Lab 2: Secure Network Administration Principles – Log Analysis

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 parse log files within Linux and Windows for information pertinent to security events on their system. Students will perform administration on Linux and Windows machines and view the logs from these tasks.

**Materials**

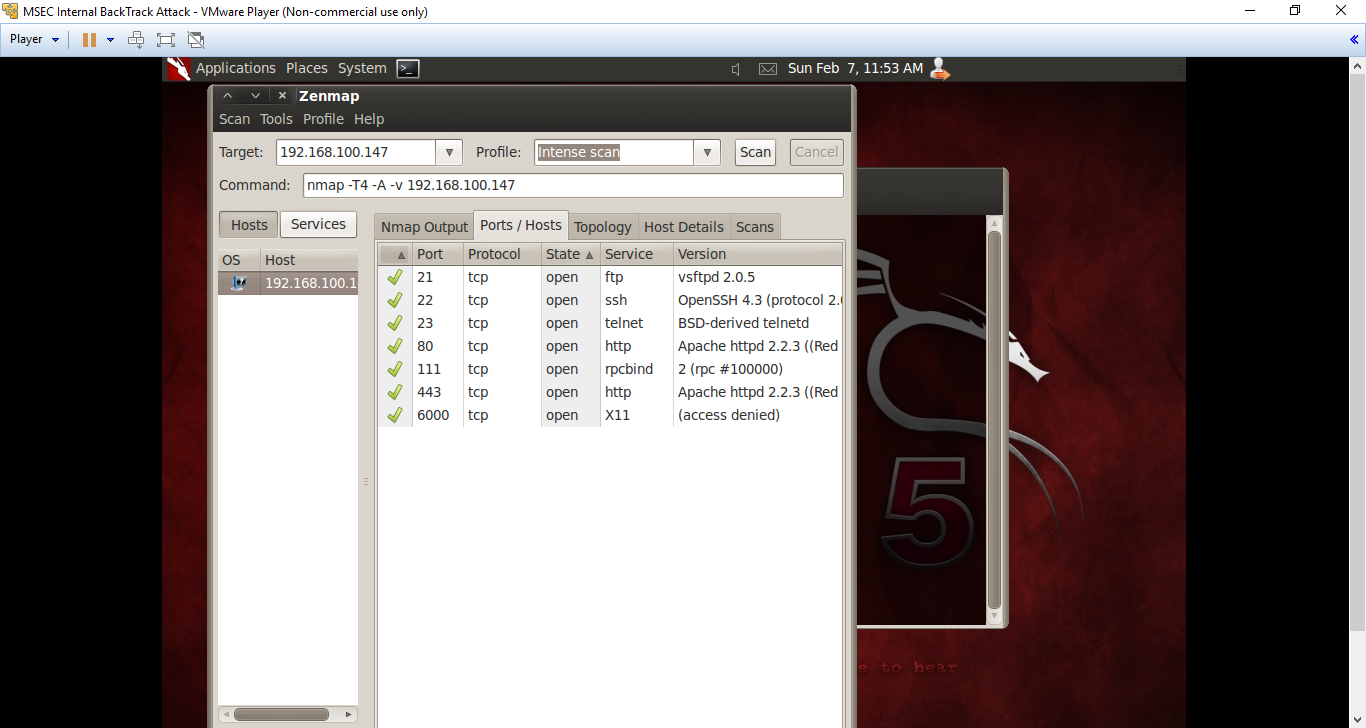
1. Backtrack 4
2. Backtrack 5
3. Red Hat Linux
4. Windows 2003 Server

