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 2018)

Date and time: **11 December 2018, 14:30h - 18:30h**

Permitted materials: ***None***

Please regard the following directions:

- The exam contains 44 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 ISO27000

Write the definition (approximately) of **information security** according to ISO27000.

Points: max 2 total score

Fill in your answer here

Maximum marks: 2

1.2 Integrity

Write the definition (approximately) of **integrity** according to ISO27000.

Points: max 1

Fill in your answer here

Maximum marks: 1

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:

○ Cryptanalysis

○ DDoS attack

○ Zero-day exploit

○ SQL injection

○ Phishing email

Maximum marks: 1

1.4 Authentication

Select the two (2) **most abstract categories of authentication**.

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

Select one or more alternatives:

□ Data authentication

□ Server authentication

□ User authentication

□ Token-based authentication

□ Entity authentication

□ Knowledge-based authentication

Maximum marks: 2

1.5 Phishing

Answer the two question on **phishing**.

Points: max 3

Which "vulnerability" is mainly exploited by phishing attacks?

Propose two (2) security methods to prevent phishing attacks.

Maximum marks: 3

1.6 GDPR

What type of data protected by the **GDPR regulation**?

Points: max 1

Fill in your answer here

Maximum marks: 1

ℹ Part 2: Cryptography

2.1 Diffie-Hellman

Which security protocol is usually associated with the names "**Diffie**" and "**Hellman**"? What is the purpose of this protocol?

Points: max 1

Fill in your answer here

Maximum marks: 1

2.2 Hash Functions I

Select the properties of (good) **cryptographic hash functions**.

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

Select one or more alternatives:

□ Collision resistance

□ Bijective

□ Assymetric

□ Confidential

□ One way

Maximum marks: 2

2.3 Hash Functions II

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

Points: max 2

Fill in your answer here

Maximum marks: 2

2.4 Digital Signature

Which keys are involved in the process of generating and verifying a digital signature?

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

Select one or more alternatives:

□ Symmetric key generated by the recipient

□ Public key of the sender

□ Public key of the recipient

□ Private key of the recipient

□ Private key of the sender

□ Symmetric key generated by the sender

Maximum marks: 2

2.5 MAC + Digital Signature

Please selected 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

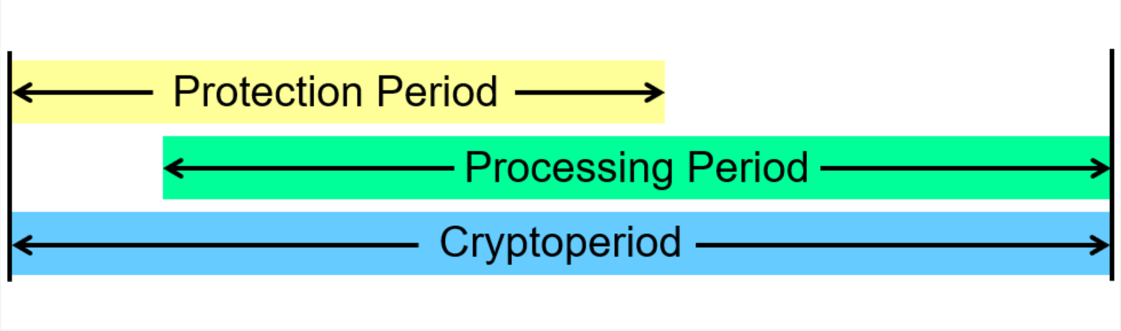
Please match the values:

	MAC	DSig	Both	None
Confidentiality	○	○	○	○
Authenticity	○	○	○	○
Non-Repudiation	○	○	○	○
Using Symmetric Crypto	○	○	○	○
Using Asymmetric Crypto	○	○	○	○
Using Hash Functions	○	○	○	○

Maximum marks: 3

Part 3: Key Management

3.1 Crypto period



Select the statements on **crypto periods** 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 total crypto period is always less than 1 year.

□ The processing period can continue after the protection period.

□ The crypto period is depended of the key length.

□ For digital signatures: signature creation is allowed in the (complete) processing period

□ For digital signatures: signature verification is allowed in the (complete) processing period.

□ The crypto period is equal to the lifetime of the associated crytographic algorithm

Maximum marks: 3

3.2 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 selecion, max 3 total score

Select the correct statement.

