Lab 10 – Monitoring LINUX log files

Lukas Fuller

IA-301 Introduction to Information Assurance

Prepared for

Professor Elizabeth Tolson

**Abstract**

Examining log files for security events is a daily task for security professionals to detect intrusion attempts on LINUX systems. This lab focuses the student on examining LINUX system log files with commands such as grep and gawk.

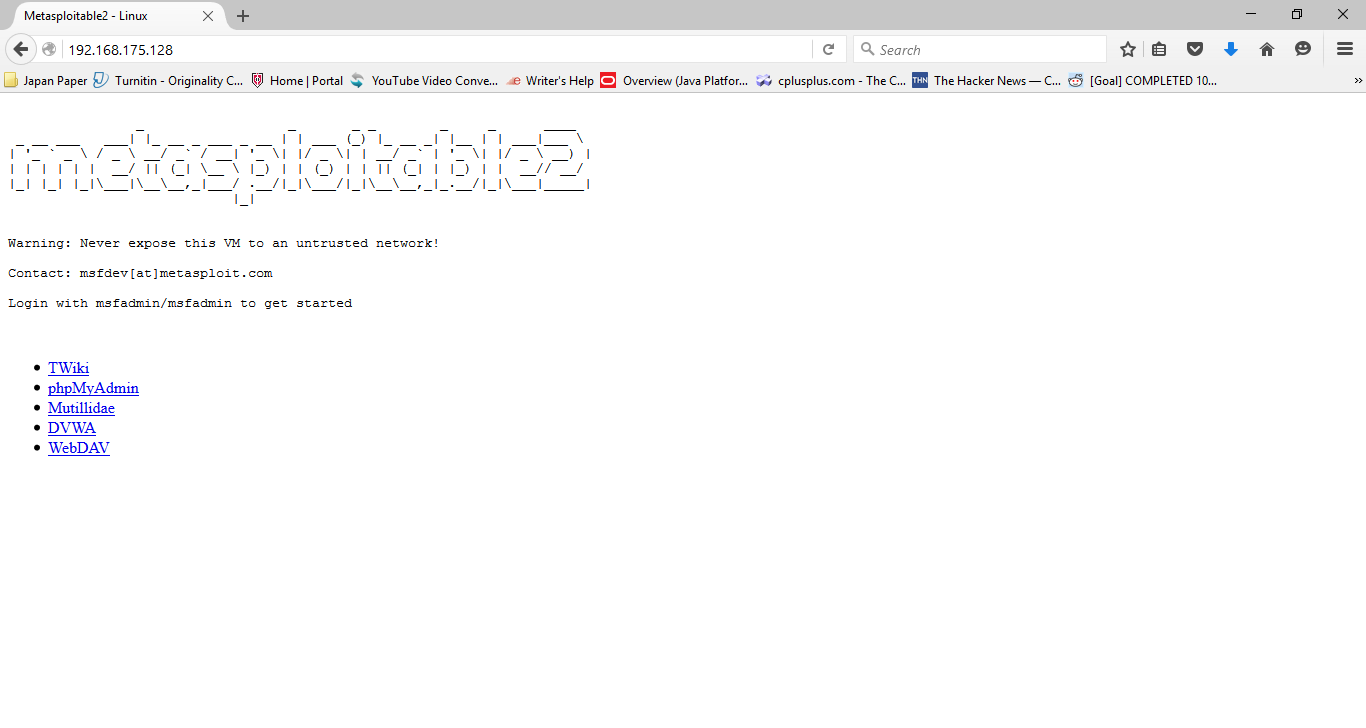
**Materials**

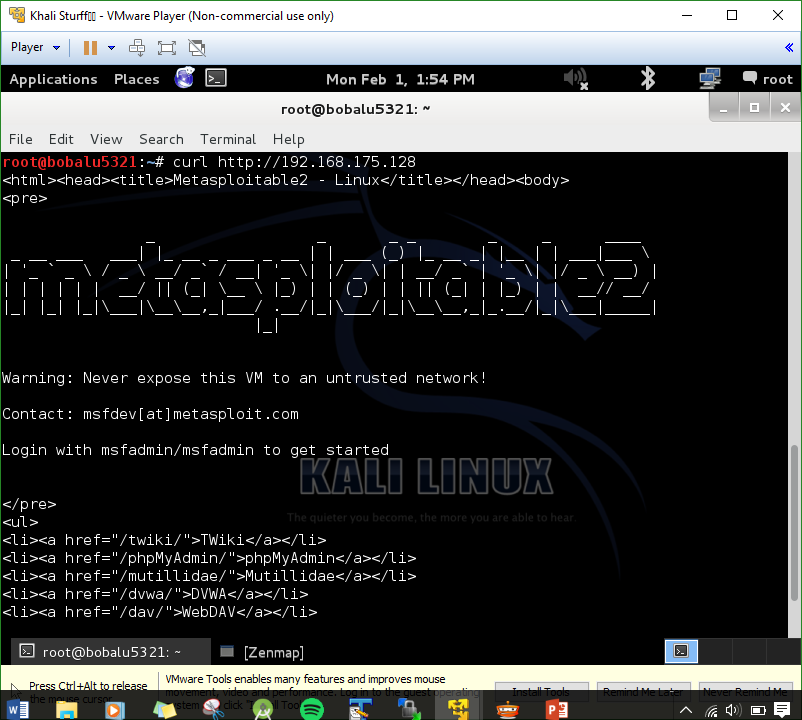
1. Backtrack 5 Virtual Machine
2. Metasploitable Virtual Machine