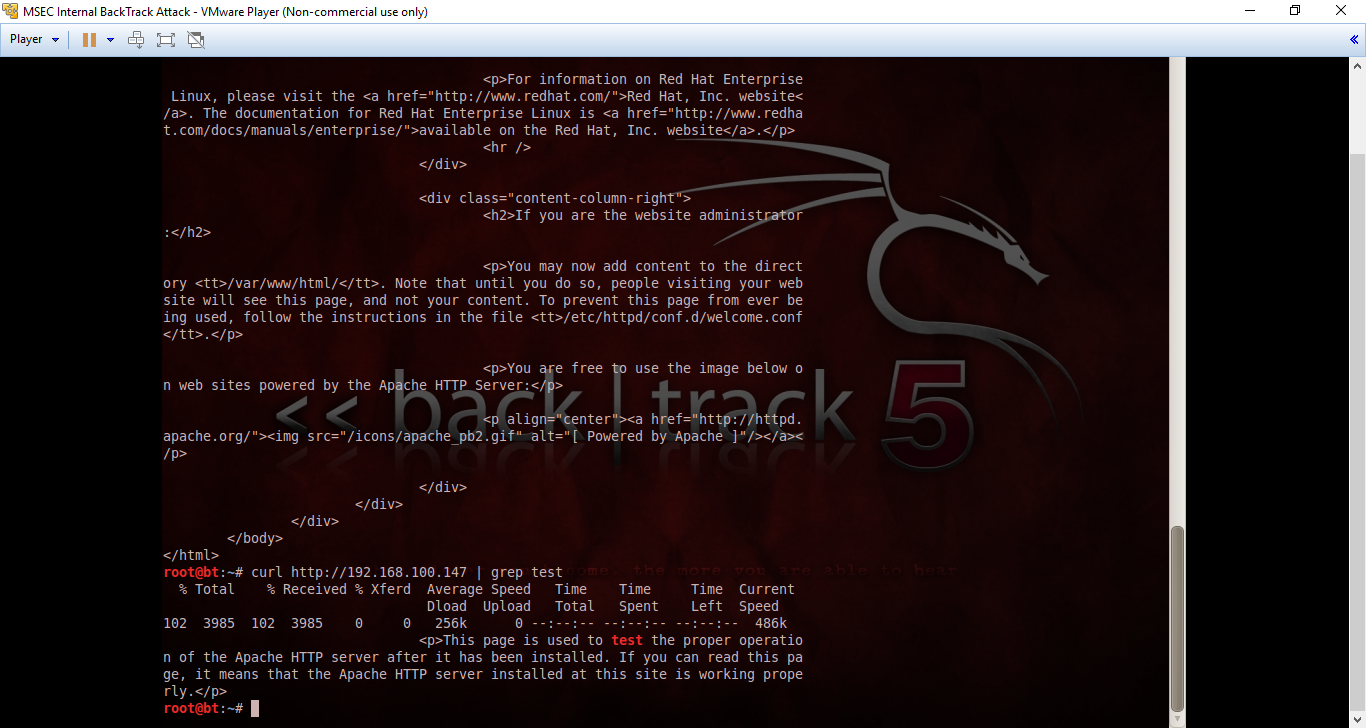
**Methodology**

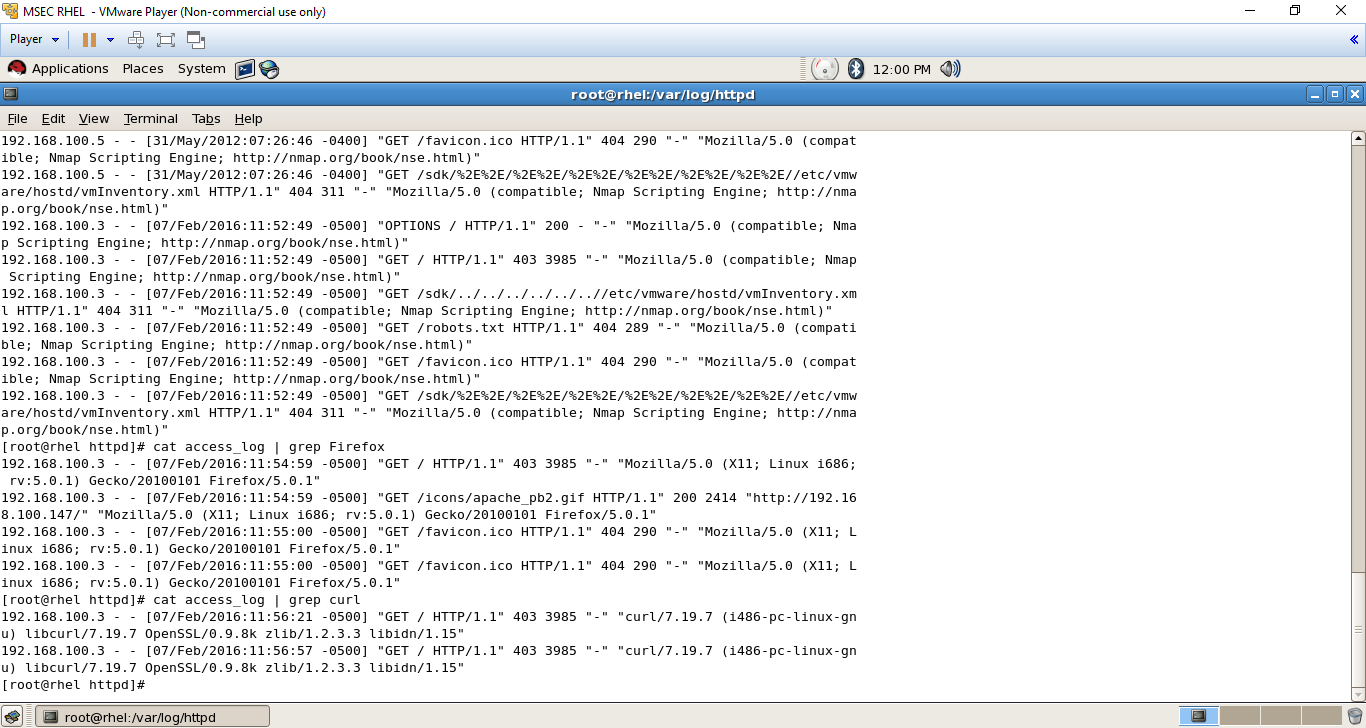
Using Backtrack 5 to perform a xhydra attack, as well as the other vm’s to serve as victims (except for backtrack 4)

