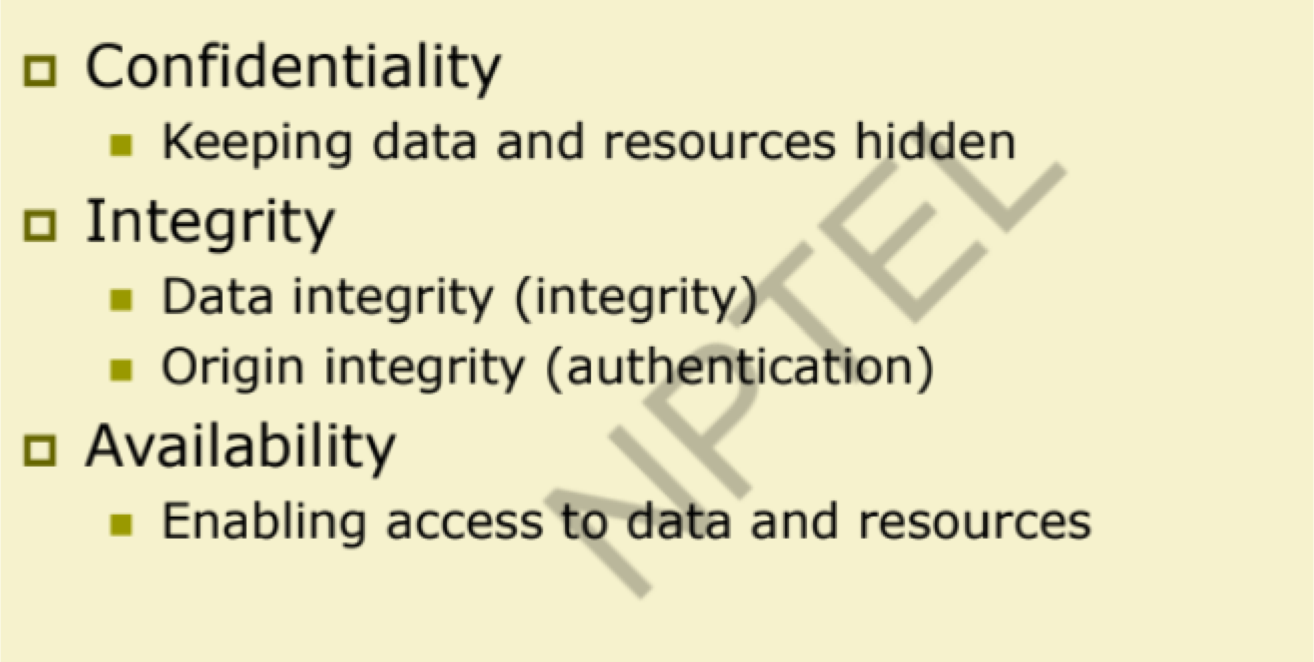
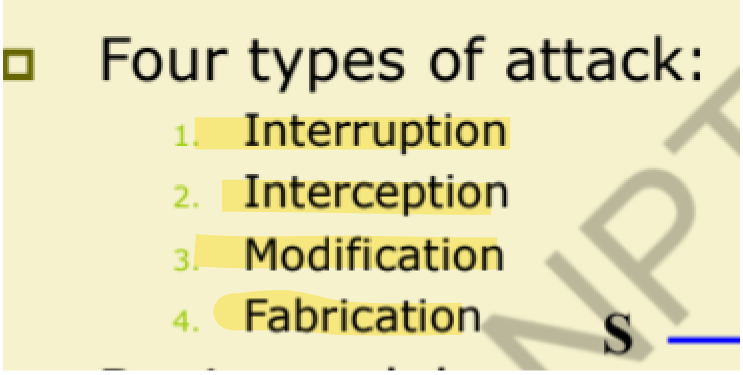
CC Week 6

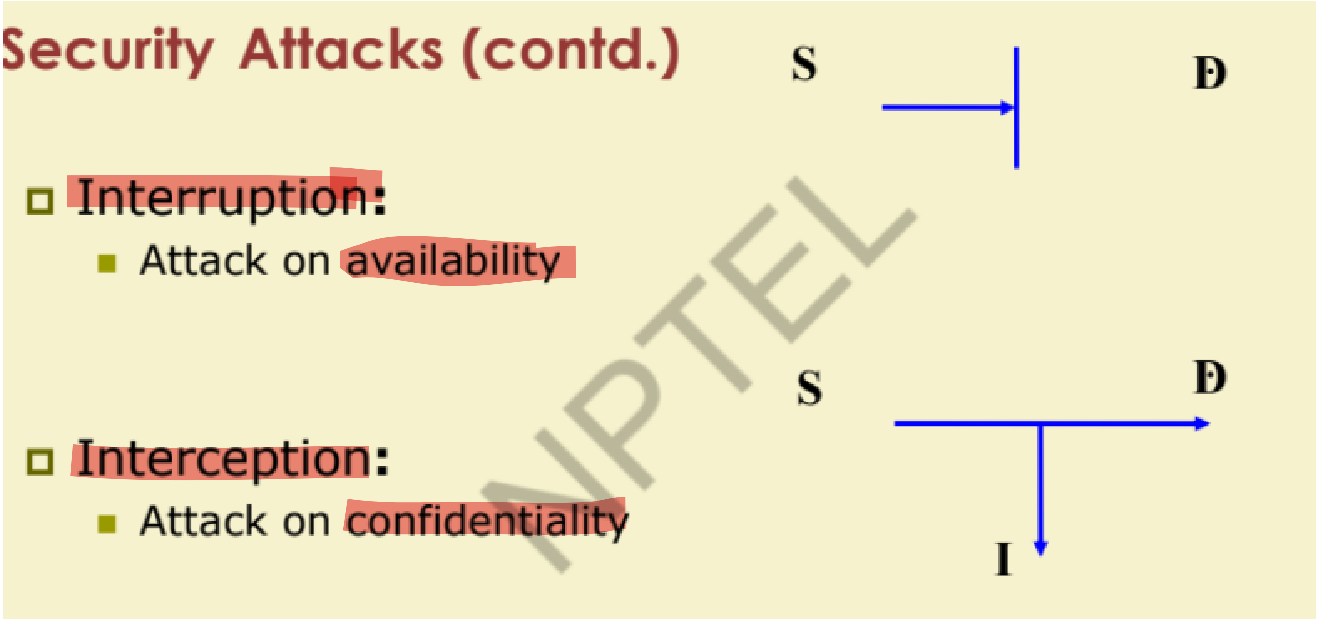
Confidentiality, Integrity, Availability



- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources



- Four types of attack:
  1. Interruption
  2. Interception
  3. Modification
  4. Fabrication

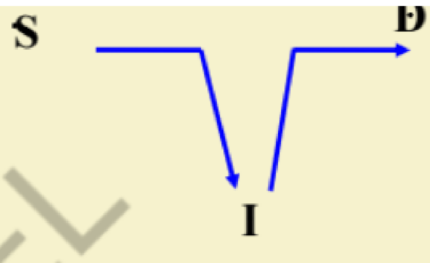


Security Attacks (contd.)

