Exam information

University of Oslo - Faculty of Mathematics and Natural Sciences

Digital exam in INF3510 Information Security (Spring 2018)

Date and time: **1 June 2018, 09:00h - 13:00h**

Permitted materials: **Language dictionary**

Please regard the following directions:

- The exam contains 44 questions with a total of 100 points (= 100 %).
- Each question states explicitly the marking scheme.
- For questions of type "matching" (i.e. a matrix) the following applies:
  - Negative points are given for incorrect rows.
  - The overall score for the total question is always at least 0 points (even if the sum over all rows is negative).
  - There is the possibility of selecting no option inside a row ("no answer"), which gives 0 points.
  - **Attention: Once you have selected any option in a row, it is NOT possible to remove all choices and go back to "no answer".**
- The questions are grouped under 10 parts that correspond approximately to 10 of the lectures in this course.
- Be concise. When answering a question, it is often sufficient to write a single expression or sentence to describe each concept that the question asks for.
- Answers can be written in English or in Norwegian.

Part 1: General Security

1 ISO27000

Write the definition (approximately) of *information security* according to ISO27000.
Points: max 2 total score
Fill in your answer here

Maximum marks: 2

2 Availability I

Write the definition (approximately) of *availability* according to ISO27000.
Points: max 1

Fill in your answer here

Maximum marks: 1

3 Availability II

Which is the most relevant *threat* against availability?
Points: 1 for correct answer, 0 for wrong or no answer
Select one alternative:

- SQL injection
- DDoS attack
- Zero-day exploit
- Cryptanalysis
- Phishing email

Maximum marks: 1

4 Authentication

Select the two (2) *most general* categories of authentication.
Points: 1 for each correct, 0 for each wrong, 0 for no answer, max 2 total score
Select two alternatives:

- Entity authentication
- Knowledge-based authentication
- Token-based authentication
- Data authentication
- Server authentication
- User authentication

Maximum marks: 2

5 Authorization

Explain the concept of *authorization* in a way consistent with the definition of confidentiality.
Points: max 1
Fill in your answer here

Maximum marks: 1

6 Data Origin

Indicate whether each characteristic in the left column is relevant for *non-repudiation* or *authentication* **of data origin**. Some characteristics are irrelevant, in that case select *'irrelevant'*.

Points: 0.5 for each correct relevance, -0.5 for each wrong, 0 for no marking in a row, max 3

Select the correct relevance:

	Non-repudiation	Authentication	Irrelevant
Implemented with digital signature	○	○	○
Implemented with MAC	○	○	○
Proof to both recipient and to any 3rd party	○	○	○
Proof only to recipient	○	○	○
Always multi-factor	○	○	○
Always based on biometrics	○	○	○

Maximum marks: 3

i Part 2: Cryptography

7 Hash Functions I

Select the properties of (good) hash functions.

Points: 1 for each correct, 0 for each wrong, 0 for now answer, max 2 total score

Select one or more alternatives:

- ☐ Bijective
- ☐ Assymetric
- ☐ Confidential
- ☐ One way
- ☐ Collision resistance

Maximum marks: 2

8 Hash Functions II

Name two (2) common applications of cryptographic hash functions.

Points: max 2

Fill in your answer here

Maximum marks: 2

9 MAC

What is the purpose of sending a message with a MAC?

Points: 1 for correct answer, 0 for wrong answer

Select one alternative:

- Any third party can authenticate the message origin.
- The recipient can authenticate the message origin.
- It protects the message confidentiality.
- It provides non-repudiation of message origin.

Maximum marks: 1

10 Symmetric Encryption

Specify the possible *key sizes* (in bits) of the AES encryption algorithm.

Points: 1 for each correct, 0 for each wrong, max 2 total score

Smallest block size:

Largest block size:

Maximum marks: 2

11 Asymmetric Encryption

Alice wants to send a message to Bob, encrypted with RSA. Which key does she use for the encryption process?