	Confidentiality required	Authenticity required	Keys are 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:

- □ A certificate contains the common name of the subject; for the Web: the server's host name.
- □ Certificates allow the user to detect phishing Web sites.
- □ For an extended validation certificate (EV), the requester must prove the honest intention of the Web site.
- □ A CA verifies the ownership of a domain before signing a certificate request.
- □ Certificates ensure authentic exchange of private keys.
- □ The trust model is based not on one, but on many root CAs.
- □ Certificate Transparency allows automatic issuing of certificates.

Maximum marks: 3

3.4 OCSP

What is the purpose of the **OCSP protocol**?
Points: 1 for correct, 0 for wrong, 0 for no selection
Select one alternative:

- ○ Checking if a certificate is still valid.
- ○ Requesting a certificate.
- ○ Requesting a CAA DNS entry.
- ○ Revocation of certificates.

Maximum marks: 1

ℹ Part 4: Communication Security

4.1 TLS I

Select the statements on **TLS** that are true.

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

Select one or more alternatives:

- □ If activated, TLS secures all TCP connections originated from that computer.
- □ The algorithms used inside a session are negotiated between client and server.
- □ For exchange of session keys, RSA is more secure than DH.
- □ The session key is created from random numbers, that are exchanged during the TLS handshake.
- □ 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.
- □ TLS ensures integrity of transferred data.
- □ Client and server must authenticate inside a TLS connection.

Maximum marks: 4

4.2 TLS II

Name two (2) **challenges/problems with TLS**.

Points: max 2

Fill in your answer here

Maximum marks: 2

4.3 TLS III

Which **TCP port** is reserved for "HTTP over TLS"?
Points: 1 for correct answer.

Answer: □ .

Maximum marks: 1

4.4 VPN

Let's assume the user *U* is using the Cloud VPN service *C* and is accessing a service *S* using a unencrypted TCP connection.
What type of information is **hidden from the user's ISP**?
Point: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score
Select one or more alternatives:

- □ The IP address of C.
- □ The IP address of U.
- □ The content of the connection.
- □ The IP address of S.

Maximum marks: 2

4.5 TOR

Which statement is true for TOR networks?
Points: 1 for correct, 0 for wrong, 0 for no selection

Select one alternative:

- ○ Each node in the network knows the previous and next node along a connection but no other peers.
- ○ The first node along a connection knows the start- and endpoint of that connection (i.e. client and server).
- ○ Each node in the network adds one layer of encryption.
- ○ Only connections to server that have a TOR proxy installed is possible.

