Question 1 : As per NIST definition, what are the three main properties of a cloud? Briefly explain each property.

1. Resource scalability.
2. On demand.
3. Pay as you go.

Question 2: Consider infrastructure as a service and platform as a service. Compare pros and cons on the cloud user viewpoint.

Infrastructure as a Service (IaaS):

Pros:

Flexibility and Control: Cloud users have full control over virtualized infrastructure components like servers, storage, and networking, allowing for customization to meet specific needs.

Scalability: Users can easily scale resources up or down as needed, making it suitable for fluctuating workloads.

Cost Savings: Pay-as-you-go pricing reduces the need for large upfront capital investments.

Cons:

Management Overhead: Users are responsible for managing the OS, updates, and applications, which can be time-consuming.

Technical Expertise Required: It may require a higher level of technical knowledge for effective use.

Platform as a Service (PaaS):

Pros:

Simplicity: PaaS abstracts infrastructure management, allowing users to focus on application development and deployment.

Productivity: Faster development and deployment cycles due to built-in development tools.

Scalability: PaaS platforms often handle automatic scaling, simplifying resource management.

Cons:

Vendor Lock-In: PaaS platforms can tie users to specific providers and technologies.

Limited Customization: Less flexibility in configuring the underlying infrastructure, which may not suit all use cases.

The choice between IaaS and PaaS depends on factors like technical expertise, control requirements, and the specific needs of the cloud user.

Question 3: it was stated that clouds extend the attack surface. how? explain briefly?

Internet Access: Cloud services are typically accessible over the internet, which means that potential attackers can target these services from anywhere in the world.

Shared Responsibility: In many cloud service models (IaaS, PaaS, SaaS), there's a shared responsibility for security between the cloud provider and the customer. Failure to secure your part of the shared responsibility can create vulnerabilities.

APIs and Interfaces: Cloud services often rely on APIs (Application Programming Interfaces) and interfaces for interaction. Insecure APIs can be exploited by attackers.

Question 4: in the topology attack, how can an attacker determine if their virtual machine is co-resident with the target’s virtual machine? Name and explain two techniques/heuristics?

1. Smarter Strategy: utilize locality.

Idea: VM instances launched right after target are likely to be co-resident with the target  
Paper claims 40% success rate

1. Brute force scheme:

figure out target’s availability zone and type Launch many probe instances in the same area Success rate: 8.4%

Question 5: In spectre and meltdown, attacker take advantage of two of the modern processor optimizations to make unauthorized access to protected memory. What are these optimizations? Explain briefly.

Spectre: Spectre is a class of vulnerabilities that primarily exploits speculative execution in modern processors. It tricks the processor into speculatively executing instructions that would not normally be executed, potentially leading to unauthorized access of protected memory.

Meltdown: Meltdown is a specific vulnerability that also exploits speculative execution, but it primarily focuses on the "out-of-order execution" aspect. It allows an attacker to access kernel memory from user-space processes.

6. We discussed the use of a trusted platform chip for security. In particular used in remote attestation for untrusted servers. Why is it important that the attacker does not have physical access to the server.

Answer: When attackers gain physical access, they can bypass security measures and compromise the server's operating system and data. Manipulate hardware components, including storage devices and network interfaces. Steal sensitive information and deploy malware. Make unauthorized configuration changes and disrupt services. Destroy data by physically damaging the server. Impersonate authorized personnel, facilitating social engineering attacks.

7. Secure remote data outsourcing was discussed. one of the techniques for this is to use sentinel blocks. Briefly explain in few sentences how a sentinel block can provide guarantee to the integrity of the file.

Answer: Sentinel blocks are used in secure remote data outsourcing to ensure the integrity of a file. These special blocks contain checksums or cryptographic hashes computed from the data within the associated file blocks. When a file is retrieved from the remote server, the recipient can verify the integrity of the file by recomputing the checksums or hashes from the received data blocks and comparing them to the values stored in the sentinel blocks. If there is any discrepancy, it indicates potential data tampering or corruption, providing a guarantee of file integrity. This technique helps ensure that the outsourced data remains unchanged and trustworthy during remote storage and retrieval.

8. To verify the integrity of remote computations. Two techniques we covered in module 6 are attestation and auditing. How do these techniques work?

**Attestation:**

Attestation involves verifying the trustworthiness of a system or its components.

It typically uses hardware or software-based mechanisms to confirm that a system's configuration, software, or firmware is as expected and hasn't been tampered with.

Attestation can use cryptographic signatures or measurements to prove the authenticity of system components.

Remote parties, like security administrators or remote servers, can request and verify these attestations to ensure the system's integrity.

**Auditing:**

Auditing focuses on monitoring and recording activities within a system or network.

It involves creating logs or records of events, such as login attempts, access to sensitive files, or system changes.

Auditing also includes the analysis of these logs to detect and investigate security incidents, compliance violations, or unauthorized actions.

Security policies and standards guide auditing to ensure that a system or network complies with regulations and best practices.

9. In module 7 the N-version approach towards detection of malware was discussed. How does the n-version malware detection work? Why is it effective than traditional antivirus tools?

This is how it works: The N-version malware detection approach works by creating multiple independent versions of a malware detection system, each using different algorithms, heuristics, or techniques for analyzing the same input data. If the majority of these versions agree on the presence or absence of malware, the system decides. This redundancy and diversity aim to enhance the system's robustness and reliability.

Why it is effective: They reduce false positives and negatives, enhance resilience to evasion techniques through diverse approaches, create multiple defense layers, adapt to evolving threats more effectively, and provide resilience against zero-day attacks by employing heuristic and behavior-based analysis.