UNIVERSITETET I BERGEN

KANDIDAT

237

PRØVE

INF140 0 Introduksjon til datasikkerhet

Emnekode	INF140
Vurderingsform	Skriftlig eksamen
Starttid	22.11.2021 08:00
Sluttid	22.11.2021 11:00
Sensurfrist	--
PDF opprettet	03.05.2024 10:48

Information

Oppgave	Oppgavetype
ℹ	Informasjon eller ressurser
ℹ	Informasjon eller ressurser
ℹ	Informasjon eller ressurser

Section 1 - Multiple-choice Questions

Oppgave	Oppgavetype
1	Flervalg
2	Flervalg
3	Flervalg
4	Flervalg
5	Flervalg
6	Flervalg
7	Flervalg
8	Flervalg
9	Flervalg
10	Flervalg
11	Flervalg
12	Flervalg
13	Flervalg
14	Flervalg
15	Flervalg

16	Flervalg
17	Flervalg
18	Flervalg
19	Flervalg
20	Flervalg

Section 2 - Multiple-alternative Questions

Oppgave	Oppgavetype
21	Flervalg (flere svar)
22	Flervalg (flere svar)
23	Flervalg (flere svar)
24	Flervalg (flere svar)
25	Flervalg (flere svar)
26	Flervalg (flere svar)
27	Flervalg (flere svar)
28	Flervalg (flere svar)
29	Flervalg (flere svar)
30	Flervalg (flere svar)

Section 2' - Comment for Section 2

Oppgave	Oppgavetype
31	Langsvar

Section 3 - Entry-type questions

Oppgave	Oppgavetype
32	Fyll inn tekst
33	Fyll inn tekst

Section 4

Oppgave	Oppgavetype
34	Langsvar
35	Langsvar

Mandatory Assignments

Oppgave	Oppgavetype
36	Tekstfelt

1 Which of the following stands alone and exploits computer networks and security holes to reproduce itself?

Select one alternative:

○ Virus

○ Trojan horse

● Worm

○ Remote Access Exploit

Maks poeng: 0.5

2 Patching is important to your computer because

Select one alternative:

○ It reduces spam in your inbox

○ Patches remove viruses

○ It provides new system functions

● It makes your computer less vulnerable to known attacks

Maks poeng: 0.5

3 Which of the following malware can modify data on your system, so that your system doesn't run correctly or you can no longer access specific data, and you are asked for ransom in order to access your data?

Select one alternative:

○ RAT

● Ransom Trojan

○ Trojan-Downloader

○ Backdoor Trojans

Maks poeng: 0.5

4 Which of the following attacks pretends to associate a certain IP address (particularly the gateway router's IP address) to its MAC address in a LAN?

Select one alternative:

○ DNS spoofing

● DHCP spoofing

○ SYN spoofing

○ ARP spoofing

Maks poeng: 0.5

5 Which of the following is the correct order of layers in TCP/IP model from top to down?

Select one alternative:

○ Application, Transport, Datalink, Network, Physical

○ Application, Network, Transport, Datalink, Physical

● Application, Transport, Network, Datalink, Physical

○ Application, Datalink, Network, Transport, Physical

Maks poeng: 0.5

6 A/An __________ is a piece of code or a segment of command inside a legitimate software that aims to cause unintended actions and behaviors.

Select one alternative:

○ worm

○ spyware

○ trojan horse

● exploit

Maks poeng: 0.5

7 A ___________ is a method in which a computer security mechanism is bypassed untraceable for accessing the computer or its information.

Select one alternative:

○ front-door

○ clickjacking

○ key-logging

● backdoor

Maks poeng: 0.5

8 Confidentiality, integrity, availability authentication, authorization and accountability are considered fundamental for

Select one alternative:

● understanding security aspects in computer systems

○ countering against security threats to computer systems

○ exploiting vulnerabilities in computer systems

○ carrying out cyber attacks in computer systems

Maks poeng: 0.5

9 You have a highly sensitive document which you need to email to a trusted third-party. What is the safest way to send this?