Maximum marks: 1

ℹ Part 5: Computer Security

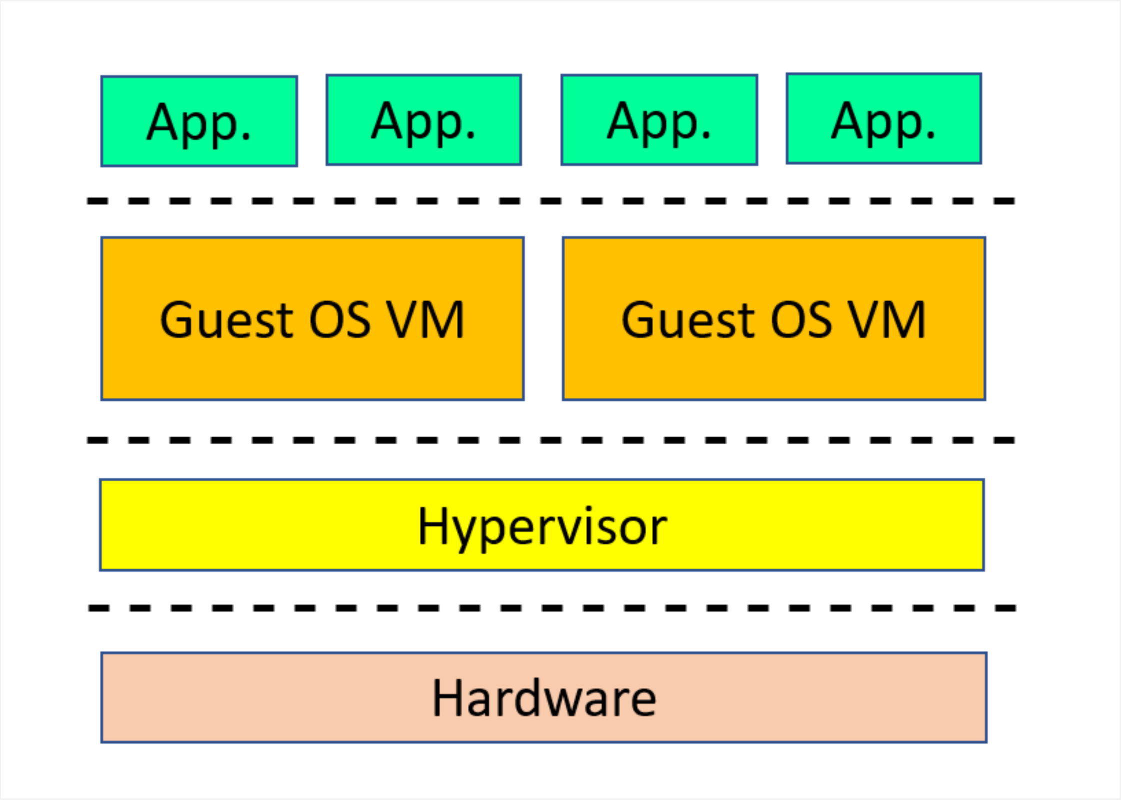
5.1 Virtualization

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

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

Maximum marks: 3

5.2 Ring Allocation



Enter the **protection ring numbers** for the "Type 1 VM Architecture" (see figure above).

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

Application: □

Guest OS VM: □

Hypervisor: □

Maximum marks: 3

5.3 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

Fill in your answer here

Which of these services is used by the Windows Bitlocker **disk encryption** application?

Points: max 1

Fill in your answer here

Maximum marks: 4

Part 6: Risk Management

6.1 Risk Assessment

What is the order of tasks in the **risk assessment** process acording to ISO 27005? Enter the numbers 1, 2 and 3 accordingly.

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

□. Risk Estimation

□. Risk Evaluation

□. Risk Identification

Maximum marks: 3

6.2 Risk Identification

Which elements are identified in the process step of **risk identification**?

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

Select one or more alternatives:

□ Assets

□ Value of assets

□ Risk mitigation strategies

□ Likelihood of incidents

□ Risk levels

□ Vulnerabilities

□ Threats

□ Existing controls

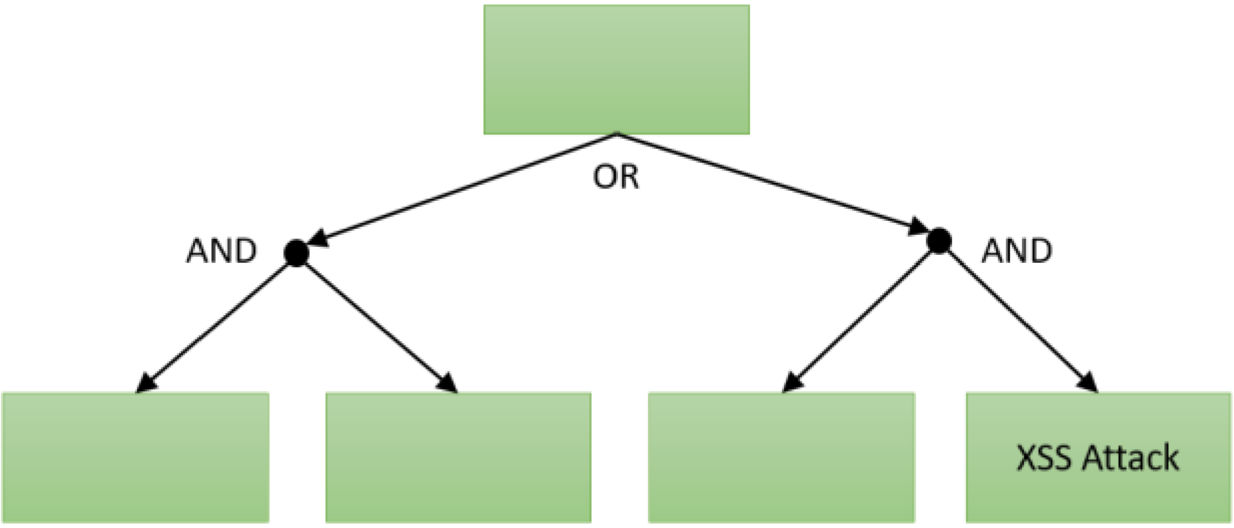
Maximum marks: 2

6.3 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: 2 total score for all answers correct, 0 if any error

