

❗**Things I learnt:**

**⭕Shell scripting refers to list of command & logical statements that is to be run on OS**

**⭕CLI is one of the way to interact with OS**

**⭕Shell is the program which collects commands from user, execute it on OS & provides the output to user**

**⭕Bash shell is one of type of shell program**

**⭕Variable is reference name given to memory location which can be used as & when required**

**⭕Exit code is special variable($?) which conveys that the monster recent command run is success or fails**

**⭕Script reffer to the collection of command with conditional statement**

**⭕Shebang help us to specify which program for execution of script should be used. Like #!/usr/bin/bash uses bash shell**

**⭕For Parameterized script we can use variable & take input from either command line or through read command, also we can take input from file**

**⭕For creation of loops we need to use for or while keywords with appropriate conditions, along with do & done keyword**

**⭕I/O redirection refers to using > or < symbols for guiding where to give out put & from where to take input respectively**

**⭕For taking input in shell we can use read command, or if we have command line argument then we can use $1(1 argument),$2(2 argument) and so on, or else we can use $@(all argument)**

**⭕We can use cut command to extract any field from data, use -d for specifying delimitor & -f for specifying the feature or column number**

**⭕We can add time stamp by using date command with appropriate options in {}**

**⭕awk is basically a very powerful command used for analysis purpose**

**⭕Watch command is used for continuously running the other commands**

**⭕awk '$9==404{ print $0 } ' access\_log | sort | wc -l //for getting total number of the false client**

**⭕For getring dd:mm:yy from date run date + %e:%b:%G**

**⭕For running multiple commands together put then in double quotes & separate them using semi colon**

**⭕touch a{1..10}.txt for creating multiple files**

**⭕Different option available with awk command are: "-F" for specifying delimitor "END" for getting last line of output produced by awk "NF" display total field in unsorted data "NR" display row number with each row**

**⭕Use sort command to sort the log file we can also specify -l to specify the feature on which we want to perform sort & also -n so sort command will treat that column as number. For counting we can use wc -l**

**⭕For creating function we need to give function name along with parentheses & fuxn body in curly braces**

**⭕Command are OS respective i.e. they require PATH for finding scripts which can be executed but function are the feature of shell, hence they dont require PATH**

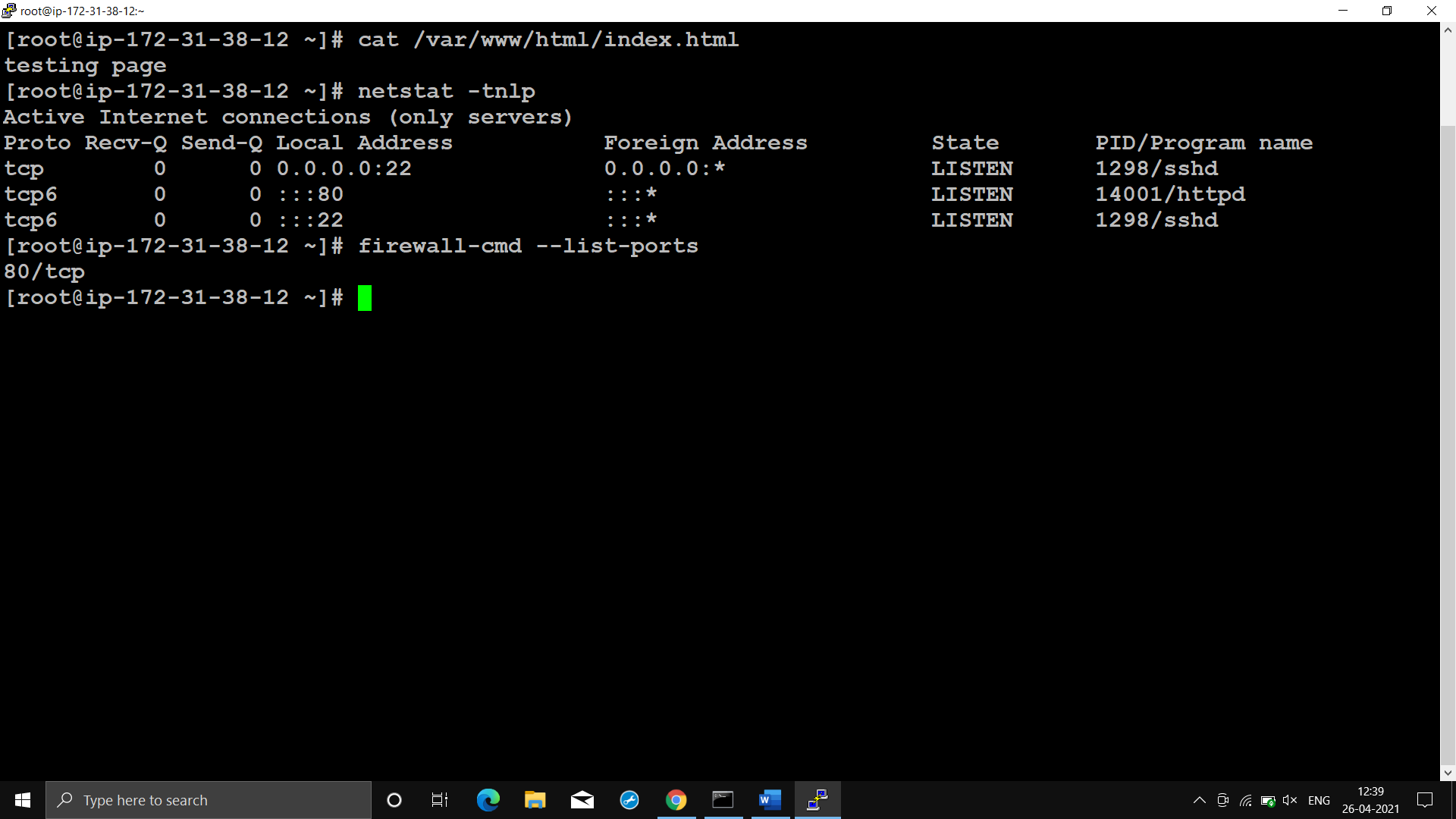
**⭕To pass the value to command which requires value on run time we can use --stdin**