Select one alternative:

○ Send the document from your work email account

● Encrypt the document first. Then send the password to the third-party using a different communication method

○ Send the document using a file sharing application

○ Make sure you scan the document with your anti-virus software first

Maks poeng: 0.5

10 The operating system access controls comprise which type of control in the following?

Select one alternative:

● Administrative controls

○ Compensating controls

○ Physical controls

○ Logical controls

Maks poeng: 0.5

11 ___________ is not an attack technique where numerous TCP segments are spoofed with a bogus source address which is then sent to a server.

Select one alternative:

○ FIN flooding

○ ACK flooding

○ SYN flooding

● Ping flooding

Maks poeng: 0.5

12 Which method of hacking will record all your keystrokes?

Select one alternative:

○ Sphere phishing

○ Keyhijacking

● Keylogging

○ Keyjacking

Maks poeng: 0.5

13 Which of the following statements best describes modern hackers?

Select one alternative:

● Highly-organised crime gangs run like businesses who deploy highly automated and sometimes highly targeted attacks against individuals and businesses for profit

○ Computer savvy people who hack individuals and businesses as a form of competition

○ All of the above

○ Bored and lonely anti-social teenagers who hack as a challenge and sometimes for profit

Maks poeng: 0.5

14 When integrity is lacking in a security system, which of the following occurs?

Select one alternative:

● Data tampering

○ Database unaccessible

○ Database crashing

○ Data leakage

Maks poeng: 0.5

15 Which of the following best describes modern cyber attack targets?

Select one alternative:

○ Companies which hold a lot of proprietary information

○ Banks and finance companies who process a lot of payments

○ Companies which hold credit card numbers of customers

● Any organisation or individual is liable to be the victim of hackers

Maks poeng: 0.5

16 You have just got an unexpected email

****

Dear Customer,

You are receiving this email because you've previously registered in our customer mail list.
 As you have bought a gas grill from us recently, we’d like to make you a special offer with 40% discount for your future purchases. Please click the following coupon to activate it no longer than 1 day after your receive this email

Retail Coupon
Expires 4/5/20
40% OFF
with coupon
Sales Floor Merchandise
SKU 2375865
0 47711 70446 9
Pep Boys

In-stock sales floor merchandise at this location only, excludes tires, parts, automotive batteries, all services (including chemicals provided in services and installed parts), gift cards, commercial, fleet and online purchases, and current promotions. May not be combined with any other sale, promotion, discount, code, coupon and/or offer.

If you don't want to receive our offers in future, you can cancel your registration it by clicking the unsubscribe link: **UNSUBSCRIBE**

****

What is the best course of action to take?

Select one alternative:

● It's a spam email. I would ignore it and block the sender's email address

○ It's wired since I haven't registered there. I need to click the link to unsubscribe it

○ It's good to receive a coupon. I should activate the coupon immediately in case I forget it later

○ It's a spam email. I need to unsubscribe it

Maks poeng: 0.5

17 According to the CIA Triad, which of the below-mentioned element is not considered in the triad?

Select one alternative:

○ Availability

○ Integrity

● Authenticity

○ Confidentiality

Maks poeng: 0.5

18 Which of the following heavily bases its security on certain hard mathematical problems?

Select one alternative:

○ DES

○ AES

● RSA

○ SHA256

Maks poeng: 0.5

19 Suicide Hackers are those

Select one alternative:

○ who are employed in an organisation to do malicious activities on other firms

○ individuals with no knowledge of codes but an expert in using hacking tools

● who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity

○ who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints

Maks poeng: 0.5

20 Compromising a user's session to exploit the user's data and do malicious activities or misuse user's credentials is called ___________

Select one alternative:

○ session sniffing

○ session spying

○ session spoofing

● session hijacking

Maks poeng: 0.5

21 Which of the following characteristics are provided by SSH?

Select one or more alternatives:

□ secure browsing webpages

☑ secure copy data from a server

☑ secure login to a server

☑ secure updating content of a web server

Maks poeng: 2

22 Which of the following processes use an access control list (ACL)?

Select one or more alternatives:

☑ a student downloads some lecture slides at mittuib

☑ a course instructor uploads lecture notes at mittuib

☑ a student wants to see a student fellow’s grade at mittuib but is rejected

☑ a student check his/her grade for a course at mittuib

□ a student logins mittuib with his/her student credentials

Maks poeng: 2

23 Which of the following are entity authentication practices in networks?

Select one or more alternatives:

- □ HTTPS
- □ Firewalls
- ☑ Password-based Authentication Protocol
- □ an employee uses UiB-VPN to download resources subscribed by UiB

Maks poeng: 2

24 Which of the following primitives can protect data integrity?

Select one or more alternatives:

- ☑ Diffie-Hellman key exchange
- ☑ AES
- ☑ SHA512
- ☑ RSA

Maks poeng: 2

25 Which of the following access control methods are used in a computer system?

Select one or more alternatives:

☑ attribute-based access control

☑ discretionary access control

□ rule-based access control

□ manpower-based access control

☑ role-based access control

Maks poeng: 2

26 Certain authentication mechanism provides 3A security features. What does 3A indicate here?

Select one or more alternatives:

□ anti-malware

☑ authorization

□ availability

☑ authentication

☑ accountability

Maks poeng: 2

27 Which of the following security controls heavily depend on cryptographic primitives?

Select one or more alternatives:

□ authorization

☑ authentication

□ availability

☑ integrity

Maks poeng: 2

28 Suppose a user’s password is hashed with SHA256 and the hash is then stored in a system. In practice, which of the following will significantly reduce the strength of hashed password and may lead to a successful password cracking?

Select one or more alternatives:

□ a dynamically varying salt is added the the calculation of the password hash

□ the user’s password consists of only 20 lower-case letters

☑ SHA256 is replaced with a fast hash function with 64-bit digest

☑ upper-case letters in the user’s password are converted to lower-case letters before the password is hashed

Maks poeng: 2

29 Which of the following statements about HTTPS are correct?

Select one or more alternatives:

□ it enables the web client to authenticate the web server by its PGP public-key certificate

□ it helps the server prevent DDoS attack

☑ it provides data confidentiality and integrity in communications

☑ it enables the web client to authenticate the web server by its X.509 public-key certificate

Maks poeng: 2

30 Which of the following are in the category of preventative security control?

Select one or more alternatives:

□ data backup

☑ firewall

☑ data encryption

☑ least-privilege access control

□ anti-malware software

□ intrusion detection system

☑ user authentication

Maks poeng: 2

31 If you have some comments for certain questions in Section 2, or if you want to add more explanation of your answers to certain questions in Section 2, you can leave them below. (This is optional, so you can skip it.)

Leave your comments below. Please repeat the question(s).

Ord: 0

Maks poeng: 0

32 Marks for answers:

- no/wrong alternative gets 0 pt
- each correct alternative gets 0.5 pt
- all correct alternatives get 3 pts

This question tests your knowledge and skills regarding OpenSSL. It's advisable to upgrade OpenSSL in case earlier versions encounter unexpected issues. (Refer to https://www.openssl.org/docs/man1.1.1 for help).

NB: Do not use the built-in OpenSSL in MacOS directly, it is a different version of OpenSSL.

Below are some OpenSSL commands and results, you can use them as a guide to answer the questions. Some commands have selected parts hidden with XXX.

