Lab 4: Protocols and Default Network Ports – Connecting to a Remote System

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 connect to remote systems running Windows and Linux and run commands to perform administrative tasks. Students will use TELNET protocol to connect to remote windows systems and the SSH protocol to connect to a system running Linux. Students will then analyze both protocols within network traffic to determine whether the protocol uses encryption or clear text.

**Materials**

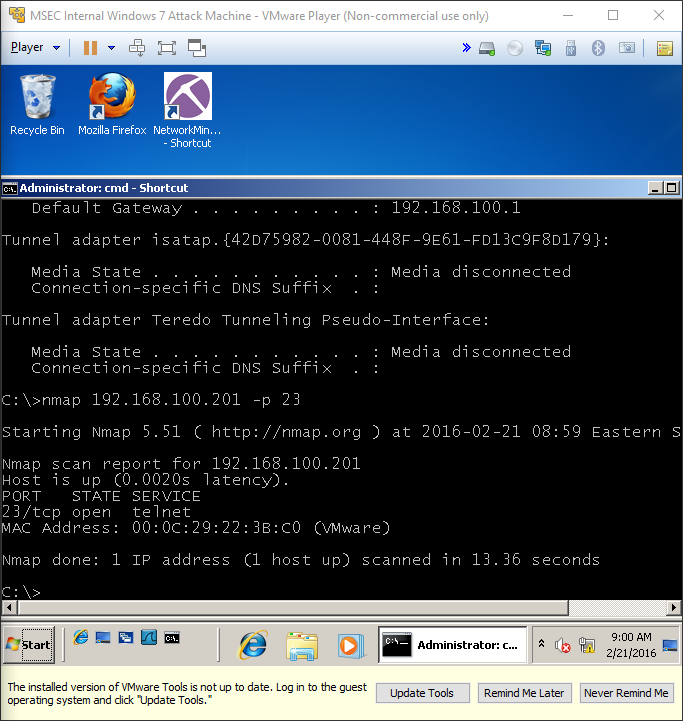
1. Backtrack 5
2. Windows 7 attack machine
3. Red Hat Linux
4. Windows 2003 Server

