Exam information

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

University of Oslo - Faculty of Mathematics and Natural Sciences

Digital exam in IN2120 "Informasjonssikkerhet" (Autumn 2019)

Date and time: **11 December 2019, 09:00h - 13:00h**

Permitted materials: ***Translation of security terms***

Please regard the following directions:

- The exam contains 43 questions with a total of 100 points (= 100 %).
- The questions are grouped under 10 parts that correspond approximately to 10 of the lectures in this course.
- Each question states explicitly the marking scheme. **There can be negative points for incorrect answers/selections.** However, the overall score for the total question is always at least 0 points (even if the sum over all answers is negative).
- 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.
- In the navigation bar on the bottom of the screen, blue bars indicate completed questions/parts.
- Answers can be written in English or in Norwegian.

Part 1: General Security

1.1 Information Security

Write the names (not the abbreviations) of the three (3) properties of **information security** according to the standard ISO 27000. Name one (1) additional property of information security (also according to the standard).

Points: max 2 total score

Fill in your answer here

Maximum marks: 2

1.2 Confidentiality

Write the definition (approximately) of **confidentiality** according to ISO 27000 and give an example for a typical security control to ensure this property.

Points: max 2

Fill in your answer here

Maximum marks: 2

1.3 Availability

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

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

What is the most relevant **security control for ensuring availability**?
Points: 1 for correct, 0 for wrong, 0 for no selection
Select one alternative

- Blockchain
- User authentication
- Awareness training
- Encryption
- Load balancing

Maximum marks: 2

1.4 Authentication

Please mark in every row if it describes an example or application of **data authentication** or **entity authentication**.
Points: 0.5 for each correct, -0.5 for wrong, 0 for no selection

Please match the values:

	entity authentication	data authentication
The integrity of a contract is protected by a digital signature.	○	○
User logs in using username and password.	○	○
TLS server authenticates using a certificate.	○	○
TLS record protocol uses HMAC for protecting the payload.	○	○

Maximum marks: 2

1.5 GDPR

Mark the statements that are true for the EU **GDPR regulation**.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total
Select one or more alternatives:

- ☐ The GDPR requires security controls for protecting business secrets.
- ☐ The GDPR forbids unauthorized processing of personal identifying information.
- ☐ The GDPR applies only to EU citizens.
- ☐ The GDPR gives users the right to request all information about them stored by a company/organization.

Maximum marks: 2

i Part 2: Cryptography

2.1 Symmetric Encryption

Mark the statements about **AES** that are true.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total
Select one or more alternatives:

- [ ] AES can be used with 2 different keys: one for encrypting and one for decrypting.
- [ ] AES can be used with different key sizes.
- [ ] AES can only encrypt messages up to the block size.
- [ ] AES can be used in different modes, which have different security properties.

Maximum marks: 2

2.2 Asymmetric Encryption

Which keys are involved in the overall process of **encrypting and decrypting using RSA**?
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score
Select one or more alternatives:

- [ ] Private key of the sender
- [ ] Symmetric key generated by the sender
- [ ] Public key of the recipient
- [ ] Symmetric key generated by the recipient
- [ ] Public key of the sender
- [ ] Private key of the recipient

Maximum marks: 2

2.3 MAC + Digital Signature

Please select for each property, if it applies to **Message Authentication Codes** (MAC), **Digital Signature** (DSig), both (MAC + DSig) or none of these two.
Points: 0.5 for each correct, -0.5 for each wrong, 0 for no selection, max 3 total score

Please match the values:

	MAC	DSig	Both	None
It ensure confidentiality of the message.	○	○	○	○
It ensures integrity of the message.	○	○	○	○
It ensures non-repudiation of the message.	○	○	○	○
Only the recipient (and the sender) can authenticate the message origin.	○	○	○	○
The implementation is based on hash functions.	○	○	○	○
Any party can authenticate the message origin.	○	○	○	○

Maximum marks: 3

2.4 Hash functions

Mark common **application(s) of cryptographic hash functions**.
Points: 1 for each correct, -1 for each wrong, 0 for no selection
Select one or more alternatives:

- [ ] Key exchange
- [ ] Asymmetric encryption
- [ ] Digital signature
- [ ] Password storage

In which of these application(s) is the **fast computation** of hash functions a disadvantage?
Points: 1 for each correct, -1 for each wrong, 0 for no selection
Select one or more alternatives

- [ ] Asymmetric encryption
- [ ] Digital signature
- [ ] Key exchange
- [ ] Password storage

Overall score: max 3 points

Maximum marks: 3

ℹ Part 3: Key Management

3.1 Crypto Period

Mark the statements on the **crypto period** of cryptographic keys that are true?
Point: 1 for each correct, -1 for each incorrect, 0 for no selection, max 2 total score.
Select one or more alternatives:

- [ ] The length of the crypto period should be adjusted according to sensitivity of the information.
- [ ] For very sensitive applications the crypto period should always be very short.
- [ ] The crypto period limits cryptanalytic attacks.
- [ ] For digital signatures, the period for signing and verifying is always the same.