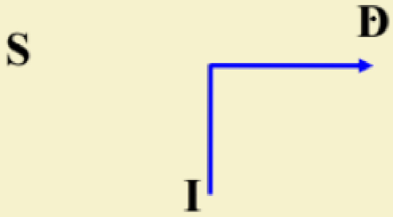
- Interruption:
  - Attack on availability
- Interception:
  - Attack on confidentiality

Security Attacks

- Modification:
  - Attack on integrity



- Fabrication:
  - Attack on authenticity



Passive and Active Attacks

- Passive attacks
  - Obtain information that is being transmitted (eavesdropping).
  - Two types:
    - Release of message contents:- It may be desirable to prevent the opponent from learning the contents of the transmission.
    - Traffic analysis:- The opponent can determine the location and identity of communicating hosts, and observe the frequency and length of messages being exchanged.
  - Very difficult to detect.

- Active attacks
  - Involve some modification of the data stream or the creation of a false stream.
  - Four categories:
    - Masquerade:- One entity pretends to be a different entity.
    - Replay:- Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
    - Modification:- Some portion of a legitimate message is altered.
    - Denial of service:- Prevents the normal use of communication facilities.

QUESTION 1:

Modification is an attack on:

A) Authenticity

[✓ B) Integrity]

C) Confidentiality

D) Availability

Correct Option: B

Detailed Solution: Modification is an attack on integrity.

QUESTION 2:

Which of the following is/are example(s) of passive attack?

A) Replay

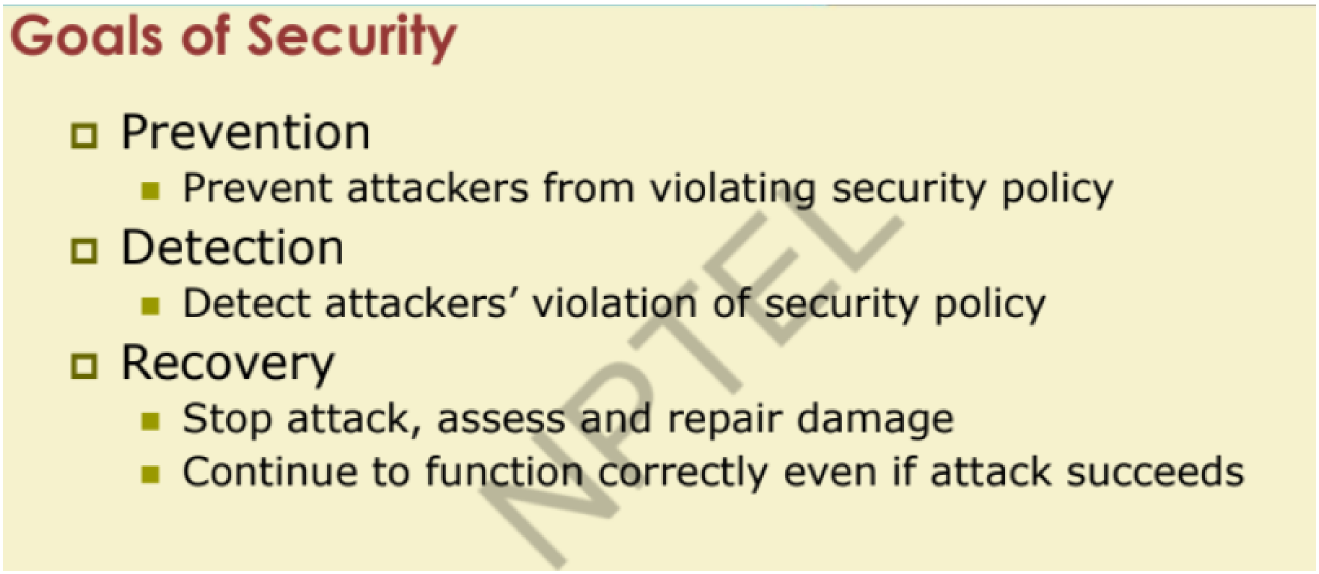
B) Denial of service

[✓ C) Traffic analysis]

D) Masquerade

Correct Option: C

Detailed Solution: Traffic analysis is an example of passive attack.



Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

QUESTION 3:

Which of the following is/are the recovery goal(s) of the security mechanism?

A) Prevent attackers from violating security policy

B) Detect attackers' violation of security policy

C) Stop attack, assess and repair damage

D) Continue to function correctly even if attack succeeds

Correct Option: C, D

Detailed Solution: Refer slide no. 8 of Cloud-Security I.

QUESTION 4:

Statement I: ✗ Authorization is the identification of legitimate users.

✓ **Statement II:** Integrity is the protection against data alteration/corruption.

A. Statement I is TRUE and statement II is FALSE.

B. Statement I is FALSE and statement II is TRUE.

C. Both statements are TRUE.

D. Both statements are FALSE.

Correct Option: B

Detailed Solution: Refer slide no. 18 of Cloud-Security I. Authorization is the determination of whether or not an operation is allowed by a certain user. Integrity is the protection against data alteration/corruption. So the first statement is false and the second statement is true.

QUESTION 5:

Which of the following is/are hypervisor risks associated with rogue hypervisor rootkits?

A) Vulnerable virtual machine applications like Vmchat, VMftp, Vmcat etc.

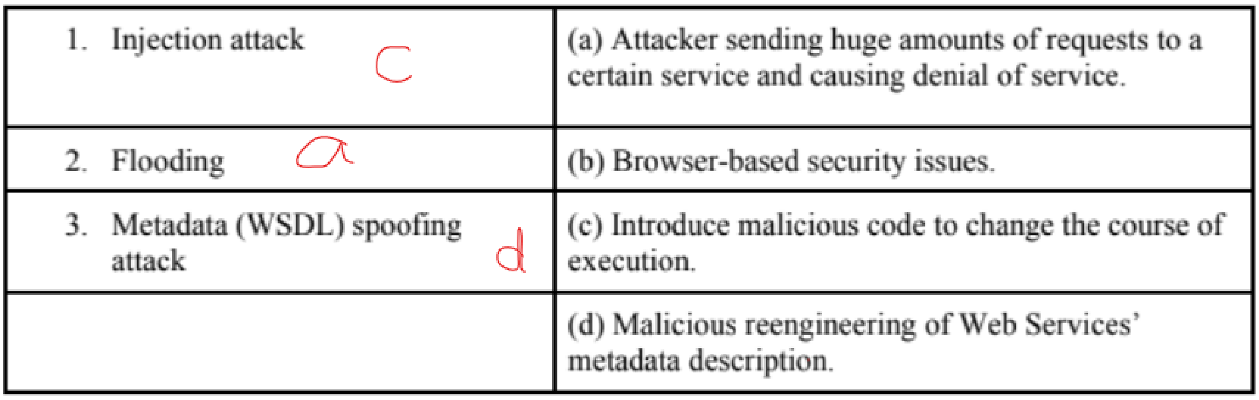
B) Hypervisor that hides itself from normal malware detection systems

C) Improper configuration of VM.