**Lab**

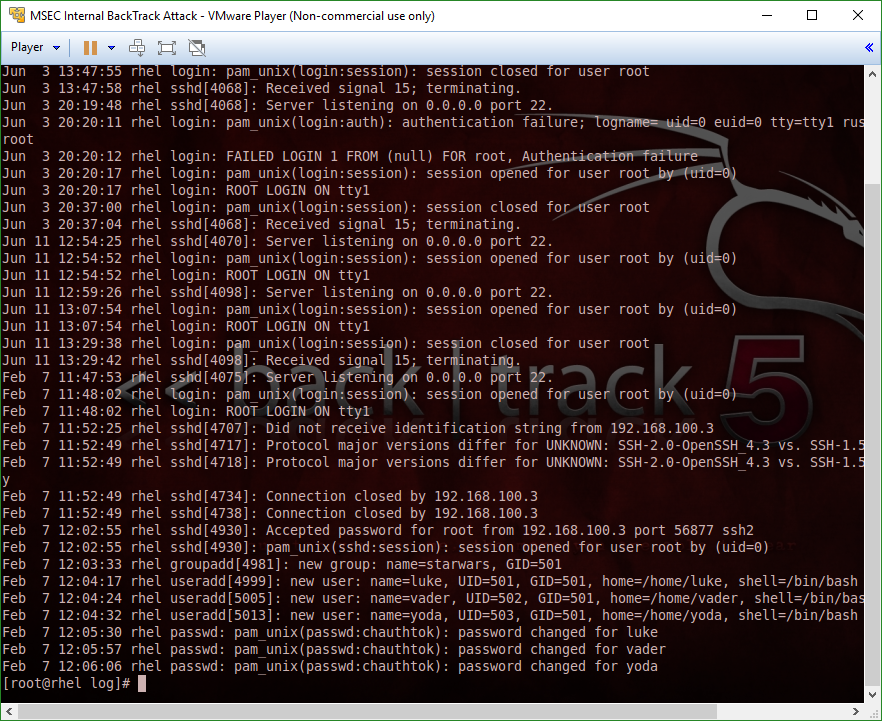
Task 1:

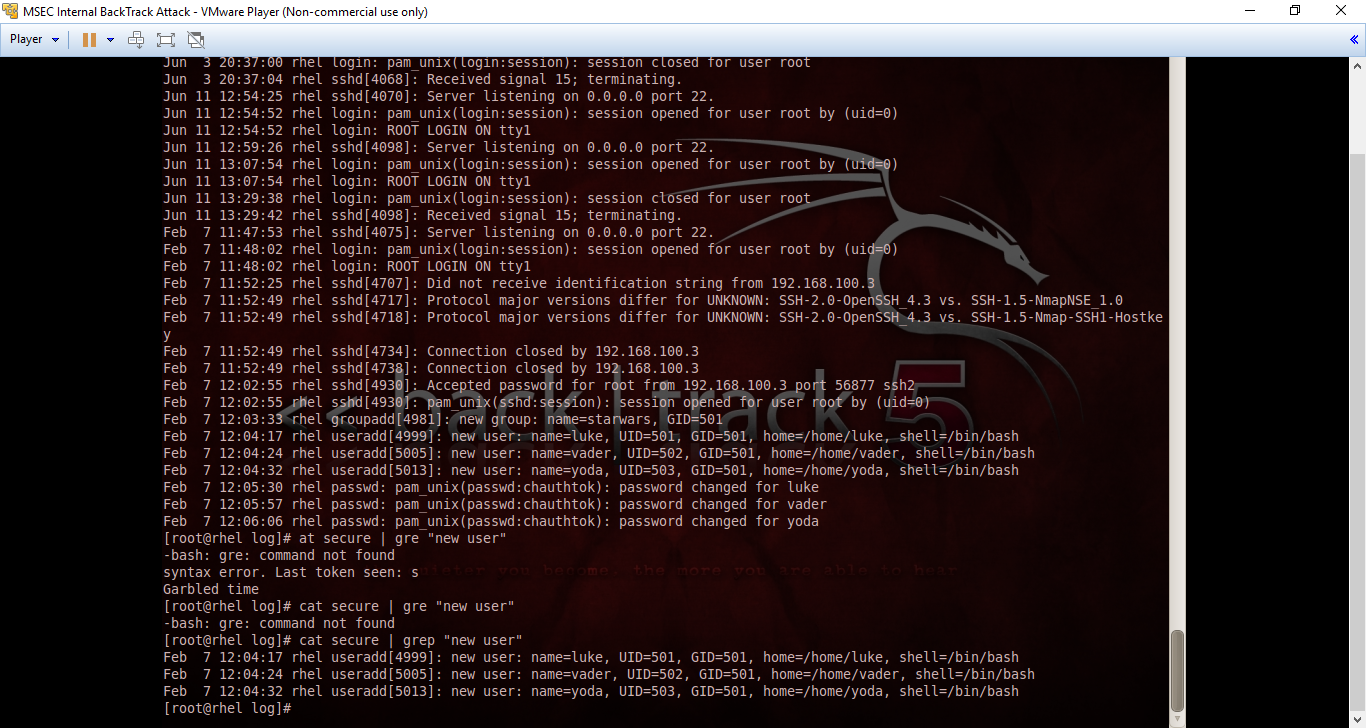
1. 

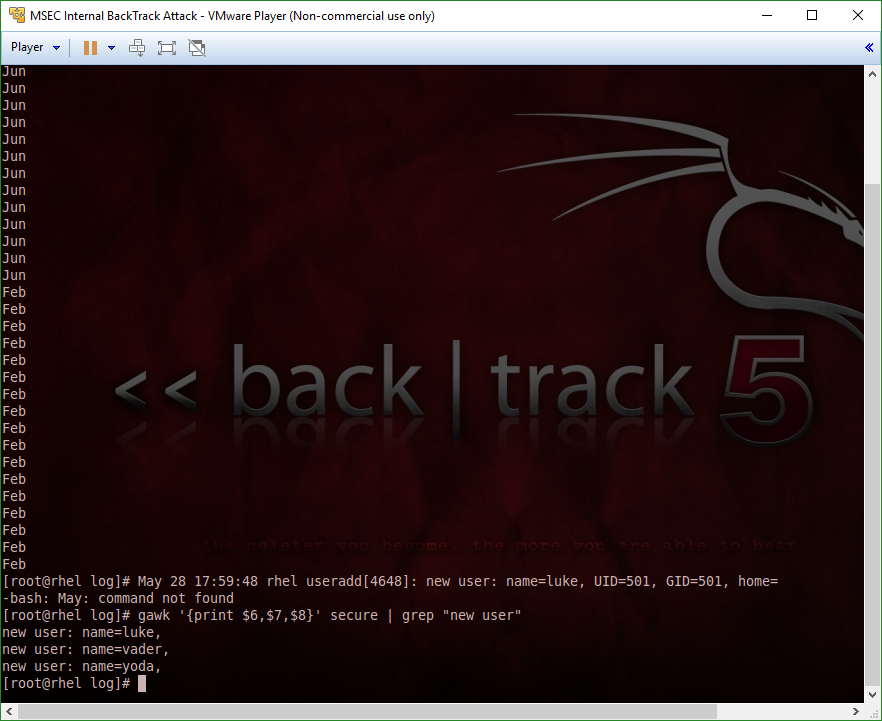
2, 

3. 