**❗PROJECT:**

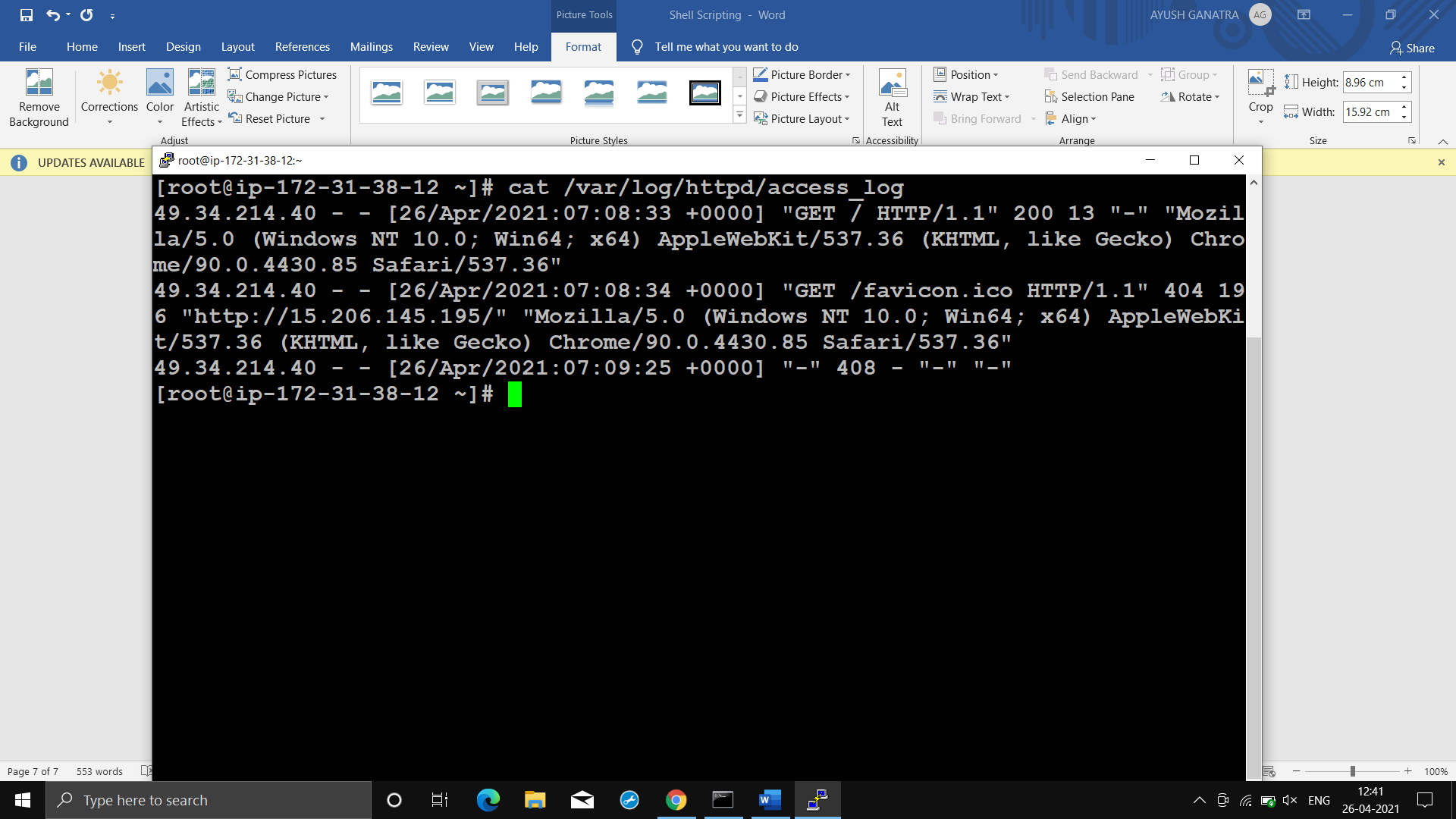
**I created a script that will collect logs of httpd server and present some of the important information to us & also detect whether anyone is trying to do DOS attack on our server or not. If in certain period of time more request are received from same ip then, simply it would as the admin whether he/she want to block the ip & if admin says yes then that ip would be blocked!!!!**