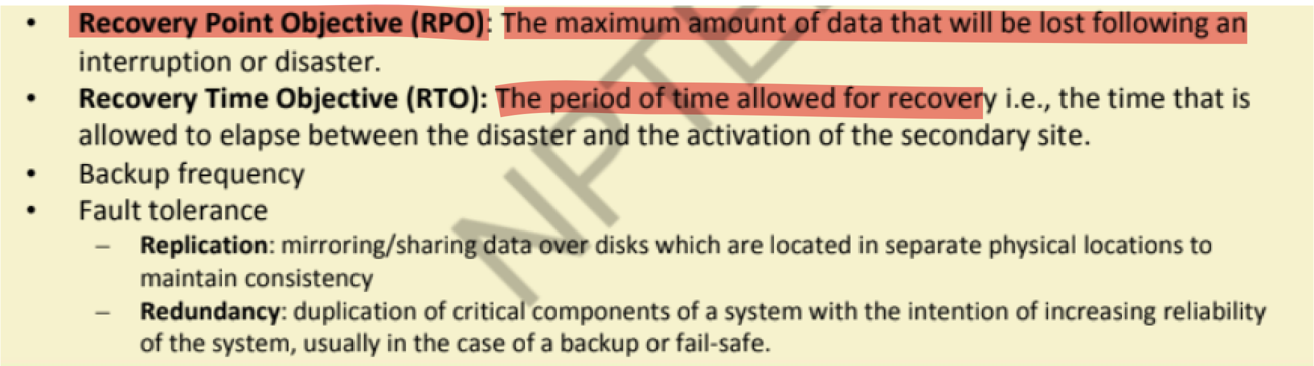
D) Hypervisor that creates a covert channel to dump unauthorized code.

Correct Answer: B, D

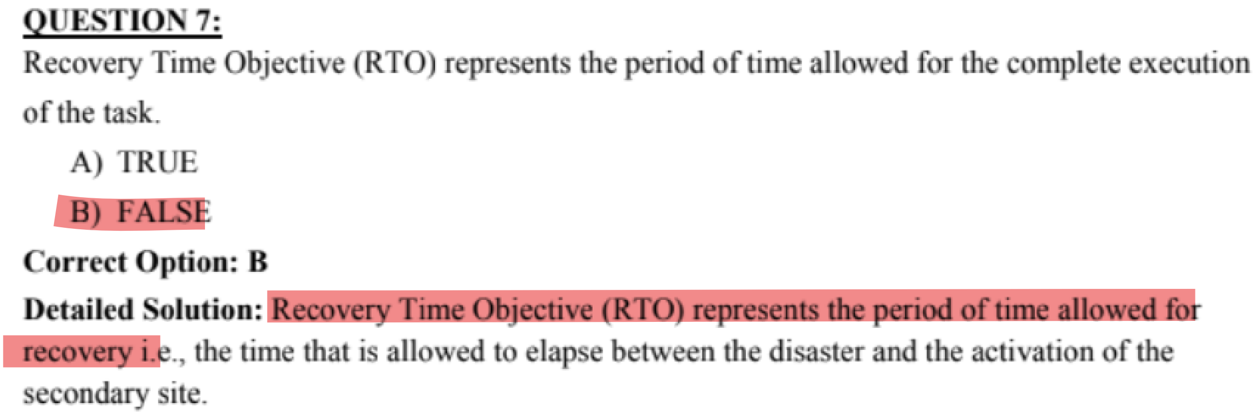
Detailed Solution: Hypervisor risks associated with rogue hypervisor rootkits include hypervisors that hide themselves from normal malware detection systems, and hypervisors that create a covert channel to dump unauthorized code.



1. Injection attack c	(a) Attacker sending huge amounts of requests to a certain service and causing denial of service.
2. Flooding a	(b) Browser-based security issues.
3. Metadata (WSDL) spoofing attack d	(c) Introduce malicious code to change the course of execution.
	(d) Malicious reengineering of Web Services' metadata description.



- **Recovery Point Objective (RPO)**: The maximum amount of data that will be lost following an interruption or disaster.
- **Recovery Time Objective (RTO):** The period of time allowed for recovery i.e., the time that is allowed to elapse between the disaster and the activation of the secondary site.
- Backup frequency
- Fault tolerance
  – **Replication**: mirroring/sharing data over disks which are located in separate physical locations to maintain consistency
  – **Redundancy**: duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.



QUESTION 7:

Recovery Time Objective (RTO) represents the period of time allowed for the complete execution of the task.

A) TRUE

B) FALSE

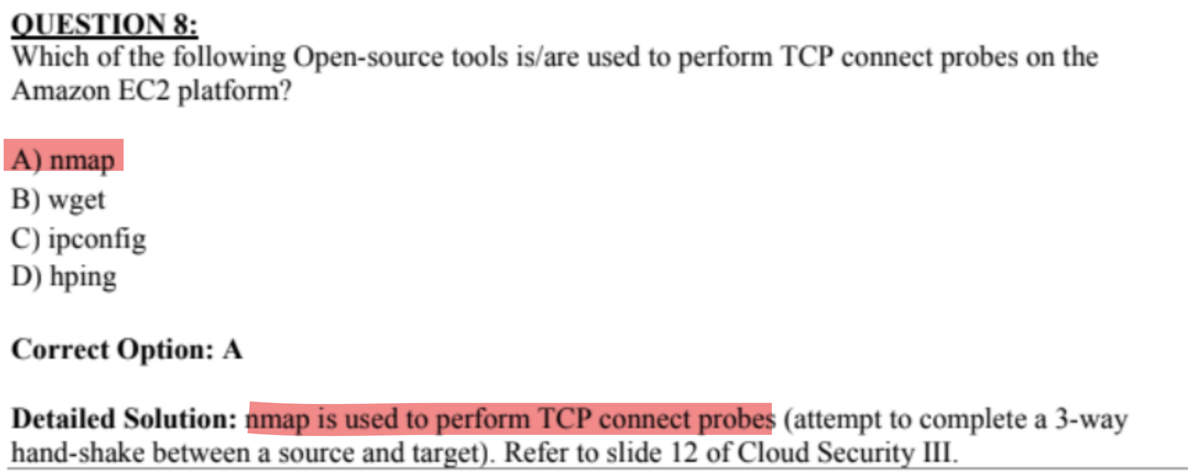
Correct Option: B

Detailed Solution: Recovery Time Objective (RTO) represents the period of time allowed for recovery i.e., the time that is allowed to elapse between the disaster and the activation of the secondary site.

