Bryan Miranda ISM4323 04/22/2022

Problem 1. [20 points] Please read the Design Case question on page 358 of the textbook   
and answer the following questions:

A. When was the incident discovered and how? **The incident was found on February 29th of that year. The hacker had access to the machine for about an hour or so. The hacker tried to access other machines within the Sunshine University with a set of 6 different credentials.**

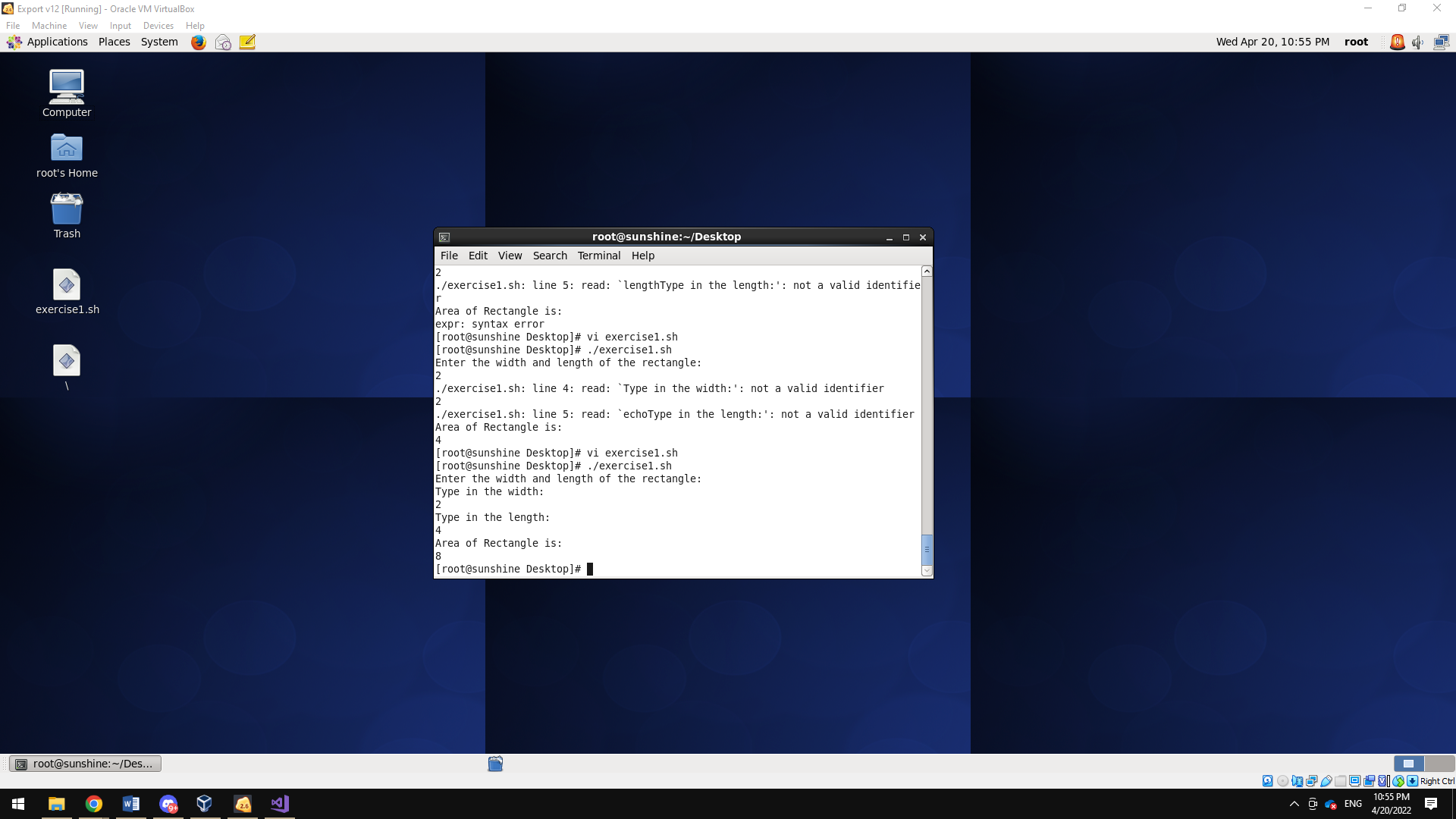
B. What critical pieces of information are missing? **The pieces of information that are missing are Extensive forensics, Windows even logs. Inbound and outbound network connections. Special attention was dedicated to inbound/ outbound traffic to database server DB1, which holds personal data for the university**