- echo XXX | openssl dgst -XXX
- openssl dgst -XXX
- openssl dgst -XXX -sign XXX -out XXX message.txt
- openssl dgst -XXX -verify XXX -XXX sig.bin message.txt
- openssl pkey -in XXX -out pubRSA.out -XXX
- openssl pkey -in XXX -
- openssl pkey -in XXX -pubin -text
- openssl genpkey -algorithm XXX -out XXX.pem

OpenSSL results

- 967fd5b5188289d0b28f7780013e93f481bdc196cdc50349627d7b89f3b74cb1
- 3abaeabe9bc26f534480dbdf406eccabe765941d4a179b94650301825fda3074
- 79f2b05296d391e129b54babbc303c05adc3fca819326cbf1832ef567053a1e4
- 5b9d87cc255d7b1adb3aed75214050dae04c76618becc8c20c8c2bda5bbd26c3
- 0c102ab608afc2ffe2965d509f4f58b5b115080ab40b89b495bb8e8b20387f25
- a8d942b73fc88043fc62b3f5db7c6fae15be151f40b5238fa7b60b65cc644aad
- a8cd456fa12ea6e550cd9a81e740b3b2e3bb5fb8aba3c0f47eaa561fe72ded0b
- 534f74b81854dcee5d8961d2e8a6a38d7589f7df370a05dff53fd2f97e1b4ad9
- 4f360119aabeed7f939cb66aa333e920747d81231902bbce436ccf7e68cd55ff
- 4a0459d5a9126c77b069099129d237cab50529086d035853d991a9c2f85bcdb1
- 92befef75cfd49497e1db835530756493a4267d5ed8fae422d5b9ccdf6b8efe8
- 296a5af3831067f135a4805a6932f93fdf9a89f74d5ac356e55890416e964f69

* In the following entries, your OpenSSL results are supposed to be included in the above list.

1. I generate a RSA key pair with Openssl and get the following RSA private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKgIBAAKCAgEAoyXJJwHW53v35k5VKkHlFFfQNCGO/rnjtpgVqZuyx5wre7J/
7qXK2P/d+8TEEBbUTrd05pnCijQFKnV3a/4tsY1NPWygVbMIBgF/eZxJFEN5+5ZJ
Ipuppfqic9DMDkhAf4/v91bmRHoVf2OHfk4CxV8u679KPor6vEgwkBFw8TJPJjTz
cM0OAWaS4SiEBlxmvQsAn5qGywD1+e93cwsvaB9pYissM3fVueIPnVgyMrnjR+Lb
kXUeZ9b2YHptuHNIPeHY6SjdsVh5ETNeYDNHp1iXQy9EPaCiq99n/FjwPwm8CUwg
DJZY20cBfSdhR2pk1E5OMzNX+OOLMyOuBApwB4SP1aQf3IYg6hyXWS5aOvz9lisc
4BIL5UGyndJjG3XxglDtTmYN+yNdwq17rJh3wMF7zUtSG9uIKHS5ZV7bR7nKSQc1
```

