NTNU
Kunnskap for en bedre verden

KANDIDAT

10056

PRØVE

IIKG1001 1 Cybersikkerhet og datanettverk

Emnekode	IIKG1001
Vurderingsform	Skriftlig eksamen
Starttid	09.12.2022 08:00
Sluttid	09.12.2022 11:00
Sensurfrist	09.01.2023 22:59
PDF opprettet	05.01.2023 02:32

Multiple-choice questions

Oppgave	Tittel	Oppgavetype
ℹ	IIKG1001 Exam - Cover page	Informasjon eller ressurser
1	(1 point)	Flervalg
2	(1 point)	Flervalg
3	(1 point)	Flervalg
4	(1 point)	Flervalg
5	(1 point)	Flervalg
6	(1 point)	Flervalg
7	(1 point)	Flervalg
8	(1 point)	Flervalg
9	(1 point)	Flervalg
10	(1 point)	Flervalg
11	(1 point)	Flervalg
12	(1 point)	Flervalg
13	(1 point)	Flervalg
14	(1 point)	Flervalg
15	(1 point)	Flervalg
16	(1 point)	Flervalg
17	(1 point)	Flervalg
18	(1 point)	Flervalg
19	(1 point)	Flervalg

20	(1 point)	Flervalg
21	(1 point)	Flervalg
22	(1 point)	Flervalg
23	(1 point)	Flervalg
24	(1 point)	Flervalg
25	(1 point)	Flervalg
26	(1 point)	Flervalg
27	(1 point)	Flervalg
28	(1 point)	Flervalg
29	(1 point)	Flervalg
30	(1 point)	Flervalg

Fill-the-gap questions

Oppgave	Tittel	Oppgavetype
31	Classful Addressing, gap filling (10 points)	Fyll inn matematikk
32	CIDR, gap filling (10 points)	Fyll inn matematikk
33	Access Control and User Management (9 points)	Sammensatt

Open-ended questions

Oppgave	Tittel	Oppgavetype
34	Open-ended question (6 points)	Langsvar
35	Open-ended question (10 points)	Langsvar
36	Open-ended question (7 points)	Langsvar

37	Open-ended question (9 points)	Langsvar
38	Open-ended question (9 points)	Langsvar
39	Final comments	Tekstfelt

1 (1 point)

Which statement is correct about the Internet?

Select one alternative:

○ The Internet is a network of networks, and it is considered as a Wide Area Network.

● Each host on the Internet is identified and addressed by a unique host ID.

○ IP addresses are used to identify application processes on the Internet.

○ The TCP/IP model is a protocol used by today's Internet, and it consists of seven layers.

2 (1 point)

Which of the following network devices is used to move data across the Internet?

Select one alternative:

● Router

○ Wireless Access point

○ Layer-2 switch

○ Wireless router

3 (1 point)

Which of the following statements is correct about the OSI (Open Systems Interconnection) model?

Select one alternative:

○ The OSI model is served as a reference model, and it is not used by today's Internet.

○ The OSI models consists of six layers: Physical, Network, Transport, Session, Presentation, and Application.

○ The application layer contains application programs such as Google Chrome, Outlook, etc.

● Each layer in the OSI model is able to directly communicate to all the other layers.

4 (1 point)

Which of the following statements is incorrect?

Select one alternative:

○ The physical address of a NIC is always the same regardless of its location.

○ A NIC might use a different IP address when it is moved to a different place.

○ Every computer or device on the Internet needs to have a unique IP address.

● Every network interface controller (NIC) is assigned an IP address by its manufacturer.

5 (1 point)

Which of the following statements is correct about the TCP/IP Model?
Select one alternative:

○ The TCP/IP model was replaced by the OSI model due to its complexity.

● It gets the name since the two most important protocols in this model are TCP and IP.

○ It consists of two protocols: TCP and IP.

○ The TCP/IP model is served as a reference model, and it is not used by today's Internet.