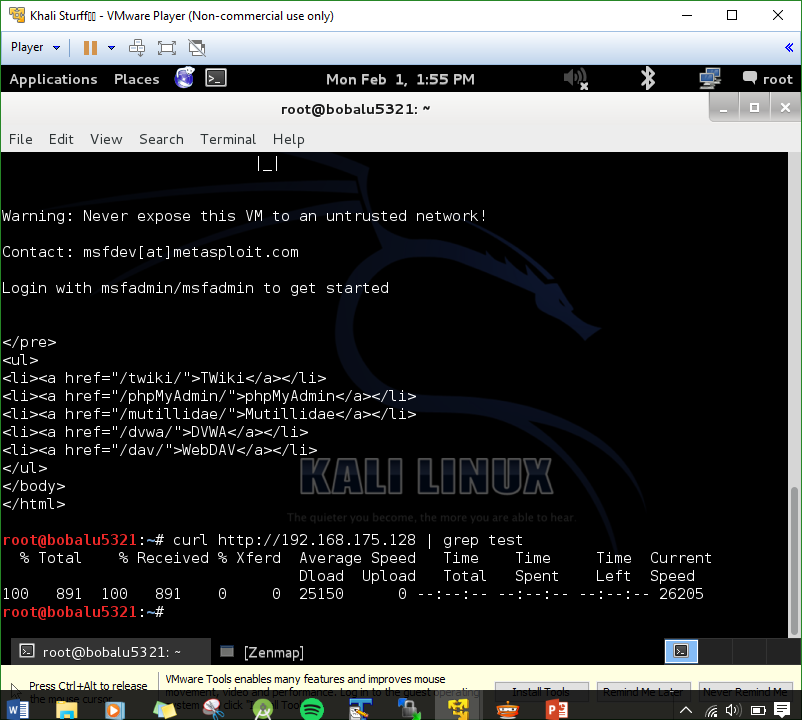
**Methodology**

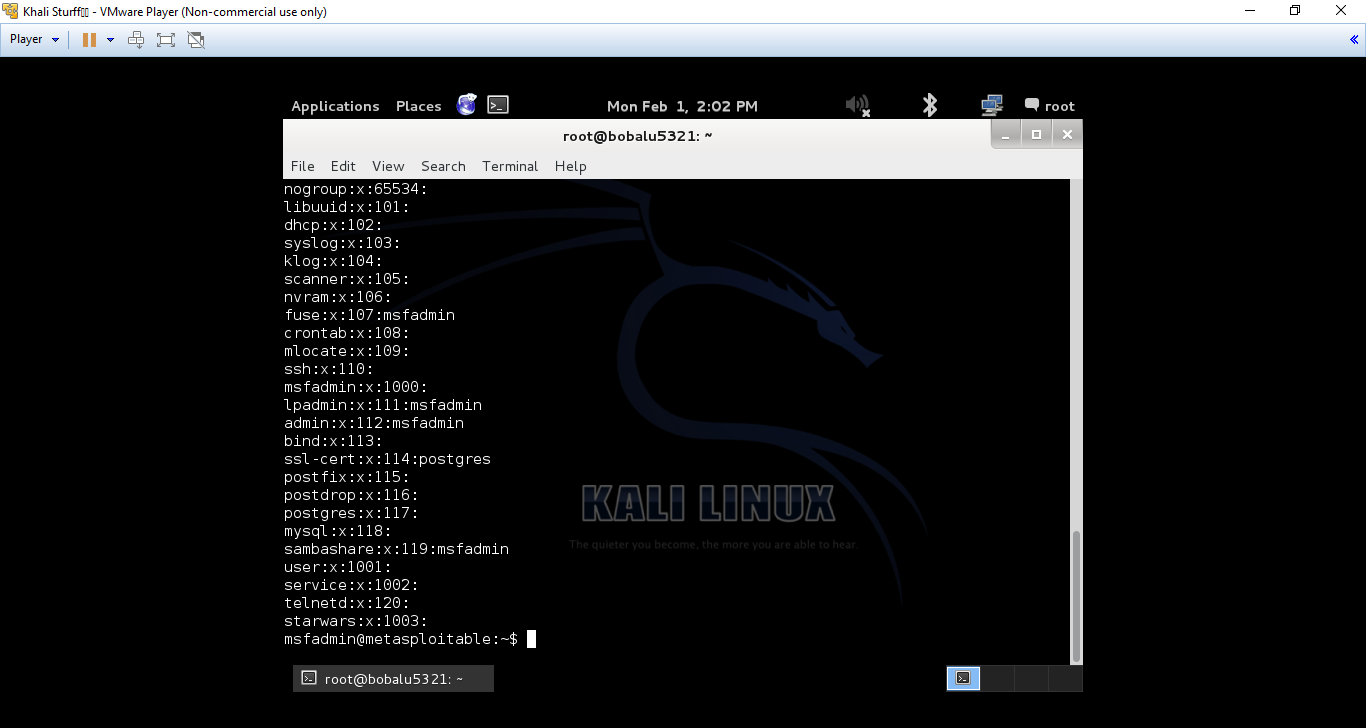
By using the zenmap, and terminal to exploit the Metasploitable VM