Points: 1 for correct answer, 0 for wrong answer

Select an alternative:

- Alice's private key
- Bob's private key
- Alice's public key
- Bob's public key

Maximum marks: 1

12 Quantum Computing

What will be the influence of quatum computing on current crypto systems?

Points: 1 for each correct, 0 for each wrong, max 2 total score

Select one or more alternatives:

- Symmetric crypto algorithms (e.g. AES) will be completely broken.
- There will be no effect.
- Symmetric crypto algorithms (e.g. AES) will need larger keys.
- Asymmetric crypto algorithms (e.g. RSA) will need larger keys.
- Asymmetric crypto algorithms (e.g. RSA) will be completely broken.
- Symmetric crypto algorithms (e.g. AES) will need shorter keys.

Maximum marks: 2

Part 3: Key Management

13 Key distribution

Select for each key type the correct statement that applys for **key distribution** of the specific key type.

Points: 1 for each correct, -1 for wrong, 0 for no answer, max 3 total score

Select the correct statement.

	Confidentiality required	Keys are not distributed	None of the other statements	Authenticity required
Asymmetric public keys	○	○	○	○
Asymmetric private keys	○	○	○	○
Symmetric keys	○	○	○	○

Maximum marks: 3

14 Certificates

Please mark the three (3) most relevant elements inside a X.509 certificate.

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 3 total score

Select one or more alternatives:

- Public key of the issuer
- Key exchange algorithm
- Signature created by the issuer
- Signature created by the subject
- IP Address of the issuer
- Public key of the subject
- Common name of the subject

Maximum marks: 3

15 **PKI**

Please mark the statements on **certificates** and **browser PKIs** (Public Key Infrastructure) which are true.
Points: 1 for each correct, 0 for wrong, 0 for no selection, max 2
Select one or more alternatives:

- Certificates ensure authentic exchange of private keys.
- Certificate Transparency allows automatic issuing of certificates.
- The trust model is based not on one, but on many root CAs.
- A CA verifies the ownership of a domain before signing the certificate.
- For an extended validation certificate (EV), the requester must proof the honest intention of the Web site.
- Certificates allow the user to detect phishing Web sites.