```
VctyKF/hDLtXkyy391wgpp60i93f9/0nsqFfvVQMzh+JX1Dm4MWMYaXk8NrhQrT5
Vk0H7jkDMH0ZqGNIPG4Bq1pB+bnBFhT2LVpwCrGedPHafSQ23w4AstLkVFy5Gwnt
AM7rTRM579PoZPh+0lKUIN/OPLtKw+0wgvk6c8tWXLBUHpFVlHioo6+MXgjQa0/+
Q6JV9BcSWzjwCsIhmNOd+Md13SPRr8LbgDdqN5InDnjfo/usktCyDQQ79CUCAwEA
AQKCAgEAlc1MNhTqTwL1TPMAIB0BSvyWoEdwFVR6Ul6zBVmBfudWxe3QqkBxUW8f
VN4HaP6NUvoAzPzCNEQvuhzB2tc4/Z7RHWVwk0AgTeNyOSfXsIOC3g/Q4gIsbIsG
P3Go7DRLhNWVcXbJWHcA5kdtUfwvbytG2hB7C5JxSBDBBof9PHsFUf+syBaAlaip
lTSuhWiyrUI9AE/TFPN86FGJTIkormKpUQpzO479IAECdWdWMF2e45LaKWVw1cf7
0fqYZJT18Fw/31c2uHCUOccBETQExxQBUB9GeY/VzhsEUCEZ98focGEFzIkAbdd0
9oYCPKDkIEySYVDzpgTI+9v3HJ643bbW6IidJMQEMOOy9UFhuOOCUclWfp7dvG5t
4+T7zTT1TRNDDz3cBPO7zdKzN9XBK229jcivFzpT1Rdv2P0UIPcqqSg46dwI19dS
N7ERcwDcOQeKgo1IvOyq3UA4tmyjzH3DaZH6uAV12sMIp+RL4DAkyBISgVeS97wR
Zw9pMQOvyKNeT/nSwr/S0P3Xkk9rwXqVi86O0JKDUROjQBM/KDXYNI0ZG4meoJiL
nOtfc7zbrgP15QNXD9lhv627/sLOI8mVoRcdgWCp9rDk16tZWeD7kApTt7hi1nqo
RJIGQPTV4EKmnNx9ECq7f3QOIsFo654bMJ53n+SKBMkzh+hzWMECggEBANItZkjb
hOyqHpvs5lF1pPeFfsZvrVycIkm4VSDo0JKeR10KkxL9X5fdVRbhxjwgzIWInSsV
YapnPDgv6De4J871xhEIS1/CTH2RA3TvRViBtCB9pqPpGC11uhOWTFbd4A8Q+ENX
n2hwcCzOMFncZ8F19f3QkcNm2Xq+6ehzADmitX/To0DuIeEO74BPXYd5+eoKkeq1
rIA41eFKpq137DOQBtB1D04apOxhrLMttRIx1nfE1al8vRGIxThOjmFWi1gNncLa
bNjF6nFrUa79H+cbh4YsZGz7WiVhI/tVq4PrXYe2RfCaEY6jOvos3mbo+OGvIME7
9ghWo1R/QA9fzJsCggEBAMa3hXr2R82QtSSfc6lEuJO/bSmPJYyLNm02lNkYEAG9
itOwfNXGD/DIO23khketU3btA0+xdmzYKWF598EvYpMtrY8uh4G6qkMyf9VyBTEP
A5MFCqIOLqVsT0pVeOsrhDsut+NBS2Bn3182N14w8sGXcLGZz/+AwIxnHNoIdsJi
s27MADyTF4vTF3eM8hmfewFWMOEMIjvD5C9HfaeAtc3QEjpdBSm20OSzJHfNaMkI
zW8/vz2vsJnYnoe0XY7H0b/NbImjyqQpMSnEvLr9oAk/VW9pLRf43KkR8TlWOWss
0RNhVh5sP2ZNP0j/LWt+q8VVlWEowekVXkjXLX4abj8CggEBAJFr6iaIBI6/kIgu
jJI2PcMpcbMZGCIIuoypZvVTQOUBcL0WkPaFqzunX7VqV7/IrdoC0UQ7Eg1WSptR
wmmzGJAhC39Dbut9w3DqAitJVoDLIXcZmVA1+o2RtELTLIS4RcwG4M+vc9NOYL8P
IvLGBmAcHy0Tv5cktXsxVySHVXOLeetM4tsNKRHQRLRRtZQEOH/P+nAcbZN2P74W
6caCgEKY964KIKHY253WYyjCilNheIP6NB+F+EeanB++ctM0j0tIeIyWltNR9Umu
iKD78LP2H0odswqYyyGr2bqP5xFqq5c37aJw5476r9bjbqpjrbhxxQoCU9QnJfFT
7I302dsCggEAcis8iFH5HPTX7guicwzIkxV3TVpN83qEMakbScNWZvmUSI1qy5N4
0xjndBLIx2OgwYIY1e+an5xt4fAmVRq5Yt/qiInuFq29ZtAbu/E/ZFIA73YFDuhh
Cm+4+ncy+sJMvYfw5KM+AEyNfHF0zCwJPQqaF5/Mbfp2JfSUEg1WNwZoGu8f761+
6LnGEMysx+XI0PXJLXOC2SGJ91P2sIb1bSLvZhLNhZLgX5VBDYe5fU8OYK1aXcGU
ED/xjPwmiILrUmxfyyacpUZ5VYsP98sB6G430sO1wcEcXhLN6ehNIvNjx+Ozi9Ub
c9ZL1s+tM8ZaQA0Uvvaguh6pxeXC4GGIFwKCAQEAqs6LN+T8/ISYTkuI7+YGOw5J
YD7sP/E+bHGpLpogjTXCVwFMn8esRMPj2gnOARO9YJXRT2u4kq4RLxM5hfDIpJDc
Lg+5uy6PM+HoFLMgHv0E5RqfFvoB3DPstaVXfXdbAEukIHi4Vi/sH80fVeNnPvm6
O/vzWNqy2D305W5nssaHUPgE8jjBs9C31rhcZgXjLgJp7yLkRQkVH+tlN78mB6mg
JIycJgbsGt+NA3tJWEjO2dh80Z7vWhZHypSG/Sfc+V70LiVEhSa8V/84yrGbIN8E
D1M7Vs1Ly1uIk540ijtG/Ey3cUNOSYKVywU+wAPRosRIgoLhB8HzcDZHC4eT0w==
-----END RSA PRIVATE KEY-----
```

Save the above private key in a file privateRSA.pem, or download it from **this link**. Answer the following questions

- The modulo n in the RSA public key has 4096 bits.
- The last byte of prime1 in hexadecimal form is 0x 9b .

You want to send your public key inside the above private key to your friend Maria. Therefore, you use an openssl command pkey to obtain the public key in the plain text form (in addition to the encoded form), store it in a file pubRSA.txt, and then send the pubRSA.txt together with its SHA256 hash to Maria.