Maximum marks: 2

3.2 Key distribution

Select for each key type the correct statement for **key distribution** of the specific key type.
Points: 1 for each correct, -1 for wrong, 0 for no selection, max 3 total score

Select the correct statement.

	Confidentiality during distribution required	Authenticity of key source required	Keys are usually not distributed	None of the other statements
Symmetric keys	○	○	○	○
Asymmetric public keys	○	○	○	○
Asymmetric private keys	○	○	○	○

Maximum marks: 3

3.3 Certificates + PKI

Please select the statements on **certificates** and **browser PKIs** (Public Key Infrastructure) that are true.

Points: 1 for each correct, -1 for wrong, 0 for no selection, max 3

Select one or more alternatives:

- [ ] Certificates allow the user to detect phishing Web sites.
- [ ] A CA verifies the ownership of a domain before signing a certificate request.
- [ ] For an extended-validation certificate (EV), the requester must prove the honest intention of the Web site.
- [ ] Certificates ensure authentic exchange of private keys.
- [ ] The trust model is based not on one, but on many root CAs.
- [ ] If a single CA is compromised, any company on the Internet can be spoofed.

Maximum marks: 3

3.4 Trust in PKI

A browser opens the web page "https://example.com". As part of the TLS connection the browser receives a server certificate. This certificate is signed by the CA "X". The certificate of "X" again is signed by the CA "Y". Mark the statements that are true for this scenario.

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

Select one or more alternatives:

- [ ] The CA "X" is called root CA.
- [ ] The certificate "Y" must be stored in the "certificate root store" of the browser (or the OS), in order to trust the certificate of example.com.
- [ ] The CA "X" is called intermediate CA.
- [ ] The certificate of example.com contains a reference to the CA "Y".

Maximum marks: 2

i Part 4: Network Security

4.1 TLS

Select the statements on **TLS** that are true.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 3 total score
Select one or more alternatives:

- [ ] The subject of the server certificate must be equal to the server's host name entered in the browser.
- [ ] For exchange of session keys, RSA is more secure than DH.
- [ ] TLS ensures integrity of transferred data.
- [ ] 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.

Maximum marks: 3

4.2 VPN

Assume the following situation: a client accesses a server trough either a cloud **VPN** or the **TOR** network. Mark the statements that are true (here "knowing" means "can learn the IP address when looking at the network communication").
Point: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score
Select one or more alternatives:

- [ ] When using a cloud VPN, the user's ISP knows the server.
- [ ] When using a cloud VPN, the VPN provider knows the client.
- [ ] When using TOR, the entry-node does not know the exit-node.
- [ ] When using TOR, the entry-node knows the server.

Maximum marks: 2

4.3 Firewall

Select the statements on **firewalls** that are true.
Points: 1 for each correct, -1 for wrong, 0 for no selection, max 2 total score
Select one or more alternatives:

- [ ] Stateful packet filters can correlate a DNS response to a prior DNS request.
- [ ] A application level gateway can always handle all protocols on top of TCP.
- [ ] A packet filter operates on the OSI layers 3 (network) and 4 (transport).
- [ ] A network firewall blocks all traffic between two networks.

