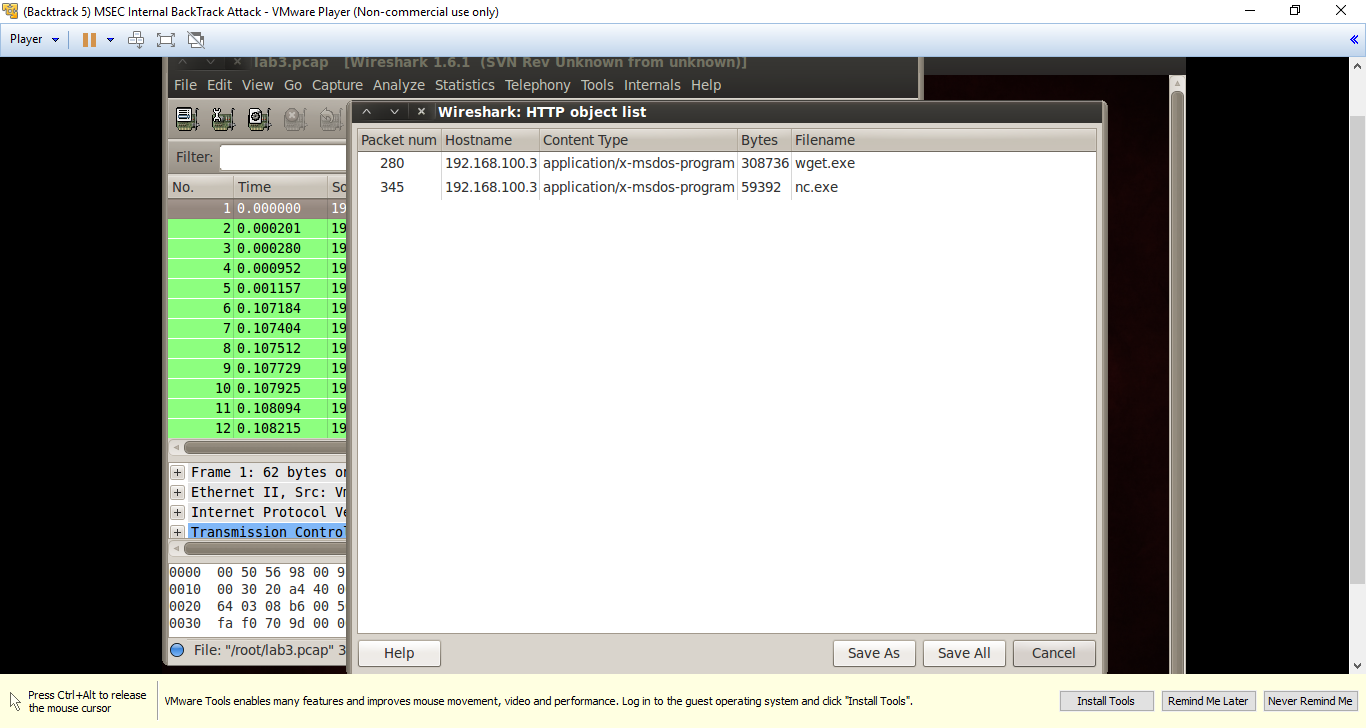
Using Backtrack 5 to copy and put files between Windows 2003 and itself, as well as setting up a permanent connection with RHL

**Lab**

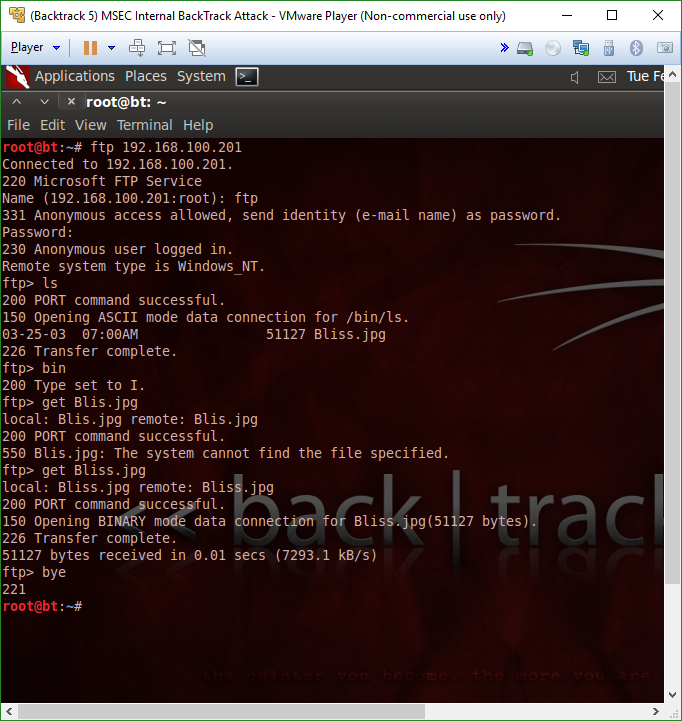
Task 1: (error)

