Assignment 1

Total: 100 Points / 10% of total grade

Due: Feb. 5, 2024

Q1 (10 points) Please describe “CIA” in security. You need to explain each of them.

**Confidentiality:**

**Confidentiality ensures that information is only accessible to authorized individuals or systems and remains protected from unauthorized access or disclosure. The goal is to prevent unauthorized users, hackers, or entities from gaining access to sensitive data. Measures such as encryption, access controls, and secure communication protocols help maintain confidentiality.**

**Integrity:**

**Integrity focuses on the accuracy, consistency, and trustworthiness of data. It ensures that information remains unaltered and reliable throughout its lifecycle. The objective is to protect data from unauthorized modification, tampering, or corruption. Techniques such as checksums, digital signatures, and version controls help maintain data integrity.**

**Availability:**

**Availability ensures that information and resources are accessible and usable when needed by authorized users. It involves preventing disruptions or downtime that could impact the availability of services. The goal is to ensure that systems are operational and responsive, even in the face of threats, attacks, or unexpected events. Redundancy, backup systems, and disaster recovery planning contribute to maintaining availability.**

Q2 (5 points) Please explain vulnerabilities, threats, and controls in security.

**Vulnerabilities are weaknesses or flaws in a system's design, implementation, configuration, or operation that could be exploited by attackers to compromise the security of the system. Vulnerabilities can exist in various components, including software, hardware, networks, and even human practices. They can arise due to coding errors, misconfigurations, outdated software, or inadequate security policies. An example of a vulnerability is an outdated web server with known security vulnerabilities, unpatched software, or weak passwords are all examples of potential vulnerabilities.**

**Threats refer to potential dangers or malicious activities that can exploit vulnerabilities and harm the confidentiality, integrity, or availability of information or systems. Threats can be intentional (such as hacking, malware, or espionage) or unintentional (such as natural disasters, hardware failures, or human errors). Threat actors may include hackers, insiders, competitors, or even environmental factors. Examples of threats include a hacker attempting to exploit a software vulnerability, a phishing attack targeting employees, or a flooding incident causing physical damage to servers.**

**Controls are security measures or safeguards implemented to mitigate or counteract vulnerabilities and threats. They are designed to reduce the risk of unauthorized access, data breaches, or other security incidents. Controls can be technical, procedural, or administrative. Technical controls include firewalls, encryption, and antivirus software. Procedural controls involve policies, guidelines, and security awareness training. Administrative controls encompass roles and responsibilities, access controls, and incident response plans. Installing a firewall to monitor and filter network traffic, enforcing strong authentication mechanisms, conducting regular security audits, and educating employees about cybersecurity best practices are all examples of controls.**

Q3 (10 points) Please write five basic approaches to the defense of computing systems and give a short example for each of them.

**Firewalls act as a barrier between a trusted internal network and untrusted external networks, controlling and monitoring incoming and outgoing network traffic. An example is a network administrator configures a firewall to block unauthorized access to certain ports, preventing external users from gaining direct access to sensitive internal servers.**

**Encryption transforms data into an unreadable format using cryptographic algorithms. It ensures that even if unauthorized individuals gain access to the data, they cannot understand or use it without the appropriate decryption key. An example is that an organization encrypts sensitive files on its servers, and only authorized users with the correct encryption keys can access and decrypt the data.**

**Access controls restrict and manage user permissions, ensuring that individuals only have access to the resources and information necessary for their roles. An employee is granted read-only access to a document repository, limiting their ability to modify or delete files, reducing the risk of accidental or intentional data manipulation is an example of access control.**

**Regular software patching and updates help eliminate known vulnerabilities that could be exploited by attackers. An IT administrator regularly applies software updates and patches to all computers in an organization to address known security vulnerabilities and enhance system resilience is an example of regular software patching and updates.**

**Security awareness training educates users about security risks and best practices which helps create a security-aware culture within an organization, reducing the likelihood of falling victim to social engineering attacks or making security-related mistakes. For example, employees undergo training on recognizing phishing emails, enabling them to identify and report suspicious messages, reducing the risk of unauthorized access through social engineering tactics.**

Q4 (5 points) Please describe three components in VM.

**The host is the physical underlying hardware which includes the CPU, RAM, storage devices and network interfaces.** **The host's physical hardware serves as the foundation for virtualization. The hypervisor interacts directly with the host's hardware to manage and allocate resources to virtual machines.**

**The hypervisor is a software layer that sits between the hardware and the virtual machines. It is responsible for managing and allocating the physical resources of the host machine to multiple virtual machines. There are two types of hypervisors: Type 1 (bare-metal) runs directly on the hardware, while Type 2 (hosted) runs on top of an existing operating system. The hypervisor abstracts and virtualizes the underlying hardware, allowing multiple virtual machines to share the same physical resources without interfering with each other. It controls the allocation of CPU, memory, storage, and network resources to the guest.**

**The "guest" in the context of a Virtual Machine (VM) refers to the virtualized operating system and applications running within an individual virtual machine. It contains it’s own OS, virtual CPU, virtual RAM, applications and virtual drivers and a virtual disk.**

Q5 (10 points) Please list the pros and cons of VMs.