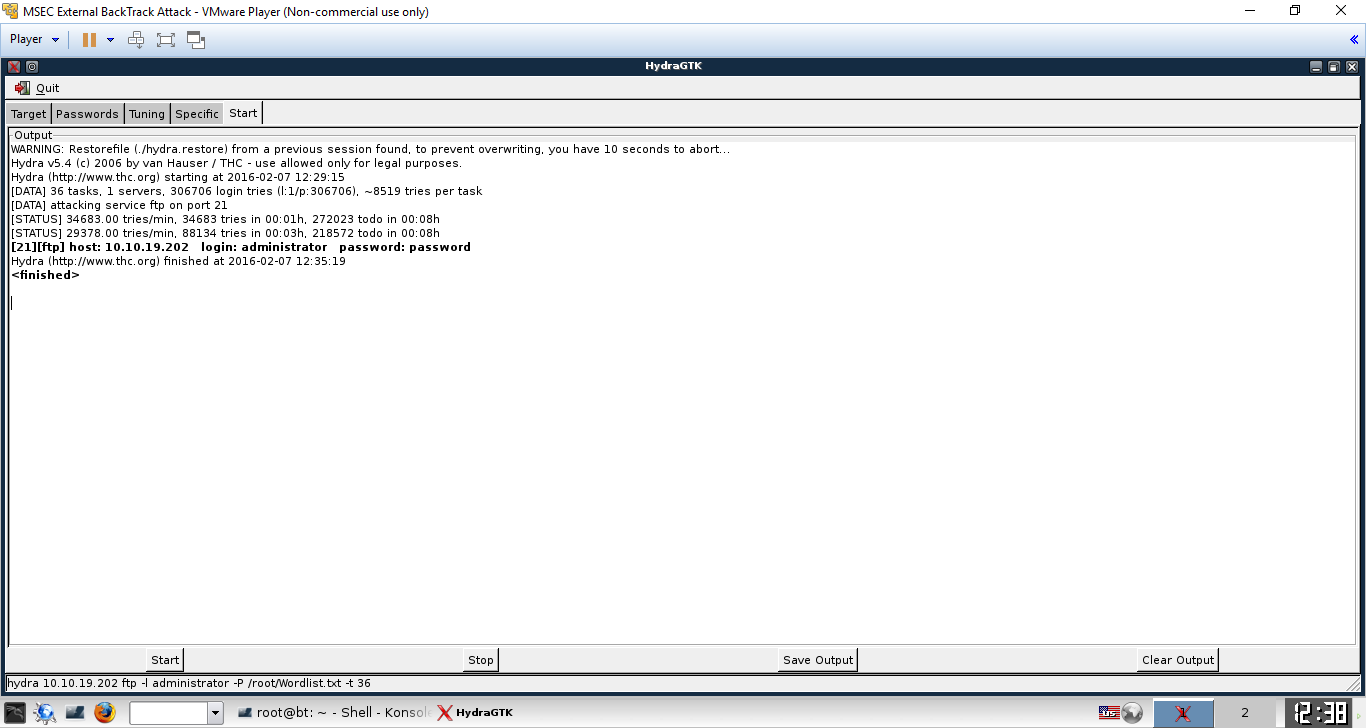
Task 2:

1. 