What is the SHA256 hash of pubRSA.txt in hexadecimal form? Given your answer below.

3abaeabe9bc26f534480dbdf406eccabe765941d4a179b94650301825fda3074

2. Suppose you have a travel plan with Maria to Spain. You have been in charge of booking all flight tickets for the travel and Maria is in charge of tourism routine.

Unfortunately, you just received a message from the Airline which informs you that the flight is cancelled due to the COVID-19 situation. The content of the **notification.pdf** is as follows

> Dear passengers,
>
> Due to the situation with COVID-19, the flight DY5529 on Dec. 15 from Bergen to Barcelona is cancelled. We sincerely apologise for the inconvenience.
>
> You are entitled for refund of your flight and you should claim for compensation no later than Nov. 15, 2021.
>
> Best Regards
> Norwegian Airline

You need to forward this message to Maria. Both you and Maria have learned cryptography from INF140, so you decide to send the file **notification.pdf** together with a digital signature.

You use your RSA private key in the above (stored in the key file privateRSA.pem) and generate a signature sig.bin on the SHA256 hash of message.txt. Then you mail the message.txt together with the signature sig.bin to Maria.

- What is the SHA256 hash of the message?

4a0459d5a9126c77b069099129d237cab50529086d035853d991a9c2f85bcdb1

- What is the SHA256 of the sig.bin in hexadecimal form? Given your answer below.

296a5af3831067f135a4805a6932f93fdf9a89f74d5ac356e55890416e964f69

3. Suppose Maria has agreed with you in advance that all your signatures will be calculated with SHA256. Upon receiving your mail, Maria wants to verify the signature of message.txt containing the bad news.

Suppose the email you sent was captured by an attacker, who changed the date Nov. 15 to Nov. 30 in the file. When Maria use OpenSSL to verify the file with sig.bin, what is the OpenSSL output?

Copy the result in the blank below.

Optional.
You can leave all your commands in the following entries. (These entries are used to double check the OpenSSL results above. They are not mandatory).

1. openssl dgst -sha256 pubRSA.txt
2. openssl dgst -sha256 -sign privateRSA.pem -out sig.bin notfification.pdf
3. openssl dgst -sha256 notification.pdf
4. openssl dgst -sha256 sig.bin
5.
6.

Maks poeng: 3

33 Marks for answers:

- no/wrong alternative gets 0 pt
- each correct alternative gets 0.5 pt
- all correct alternatives get 3 pts

Consider the following paragraphs about security and cryptography with missing words/phrases. Select the correct word/phrase from the following list, and provide your answers in the blanks:
access control; active attack; passive attack; assets; confidentiality; security attributes; asymmetric; attack; authenticity; availability; countermeasure; integrity; intelligence; key; masquerade; modification; non-repudiation; ciphertext; passive; administrative; plaintext; security policy; private-key; public-key; receiver; release message contents; replay; RSA; sender; symmetric; threat; traffic analysis; vulnerability;