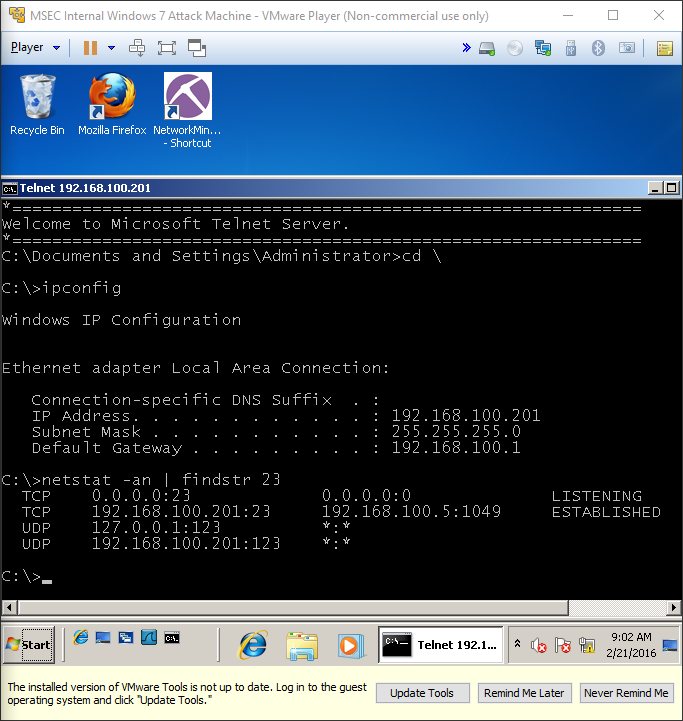
**Methodology**

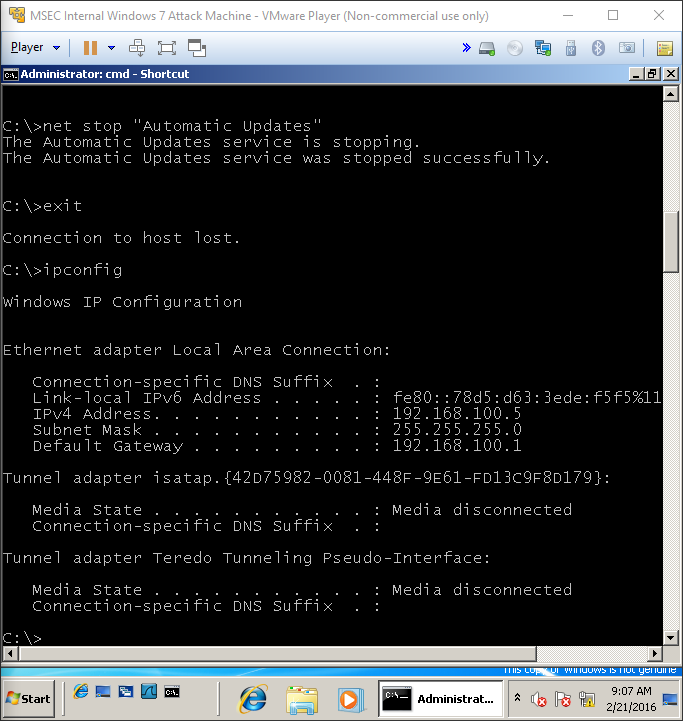
Using Windows 7 command line and PuTTY to access a remote server and Wireshark to view the communication

**Lab**

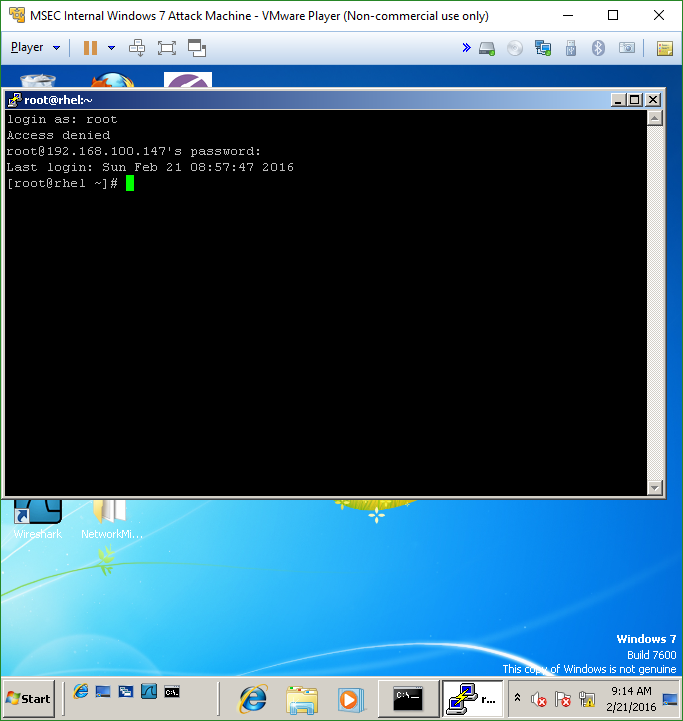
Task 1:

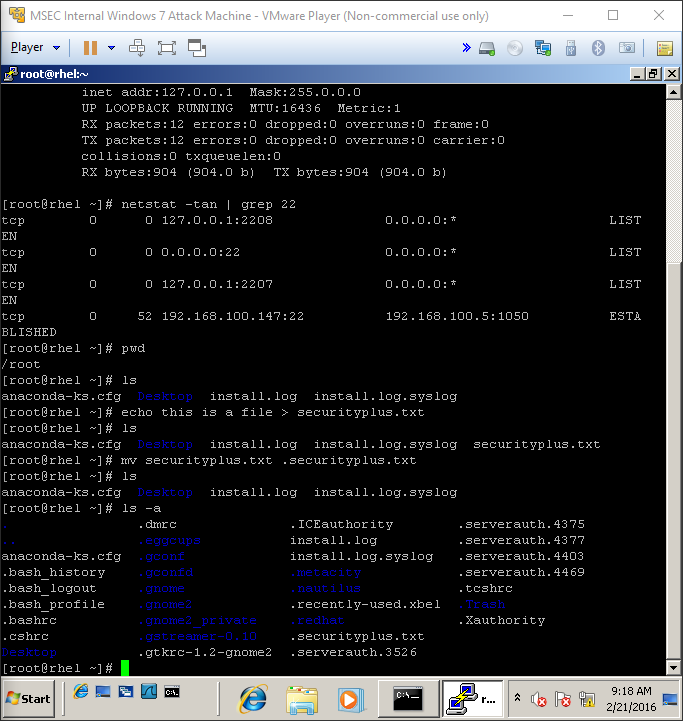
1. 