**Pros:**

**VMs offer cost-effective solutions by running multiple operating systems on a single physical computer, saving space and management efforts. They support legacy applications, reducing migration costs. For example, a Linux VM can run on a Windows host. VMs ensure isolation, enabling integrated disaster recovery and application provisioning without protection issues. Each VM is completely segregated from others, ensuring data integrity and security.**

**Cons:**

**Virtual machines are not as efficient as a real one when accessing the  
hardware  
When multiple virtual machines are simultaneously running on a host  
computer, one virtual machine can be affected by other running virtual  
machines, depending on the workload**

Q6 (30 points) Please setup a Type 2 hypervisor (e.g., VMWare Player) in your computer with a Kali Linux or Ubuntu. Then, open a terminal/command prompt in your host system and try to Ping your guest system and vice versa. If you are not sure how to use Ping command, please read this article (<https://www.redhat.com/sysadmin/ping-usage-basics>

[Links to an external site.](https://www.redhat.com/sysadmin/ping-usage-basics)).

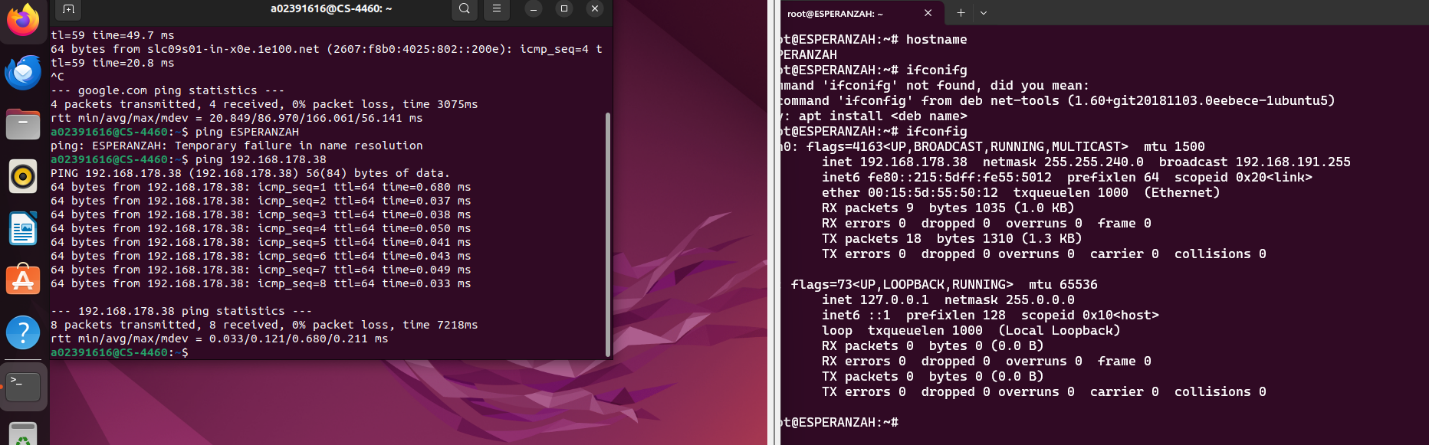
Please answer the following question: did you successfully use Ping command to communicate between Host system and Guest system? If yes, briefly describe how it works and attach a screenshot of the terminal/command prompt output. If not, check (1) your guest system network mode (e.g., bridged?); (2) your guest system firewall policy about Ping traffic. You need to make it work!

Host to VM

A screenshot of a computer

Description automatically generated

 VM to Host



**Pinging is a network utility used to test the reachability of a host on an Internet Protocol (IP) network. The Ping utility works by sending Internet Control Message Protocol (ICMP) Echo Request messages to the target host and waiting for Echo Reply messages. This process helps in assessing the round-trip time it takes for a packet to travel from the source to the destination and back.**

Q7 (30 points) In this task, you need to examine the performance of DES, 3DES, AES, and RSA in guest and host systems. You need to measure the performance of them in terms of the time to complete the encryption and decryption with different algorithms for the files with different sizes (e.g., 50 KB, 1MB, 2MB).

Hint: you should not write your own DES algorithms. E.g., in Python, you can find DES, AES, RSA with the library Crypto (https://pycryptodome.readthedocs.io/en/latest/src/introduction.html). Note that, you can choose any language for this question.

Hint2: you can run the tasks 100 times and calculate the average time for the benchmark

In your submission, in addition to the source code, you need to submit two column charts for the benchmarks of the encryption and decryption using DES, 3DES, AES, RSA in both guest and host systems. You also need to describe your observations.

1. performance comparison between DES, 3DES, AES, RSA and explain it happens;

AES outperforms on every run and RSA is generally by far the slowest method. The reason behind this is that RSA is an asymmetric cipher which has intense mathematical complexity which takes a lot of time, especially since the RSA key size’s are generally larger. AES does better than 3DES and DES because it has an efficient algorithm. 3DES is slower than DES due to it’s triple encryption process, which makes it more secure but much slower. DES has become basically obsolete because of it’s small key size and vulnerability to attacks.

(b) performance comparison between guest and host systems and explain why it happens.

**Normally the host system would perform better, however I was running several other CPU heavy programs while running the program hence the slower times.**

**The reason the guest system is generally slower is because the hypervisor needs to translate the system instructions and manage memory allocation which leads to additional processing overhead. The host system has direct access to the physical CPU which gives a better performance while the guest system must compete with other VM’s and relies on the hypervisor for resource allocation. I/O operations are slower within the guest system because it does not have physical access to the I/O devices while the host system does.**