Network probing involves investigating public servers hosted on Amazon Web Services (AWS) and checking if they are sharing resources with other servers, a concept known as co-residence.

1. **nmap**: This tool is used to perform TCP connect probes.
2. **hping**: This tool is used to perform TCP SYN traceroutes.
3. **wget**: This tool is used to retrieve web pages from servers.
   There are two types of probes:

- **External probe**: This originates from a system outside of AWS's EC2 (Elastic Compute Cloud) and targets an EC2 instance. It helps determine how external systems interact with EC2-hosted servers.
- **Internal probe**: This originates from within an EC2 instance and targets another EC2 instance. It helps understand the internal network dynamics within AWS, such as communication between different EC2 instances.



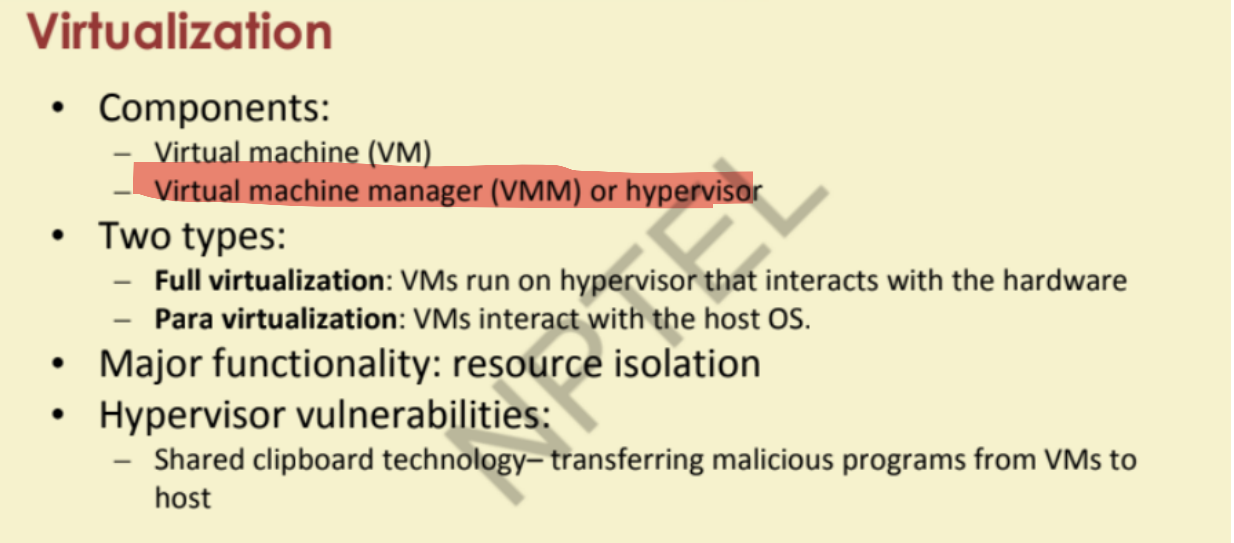
QUESTION 8:

Which of the following Open-source tools is/are used to perform TCP connect probes on the Amazon EC2 platform?

A) nmap
B) wget
C) ipconfig
D) hping

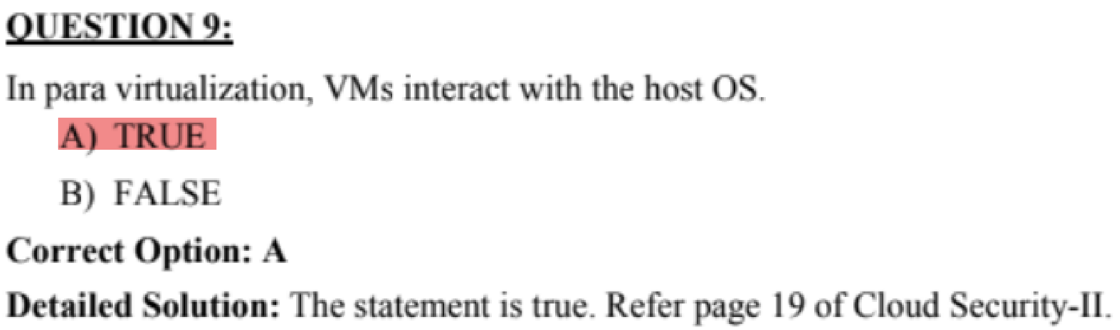
Correct Option: A

Detailed Solution: nmap is used to perform TCP connect probes (attempt to complete a 3-way hand-shake between a source and target). Refer to slide 12 of Cloud Security III.



Virtualization

- Components:
  - Virtual machine (VM)
  - Virtual machine manager (VMM) or hypervisor
- Two types:
  - **Full virtualization**: VMs run on hypervisor that interacts with the hardware
  - **Para virtualization**: VMs interact with the host OS.
- Major functionality: resource isolation
- Hypervisor vulnerabilities:
  - Shared clipboard technology– transferring malicious programs from VMs to host



QUESTION 9:

In para virtualization, VMs interact with the host OS.

A) TRUE

B) FALSE

Correct Option: A

Detailed Solution: The statement is true. Refer page 19 of Cloud Security-II.

1. **Conflict Removal**: Conflict removal refers to resolving conflicts that arise when assigning roles or permissions to users or entities within a system.
2. **Virtual Role**: concept used in role-based access control (RBAC) systems. It is a role that is dynamically created to resolve conflicts or enforce access control policies. Virtual roles are not predefined but are generated as needed to fulfill specific access requirements.