Maximum marks: 2

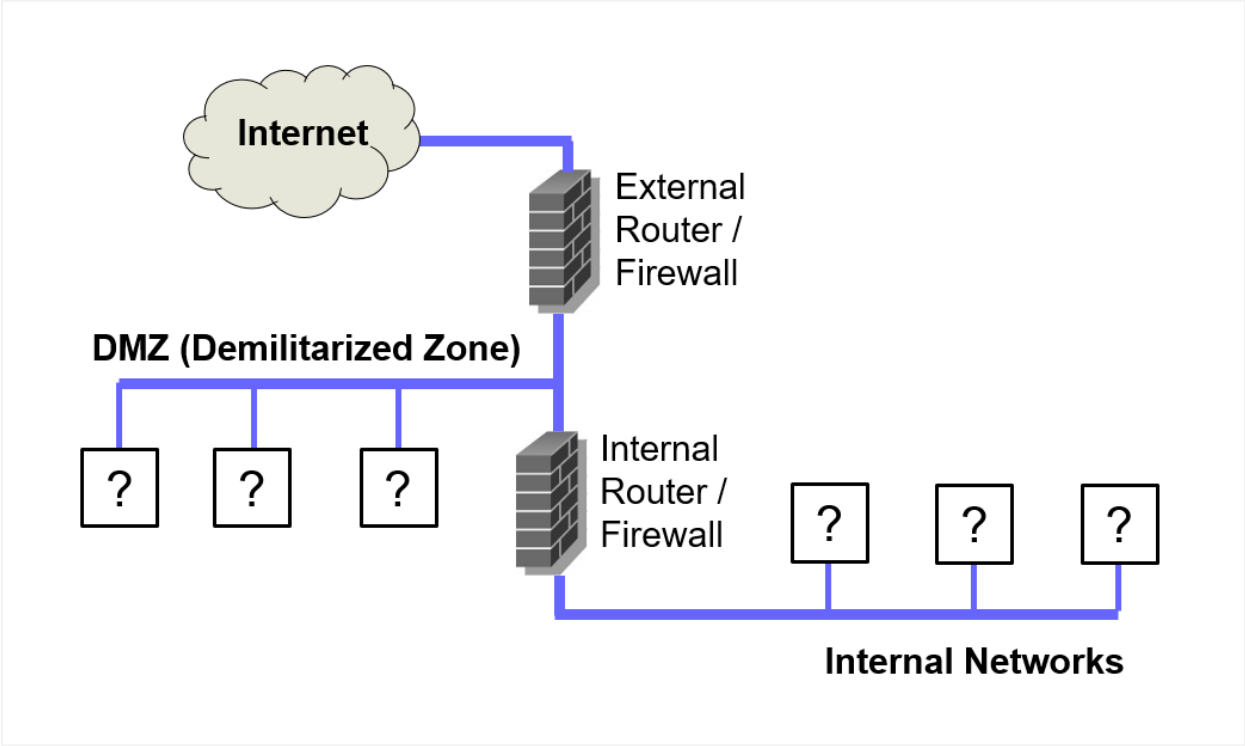
4.4 IDS

The two main techniques used in **Intrusion Detection Systems** (IDS) 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 no selection
Select the relevant IDS technique for each property:

	Signature Detection	Anomaly Detection
Can only detect known attacks	○	○
Based on learning normal behaviour	○	○

Maximum marks: 1

4.5 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 each wrong, 0 for no selection, max 2 total score

Select correct placement of each type of system:

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

Maximum marks: 2

ℹ Part 5: Incident Response

5.1 Incident Response

Mark the statements on **incident response** that are true.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total
Select one or more alternatives:

- [ ] Incident response is a reaction to unexpected events.
- [ ] Incident response shall reduce negative consequences of an incident.
- [ ] As incident response reacts on unexpected events, it can not be planned.
- [ ] Incident response is a proactive process (like SIEM or SOC).

Maximum marks: 2

5.2 Incident Response Phases I

What is typical order of **phases in incident response**?
Points: 2 for correct, 0 for wrong, 0 for no selection
Select one alternative:

- ( ) Analysis - Containment - Eradiction - Normalisation
- ( ) Containment - Normalisation - Eradiction - Analysis
- ( ) Eradiction - Analysis - Normalisation - Containment
- ( ) Normalisation - Containment - Analysis - Eradiction

Maximum marks: 2

5.3 Incident Response Phases II

Consider the incident from the workshop: "ransomware has encrypted important data from the research department and is requesting 100.000 $ in bitcoin".

Select for each measure to which **phase in incident response** it belongs.