**❗Glimps of my project:**

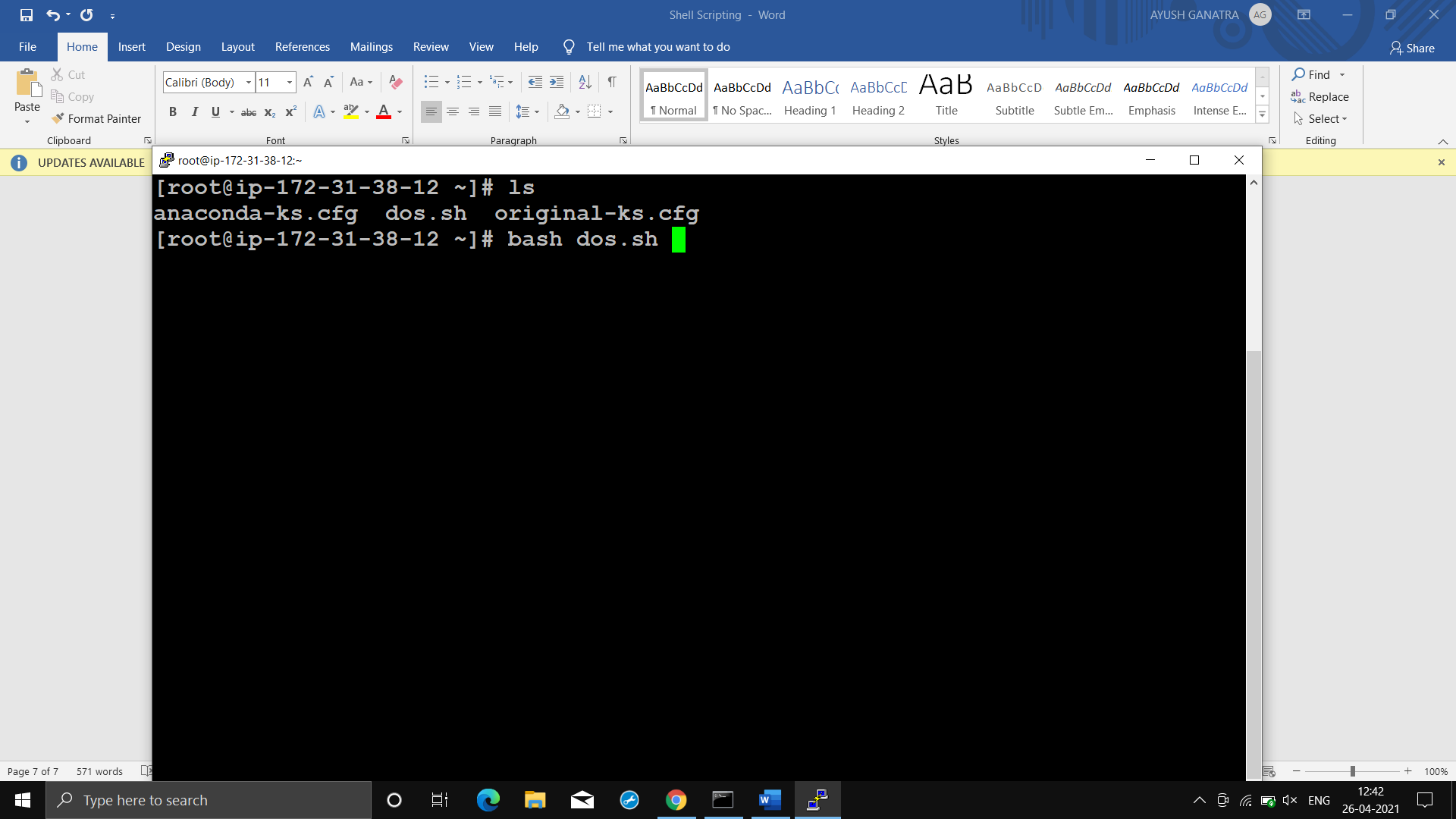
**80 port is active & I have my web page in the document root of apache web server.**