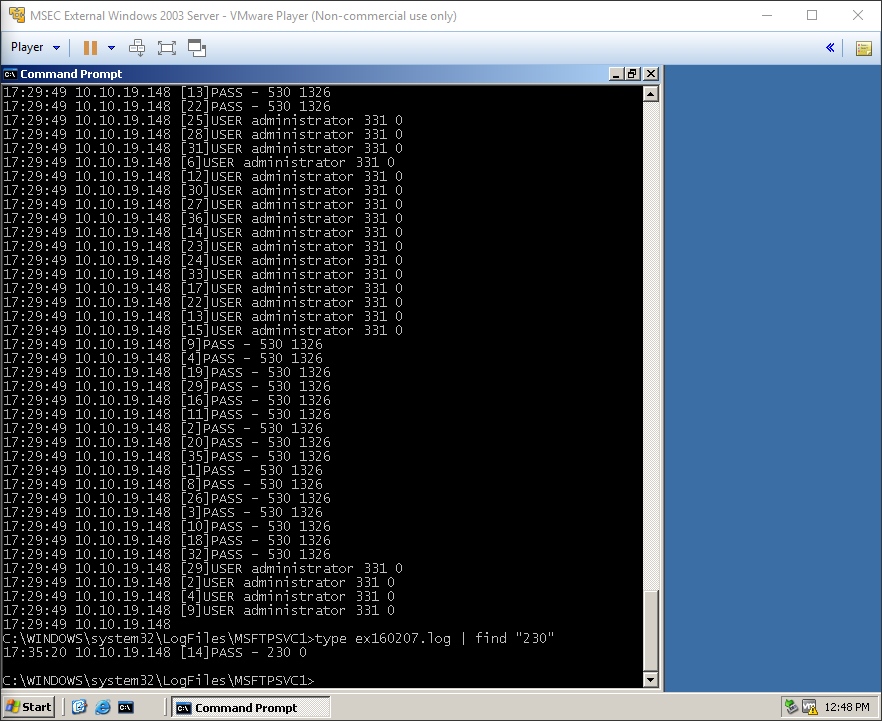
2.

3.

Task 3

1. 

2.