Points: 1 for each correct, -1 for wrong, 0 for no selection, max 6 total score

Please match the values:

	Containment	Analysis	(none of these)	Eradiction	Normalisation
Unplugging infected computers from network	○	○	○	○	○
Payment of ransom	○	○	○	○	○
Erasing hard drives of infected computers	○	○	○	○	○
Collecting log files from IDS systems	○	○	○	○	○
Restoring data from backup	○	○	○	○	○
Performing backups before attack	○	○	○	○	○

Maximum marks: 6

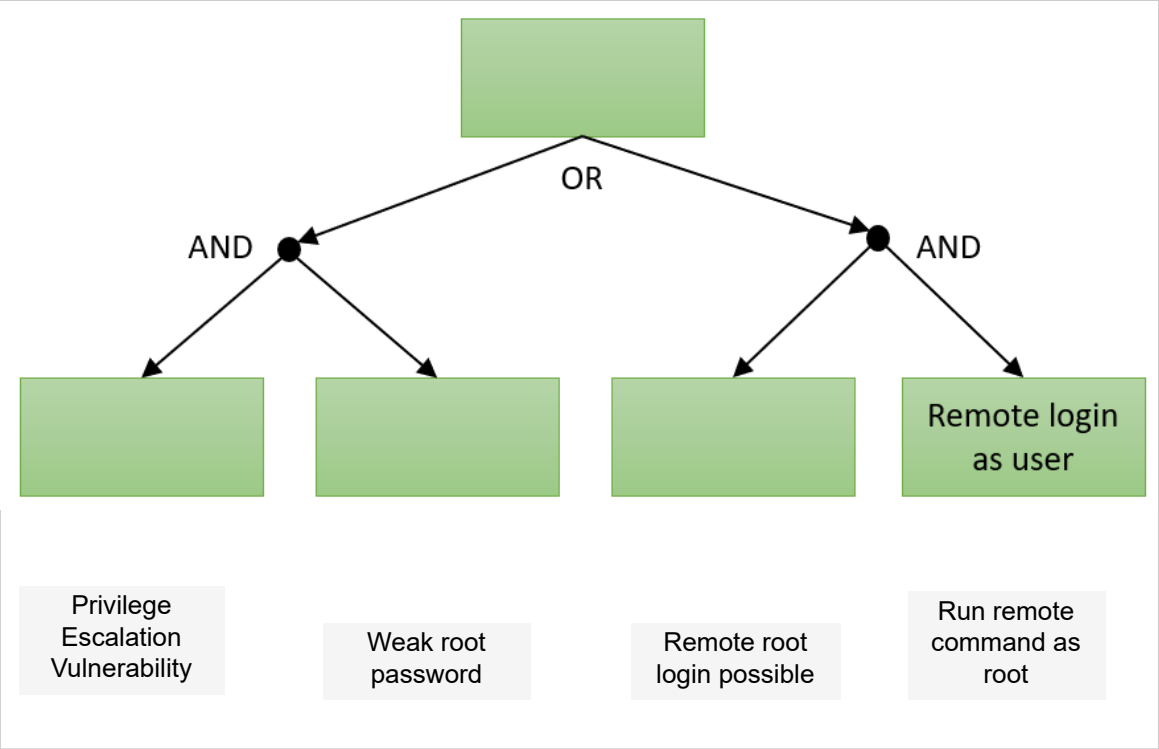
i Part 6: Risk Management

6.1 Threat Tree

Below you see a **threat tree** with one node already filled. Move the four (4) terms below the tree to right position inside the tree.

Points: 3 total score for all answers correct, 0 if any error

Move the terms to the tree nodes



Maximum marks: 3

6.2 Risk Estimation I

The following values are the result of a **risk estimation** analysis:

- Annualized Rate of Occurence: ARO = 12
- Exposure Factor: EF = 1 (100%)
- Asset Value: AV = 2000 $

How is this type of analysis called?

Point: 1 for correct, -1 for wrong answer, 0 for no selection

Quantitative	Qualitative
○	○

You have to calculate the Annualized Loss Expectancy (ALE) for the given case. What is the unit for the ALE?

Point: 1 for correct, -1 for wrong answer, 0 for no selection

- ○ %
- ○ $
- ○ (no unit, plain number)

Maximum marks: 2

6.3 Risk Estimation II

The following values are the result of a **risk estimation** analysis:

- Annualized Rate of Occurence: ARO = 12
- Exposure Factor: EF = 1 (100%)
- Asset Value: AV = 2000 $

Calculate the Annualized Loss Expectancy (ALE) (enter just the number; without any unit if there is any).

Point: 1 for correct

ALE = [ ]

Maximum marks: 1

6.4 Risk Analysis

Select for each statement whether it is true for **qualitative** or **quantitative** risk-analysis methods.

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

Please match the values:

	Quantitative	Qualitative
The risk levels are obtained with a look-up table.	○	○
The input parameters are easy to estimate.	○	○
The resulting risk levels are absolute.	○	○
The risk levels are obtained with computation.	○	○

Maximum marks: 2

6.5 Risk Identification

What is most logical order in **risk identification**? Enter the numbers 1, 2 and 3 accordingly.