Maximum marks: 2

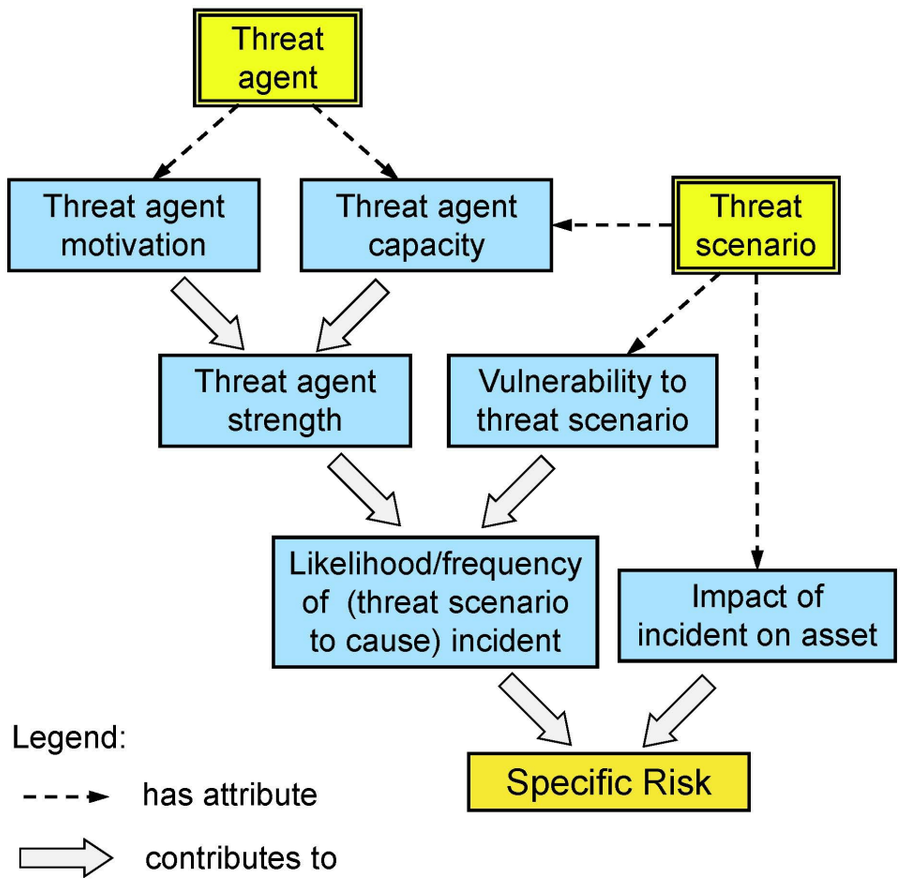
16 **Certificate Revocation**

Please name two (2) common methods for **certificate revocation**.
Points: max 2
Fill in your answer here

Maximum marks: 2

i **Part 4: Risk Management**

17 **Practical Risk Model**



Select two elements from the diagram that must be specified in a typical practical method for qualitative assessment of risks.

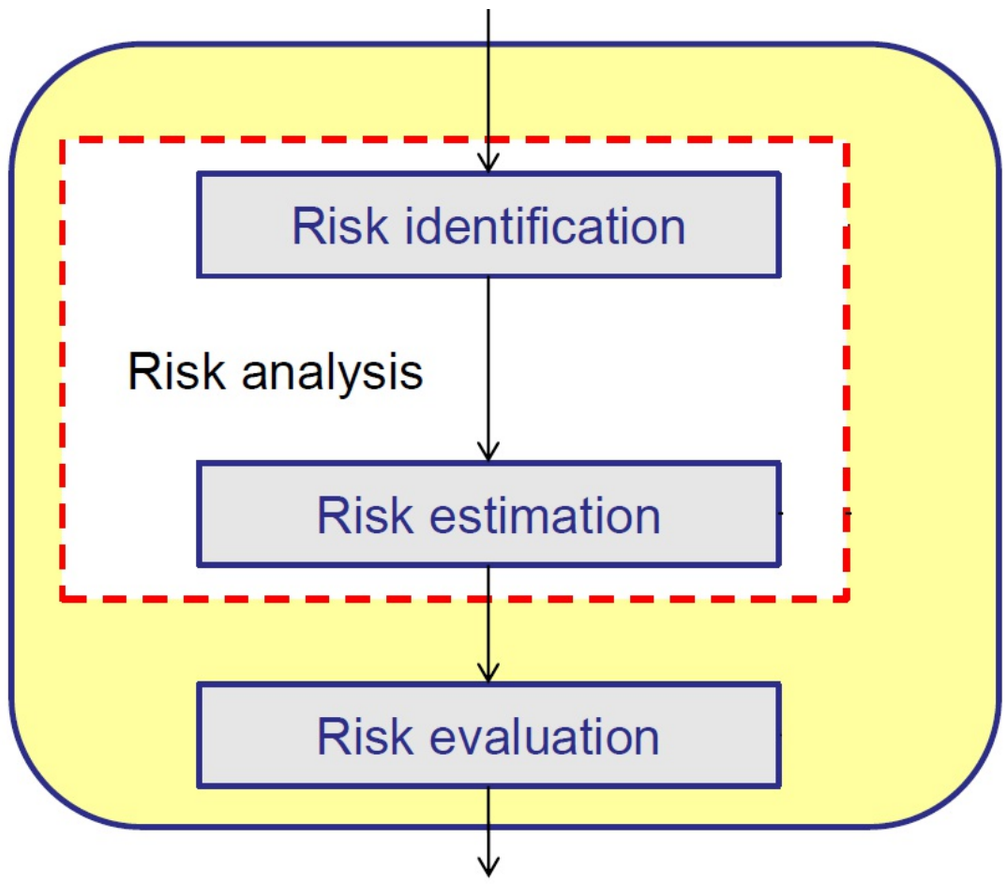
Points: 1 for each correct selection, 0 for each wrong, 0 for no selection, max 2 total score

Select two alternatives:

- Threat agent motivation
- Threat agent strength
- Likelihood of incident
- Impact on assets
- Vulnerability to threat scenario
- Threat agent capacity

Maximum marks: 2

18 Risk Accessment



Risk Identification and Risk Estimation are different steps as part of risk assessment in the risk management

process.