C. Based on what you know, what else would you consider looking into in order to make a better determination of the final consequences of the incident? Be as detailed as you can. **I would determine if any of the employees that left the job within the past 180 days still had access to these kinds of controls. This to me seems like an internal job. The user had a set of credentials already and knew what to look for and on what particular server/ database. In addition I would also consider looking into the logs and the IP Address of that user to see if they forgot to trace their steps.**

D. What would be your recommendations for improvement? **Some recommendations of mine would be to get rid of department silos. Prioritize threats based on risk analysis and be more realistic with security staffing. Several companies think they have good security until their information gets compromised so easily.**

**Part A**

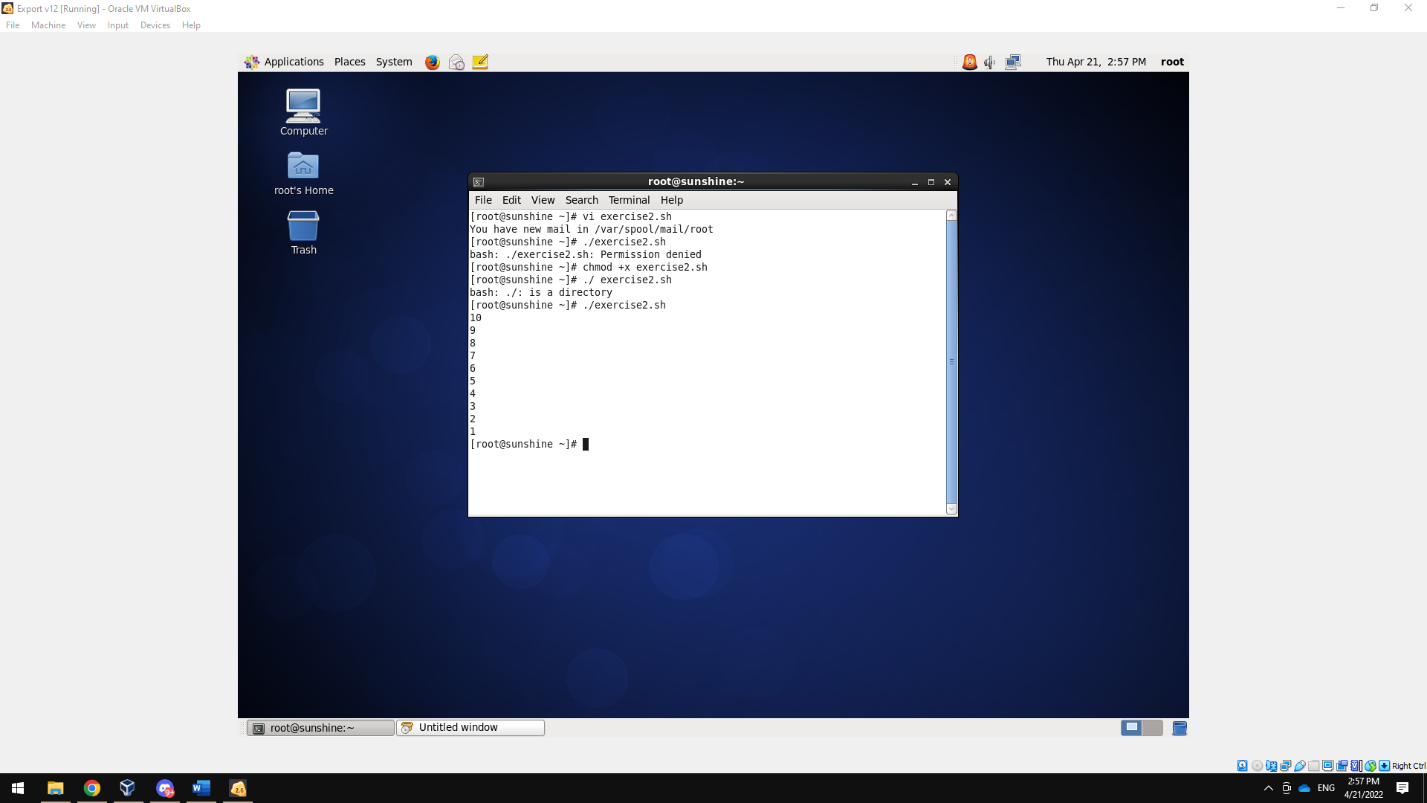
**Image 1 is the execution and image 2 is the code**