Points: 2 total for all answers correct, 0 total if any error

- [ ] Identify exploitable vulnerabilities
- [ ] Identify a relevant threat
- [ ] Identify impact

Maximum marks: 2

ℹ Part 7: User Authentication

7.1 Authentication Factors

Name the three (3) general credential categories (called **authentication factors**) and give one example for each of them

Points: 0.5 for each correct factor, 0.5 for each correct example, 0 for wrong/no answer, max 3 total

Give one (1) example of a wide-spread commercial **2-factor authentication system** and name the involved factors.

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

Maximum marks: 4

7.2 Password Handling

Please answer the following questions on **password handling**.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 3 total score

Image the following situation: an attacker has stolen a password file containing hashed passwords. Which of the following methods can make **brute force attacks** on a specific password inside this file more difficult?
Select one or more alternatives:

- [ ] Using "slow" hash functions (e.g. scrypt)
- [ ] Salting
- [ ] Access control for the password file
- [ ] Complex password

Which of the following methods can be influenced by the user (i.e. the owner of the password)?
Select one or more alternatives

- [ ] Using "slow" hash functions (e.g. scrypt)
- [ ] Salting
- [ ] Complex password
- [ ] Access control for the password file

Maximum marks: 3

7.3 Biometric Authentication

Compare the two **biometric authentication** methods *face recognition* and *fingerprint scan*. For each criterion mark the method that is *better* or *more secure*.

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

Please mark the "better" / "more secure" method:

	Face	Finger
Permanence	○	○
Universality	○	○
Uniqueness	○	○
Circumvention (e.g. presentation attacks)	○	○

Maximum marks: 2

7.4 Authentication Tokens

What is the main advantage of passwords/PINs generated by an **authentication token** compared to "normal" passwords/PINs?

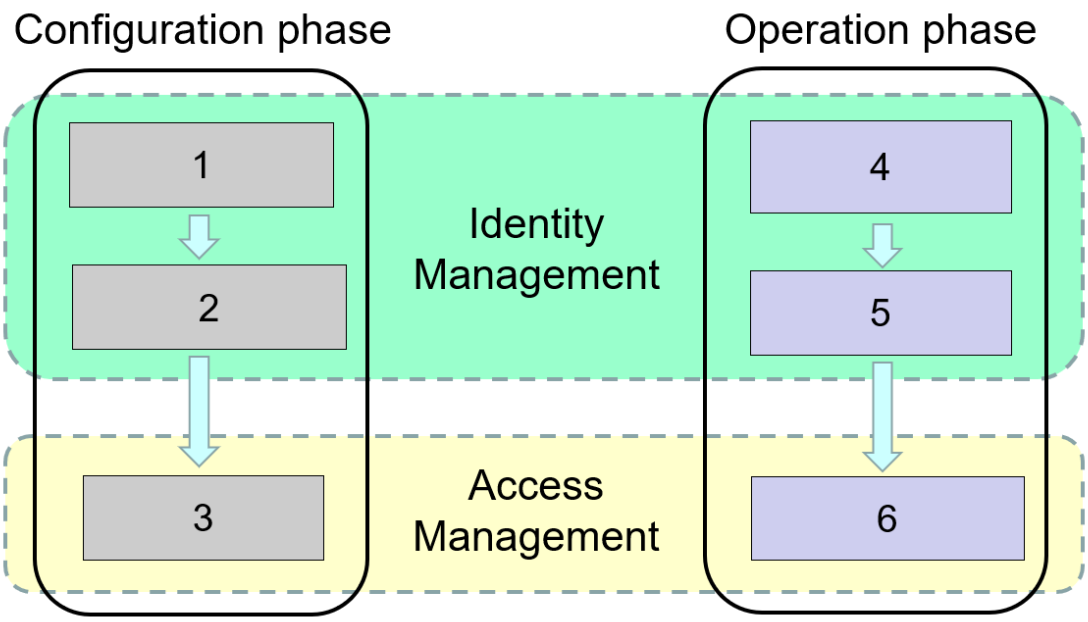
Points: max 1

Enter text here

Maximum marks: 1

ℹ Part 8: Identity & Access Management

8.1 Phases in Identity & Access Management



The diagram shows that the configuration phase and the operation phase of **Identity & Access Management** (IAM) 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	○	○	○	○	○	○
Access Authorization	○	○	○	○	○	○
Self Identification	○	○	○	○	○	○
Provisioning of credentials	○	○	○	○	○	○
Registration of identities	○	○	○	○	○	○

Maximum marks: 3

8.2 Federation I

Order the steps in a typical **federated Web authentication** scenario by entering the numbers 1 to 5.
Points: 2 total score for all correct, 0 if any error

- [ ]. User authenticates to the Identity Provider.
- [ ]. User is redirected to the Service Provider.
- [ ]. User is redirected to the Identity Provider.
- [ ]. User gets access to the resource at the Service Provider.
- [ ]. User tries to access a resource at the Service Provider.