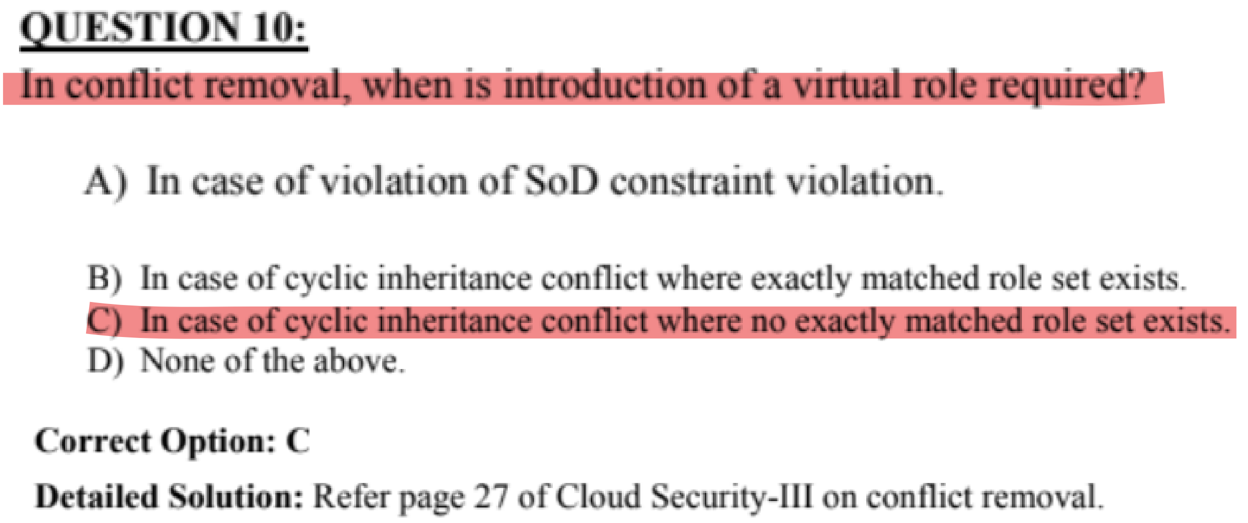
Now, let's look at the scenarios:
A) **In case of violation of SoD (Segregation of Duties) constraint violation**: SoD is a security principle that aims to prevent conflicts of interest and fraud by ensuring that no single individual or entity has complete control over a critical

process or transaction. If there is a violation of SoD constraint, it doesn't necessarily require the introduction of a virtual role; instead, the conflicting permissions or roles need to be adjusted or resolved.

B) **In case of cyclic inheritance conflict where exactly matched role set exists**: Cyclic inheritance conflicts occur when roles are assigned in a way that creates a loop or cycle in the role hierarchy. If there is an exactly matched role set within this cycle, it can lead to conflicts. In such cases, introducing a virtual role might be necessary to break the cycle and resolve the conflict.

C) **In case of cyclic inheritance conflict where no exactly matched role set exists**: Similar to scenario B, if there is a cyclic inheritance conflict but there is no exact match within the role set to resolve it, introducing a virtual role becomes necessary to break the cycle and resolve the conflict dynamically.

cyclic & no matched = virtual role needed



QUESTION 10:

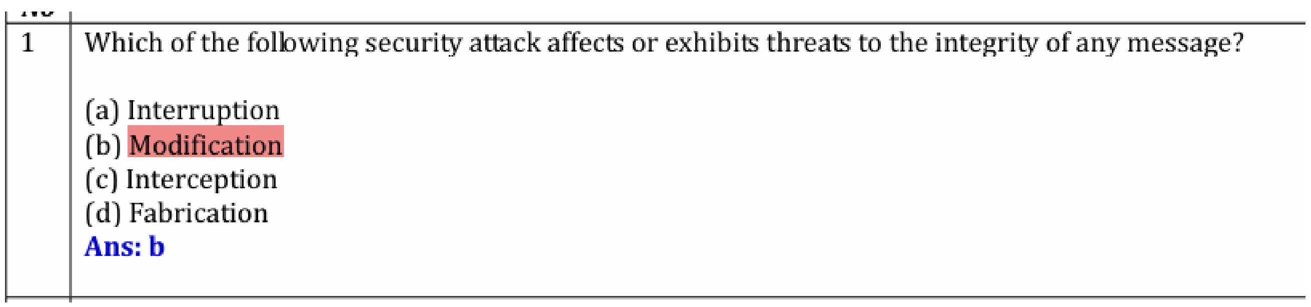
In conflict removal, when is introduction of a virtual role required?

A) In case of violation of SoD constraint violation.

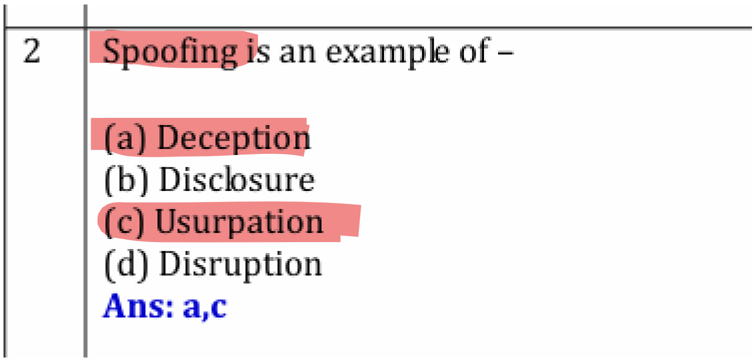
B) In case of cyclic inheritance conflict where exactly matched role set exists.
C) In case of cyclic inheritance conflict where no exactly matched role set exists.
D) None of the above.

Correct Option: C

Detailed Solution: Refer page 27 of Cloud Security-III on conflict removal.

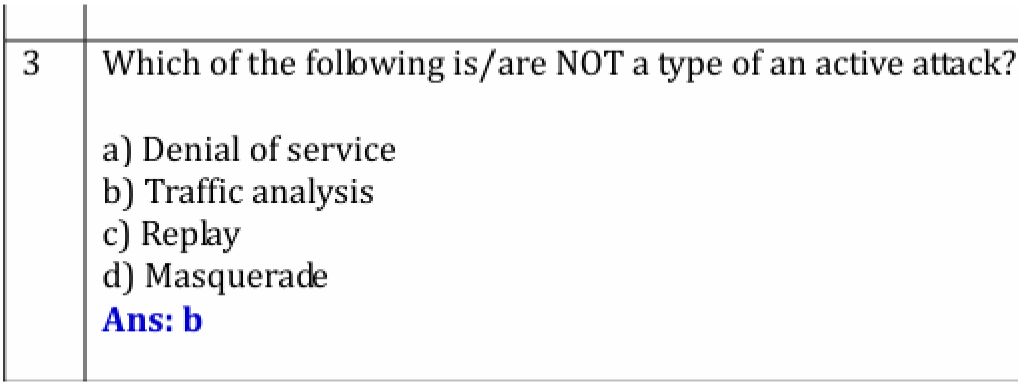


1	Which of the following security attack affects or exhibits threats to the integrity of any message? (a) Interruption (b) Modification (c) Interception (d) Fabrication **Ans: b**