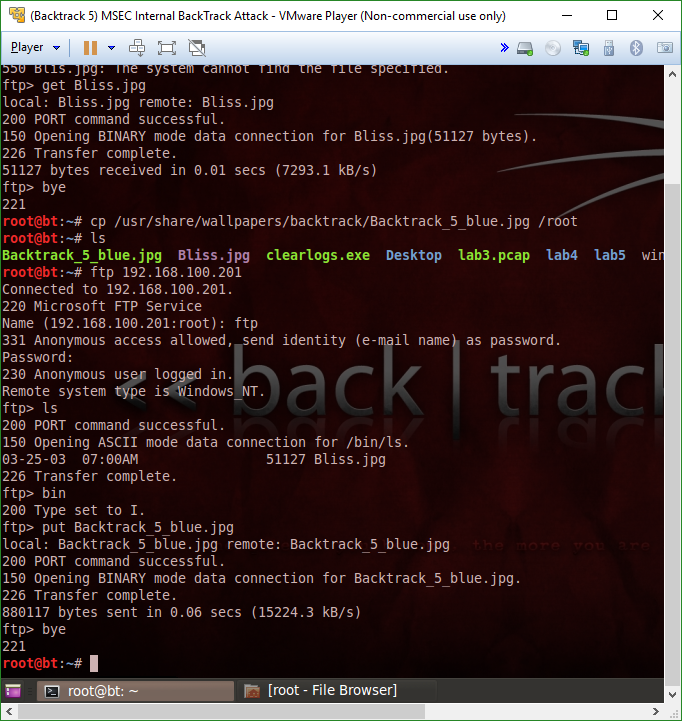
1. 

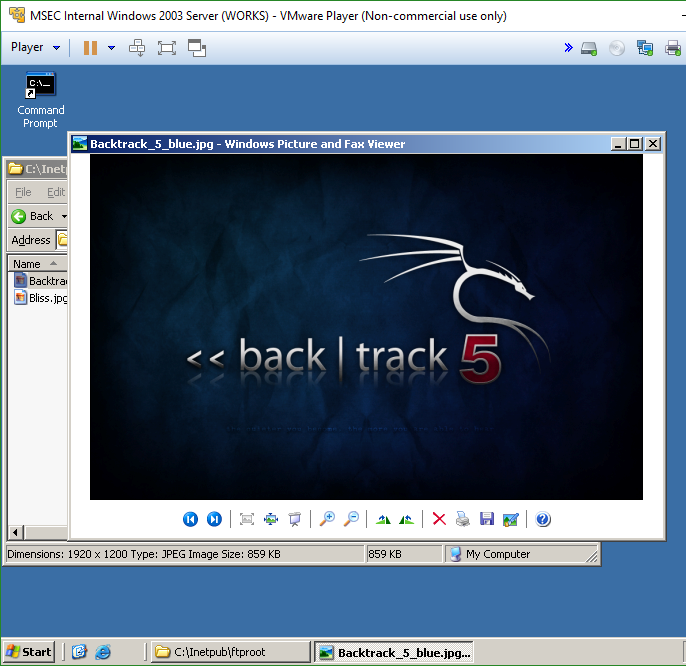
2, 

3. 

