IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY
ISERink

Student L14A1

This activity is here to help you get a beginning grasp on how to analyze logs. The types of logs this activity is going to look at is Apache Web Server Access logs. You will be provided with a short scenario and a sample log file and you job will be to answer questions based on the log file. Will you be able to find out who the attacker is?

Scenario:

A financial company runs their own social networking website for their employees. They had a breach recently and have brought you in to find out who did it. Unfortunately, most of their logs were wiped clean and the only ones they have left are some Apache Access logs. Answer the questions below while analyzing the logs so you can report to the company with your findings.

Instructions: View the provided sample log file as you complete the questions in this activity.

Apache log files come in the form of:

IP_Address User_Name Date_and_Time_Accessed “Access_Method URL_Accessed Protocol” Status_Code Number_of_Bytes_Transferred “Referring_Site” “User_Agent_Info”

1. Based on the accessed URLs, which IP Address do you believe belongs to the Web Site Administrator? Why?

2. Which IP Address do you believe belongs to an attacker trying to find vulnerabilities in the website?

3. What status code was the attacker getting when he was looking for vulnerabilities? Why was he

getting this error code?

4. How is the attacker attempting to access the web site? Specifically, what protocol and what browser.

5. What are the IP Addresses of the legitimate users?
