**Undergraduate Program in Information Assurance Engineering**

# IA-301: Introduction to Information Assurance

Lab 10 – Monitoring LINUX log files

**Lab Objective:**

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.

Reference: CSSIA Security + Lab Manual lab # 2

**Laboratory Deliverable:**

1. Screenshot of Step 5
2. Screenshot of Step 6
3. Screenshot of Step 7
4. Screenshot of Step 19
5. Screenshot of Step 26

**Materials:**

1. Backtrack 5 Virtual Machine
2. Metasploitable Virtual Machine

**Instructions:**

1. Log on to a pen testing distribution (Backtrack or Kali).
2. Log on to metasploitable.
3. In the pentesting distro, run a zenmap intense scan on the IP address of metasploitable.
4. View the Ports/Hosts tab, notice port 80 open.
5. Fire up a web browser, open the address http://<ip address of metasploitable>/.
6. The page works, now open up the terminal and issue the curl command:

curl http://<ip address of metasploitable>/

1. curl http://<ip address of metasploitable>/ | grep test
2. Switch to metasploitable.
3. cd /var/log/apache2
4. cat access.log
5. cat access.log | grep nmap
6. cat access.log | grep Firefox #if that doesn’t work grep for ‘Mozilla’
7. cat access.log | grep curl
8. Now switch back to the pen testing distro.
9. SSH msfadmin@<address>
10. FAIL TO AUTHENTICATE TWICE. Just enter the wrong password.
11. Authenticate.
12. sudo groupadd starwars
13. cat /etc/group
14. sudo useradd luke –g starwars
15. sudo useradd vader –g starwars
16. sudo useradd yoda –g starwars
17. sudo passwd luke #the password is ‘son’
18. sudo passwd vader #the password is ‘dad’
19. sudo passwd yoda #the password is ‘green’
20. Now let’s look at the logs…cd /var/log; ls
21. There is no secure log in Ubuntu, have the students take note that in many other distros there is a /var/log/secure log for all ssh events. We will instead look to auth.log. This will show us the SSH login attempts.
22. grep as needed. *students explore*
23. cd /etc; ls
24. cat syslog.conf
25. Students will now search around and see how the log files are configured; where things go, why, etc.

==END==

**Questions:**

1. What is Metasploit?
2. Discuss how you used the command: SSH
3. Discuss how you used the command: grep
4. Discuss how you used the command: sudo

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