Mention two (2) elements of *Risk Identification* and two (2) elements of *Risk Estimation*.

Points: 1 for each correct element, max 4 total score

Risk Identification

Risk Estimation

Maximum marks: 4

19 Threat modelling

Select two (2) relevant approaches for identifying/modelling threat scenarios.

Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score

Select two alternatives:

- Vulnerability-centric threat modelling
- Asset-centric threat modelling
- Impact-centric threat modelling
- Attacker-centric threat modelling

Maximum marks: 2

20 Risk Levels

Please mention for qualitative and quantitative risk analysis one example each.

Points: 1 for each correct answer, max 2 total score

Qualitative

Quantitative

Maximum marks: 2

Part 5: Computer Security

21 Protection Rings

Assign the protection rings to the modes.

Points: 0.5 for each correct, -0.5 for wrong, 0 for no answer, max 3 total score

Please match the values:

	Kernel Mode	User Mode	Hypervisor mode	Not used (anymore)	Does not exist
-1	○	○	○	○	○
0	○	○	○	○	○
1	○	○	○	○	○
2	○	○	○	○	○
3	○	○	○	○	○
4	○	○	○	○	○

Maximum marks: 3

22 Virtualization

Select the statements on platform virtualization which are true.

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score

Select one or more alternatives:

- A guest OS can access another guest OS, which is located on the same host system.
- Platform virtualization helps in malware protection.
- The hypervisor offers virtual hardware interfaces to the VMs.
- The hypervisor is always running on top of the host OS.
- Guest VMs on the same host system must have the same OS.
- Platform virtualization increases the energy demand.

Maximum marks: 2

23 Trusted Computing

Explain (shortly!) the motivation/idea of trusted computing.

Points: max 2

Fill in your answer here

Maximum marks: 2

24 TPM

TPM (Trusted Platform Module) is a hardware chip which supports three (3) main security services on computing platforms. List these three main *TPM-supported services*:

Points: max 3 total score

Fill in your answer here

Maximum marks: 3

Part 6: User Authentication

25 Authentication Factors

Name the three (3) general credential categories (called *authentication factors*)

Points: 0.5 for each correct answer, 0 for wrong, 0 for no answer

Give an example for an existing wide-spread 2-factor authentication system.

Points: 0.5 for correct answer, 0 for wrong, 0 for no answer

Maximum marks: 2

26 Password Storage

Select the relevant *security method* for implementing each requirement in password databases.

Points: 0.5 for each correct, -0.5 for wrong, 0 for no answer, max 2 total score

Select the relevant security method:

	Access Control	Hashing	Complex password	Salting
Only authorized enties can read the password database	○	○	○	○
Attackers can not crack a salted and hashed password in the database	○	○	○	○
Passwords are not readable in the database	○	○	○	○
Pre-computed hash tables can not be used to crack passwords	○	○	○	○

Maximum marks: 2

27 Biometrics

Name one (1) advantage and two (2) disadvantages/problems/challenges of *biometric authentication*.
Points: 1 for each correct answer, 0 for wrong answer, 0 for no answer, max 3 total score.

Advantage

Disadvantages/Problems/Challenges

Maximum marks: 3

28 Authentication Tokens

Mention and briefly describe the two (2) types of *synchronised authentication tokens*.
Points: 1 for each correct, 0 for no answer, 0 for wrong answer, max 2 total score

