Assignment on Cybersecurity I for CS50L

Total points 10/10

Starting in 2021, all assignments in CS50L are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. Please do not resubmit an assignment if you have already obtained a passing score. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50l (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

maz786@outlook.com

Name *

Mazafer Ul-Raqib

edX Username *

Mazafer

What is your GitHub username?

You only need to tell us if you are concerned about checking your progress in the course and/or you want a free CS50 Certificate after you satisfy all of the requirements of the course. If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50l to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50l is important! If you do decide to provide us with a GitHub username, BE CERTAIN IT IS CORRECT. If you provide the wrong username, you will not be able to see your scores.

https://github.com/maz786

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source or (b) another student's work in the course, in *any* of the course's ten assignments, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard.

◉ I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers or collaborate with any other students in this course .

Describe at least one key difference, other than size/storage capacity, between RAM and hard disk. 1/1

The kind of data storage that each offers is a significant distinction between RAM and a hard disc. A sort of volatile memory called RAM (random access memory) is used to temporarily store data while a computer is running. This implies that any data kept in RAM is gone when the machine is powered down. However, a hard drive is a form of non-volatile storage that keeps data on a computer indefinitely, even when the power is off.

The speed at which data can be accessed is another significant distinction between RAM and a hard disc. As RAM is intended to enable quick access to data that the computer is presently consuming or processing, it provides for significantly faster data access than a hard disc. As opposed to a hard drive, which requires sequential access since the data is physically stored on spinning discs, a hard drive has a slower data access rate.

Additionally, there are variations in terms of price and robustness. On a per-gigabyte basis, RAM often costs more than hard drives, but because of their mechanical construction, hard discs are more vulnerable to physical harm and failure.

How much RAM might a typical laptop have these days? 1/1

4–16 GB of RAM

How much disk space might a typical laptop have these days? 1/1

250 GB to 1 TB

How does a 32-bit system differ from a 64-bit system? 1/1

And why do the ways in which they differ matter?

The method that a 32-bit system processes data and the amount of RAM that it can access are two different things from a 64-bit one.

The CPU can only access up to 4 GB of memory in a 32-bit system. This means that no matter how much memory is installed on the computer, every programme running on a 32-bit system can only use a maximum of 4 GB of memory. A 64-bit machine, on the other hand, has access to much more RAM, generally several terabytes worth. Since a 64-bit system allows for the usage of additional RAM, applications operating on it can perform better and manage heavier workloads.

The performance and capabilities of the computer are impacted by the distinction between 32-bit and 64-bit systems. A 64-bit system may run 64-bit applications, which are created to take use of the extra memory and processing capacity available on a 64-bit system, and can typically handle more demanding tasks and bigger workloads than a 32-bit system. However, a 32-bit system can only run 32-bit programmes, therefore it might not be adequate if you have a particular programme or workload that needs a 64-bit system.

What can we do to ensure the data on our hard drives is truly erased? 1/1

Quick erase: This technique merely purges the file system structures from the hard drive, giving the impression that the data has been erased, but the data is really still present and may be recovered with the use of specialised software.

Single overwrite: Using this technique, the entire hard disc is written with data in a single pass, replacing any existing data with the new data. Although the data can still possibly be recovered with specialised software, this method is only partially effective at making the data unrecoverable.

Multiple overwrite: Using various patterns, this technique repeatedly writes data across the entire hard disc. Using specialist software and cutting-edge forensic procedures, the data may still be able to be recovered using this method, which is far more effective at making it unrecoverable.

Cryptographic erasure: This technique encrypts the data on the hard disc, makes it unrecoverable, and then deletes the encryption keys. As it makes it nearly impossible to recover the data even with sophisticated forensic techniques, this approach is the most reliable way to ensure that the data on a hard disc is truly deleted.

What is "virtual memory" and why do our computers use it? 1/1

By temporarily moving pages of data from random access memory (RAM) to disc storage, a computer can make up for physical memory shortages thanks to the virtual memory capability of its operating system (OS). As a result, a computer can use the hard drive as a "overflow" region for memory, allowing it to run more complex or many applications at once.