Move the terms to the tree nodes



XSS Vulnerability

Eavesdropping

Unencrypted Connection

Cookie Theft

Maximum marks: 2

6.4 Risk Estimation

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

- Annualized Rate of Occurance: ARO = 10
- Asset Value: AV = 5000 $

How is this type of analysis called?
Point: 1 for correct, 0 for wrong answer

○ Relative/semi-quantitative

○ Qualitative

○ Quantitative

You have to calculate the Annualized Loss Expectancy (ALE) for the given case. What is the unit for the ALE?
Point: 1 for correct, 0 for wrong answer

○ (no unit, plain number)

○ $ / year

○ %

○ $

Calculate the ALE (enter just the number; without any unit if there is any).
Point: 1 for correct, 0 for wrong answer

ALE = □

Maximum marks: 3

ℹ Part 7: User Authentication

7.1 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 a wide-spread commercial **2-factor authentication system** and name the involved factors.

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

Maximum marks: 2

7.2 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 selection, max 2 total score

Select the relevant security method:

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

Maximum marks: 2

7.3 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

7.4 Authentication Tokens

Please select for the following statements on **authentication tokens**, if they are true or not.

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

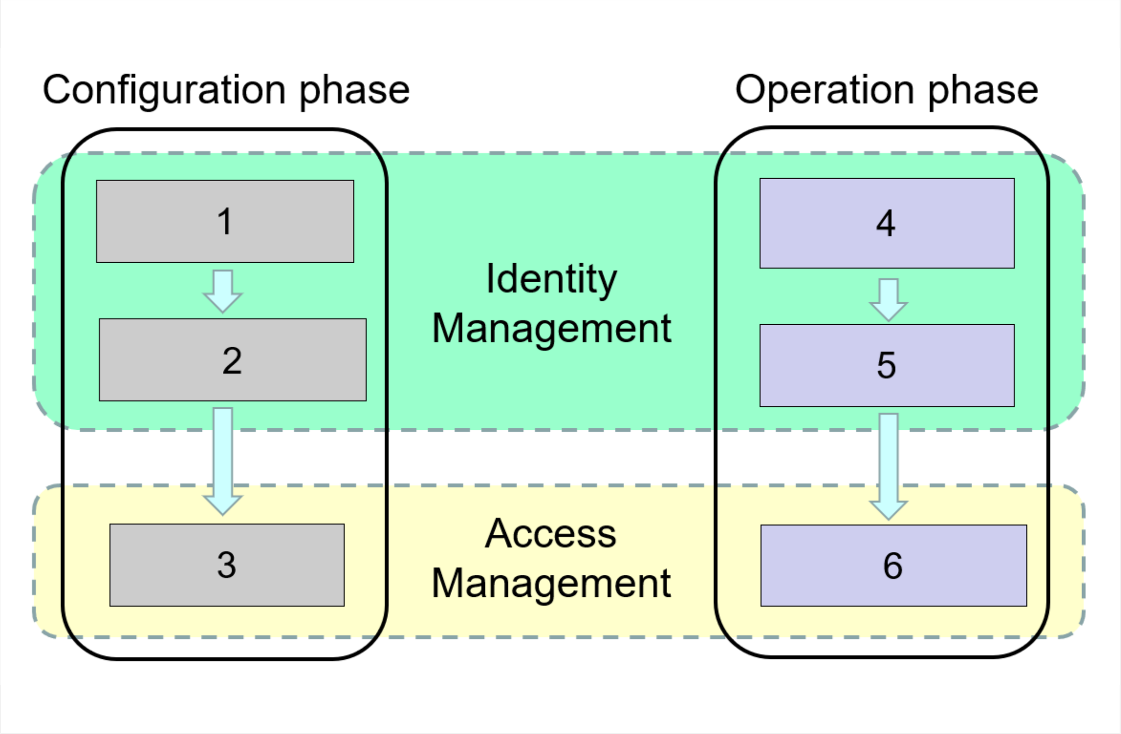
Please match the values:

	True	False
When authenticating with a "Counter-based OTP Token", the user must enter the counter value.	○	○
The response generated by a "Challenge Response Based Tokens" can be captured and used at a later time.	○	○
"Clock-based OTP Tokens" must have the same internal time like the authentication server.	○	○

Maximum marks: 3

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	○	○	○	○	○	○
Authorization	○	○	○	○	○	○
Self Identification	○	○	○	○	○	○
Provisioning	○	○	○	○	○	○
Registration	○	○	○	○	○	○

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 ressource at the Service Provider.
- □. User accesses a resource at the Service Provider.