6 (1 point)

Which of the following network devices enables wireless devices to connect to a wired network?
Select one alternative:

○ Repeater

● Wireless access point

○ bridge

○ Hub

7 (1 point)

Which of the following is incorrect about network topologies?

Select one alternative:

○ Mesh topology aims to provide great reliability even though it is expensive.

● A single break in the cable of a ring topology would bring down the entire ring network.

○ It is possible to combine multiple types of network topologies to build a network.

○ Bus topology is considered efficient because multiple computers can send signals at the same time.

8 (1 point)

Which transport-layer protocol is usually used for web browsing and email transfer?

Select one alternative:

● TCP (Transmission Control Protocol)

○ UDP (User Datagram Protocol)

○ HTTP (Hypertext Transfer Protocol)

○ IP (Internet Protocol)

9 (1 point)

Which of the following statements is incorrect regarding Classful Addressing and Classless Inter-Domain Routing (CIDR)?

Select one alternative:

○ CIDR was introduced to replace Classful Addressing.

○ CIDR allows an IP address space to be further divided into multiple subnetworks.

○ Classful Addressing is a subnetting approach to break the IPv4 address space.

● Classful Addressing guarantees that all IP addresses can be freely allocated to people.

10 (1 point)

What is incorrect regarding public IP addresses and private IP addresses?

Select one alternative:

○ Public IP addresses are reachable for anyone on the Internet, but private IP addresses are not.

○ The same private IP addresses can be used by many local networks.

● Public IP addresses are mostly free of charge, but private IP addresses are not.

○ Public IP addresses are provided by Internet Service Providers (ISP), but private IP addresses are not.

11 (1 point)

Which of the following statements is correct about WWW?

Select one alternative:

○ When we talk about WWW, we mean the Internet.

● WWW refers to all online contents accessible over the Internet.

○ WWW is owned by cloud service providers such as Google and Amazon.

○ Wi-Fi is the key network protocol enabling WWW.

12 (1 point)

What are the necessary ingredients to build a trustworthy website?

Select one alternative:

○ HTTPS & a self-signed TLS certificate

○ Cookies & Hyperlinks

● HTTPS & a valid TLS certificate issued by a trusted Certificate Authority

○ HTML & Hyperlinks

13 (1 point)

Which is NOT a benefit of using a VPN (Virtual Private Network)?

Select one alternative:

○ VPNs can protect our data from being eavesdropped when we are in a public Wi-Fi network.

● VPNs can protect our computers from viruses.

○ VPNs can keep our online activities private if our VPN servers don't record any our online activities.

○ VPNs enable us to watch videos or TV channels that are only available in certain countries.

14 (1 point)

If the last character of a shell prompt is a dollar sign (i.e., $), it means that the user who uses the command line interface is ________. However, if the last character is ____, it means that the user is the root user.

Select one alternative:

○ A regular user, ~

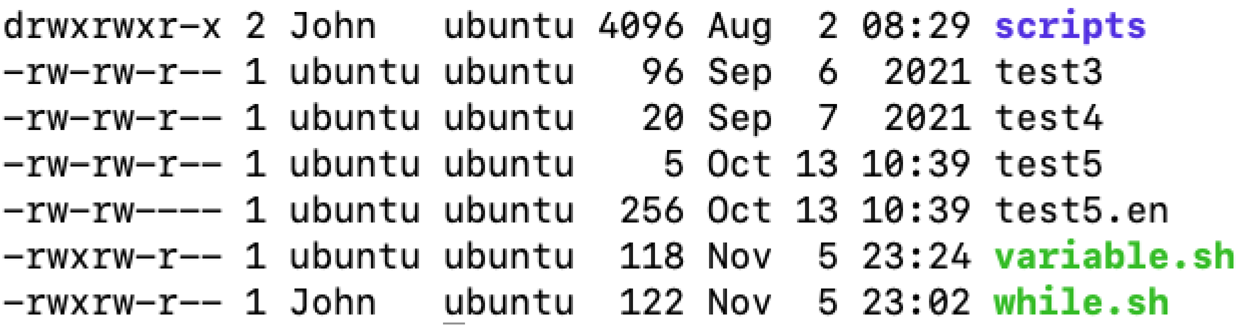
● A regular user, #

○ A superuser, ~

○ A superuser, #

15 (1 point)