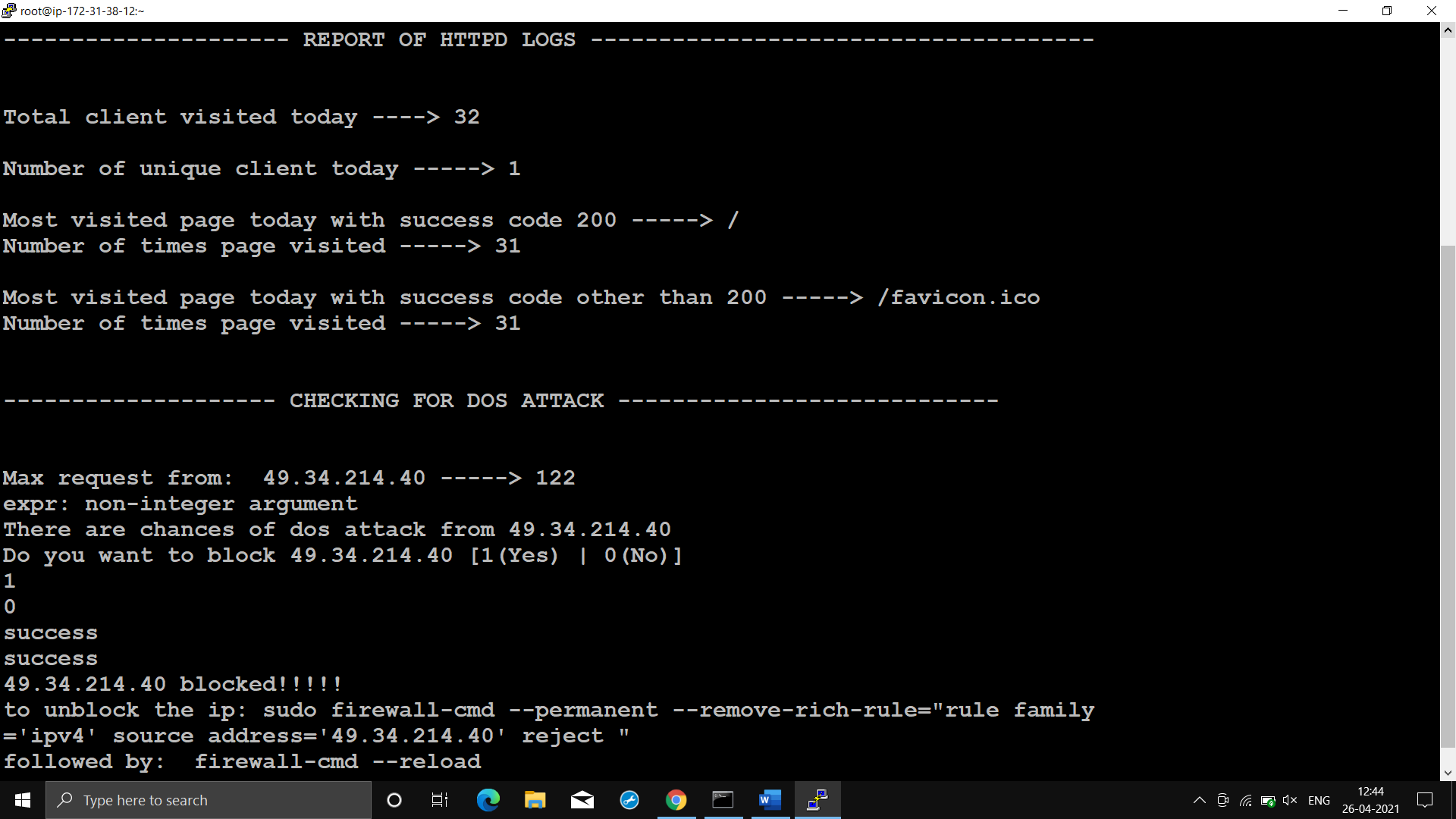
**🔹Request till now:**



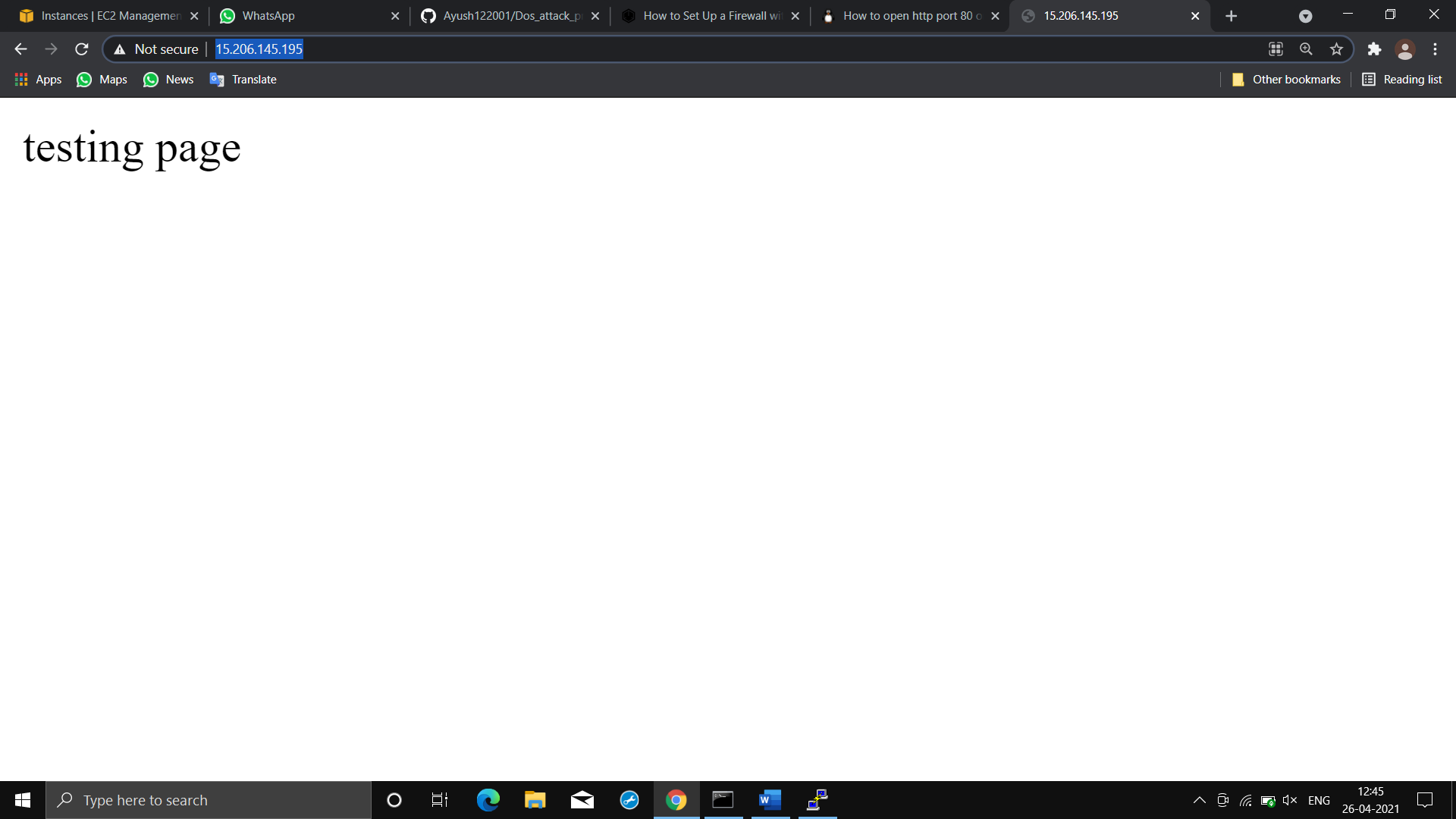
**🔹Lets run the script:**



**🔹Output:**



**🔹Before:**



**🔹After:**