Fill in your answer here

Maximum marks: 2

29 Authentication Assurance Level

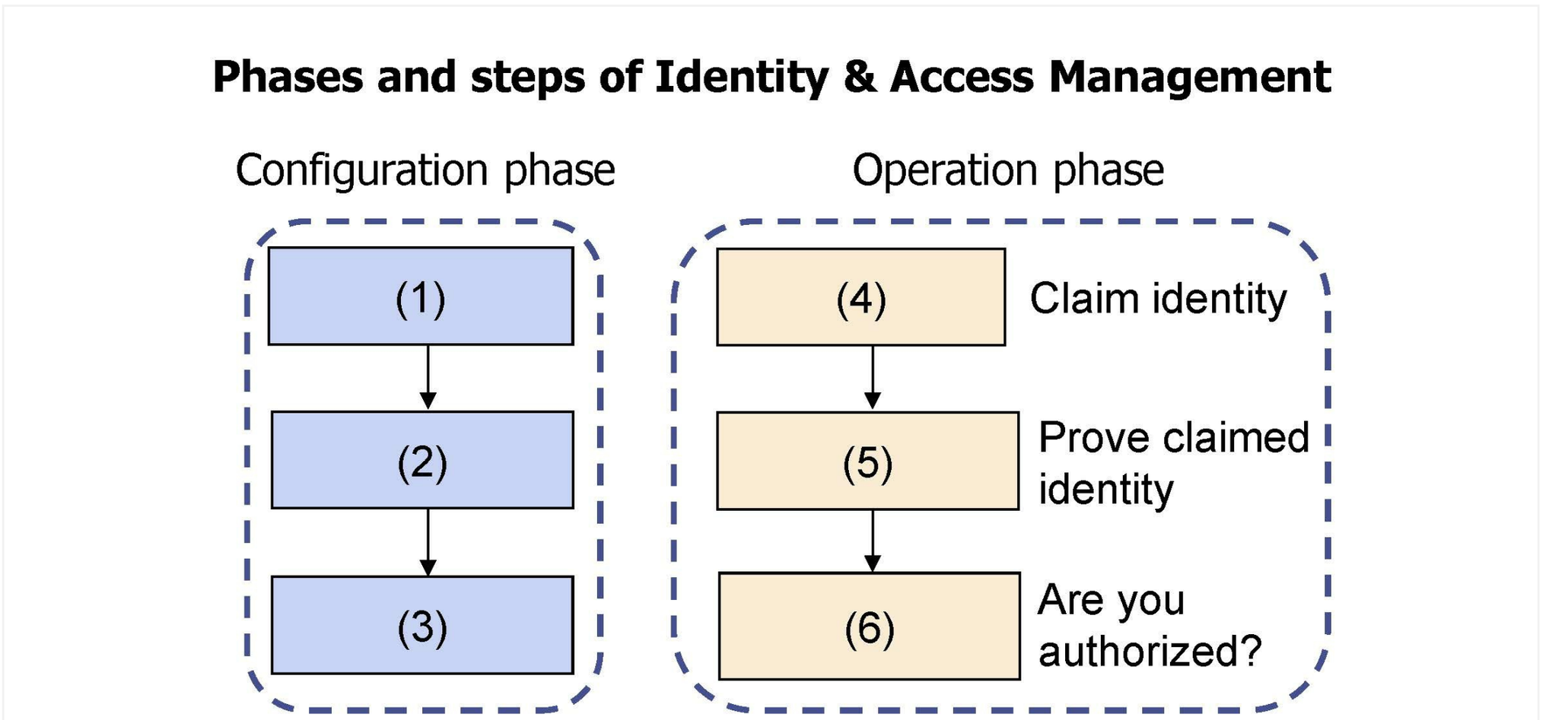
How many AALs (Authentication Assurance Levels) do the European eIDAS framework specify ? [ ] .

Points: 1 for correct, 0 for wrong, 0 for no answer

Maximum marks: 1

Part 7: Identity & Access Management

30 Phases in Identity & Access Management



The diagram shows that the configuration phase and the operation phase of IAM (Identity & Access Management) consists of steps which represent specific activities. Match each activity in the left column with the corresponding step in the diagram.