The following picture shows all contents in one directory.



```
drwxrwxr-x 2 John   ubuntu 4096 Aug  2 08:29 scripts
-rw-rw-r-- 1 ubuntu ubuntu   96 Sep  6  2021 test3
-rw-rw-r-- 1 ubuntu ubuntu   20 Sep  7  2021 test4
-rw-rw-r-- 1 ubuntu ubuntu    5 Oct 13 10:39 test5
-rw-rw---- 1 ubuntu ubuntu  256 Oct 13 10:39 test5.en
-rwxrw-r-- 1 ubuntu ubuntu  118 Nov  5 23:24 variable.sh
-rwxrw-r-- 1 John   ubuntu  122 Nov  5 23:02 while.sh
```

Which of the following statements is incorrect?

Select one alternative:

○ "test3" is a file.

○ Only user "ubuntu" can execute "variable.sh"

○ "john" is the user who owns "scripts".

● No one can read the contents of "test5.en" except user "ubuntu" and group "ubuntu".

16 (1 point)

Encryption techniques are most commonly used to support this security principle:

Select one alternative:

● Confidentiality

○ Integrity

○ Availability

○ Password

17 (1 point)

The Cyber Kill Chain framework aims to identify the tactics and strategies followed by the

Select one alternative:

○ organizations

○ military forces

○ it is mostly about uncovering vulnerabilities - none of the other options

● threat actors

18 (1 point)

___________ are what we’re trying to protect, _________ are what we’re trying to protect against and _____________ are weaknesses or gaps in our protection efforts:

Select one alternative:

○ Threats, attacks, malware

○ Systems, attacks, breaches

● Assets, threats, vulnerabilities

○ Data, attackers, end users

19 (1 point)

A threat initiated from a human actor with negative intent, is else known as:

Select one alternative:

○ Honeypot

○ Unconscious threat

● Conscious threat

○ Insider threat

20 (1 point)

The ability of a system to maintain or restore its functionality after being exposed to a known/unknown source of risk or incident is defined as:

Select one alternative:

○ resilience

● recovery

○ defense in depth

○ asset evaluation

21 (1 point)

These are dedicated network devices, or single tools in a server or firewall that scan data, looking for malicious traffic, but do not act against it:

Select one alternative:

○ Security Information and Event Management systems

● Intrusion Detection Systems

○ Intrusion Prevention Systems

○ Data Loss Prevention software

22 (1 point)

This is used when tricking an attacker so that the network administrator can capture, save and analyze the behavior of an attack:

Select one alternative:

○ Nmap

○ Netflow

● Honeypot

○ IDS

23 (1 point)

Which statement is correct about privacy?
Select one alternative:

○ Privacy is best known for causing major problems for social media and comment fields

○ A privacy breach can lead to the so-called “CEO fraud”

○ Privacy means you cannot know who is doing what

● Privacy is not absolute

24 (1 point)

Which statement is correct?
Select one alternative:

○ ICT security includes cybersecurity

○ Cybersecurity includes ICT security.

● Cybersecurity and ICT security are the same.

○ Cybersecurity and ICT security are not related.

25 (1 point)

The "function" in function-based risk assessment, is a term that describes:

Select one alternative:

● tasks and deliverables for which the organization is responsible

○ mathematical formulas that describe the risk values in the system

○ how to compare the benefits of a specific security activity (code analysis, etc) against the cost of doing the activity

○ the features provided by third-party vendors used in your system

26 (1 point)

In risk control, the strategy that attempts to eliminate or reduce any uncontrolled risk through the application of controls and safeguards is else known as:

Select one alternative:

○ risk defense

○ risk termination

○ risk transfer

● risk mitigation

27 (1 point)

Which statement is correct?