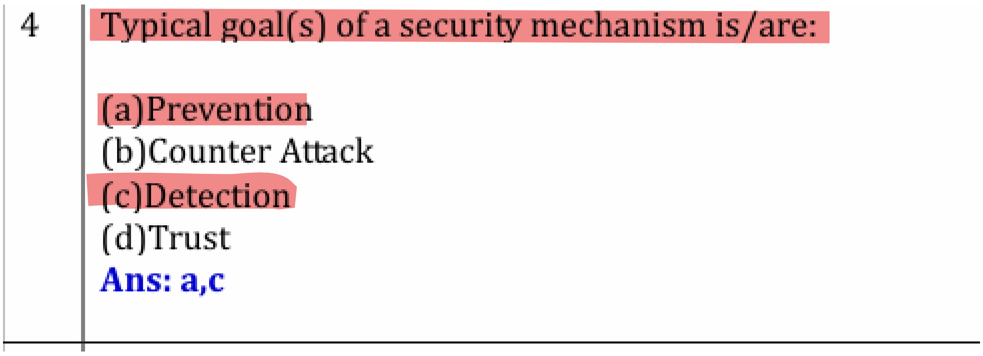


2	Spoofing is an example of – (a) Deception (b) Disclosure (c) Usurpation (d) Disruption **Ans: a,c**

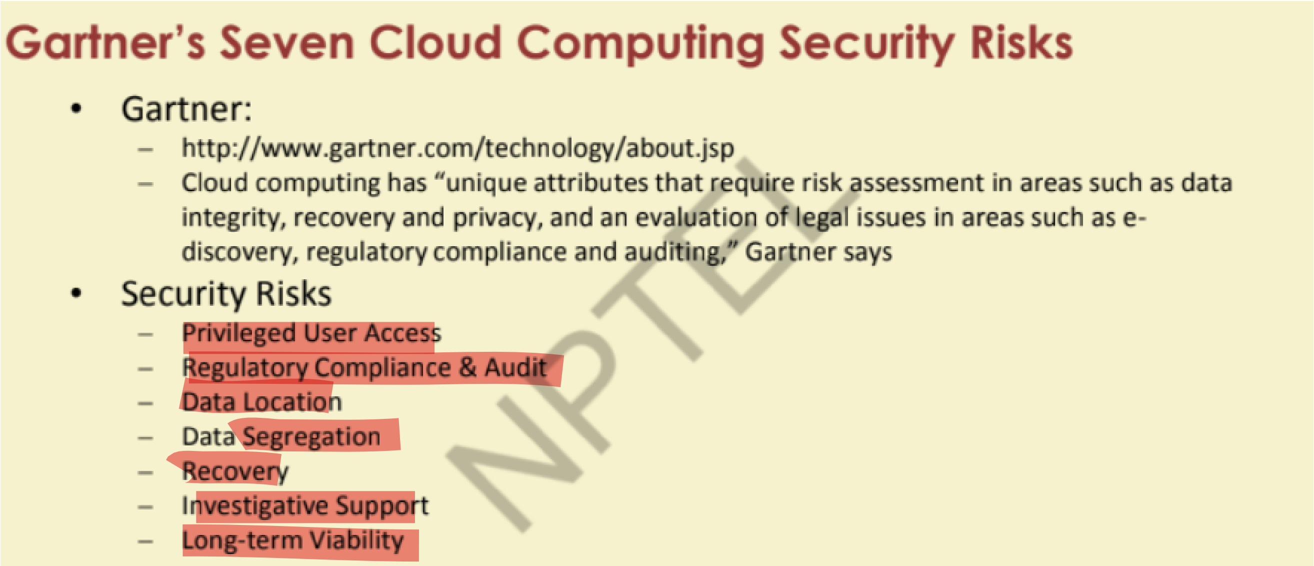
1. **Spoofing**: Spoofing is the act of disguising oneself as trusted source to deceive or trick systems, individuals, or organizations.
2. **Deception**: Deception refers to the act of misleading or causing someone to believe something that is not true.
3. **Usurpation**: Usurpation is the unauthorized or illegal seizure or takeover of something, such as power, authority, or property, typically without proper authorization or consent.
4. **Disclosure**: Disclosure is the act of revealing or making information known.



3	Which of the following is/are NOT a type of an active attack? a) Denial of service b) Traffic analysis c) Replay d) Masquerade **Ans: b**



4	Typical goal(s) of a security mechanism is/are: (a)Prevention (b)Counter Attack (c)Detection (d)Trust **Ans: a,c**



Gartner's Seven Cloud Computing Security Risks

- Gartner:
  - http://www.gartner.com/technology/about.jsp
  - Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing," Gartner says
- Security Risks
  - Privileged User Access
  - Regulatory Compliance & Audit
  - Data Location
  - Data Segregation
  - Recovery
  - Investigative Support
  - Long-term Viability

6 Which of the following is/are Gartner's cloud computing security risks?

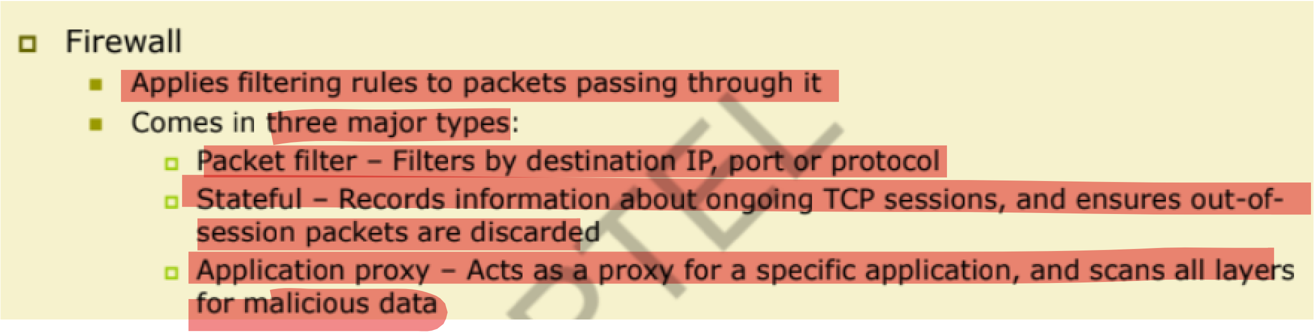
(a) Data Location
(b) Long-term Viability
(c) Privileged User Access
(d) Operating System Vulnerability
Ans: a,b,c

7 In cloud "Recovery Time Objective" (RTO) depicts:

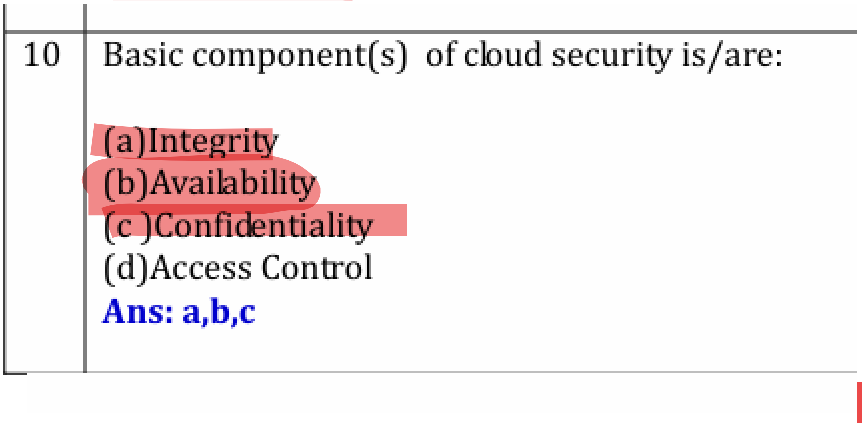
(a)The period of time allowed for recovery
(b)Percentage of data recovered
(c)Maximum amount of data recovered
(d)None
Ans: a

8 Which type(s) of firewall record(s) information about ongoing TCP sessions and ensures out-of-session packets are discarded?