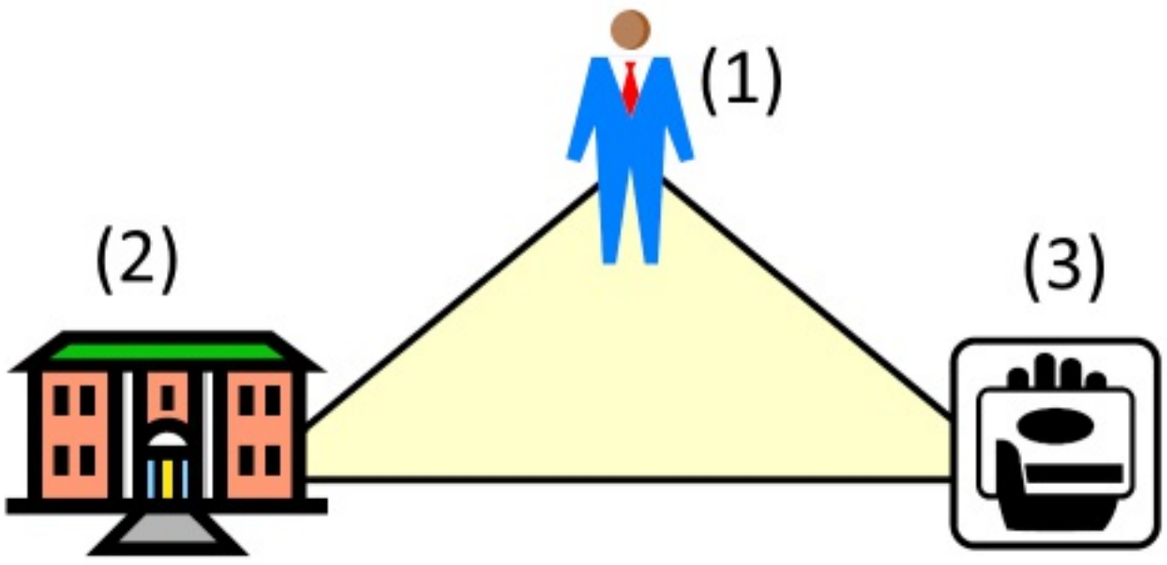
Points: 0.5 for each correct, -0.5 for each wrong, 0 for no selection, max 3

Match activity with step number:

	1	2	3	4	5	6
Access Control	○	○	○	○	○	○
Authentication	○	○	○	○	○	○
Authorization	○	○	○	○	○	○
Self Identification	○	○	○	○	○	○
Provisioning	○	○	○	○	○	○
Registration	○	○	○	○	○	○

Maximum marks: 3

31 Federation I



Name the three components in a standard *federation* environment.

Points: 1 for each correct answer, 0 for wrong, 0 for no answer, max 3 total score

(1)

(2)

(3)

Maximum marks: 3

32 Federation II

Select the *federation type* of the eduroam system.

Points: 1 for correct, 0 for wrong, 0 for unanswered

Select an alternative:

- Distributed Identity + Distributed Authentication
- Centralized Identity + Distributed Authentication
- Distributed Identity + Centralized Authentication
- Centralized Identity + Centralized Authentication

Maximum marks: 1

33 Access Control

Select the correct statements on *access control* (DAC = Discretionary Access Control, MAC = Mandatory Access Control, RBAC = Role-Based Access Control, ACL = Access Control List)

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 3 total score

Select one or more alternatives:

- RBAC can be combined with DAC.
- DAC is used in Linux systems.
- MAC is typically implemented with ACLs
- An ACL maps a user to role.
- In MAC the user defines the access to the resource he has created.
- In RBAC, users can own multiple roles.

Maximum marks: 3

Part 8: Communication Security

34 Security Protocols

Specifiy the respective OSI layers TLS and IPSec are operationg on.
Points: 1 for each correct, 0 for wrong, 0 for no answer.