Select one alternative:

● Internal threats are more harmful than external threats, because external threats do not have access to internal systems and core activities

○ Internal threats are less harmful than external threats because the world population and their access to the Internet is constantly increasing

○ Internal threats are more harmful than external threats, because they have access to different levels of user or administration rights

○ Internal threats are less harmful than external threats because of the number of targeted attacks organized by unknown sources is constantly increasing

28 (1 point)

The specific abilities, skills or tools a threat actor has at his disposal are linked to the actor's:

Select one alternative:

○ opportunities

● capabilities

○ intentions

○ threat surface

29 (1 point)

The Cyber Kill Chain framework is composed of several stages, with specific goals. Gathering information about the target is usually done during the _______________ stage:

Select one alternative:

○ Action

○ Exploitation

● Reconnaisance

○ Weaponization

30 (1 point)

Public-key encryption is a central part of:

Select one alternative:

○ DES

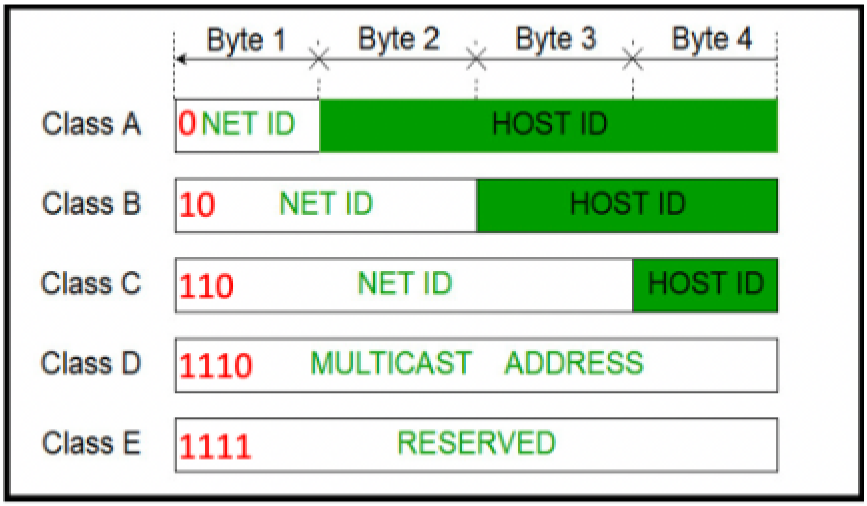
○ Symmetrical encryption

● Asymmetrical encryption

○ Enigma

31 Classful Addressing, gap filling (10 points)

See the picture below and answer the following questions.



(2 points) How many networks does class A provide?

Fill in your answer here 2^{32}

(2 points) How many networks does class B provide?

Fill in your answer here 2^{16}

(2 points) How many IP addresses does class C provide?

Fill in your answer here 2^{8}

(2 points) How many IP addresses in each network of class B can be allocated to computers?

Fill in your answer here 2^{16}

(2 points) How many IP addresses in class D can be allocated to computers?

Fill in your answer here 256

32 CIDR, gap filling (10 points)

Please fill the correct answer in each gap.

(2 points) Given a network of 200.221.140.0/24, the first 2^8 bits of the subnet mask are all "1".

(2 points) How many IPv4 addresses can a /25 CIDR block provide in total?

Fill in your answer here 2^7

(2 points) How many subnets can be provided by the network of “80.220.180.0/12”?

Fill in your answer here 2^{20}

(2 points) How many subnets will be generated by extending a net ID from 24 bits to 29 bits?

Fill in your answer here $2^{32-29} - 2^{32-24}$

(2 points) Given a network of 200.221.140.0/24, how many bits should be taken from the host ID part in order to create 16 subnets?

Fill in your answer here 2^{10}

33 Access Control and User Management (9 points)

There are 9 questions in this part. Each question is worth 1 point.

Assume that you are a system administrator at a small company, and you are the person who installs and maintains the Ubuntu system in your company. "amy" is your account name in this system.

