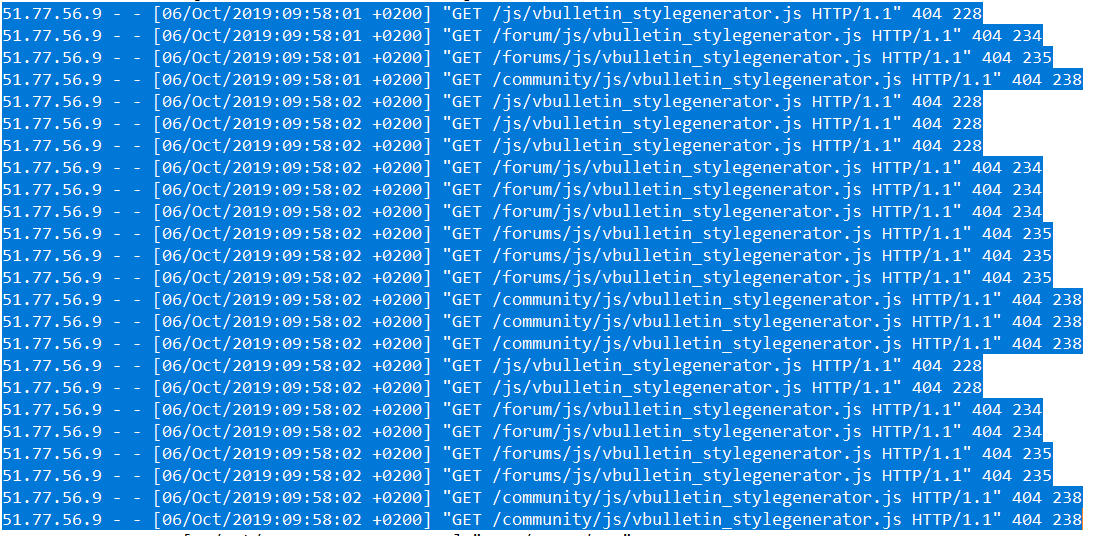
Assignment 3: Web Scanning and SMB Scanning [40 points]

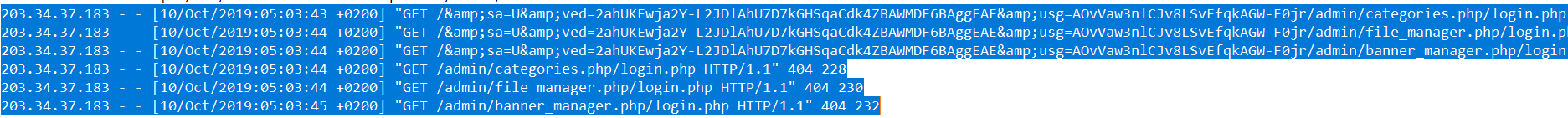
**Part 1: Log Analysis**

Q1: Find 3 examples indicative of malicious web scanning in the access\_log.txt file (note that requesting the robots.txt file is not necessarily malicious, all web crawlers do this). Provide the IP address(es) performing the scan and a brief explanation of why the scan is clearly malicious. [9 points]

1. 51.77.56.9. The scan appears malicious as there are a lot of 404 errors from the same address. The 404 error represents a not found code. The requests indicate that the address is trying various paths looking for a javascript file titled “vbulletin\_stylegenerator.js”



1. 203.34.37.183 The scan appears malicious as the IP address is requesting multiple admin paths and receiving 404 errors back. This leads me to believe that the address is trying to access something that they do not have access too.



1. 154.48.234.88 This scan also appears suspicious as this IP address is also looking to gain access to multiple admin paths. The 404 errors indicate that the paths are not found. A few of the URLs look as if SQL injections are trying to be performed.



**Part 2: SMB Scanning**

The server.cs491 machine is hosting an SMB share. You have an account on the SMB server with the credentials [user:password] which can be used to answer the following questions.

Q1: the SMB server is sharing a file containing a flag. What is the value of the flag? [6 points]

CS491{XGRU-7955}

Q2: what is the name of the other user with an account on the SMB server? How did you find this information? [6 points]

dkbarnes

rpcclient -U user server.cs491

enumdousers

**Part 3: Web Scanning**

For the following questions you should be scanning the web server running on port 80 on the server.cs491 machine. Make sure you are not scanning the servers used for the programming assignment.

Q1: What is the name and version of the web server running on the host? [4 points]

Apache httpd 2.4.46 (Unix)

Q2: There are three flags somewhere on the webserver. Provide the flags as well as an explanation of how you found them. [15 point]

Flag1: Found through accessing robots.txt file.

1. CS491{LMJS-3113}

Flag2: Found through using word list.

1. CS491{PPHJ-2273}

Flag3: I altered the dirbuster word list and added .html to each word. I used my python script from the project to test the entire word list as dirbuster has size constraints. server.cs491/lab\_activites.html

1. CS491{RXLT-1715}