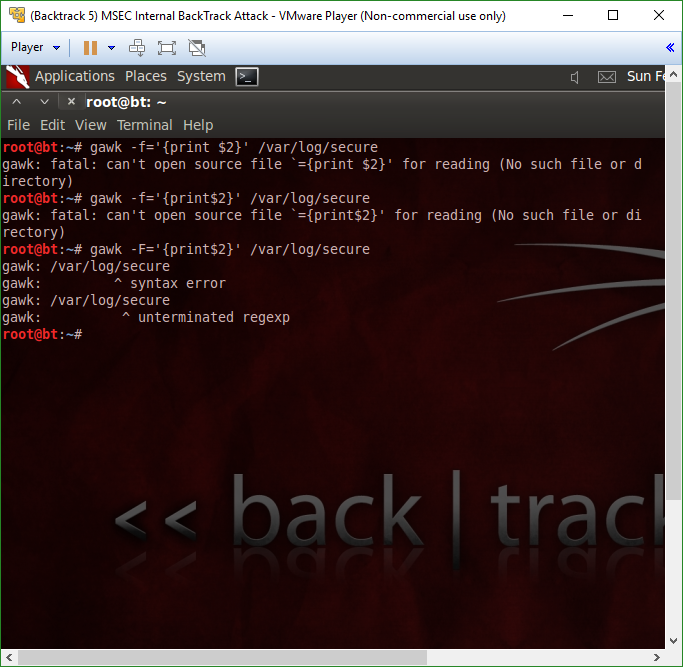
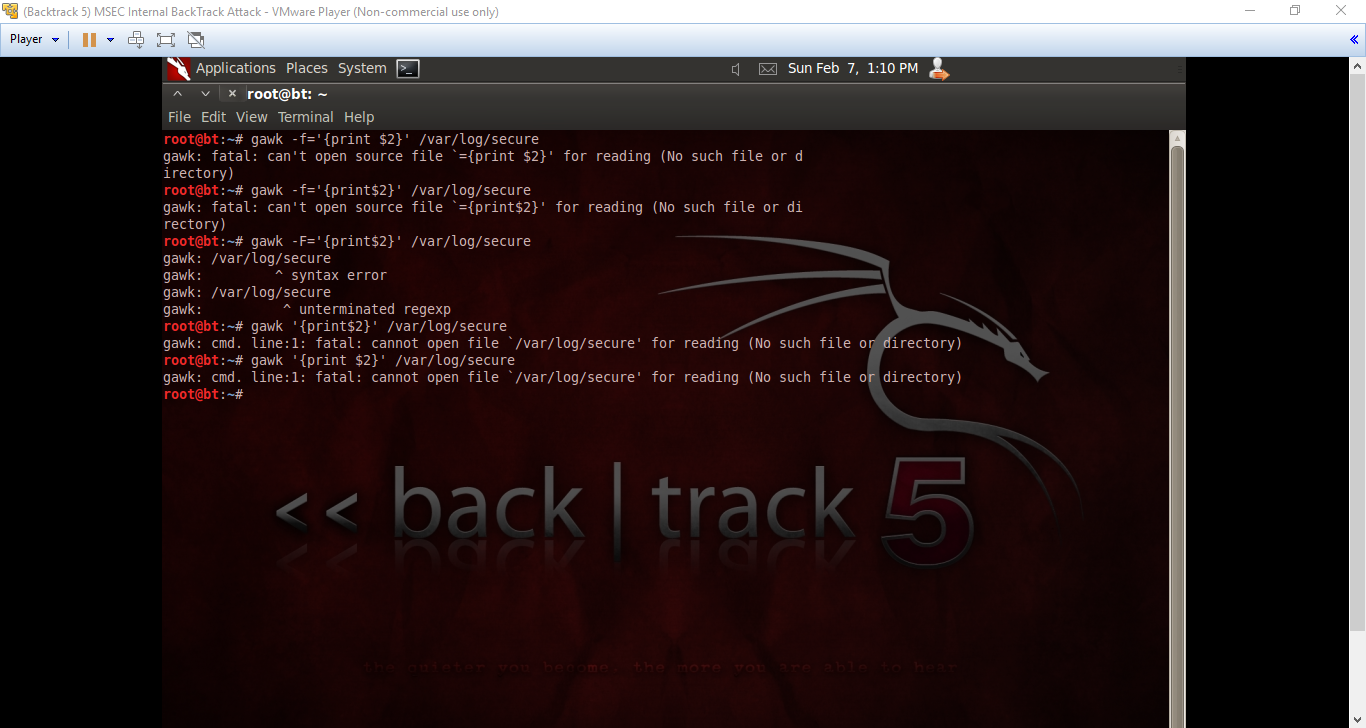
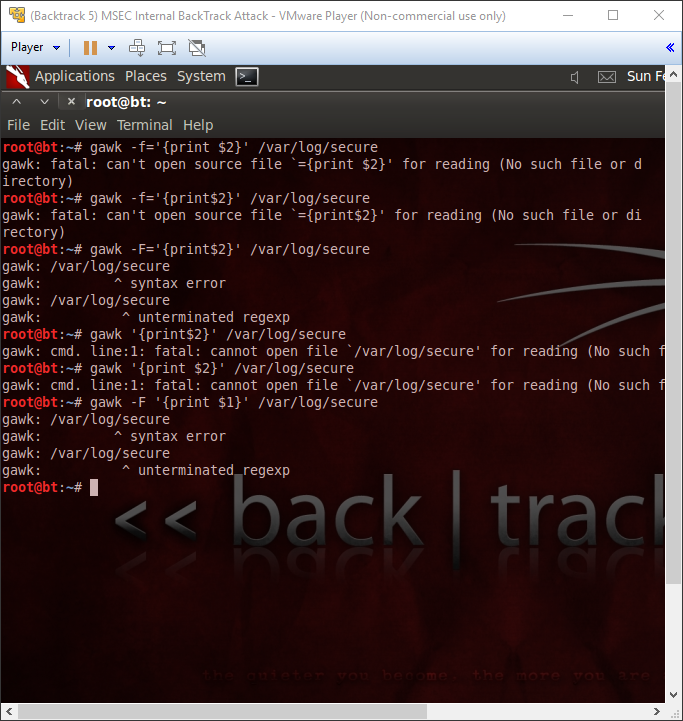
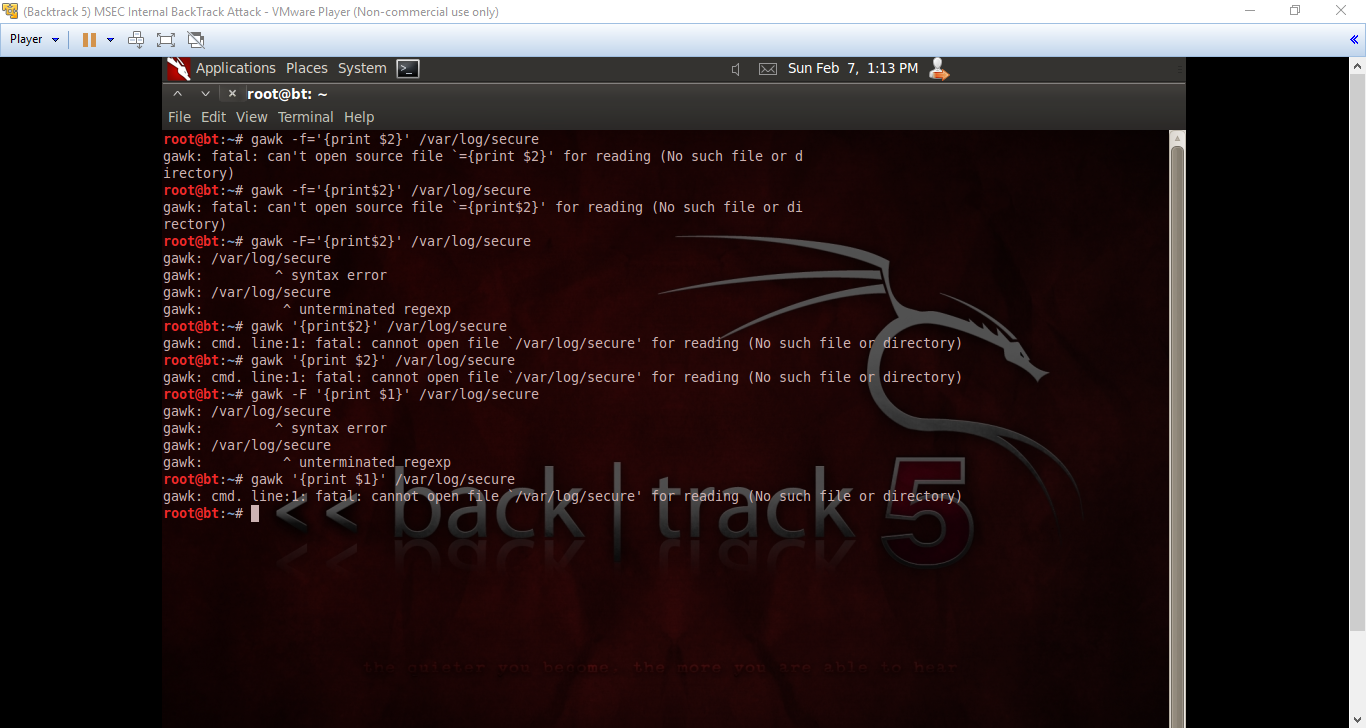
3.