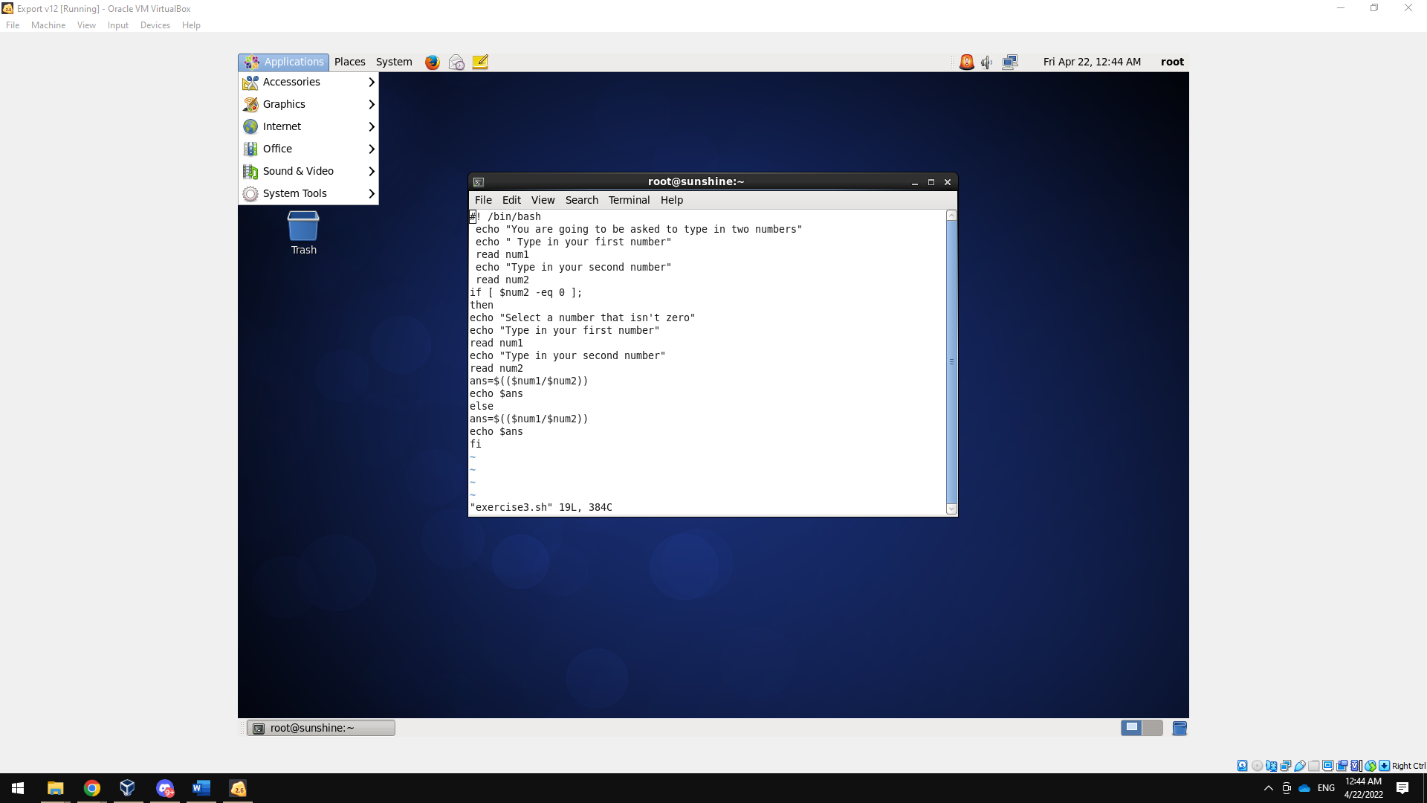