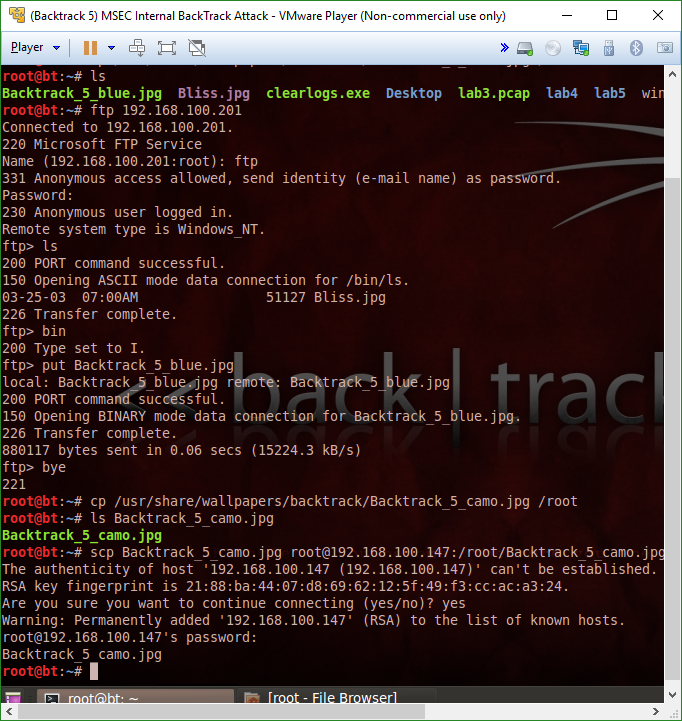
Task 2:

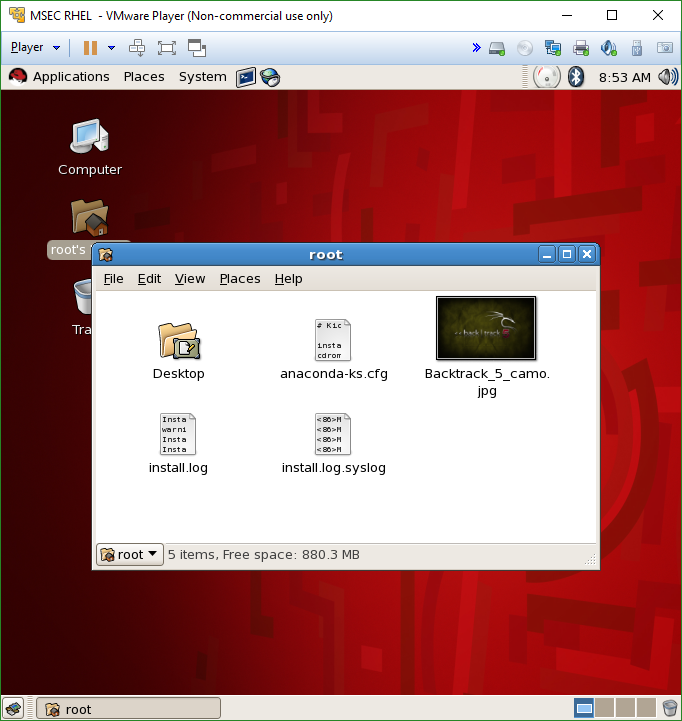
1. 

2.

3.

Task 3

1. 

2.

**Questions:**

Task 1

1. What is the command to check to see if the web server is running on Linux? **netstat**
2. How do you parse HTTP objects out of Wireshark? **By exporting the objects**
3. How can you display all of the options for the wget command? **Wget --help**
4. What does HTTP stand for and what port does it use? **HyperText Transfer Protocol, it uses port 80**

Task 2

1. What are the two ports that FTP uses? **20 and 21**
2. What is the command to upload a file to an FTP server? **Put**
3. Which ftp command should be used before uploading a picture file? **Bin**
4. What is the default directory where Windows FTP files are stored? **Inetpub\ftproot**

Task 3

1. What port does SSH and SCP use by default? **22**
2. What does SCP stand for? **Security Copy**
3. How is SCP different from the FTP protocol? **FTP is not set up on all computers**
4. What benefit does using SCP provide over other protocols? **SCP is encrypted**

**Conclusion**

I had a few issues with the first and second task due to using the incorrect Windows 2003 server, however I thankfully got it sorted out after a bit of troubleshooting. However, besides that hiccup, the rest of the lab was rather self-explanatory when dealing with how the ftp connection works between hosts. Also, it was interesting to see how the communication over ftp looked like in the first task when using wireshark. In conclusion, I think I learned more about the scp and ftp connection and what it looks like from a hacker’s perspective.

**Grading Rubric**

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