1. What is your home directory by default? Please type the complete absolute pathname:

/home/amy

2. Who are you actually? What can you do in the system?

● You are a superuser, and you can execute any commands with the sudo command.

○ You are a superuser, and you can execute any commands without using su or sudo.

○ You are the root account, and you can do anything in the system.

○ You are the root user, and you can do anything with the su command.

As you know that "useradd", "usermod", and "userdel" are the commands to create a new user account, modify any attributes associated with an existing user account, and delete an existing user account, respectively.

Here are some hints for the options used by useradd:
d: To specify a home directory for the account. Only valid in combination with option m.
e: To specify an expiration date for the account.
f: To specify the inactivity field.
g: To assign an existing group to be the account's primary group.
G: To add the account to multiple groups.
m: To create a default home directory for the account.
o: To assign a non-unique UID for the account. Only valid in combination with another option.
u: To assign a specific UID for the account.
s: To assign a login shell for the account.

3. Erik Owe is a new employee in your company. What command can you use to create an user account for him so that the following requirements are all met?

- His account name should be "Erik".
- He wants to have a home directory called "erik" directly under the root directory.
- He wants to use "bash" as his login shell.

Fill in your answer here: useradd Erik -s /bin/bash -d /erik

4. After you create the user account for Erik Owe, he told you that he cannot use that account because it is in a locked state. How can you help him to solve the problem?

Select one alternative

● Set a password for his account by typing "sudo passwd Erik".

○ Inform him to set a password.

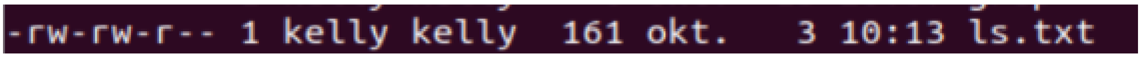
○ Recreate a new user account for him.

○ Extend the expiration period for his account.

5. Finally... Erik can use his account, and he is very happy. After several months, you are informed that he is going to leave your company because he got another job offer (Oh no!!!). What command can you use to delete his user account (including his home directory)? Please fill in your answer here: userdel erik

6. File mode rw--wx--x is equivalent to 631 in Octal Number Representation.

7. See the following picture. Which pair of commands will result in equal access permissions?



```
-rw-rw-r-- 1 kelly kelly  161 okt.  3 10:13 ls.txt
```

Select one alternative

● chmod o+2 ls.txt
chmod 666 ls.txt

○ chmod a=rwx ls.txt
chmod 666 ls.txt

○ chmod u+x,o-r,g+x ls.txt
chmod 770 ls.txt

○ chmod ug-w ls.txt
chmod 222 ls.txt

8. What command enables user "kelly" to own file "Exam" and enables group "root" to own file "Exam"?

Select one alternative

○ sudo chown kelly:root Exam

○ chown root:kelly: Exam

○ sudo chown root:kelly Exam

○ chmod kelly:root Exam

9. What permission does an user need to have in order to enter a directory?

Select one alternative

○ r

○ -

○ x

○ w

Before you move on, please check your answers and remove all unnecessary whitespace characters from your answers.

34 Open-ended question (6 points)

(3 points) What is the problem with Classful Addressing?

(3 points) How can CIDR help address the problem?

Fill in your answer here

Classful Addressing is solving the problem of limited number of IP addresses in IPv4. The problem was solved by introducing 2^128 addresses in IPv6 by expanding the public address space.

CIDR can help solve the problem with limited numbers of public addresses by using IPv6 addresses which using a number space of 2^128 public addresses instead of 2^32 public addresses in the IPv4 addressing
space.