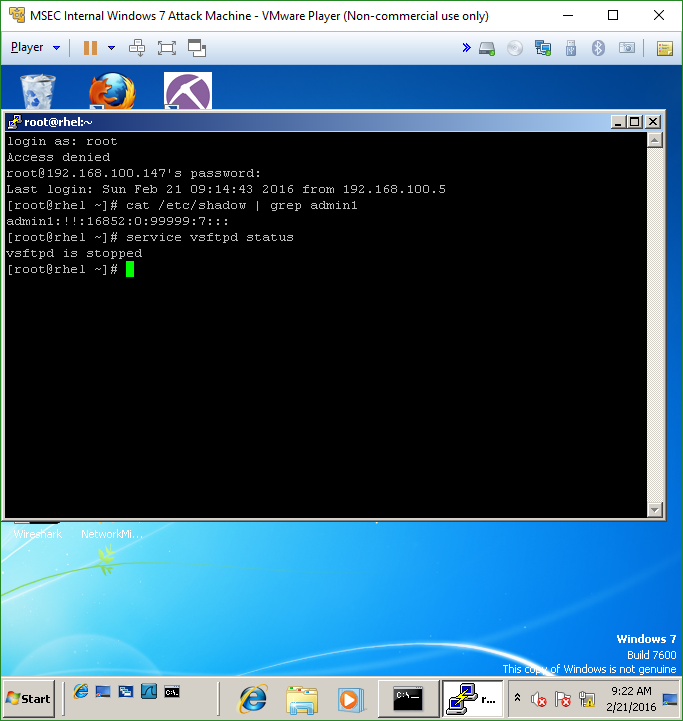
2, 

3. 

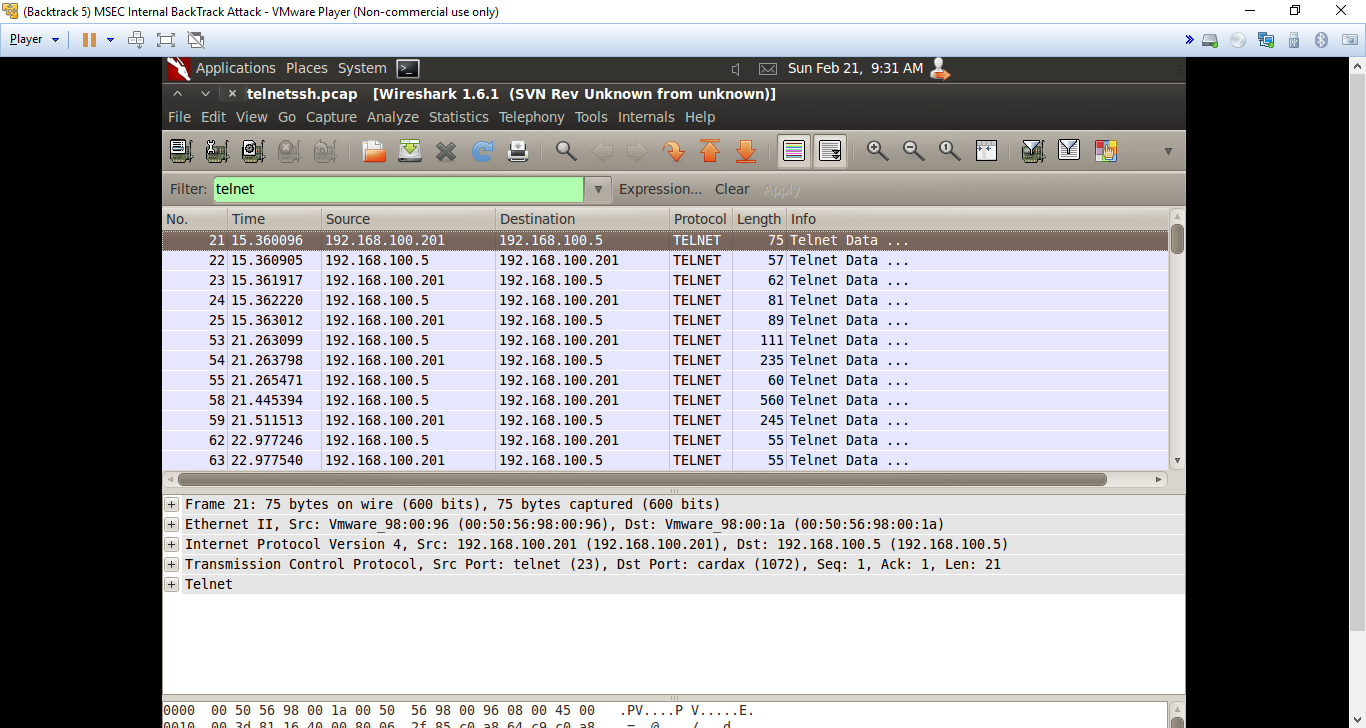
Task 2:

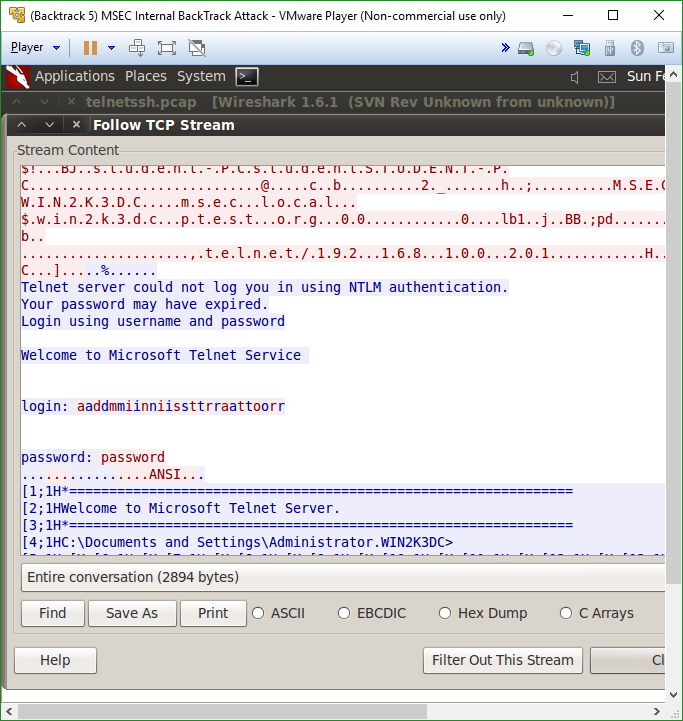
1. 

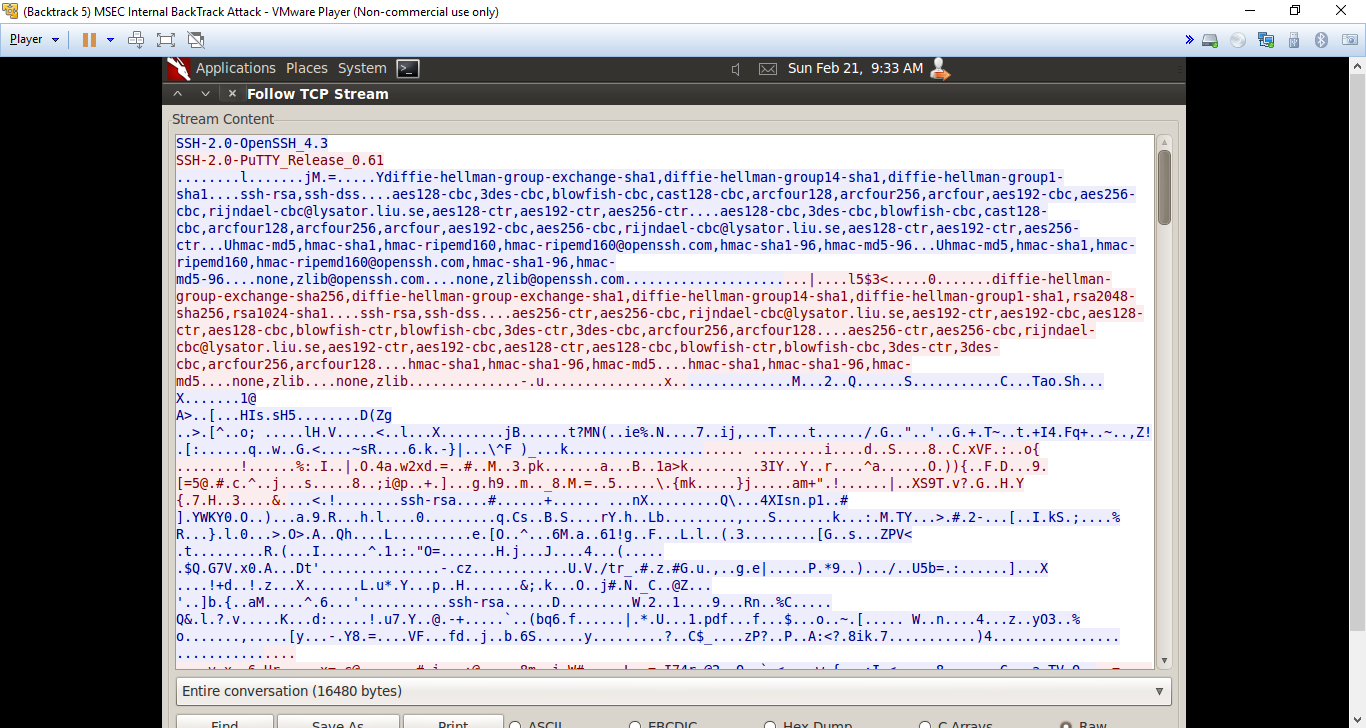
2.