Maximum marks: 2

8.3 Federation II

Select the **federation type** of the eduroam system.

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

Select an alternative:

○ Distributed Identity + Distributed Authentication

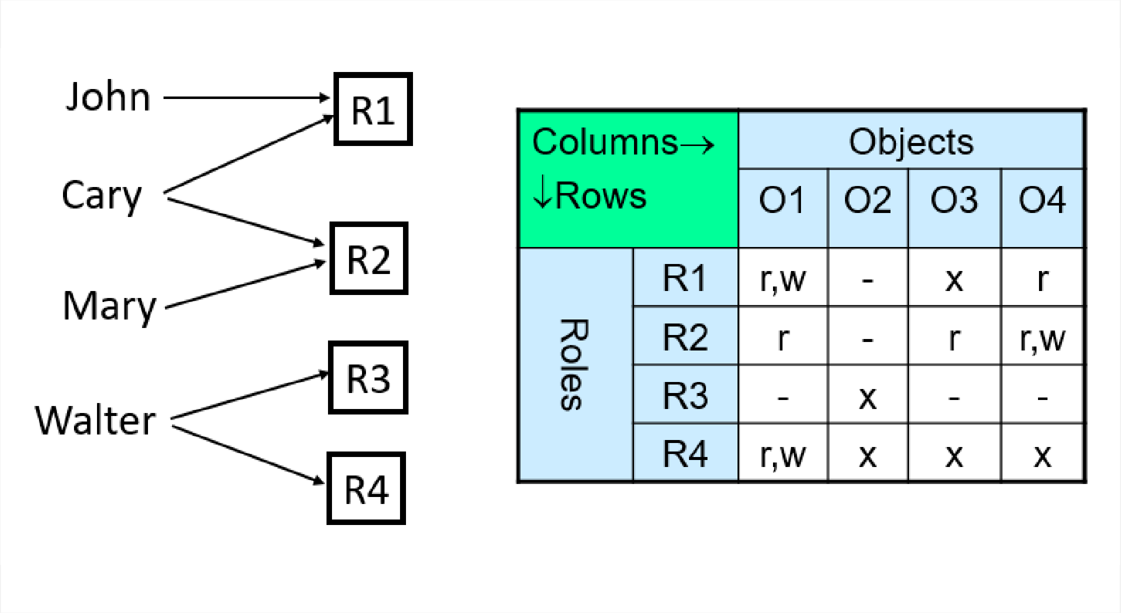
○ Centralized Identity + Centralized Authentication

○ Distributed Identity + Centralized Authentication

○ Centralized Identity + Distributed Authentication

Maximum marks: 1

8.4 Access Control



Columns→ ↓Rows		Objects			
		O1	O2	O3	O4
Roles	R1	r,w	-	x	r
	R2	r	-	r	r,w
	R3	-	x	-	-
	R4	r,w	x	x	x

Above you see an **access control policy**.
Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 4 total score

What type(s) of access control principle(s) is/are illustrated?
Select one or more alternatives:

□ Mandatory (MAC)

□ Attribute-based (ABAC)

□ Role-based (RBAC)

□ Discretionary (DAC)

To which file(s) can Cary append further data (i.e. add data at the end of file)?
Select one or more alternatives

- □ O1
- □ O2
- □ O3
- □ O4

Maximum marks: 4

ℹ Part 10: Network Perimeter Security

9.1 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:

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

Maximum marks: 2

9.2 TLS Inspection

Mark the statements on **TLS inspection** that are true.

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

Select one or more alternatives:

- □ Works only with outdated TLS versions
- □ Always creates a browser warning that, however, is ignored by most users
- □ Two TLS connections are created: Client to Proxy and Proxy to Server
- □ Requires an additional root certificate installed on clients.

Maximum marks: 2

9.3 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.