**Questions:**

Task 1

1. Where is the access\_log file located on a Linux system? **Within the httpd directory (cd /var/log/httpd)**
2. What is contained within the access\_log file? **The information of scans and connection using either zenmap to scan or Firefox/curl to connect**
3. What does curl stand for? **It’s used for transferring files**
4. How do you grep for the word nmap within the access\_log? **Cat access\_log | grep nmap**

Task 2

1. What are the results from typing the following command?
   1. Gawk -F= ‘{print $2}’ /var/log/secure 
2. What are the results from typing the following command?
   1. Gawk ‘{print $2}’ /var/log/secure
3. What are the results from typing the following command?
   1. Gawk -F= ‘{print $1}’ /var/log/secure 
4. What are the results from typing the following command?
   1. Gawk ‘{print $1}’ /var/log/secure 

Task 3

1. What is xHydra? **A dictionary attack**
2. Where are FTP Log files stored in Windows? **Within the MSFTPSVC1 directory (within c:\Windows\system32\logfiles\msftpsvc1)**
3. What is the code for a successful FTP login? **230**
4. How can the find command be used to locate the number 230 within a logfile? **Type ex160207.log | find “230”**

**Conclusion**

This lab I was able to complete it much easier compared to the last lab. I think I finally resolved the connection issues I was having, and now learning the different commands like gawk or the xhydra attack was pretty interesting. There was another type of dictionary attack that we used in my previous IAE class, however, this one seems much simpler to use with the GUI. Overall I was able to complete this lab without much of a hassle, and I was able to learn the information explained.

**Grading Rubric**

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