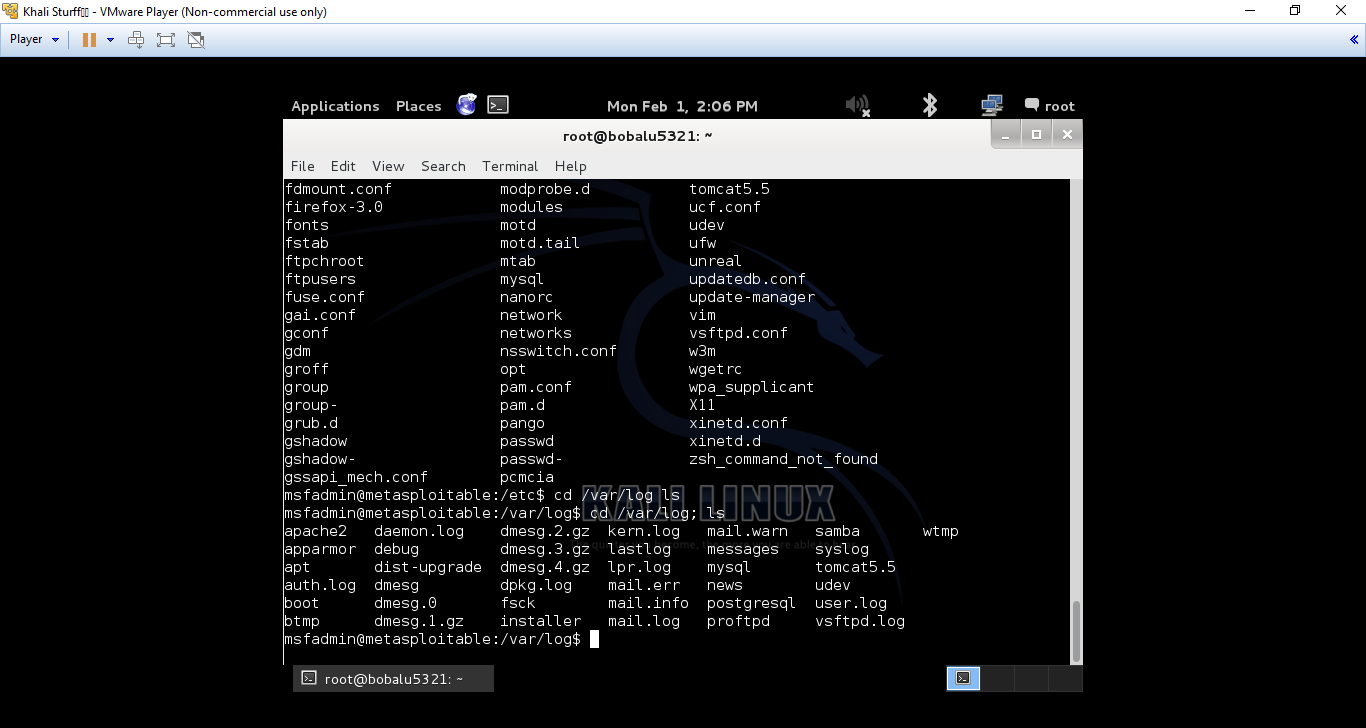
**Lab**











**Questions:**

1. What is Metasploit? **Metasploit is a type of software that allows users to pen test vulnerabilities**
2. Discuss how you used the command: SSH. **From how I used it, it appears to login to a user via port 80, or that’s what I assumed from the notes since it highlighted on the fact that port 80 was in fact open.**
3. Discuss how you used the command: grep. **Grep will copy text down from where you direct it to, saving time from having to enter a text editor and manually creating the file or saving the file.**
4. Discuss how you used the command: sudo. **Sudo executes a command as admin, which is why every time you run the command you have to enter the password for the account with admin rights.**

**Conclusion**

This lab covered some commands like grep and sudo which I’m familiar with and commands like addgroup and curl which I previously was not familiar with in order to access a log file of users and add users to the list. The main hassle I had was setting up the VM’s networks, but other than that I think I enjoyed this lab. It provided me with more familiarity with the VM’s and how they work as well as more knowledge on the LINUX environment which can be very helpful later down the line for servers and such.

**Grading Rubric**

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