In cyber security, the CIA triad, standing for confidentiality, integrity and availability, respectively, embodies the fundamental security objectives for both data and for information and computing services. In addition, authenticity, which is the property of being genuine and being able to be verified and trusted, and accountability, which aims to uniquely trace an entity's action, are also frequently mentioned to present a complete picture of cyber security.

Among terminologies of cyber security, a security vulnerability is any weakness in an information system, system security procedures, internal controls that could be exploited or triggered by a threat source. A/an attack is any kind of malicious activity that aims to collect, disrupt, deny, degrade, or destroy information system resources. Security controls are generally divided as physical controls, administrative controls and technological controls. Among technological controls, one critical technique is the access control, which limit information system access to authorised users, processes acting on behalf of authorised users, or devices.

Cryptographic techniques are the key building blocks for most security controls. In addition to encryption techniques, digital signature realised by public-key cryptography provides the property of non-repudiation that prevents a sender from denying the messages it previously sent, which has critical importance for today's massive E-commerce on the Internet.

Maks poeng: 3

34 (i). List the different layers in the TCP/IP protocol stack. Name at least three security-oriented protocols for the TCP/IP model. (1 pt)

(ii). What are the basic components of an IDS system? List at least 3 requirements of an IDS system. (2 pts)

(iii). Describe the DNS poisoning attack and it possible consequences. (2 pts)

(iv). Describe the mandatory access control and discretionary access control. Explain the difference between them. (2 pts)

Fill in your answer here

1:

-physical layer, datalink layer, network layer, transport layer, application layer.

-WPA2, TLS, SSH

2:

-sensors, analyzers, user interface

-Being able to run without human input

-Having scalability so that it can monitor a large system with many users

-Detect atempts by an attacker to modify the IDS

3:

-DNS posioning is when an attacker manages to change the ip address corresponding to a website link within a DNS cache. it can be changed in the local dns cache or on a dns server.

-the dns server will return the wrong ip address and the consequences of such an attack might be that a user tries to visit their banks website, but gets redirected to a phising site that looks identical to the real site. the user then enters their passwords, which then gets logged by the attacker.

4:

-Discretionary access control (DAC) is when the creator of a file or directory gets to decide the access rights for other users and groups. the access rights are stored in ehter an access control list, a capability list, or in an access matrix

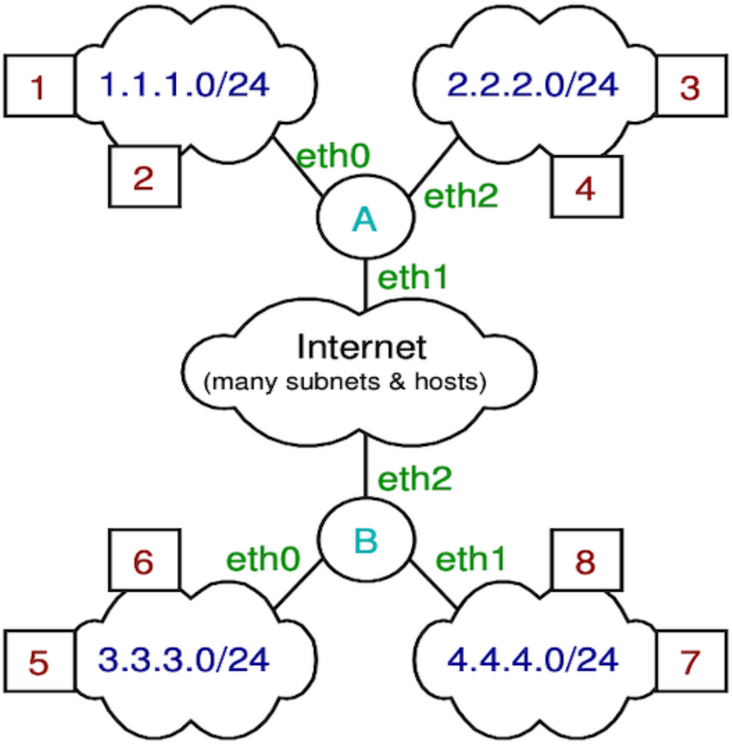
-Mandatory access control (MAC) is when the system administrator decides the access policy for files and directories. each subject is assigned a securito clearance, and each object is assigned a security level. and a subject can only access an object after their clearance is checked and is the same or higher then the objects security level.