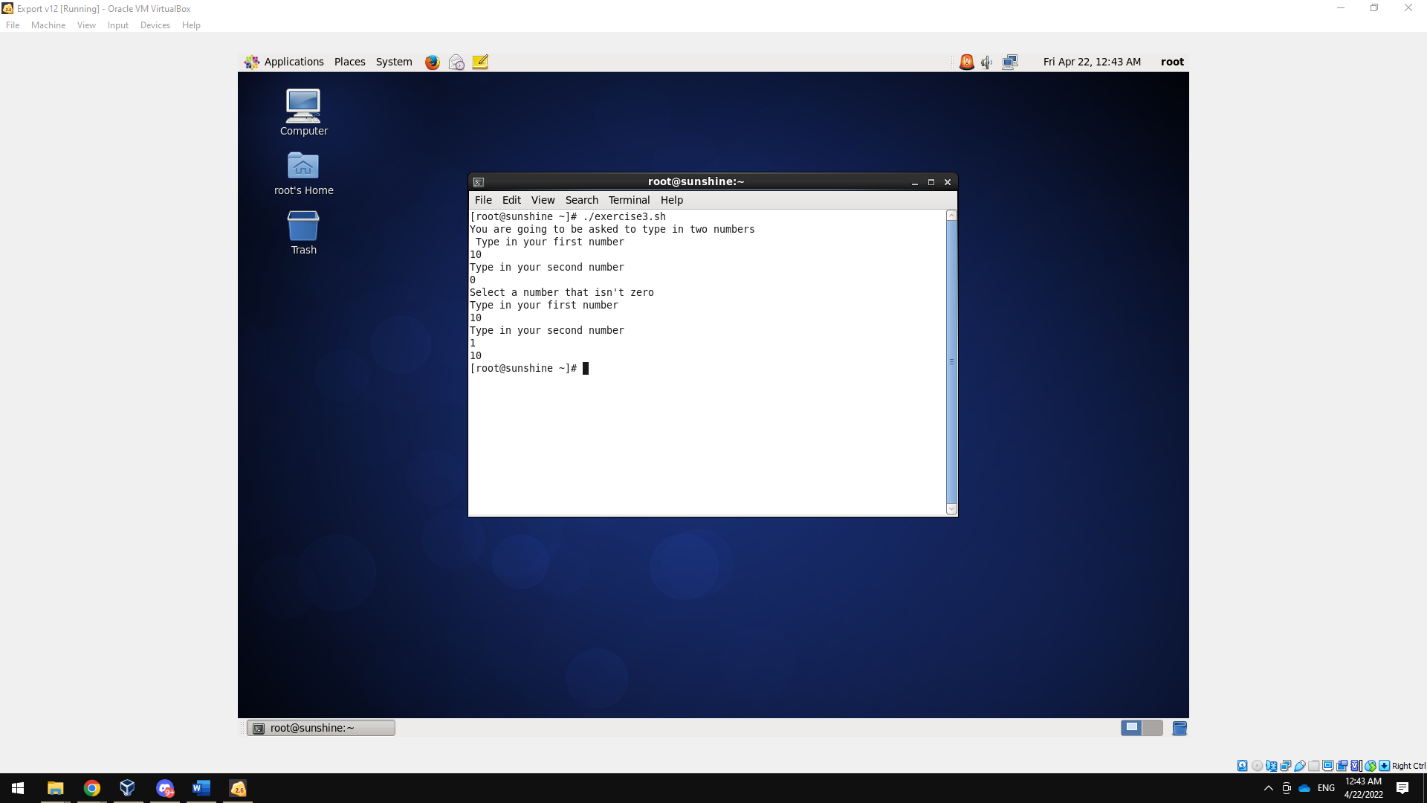