Ord: 65

35 Open-ended question (10 points)

Please choose and correctly define 5 (five) of the following (2 points / correct definition):

1. *anonymity*
2. *asset*
3. *assymetrical encryption*
4. *availability*
5. *BSIMM*
6. *command & control*
7. *conscious threat*
8. *cybersecurity*
9. *(risk) defense strategy*
10. *identifier*
11. *(risk) mitigation*
12. *OWASP*
13. *phishing attack*
14. *privacy*
15. *risk*
16. *symmetrical encryption*
17. *threat*
18. *vulnerability*
19. *weaponization*
20. *zero-day (attack)*

Fill in your answer here

Assymetrical encryption is the matematical function and framework based on the work of Rivest, Shapir and Adler at Massachusetts Institute of Technology in Cambridge, MA.
One algorithm for assymetrical encryption is RSA and common implementations of OpenPGP such as PGPi and Gnu Privacy Guard provides with 4096-bits and 8192-bits public and private keys.

Availability is the term that describes the quality of systems and methods that provide public or private access to information resources in a timely fashion.

Risk is a matematical theory that describes the probability of an organizations system's human factors and the economical challenges of maintaining cybersecurity in computer systems that run financial systems.

Vulnerability is the possible security breaches in a computer system.

Zero-day (attack) become known as vulnerabilites in a computer systems as soon as the source code maintainers and developers become aware of them.

Ord: 140

36 Open-ended question (7 points)

Give a brief description of the different categories of vulnerabilities. Please provide at least one example from your own for each of those.

Fill in your answer here

Vulnerabilities come in buffer overflows, time-attacks and identification breaches.

One known buffer overflow vulnernability is the strcpy vulnerability where a buffer is overwritten with random data.

strcpy(buffer, NULL);

Ord: 28

37 Open-ended question (9 points)

During the risk assessment phase, the assigned team has to provide a system description for the organization/unit under assessment. Please choose an example of your own (not health services), and then provide a related system description. Use the following structure to describe the system:

1. Human, technical and organizational elements involved (3 points)
2. Function/s provided (3 points)
3. Assets that will help provide the function/s (3 points)

Fill in your answer here

I can describe a system for Public Voice Communication in https://folk.ntnu.no/olekaam/ntnu/bachelor/Aamot,2025.pdf

1. Humans can use computers to communicate better (Licklider, 1969). The technical implementation is C11. The organizational elements involved is GNOME Foundation (foundation.gnome.org) and my company Aamot Software. We provide a web site and a software application for the Voicegram service on www.gnomevoice.org and https://wiki.gnome.org/Apps/Voice

2. Functions provides are the Public Voice Communcation service known as Voicegram, with recording, mapping and streaming of voice data on the World Wide Web. I have describes Voicegram Specification on https://wiki.gnome.org/Voicegram

3. The assets are the software on the NTNU Gitlab account on https://gitlab.stud.idi.ntnu.no/olekaam/voice.git

Ord: 101

38 Open-ended question (9 points)

A local company has recently experienced a data breach. The owners would need *your team's* help to understand more about the process.

a) (3 points) Based on the CIA triad, choose a principle of your choice and describe its relevance and how it can be breached.

b) (6 points) There is discussion within the team on the right approach to be chosen for analyzing the incident *(McCumbers' cube vs Cyber Intrusion Kill Chain)*. Describe the respective components and actual relevance of each approach. What would be your final choice? Why? Build up on the example chosen in a) and extend it with more examples where possible

Fill in your answer here

a) I will use the principle of Reconnaisance to mitigate the threats and the possible zero-day attacks on the organization.   It is a method for describing the mathematical risk factors of the ICT system before the zero-day attack happen.

b) The McCumbers' cube is the 3x3x3 dimensional description of Reconnaisance principles for restoring and recovering data in the system after the data breach has happen. The risk vectors are

b.1) possible zero-day exploits with DDOS attacks in the system
b.2) possible time to fix the exploits and the time to limit the intruders
b.3) possible human resources to do the job of fixing the exploits and limit the intruders

b.1) Read the Security Advisories
b.2) Patch the systems
b.3) Pay the personell

Ord: 122

39 Final comments

[Non-graded] This section is meant to collect your feedback about this exam. Feel free to comment below, especially if you feel that some questions were not clear enough to you.

Thank you in advance,

Erjon & Kelly

Fill in your feedback here

Thanks for the excellent exam. I finished 10:15 after 1 hour and 15 minutes.