(a) Stateful
(b) Application proxy
(c) Packet filter
(d) None of these
Ans: a



- Firewall
  - Applies filtering rules to packets passing through it
  - Comes in three major types:
    - Packet filter – Filters by destination IP, port or protocol
    - Stateful – Records information about ongoing TCP sessions, and ensures out-of-session packets are discarded
    - Application proxy – Acts as a proxy for a specific application, and scans all layers for malicious data



10	Basic component(s) of cloud security is/are: (a)Integrity (b)Availability (c)Confidentiality (d)Access Control **Ans: a,b,c**

CIA

QUESTION 1:

In a cyber-attack, if one entity is pretending to be another one, then it is called.

a) Denial of Service

b) Replay

c) Masquerade

d) Modification

Correct Answer: c

Detailed Solution: Masquerade is "one entity pretends to be a different entity".

QUESTION 2:

Security responsibilities of a IaaS cloud service provider is typically upto

a) Guest OS

b) Application

c) Solution Stack

d) Hypervisor

Correct Answer: d

Detailed Solution: Security responsibilities of a IaaS cloud Service provider is typically upto hypervisor.

QUESTION 3:

Which of the following security property ensures that subscriber can't deny the action done by him/her.

a) Authorization

b) Non-repudiation

c) Confidentiality

d) Integrity

Correct Answer: b

Detailed Solution: Non repudiation is able to trace what happened and prevent denial of action.

QUESTION 4:

What is honeypot?

a) Manages network traffic filtering rule

b) Scans suspected messages and send alerts

c) Simulates a decoy with services

d) All of the above

Correct Answer: c

QUESTION 5:

Which of the following are the Gartner's seven cloud computing risks?

a) Regulatory Compliance & Audit

b) Data Location

c) Data Segregation

d) All of the above

Correct Answer: d

Detailed Solution: Refer slide no. 10 of Cloud-Security II.

QUESTION 6:

The ____________ amount of data that will be lost due to an interruption or disaster is defined in Recovery Point Objective

a) minimum

b) maximum

c) average

d) None of these

Correct Answer: b

Detailed Solution: RTO defines the maximum amount of data that will be lost following an interruption or disaster.

QUESTION 7:

Which open source tools can be used to probe http and https port?

a) mmap

[✓ b) hping]

c) wpget

d) All of the above

Correct Answer: b

Detailed Solution: nmap, hping, wget are used to prove port 80 (http) and 443 (https)

QUESTION 8:

Cloud-based collaboration can be

a) Federated

b) Loosely-coupled

[✓ c) All of the above]

d) None of these

Correct Answer: c

Detailed Solution: Cloud-based collaboration can be tightly-coupled or federated as well as loosely-coupled.

QUESTION 10:

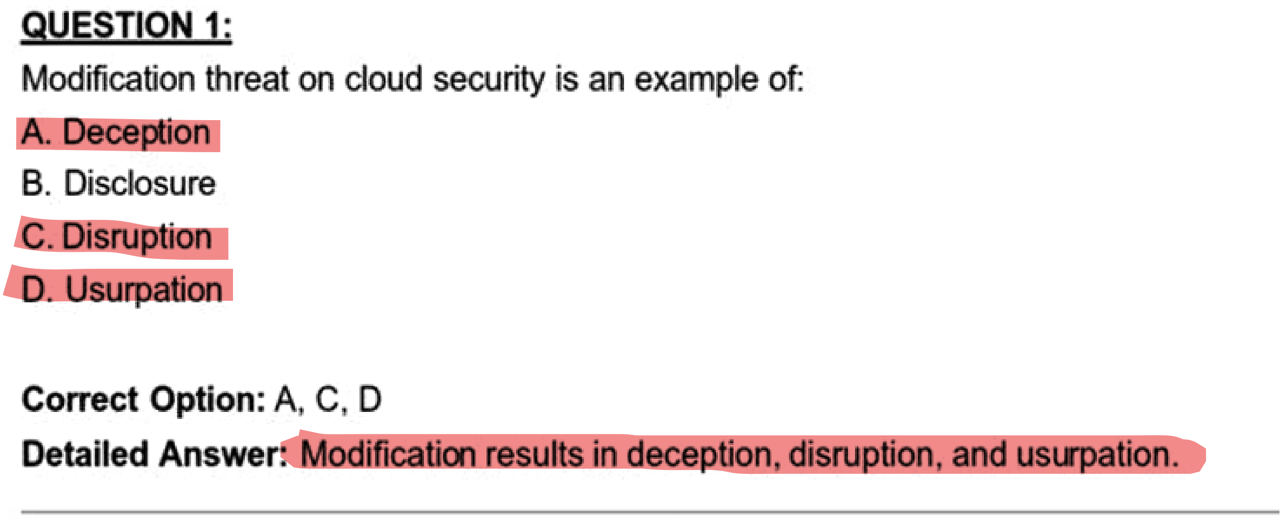
Fabrication security attack is an attack on authenticity

[✓ a) True]

b) False

Correct Answer: a

Detailed Solution: Fabrication security attack is an attack on authenticity.



QUESTION 1:

Modification threat on cloud security is an example of:

[✓ A. Deception]

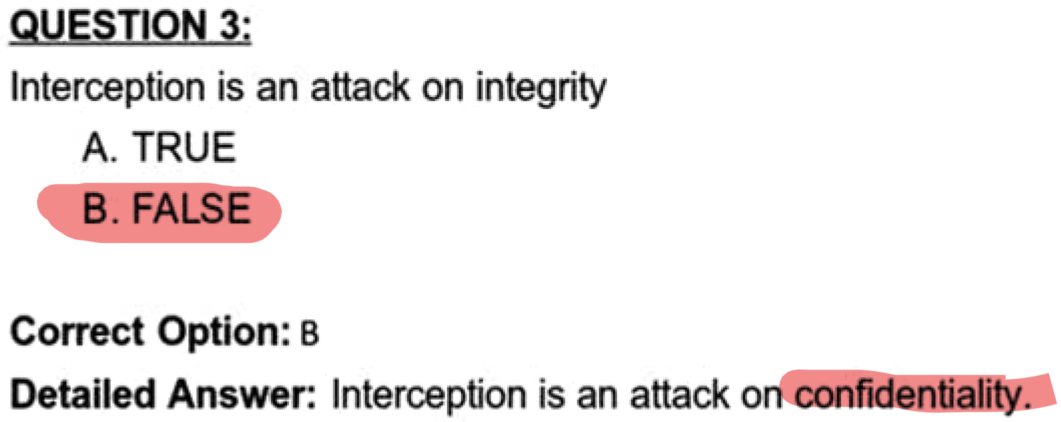
B. Disclosure

[✓ C. Disruption]

[✓ D. Usurpation]

Correct Option: A, C, D

Detailed Answer: Modification results in deception, disruption, and usurpation.