When a computer's physical memory is at capacity, the operating system will transfer some data from RAM to a unique file on the hard drive known as the "page file." By doing this, RAM space is made available for the computer to use for other things. The data that has been moved to the page file is read back into RAM by the computer when it is required.

Virtual memory is automatically handled by the OS and is transparent to the user. The user doesn't have to worry about determining what data to move to the page file or how much virtual memory to use. The OS takes care of each of these details automatically to give the user the greatest performance.

Virtual memory is automatically handled by the OS and is transparent to the user. The user doesn't have to worry about determining what data to move to the page file or how much virtual memory to use. The OS takes care of each of these details automatically to give the user the greatest performance.

What is a "packet sniffer"? How does it work? 1/1

A software or hardware tool called a packet sniffer (sometimes referred to as a packet analyzer or network sniffer) gathers and analyses network data in order to find problems, solve them, and keep track of network activities. To function, packet sniffers intercept and record network traffic as it flows via a router, switch, or computer.

There are several uses for packet sniffers, including:

Packet sniffers can be used to find problems with the performance of the network, such as lag times or missed connections.

Data leaks and other security lapses, such as illegal access, can be found using packet sniffers.

Traffic analysis: To analyse network traffic and spot trends, packet sniffers can be used to watch network traffic.

In order to investigate occurrences or crimes, packet sniffers can be employed to record and analyse network traffic.

Data packets passing through a network interface, such as an Ethernet port or wireless network adapter, are captured by packet sniffers as they operate. The data packets are examined by the packet sniffer, which then shows details about them including the source and destination IP addresses, the type of protocol being used (such as TCP, UDP, HTTP, etc.), and the payload data.

On a device that is directly linked to the network or on a device that is connected to the network via a hub or switch, packet sniffers can be used. The packet sniffer must be used in "promiscuous mode," which enables it to intercept any packets travelling through the network interface, regardless of their intended destination, in order to record all of the traffic on a network.

From a professional responsibility standpoint, why is it so important to establish compliance protocols for securing client data? 1/1

For a variety of reasons, establishing compliance standards for protecting customer data is crucial.

Legal requirements: Many nations have laws and regulations requiring businesses to safeguard the private and confidential information of their customers. These rules and regulations frequently outline the kinds of security precautions that must be taken to protect client data, and businesses that don't follow them risk fines and other consequences.

Ethics: Professionals have an ethical commitment to protect client data in addition to legal requirements. Clients entrust experts with their private information, so it's crucial to honour this confidence by taking the necessary precautions to protect the data.

Reputation: A company's reputation and the trust of its customers may suffer if it fails to protect the data of its clients. Serious repercussions could result from this, including diminished brand recognition and commercial losses.

Risk management: A crucial component of risk management is establishing compliance standards for protecting customer data. Organizations can lower the risk of data breaches and other security incidents that could endanger the data by taking the necessary precautions to secure client data.

In general, implementing compliance standards for preserving client data is crucial for safeguarding an organization's interests in law, morality, and reputation, as well as for successful risk management.

Do you see a difference between the professional responsibility requirements for lawyers to safeguard client files on paper versus digital representations thereof? Why or why not? 1/1

Legal professionals are required to protect client files regardless of whether they are in paper or digital form, and this is generally true. The most important aspect is the necessity to protect the sensitive and secret information in the files from unauthorised access or disclosure.

In all situations, attorneys have a responsibility to take reasonable precautions to prevent unauthorised access to or disclosure of the personal information about their clients. This may entail putting in place different technical, organisational, and physical safeguards to protect client files, such as locking filing cabinets or rooms for paper records or using password-protected electronic file systems for digital records.

When working with digital client files, there might be some additional factors to take into account, such as the need to make sure that the proper technical security measures are in place to prevent unauthorised access or data breaches and the requirement to keep up with technological and cybersecurity advancements. However, these are merely extra considerations that attorneys must make in order to uphold their ethical duty to protect the client information.

57 6f 75 6c 64 20 79 6f 75 20 6c 69 6b 65 20 61 20 66 72 65 65 20 70 6f 69 6e 74 3f 1/1

This may be in code, but your answer shouldn't be!

Would you like a free point?

Debrief

About how many MINUTES would you say you spent on this assignment? *

Just to set expectations for future students.

666