Maximum marks: 2

8.3 Federation II

Select the **federation type** of the Norwegian "ID-porten" system.
Points: 1 for correct, 0 for wrong, 0 for no selection
Select an alternative:

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

Maximum marks: 1

8.4 Access Control I

Mark for each statement appropriate access control method.

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

Please match the values:

	ABAC	MAC	DAC	RBAC
The owner of an object can authorize access to his/her object	○	○	○	○
Is used typically in military contexts	○	○	○	○
Is the most flexible models; all other model can be implemented using this	○	○	○	○
Each user receives one or more roles	○	○	○	○

Maximum marks: 2

8.5 Access Control II

Your task is the development of an **access control system** for a new document storage system for your company. Which access control measures are reasonable?

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

Select one or more alternatives:

- ☐ DAC
- ☐ RBAC
- ☐ ABAC
- ☐ MAC

Maximum marks: 2

ℹ Part 9: Ethical Hacking

9.1 Ethical Hacking

What separates an **ethical hacker** from an illegal hacker?

Points: max 2

Fill in your answer here

Maximum marks: 2

9.2 Attack Phases

What is the typical **order of steps** when **attacking a system**? Enter a number between 1 and 4 for each step.

Points: 2 for all correct, 0 for any error

- [ ] Gain access
- [ ] Information gathering
- [ ] Scanning for weakness
- [ ] Maintain access

Maximum marks: 2

9.3 Reverse Engineering

Pair the keyword with its correct definition.

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

Please match the values:

	Instruction	Decompile	Static analysis	Disassemble	Register	Dynamic analysis
Small memory unit	○	○	○	○	○	○
A single operation by the processor	○	○	○	○	○	○
Turn executable file into high-level language	○	○	○	○	○	○
Turn machine code into assembly language	○	○	○	○	○	○
Analysing code without running program	○	○	○	○	○	○
Analysing code and behaviour by running program	○	○	○	○	○	○

Maximum marks: 3

9.4 Buffer Overflow

Select for the statements about **buffer overflow** if they are true and false.
Points: 0.5 for each correct, -0.5 for each wrong, 0 for no selection, max 3 total

	True	False
Most buffer overflows are caused by user input.	○	○
An attacker can crash a program using this exploit.	○	○
An attacker can divert the execution path using this exploit.	○	○
32-bit sytems are vulnerable to this exploit, but not 64-bit systems.	○	○
By filling an array with non-ASCII characters a stack overflow is triggered.	○	○
A stack overflow overwrites more memory locations than intended by the system.	○	○

Maximum marks: 3

ℹ Part 10: Application Security

10.1 OWASP

Select attacks/threats/vulnerabilities that are included in the **OWASP Top 10** list.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score
Select one or more alternatives:

- ☐ Trojan horse
- ☐ Injection
- ☐ Broken Authentication
- ☐ Open TCP port

Maximum marks: 2

10.2 Web Security

A Web page allows visitors to leave comments, which can be read later by other users. Which attack might be possible through this feature (if not implemented correctly)?
Points: 2 for correct, 0 for wrong, 0 for no selection
Select one alternative:

- XSS
- DDoS
- SQL Injection
- Broken Authentication

Maximum marks: 2

10.3 Cloud Security

Mark the statements regarding cloud computing security that are true.
Points: 1 for each correct, -1 for wrong, 0 for no selection, max 2 total
Select one or more alternatives:

- Office 365 is an example of Infrastructure-as-a-Service (IaaS).
- Cloud computing offers the possibility for increased availability.
- Storage of data in international data centers can be in conflict to data protection laws.
- The use of multi-tenant environments increases the security.

Maximum marks: 2

10.4 DevSecOps

Name one **technical** and one **business benefit** of DevSecOps.
Points: max 2
Fill in your answer here

Explain (shortly) the meaning of **Shift-Left** in DevSecOps.
Points: max 2
Fill in your answer here

Maximum marks: 4