TLS: , IPSec:

Maximum marks: 2

35 TLS I

Select for the following statements if they are true or false.
Points: 0.5 for each correct, -0.5 for reach wrong, 0 for no answer, max 4 total score

Please match the values:

	false	true
The session key is created during the TLS handshake from 3 random numbers.	○	○
TLS ensures integrity of transferred data.	○	○
If activated, TLS secures all TCP connections originated from that computer.	○	○
For exchange of session keys, RSA is more secure than DH.	○	○
Client and server must authenticate inside a TLS connection.	○	○
The algorithms used inside a session are negotiated between client and server.	○	○
HTTP and HTTPS can be offered on the same TCP port.	○	○
The subject of the server certificate must be equal to the server's host name entered in the browser.	○	○

Maximum marks: 4

36 TLS II

Name two (2) weaknesses/attacks for TLS.

Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score

Fill in your answer here

Maximum marks: 2

37 TOR

Explain the metaphor "onion" in the TOR system.

Points: max 2 total score

Fill in your answer here

Maximum marks: 2

Part 9: Network Perimeter Security

38 Firewall

Select the statements on firewalls which are true:
Points: 1 for each correct, 0 for wrong, 0 for no answer, max 2 total score
Select one or more alternatives:

- The Linux iptables is an implementation of an application layer proxy.
- A network firewall is named like this, because it completely separates two networks.
- Stateful packet filters can correlate a DNS response to a prior DNS request.
- A application layer proxy can handle all protocols on top of TCP.
- In proxy mode, the client makes a TCP connection to the firewall and the firewall creates a second TCP connection to the server.
- A packet filter operates on network layer 3 and 2.