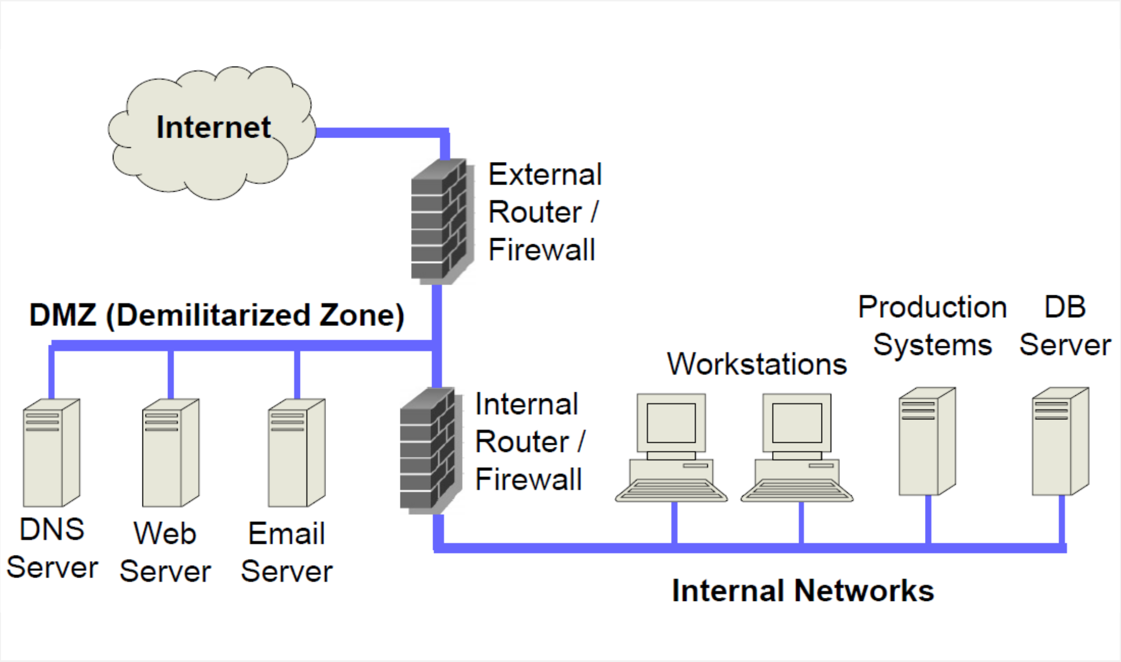
Points: 1 for each correct, -1 for wrong, 0 for no selection, max 3 total score

Select the relevant IDS technique for each property:

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

Maximum marks: 3

9.4 DMZ



Above you see a common **DMZ-based network architecture**. Asume a typical firewall configuration. Select for the following firewall rules, if they apply to the internal or the external firewall (or both or none of them).

"Incoming" means "from Internet to DMZ" or "from "DMZ to Internal"; "outgoing" the opposite direction.

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

Please match the values:

	Internal	External	Both	None
Block incoming connections to port 80 (HTTP)	○	○	○	○
Allow outgoing connections to port 80 (HTTP)	○	○	○	○
Activate stateful filtering	○	○	○	○
Allow incoming connections to port 25 (SMTP)	○	○	○	○

Maximum marks: 2

9.5 Attack detection

What is a system called that appears to the outside like a normal, valuable network ressource, but has the only pupose to **lure attackers** and analyse their behaviour?

Points: max 1 total score

Fill in your answer here

Maximum marks: 1

ℹ Part 10: Application Security

10.1 Botnet

What are the most common attacks executed by a **botnet**?

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

Select one or more alternatives:

□ DDoS

□ Sending SPAM

□ XSS

□ SQL Injection

Maximum marks: 2

10.2 Web Security

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 email:

admin@company.com

and as password:

x' or '1' = '1

What will happen?

Points: max 2

Fill in your answer here

What is the name of this type of attack?

Points: max 1

Fill in your answer here

Maximum marks: 3

10.3 Data protection

Mark those statements that are demanded by the **GDPR regulation**.

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

Select one or more alternatives:

□ All personal identifying data must be anonymized.

□ It is forbidden to store process highly sensitive data (e.g. medical data).

□ Only data necessary for the given purpose can be processed.

□ The user can request an overview of all his/her stored data from a service.

□ Stored data must be erased when it is not required any more.

□ The user must be informed which algorithms are used for encryption.

Maximum marks: 3

10.4 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:

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

Maximum marks: 2