**A screenshot of a computer

Description automatically generated**

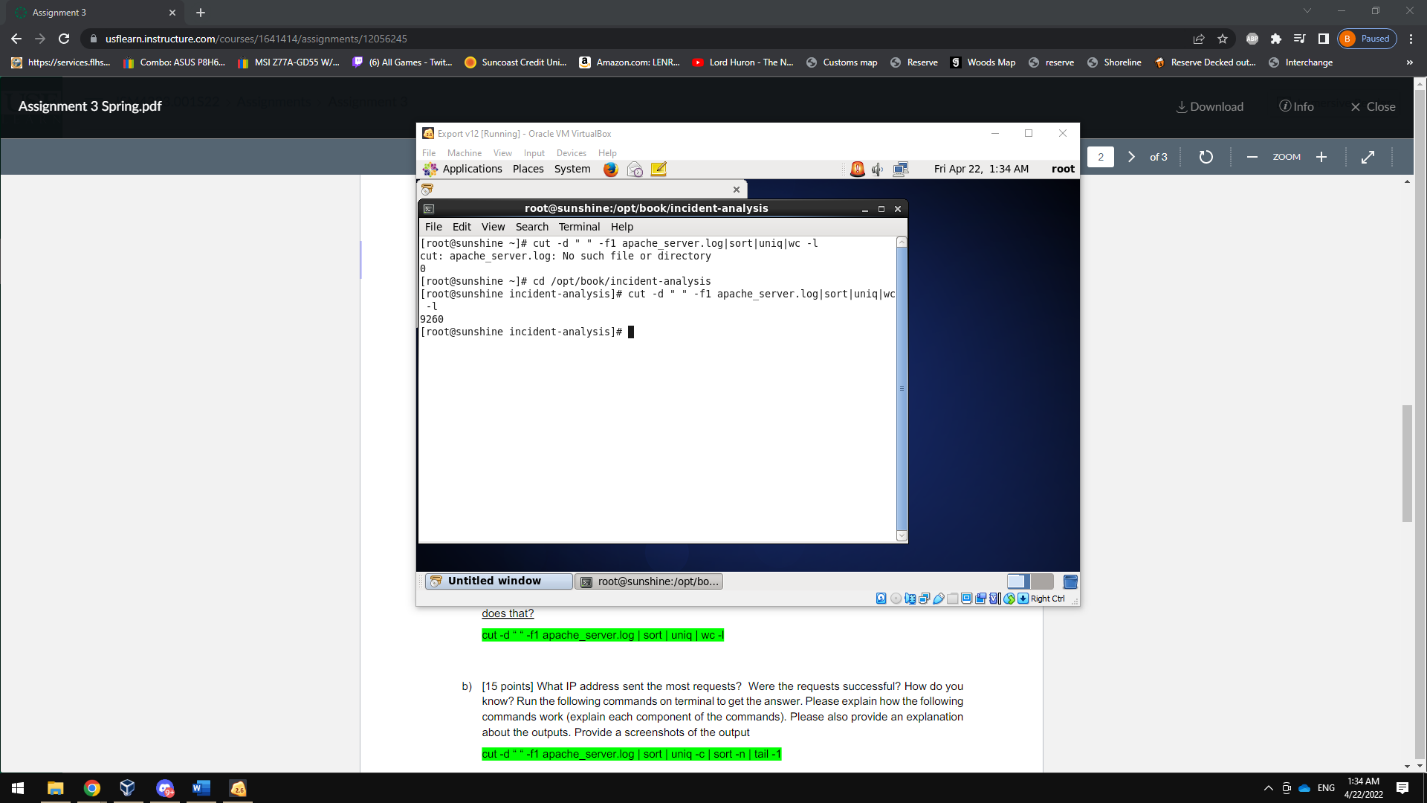
**Part BA screenshot of a computer

Description automatically generated**

**Part C**

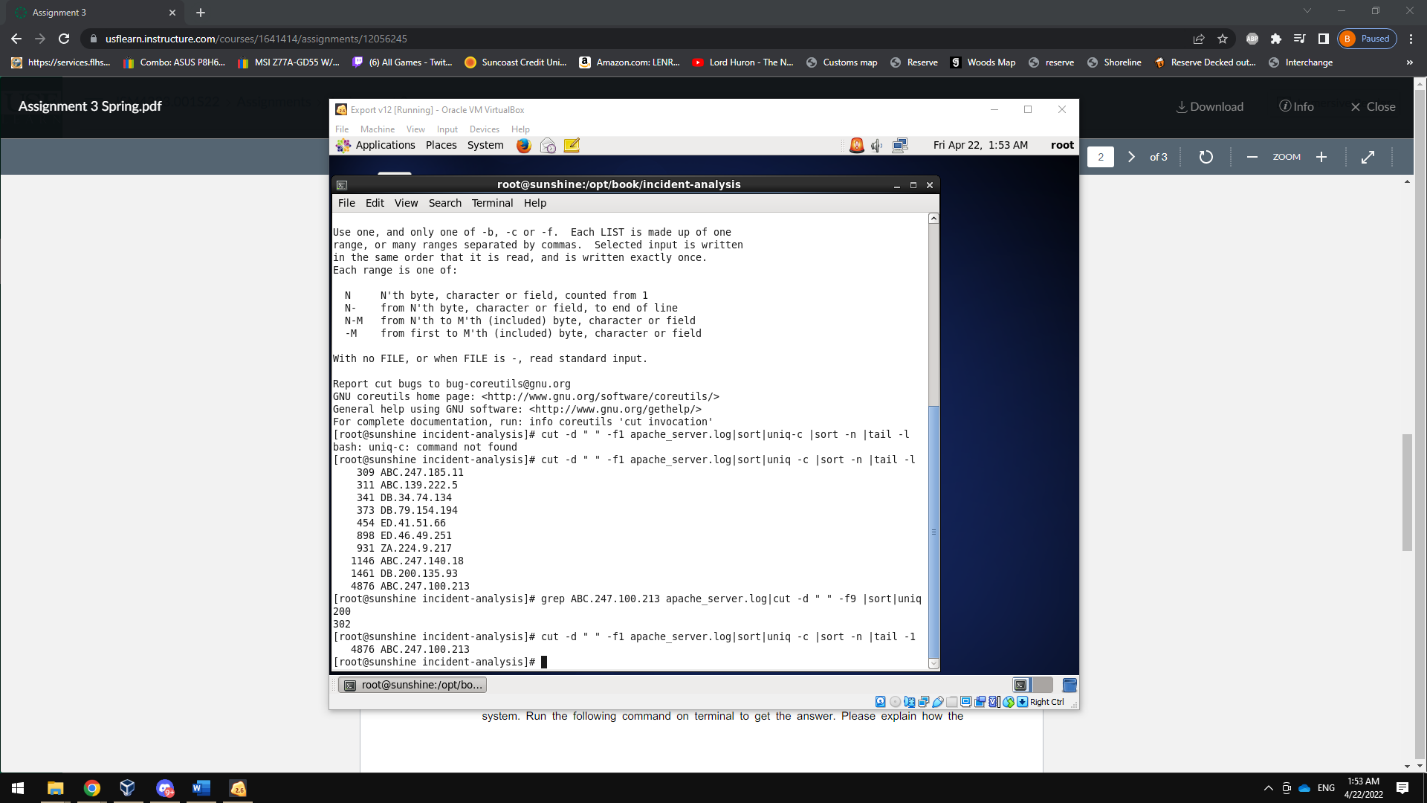
Problem 3

1. In essence what this code is trying to interpret is with -d is a selected number of fields. -f1 interprets the Apache server logs , sort goes through the Ips and gives you a total amount and uniq gives you the amount of unique IP addresses in this case. Which are 9260



1. The IP that has the mosts requests was grep ABC.247.100.213

In essence what this particular command is calling is relatively the same as the previous question but the sort gives you the number and the tail portion gives you the last option at least to my understanding.



1. This command is useful when it comes to figuring out the pathing of a particular IP address, it shows all the activity and the logs / information of the device used .