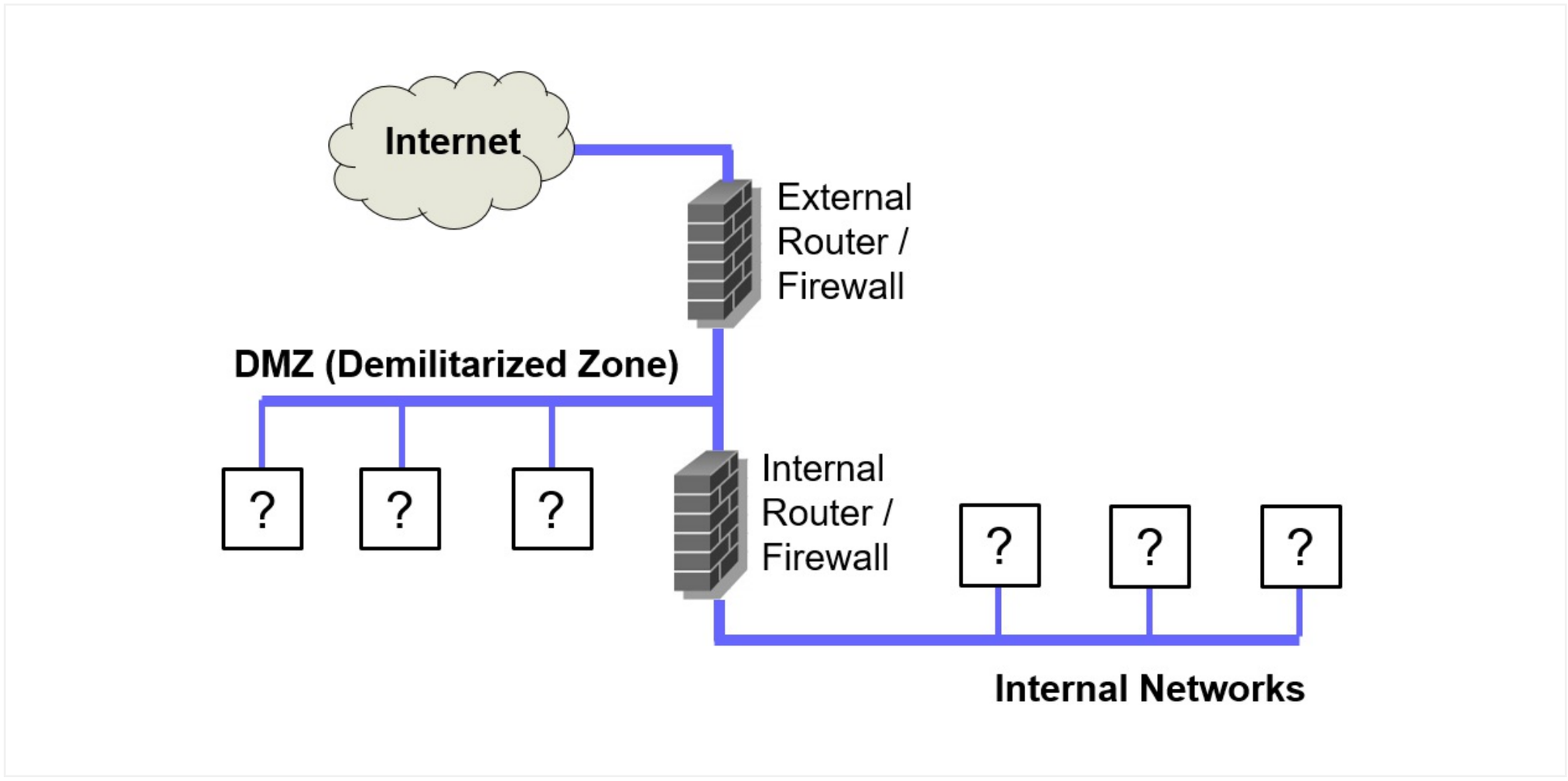
Maximum marks: 2

39 TLS Inspection

Briefly explain how a user can know whether the TLS-encrypted traffic from a workstation in a company to a remote server on the Internet is being inspected in the company gateway firewall.
Points: max 2 total score
Fill in your answer here

Maximum marks: 2

40 DMZ



In the case of two firewalls with a so-called DMZ (Demilitarized Zone) between them, servers/systems can be connected to either the DMZ or to internal networks. Select the typical location for connecting the servers/systems in the left column below.

Points: 0.5 for each correct, -0.5 for wrong, 0 for unanswered, max 3 total score

Select correct placement of each type of system:

	DMZ	Internal Networks
Database Server	○	○
DNS Server	○	○
Email server	○	○
Production Server	○	○
Web Server	○	○
Workstation	○	○

Maximum marks: 3

41 IDS

The two main techniques used in IDS (Intrusion Detection Systems) are Signature-Based Detection and Anomaly-Based Detection respectively. Select the *relevant IDS technique* for each property in the left column below.

Points: 0.5 for each correct, -0.5 for wrong, 0 for unanswered, max 3 total score

Select the relevant IDS technique for each property:

	Signature Detection	Anomaly Detection
Based on known attacks	○	○
Can detect unknown attacks	○	○
Can only detect known attacks	○	○
Generates relatively few false intrusion alarms	○	○
Based on learning normal behaviour	○	○
Generates relatively many false intrusion alarms	○	○

Maximum marks: 3

Part 10: Application Security

42 Malware

Select the relevant type of malware according to each description in the left colum below.

Points: 1 for each correct, -1 for wrong, 0 for no answer, max 4 total score

Select the relevant type of malware:

	Trojan	Exploit	Worm	Virus
A self-replicating independent malicious program	○	○	○	○
Self-replicating malicious code which is injected into other programs	○	○	○	○
Malicious software or data that exploits a software/hardware vulnerability in systems	○	○	○	○
A user-installed program with hidden malicious functionality	○	○	○	○

Maximum marks: 4

43 OWASP

Mention the meaning of the acronym *OWASP*, and brielfy describe what the *'OWASP Top 10'* is.

Points: max 2 total score)

Fill in your answer here

Maximum marks: 2

44 SQL Injection

Assume a Web login, where the user can enter an email address and a password. The entered parameters (<*email*> and <*passwd*>) are forwarded to the following SQL statement inside the Web application:

SELECT userid FROM user WHERE email = '<*email*>' AND passwd = *'<passwd*>';

If the SQL result is not empty, the user is authenticated.

An attacker enters as password:

x' or '1' = '1

What will happen?

Points: max 2

Fill in your answer here

What countermeasures can be applied to fix the previous problem?

Points: max 2

Fill in your answer here

Maximum marks: 4