3.

Task 3

1. 

2.

3.

**Questions:**

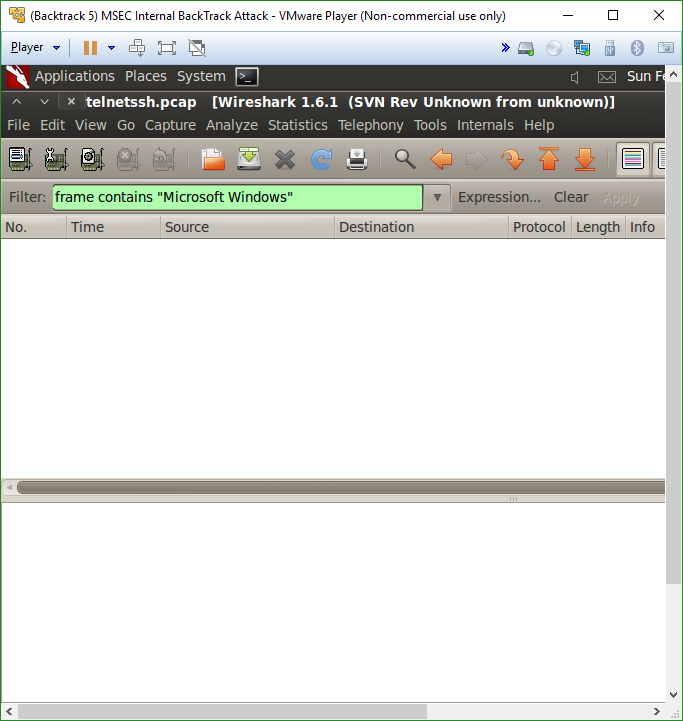
Task 1

1. What command can be used to show an active TELNET connection? **Netstat**
2. What is the command that can be used to display files on a remote system when an administrator is connected via a TELNET session? **Dir**
3. How can you create a file on a remote system during a TELNET session? **Echo the desired words then append them to a .txt file (echo “stuff” stuff.txt)**
4. What command can be used to determine if a remote system is running TELNET? **Ipconfig**

Task 2

1. What port does Security Shell use? **22**
2. Is there a native SSH client or server on Microsoft Windows systems? **No**
3. What is the file in Linux that contains the password hash? **Shadow**
4. What are two methods that can be used for creating a file during a remote secure shell (SSH) connection within Linux? **Echo words and append them to a .txt file or enter the vi editor**

Task 3

1. Type frame contains PuTTY in the Wireshark filter pane and click Apply. Determine which version of PuTTY is in use. **SSH-2.0-PuTTY\_Release\_0.61**
2. If you type frame contains shadow in the Wireshark filter pane, why are there no results in the root account viewed in the shadow file remotely? **Because they are hidden**
3. Name a user account that was displayed in the clear text traffic. **For some reason nothing appeared…**
4. Name the file that was created, and then hidden.  **^**

**Conclusion**

The lab was surprisingly quick although, at first I ran into some problems with my version of Windows not being legitimate, so I re-downloaded the VM and updated it, and thankfully it works fine now. But regarding the ssh connection, it was relatively simple to perform, with the only real issue being making sure you are typing the correct commands. After I get used to typing more and more commands it will probably be drilled into my head, however at a first glance remembering every command to perform certain operations can be a little daunting. Also, using Wireshark to view the cleartext and encrypted ssh communication was interesting as always. Overall this lab has helped me understand more about how the vm’s work and how TELNET, SSH, and Wireshark operate as well.

**Grading Rubric**

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