QUESTION 3:

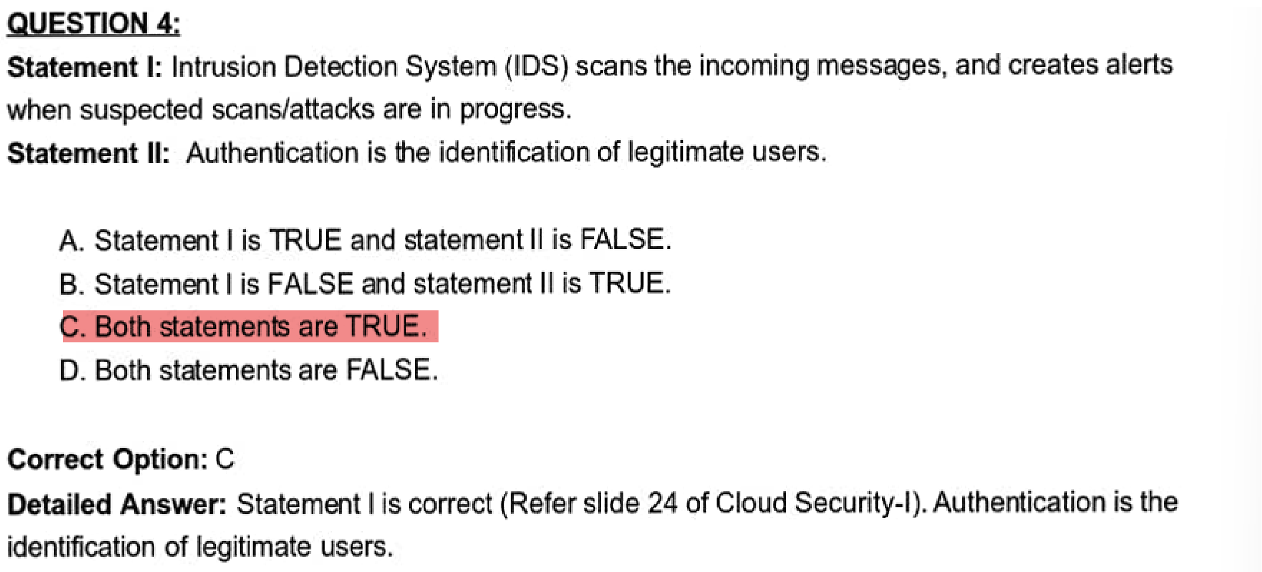
Interception is an attack on integrity

A. TRUE

[✓ B. FALSE]

Correct Option: B

Detailed Answer: Interception is an attack on confidentiality.



QUESTION 4:

Statement I: Intrusion Detection System (IDS) scans the incoming messages, and creates alerts when suspected scans/attacks are in progress.

Statement II: Authentication is the identification of legitimate users.

A. Statement I is TRUE and statement II is FALSE.

B. Statement I is FALSE and statement II is TRUE.

[✓ C. Both statements are TRUE.]

D. Both statements are FALSE.

Correct Option: C

Detailed Answer: Statement I is correct (Refer slide 24 of Cloud Security-I). Authentication is the identification of legitimate users.

QUESTION 7:

The correct statement(s) for necessary and sufficient conditions for the detection of inheritance conflict is/are:

A. Sufficient condition: current entry role and at least one exit role forms conflicting pair

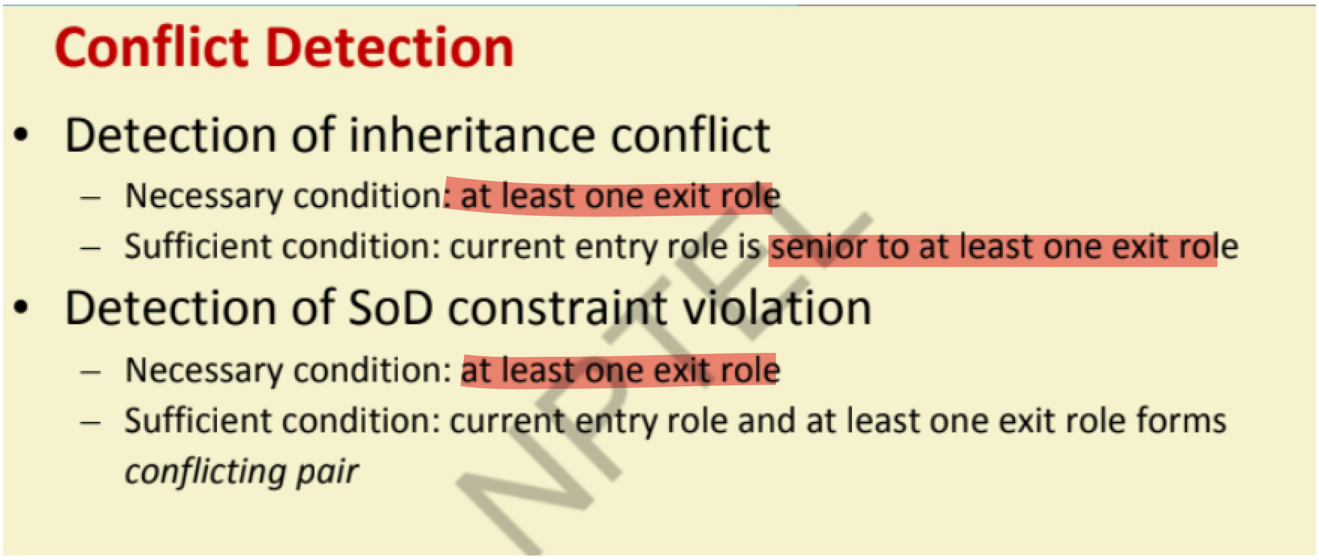
B. Sufficient condition: current entry role is senior to at least one exit role

C. Necessary condition: current entry role is senior to at least one exit role

D. Necessary condition: at least one exit role

Correct Option: B, D

Detailed Answer: Refer necessary and sufficient conditions for the detection of inheritance conflict Page-26 of Cloud Security-IV



Conflict Detection

- Detection of inheritance conflict
  - Necessary condition: at least one exit role
  - Sufficient condition: current entry role is senior to at least one exit role
- Detection of SoD constraint violation
  - Necessary condition: at least one exit role
  - Sufficient condition: current entry role and at least one exit role forms *conflicting pair*