-the difference between the two is who has control over who can access the objects.

Ord: 253

Maks poeng: 7

35 The following figure shows a network topology.



As shown in the figure, two subnets 1.1.1.0/24 and 2.2.2.0/24 connect to the Internet via Router A; two subnets 3.3.3.0/24 and 4.4.4.0/24 connect to the Internet via Router B.

In each subnet, although only two hosts are displayed in the figure, we assume there are more hosts in the network. For simplicity, each host number indicates the last byte in the IP address, e.g., host 4 in network 2.2.2.0/24 has IP address 2.2.2.4.

Suppose you are the IT administrator for the two subnets 3.3.3.0/24, 4.4.4.0/24 attached to Router B and need to add rules to the firewall running on Router B.

Part 1. The default policy for the firewall is **ACCEPT**.

For each of the following policies, adding the corresponding rule(s) to the firewall table. The rules should be in a compact format. E.g.: Use the format “4.4.4.4:25” to show both IP address and port number in the “Source” and “Destination” columns.

For each question, assume the firewall table has been flushed and there is no existing rule in the table, namely, your answer in Question (ii) is independent of your answer in Question (i).

Question (i). Block all hosts on networks 1.1.1.0/24, 2.2.2.0/24 from SSHing host 7 in the network 4.4.4.0/24 (1pt);
Question (ii). Block host 8 from browsing to any websites in network 1.1.1.0/24 (1pt)
Question (iii). Block all hosts in network 2.2.2.0/24 except host 3 from Pinging host 6 in the network 3.3.3.0/24 (1pt)

Create a table as below and add rules for the above questions. You are free to add more rows for each question. (You can create a table with the icon of table in the tool bar)

Question	Source	Destination	Protocol	Action

(i)				
(ii)				
(iii)				

Part 2. Now assume the firewall at Router B has default policy **DROP**. Suppose the current content in the firewall table is:

Source	Destination	Protocol	Action
1.1.1.1:*	4.4.4.0/24:22	TCP	Accept
3.3.3.6:*	2.2.2.0/24:25	TCP	Accept
4.4.4.0/24:*	1.1.1.1:*	TCP	Accept
3.3.3.0/24:*	1.1.1.2:80	TCP	Accept
4.4.4.8:*	*:443	TCP	Accept
any	any	any	Default

The following TCP SYN segments have recently been received by the firewall

- Segment 1 arrived on interface eth0 with source 3.3.3.6:40123 and destination 2.2.2.3:25
- Segment 2 arrived on interface eth1 with source 4.4.4.8:50345 and destination 1.1.1.1:443
- Segment 3 arrived on interface eth0 with source 3.3.3.5:50789 and destination 1.1.1.2:80

Question (iv). What will happen to the three TCP segments? Update the following SPI table at the firewall. (2pt)

Source	Destination	State

Question (v). According to your SPI table from the answer above, explain what will happen for the following segments that arrive at Router B later and justify your answer. (2 pts)

- Segment 1 arrives on interface eth2 with source 1.1.1.1:443 and destination 4.4.4.8:50345
- Segment 2 arrives on interface eth2 with source 1.1.1.2:80 and destination 3.3.3.5:50789
- Segment 3 arrives on interface eth2 with source 1.1.1.2:443 and destination 4.4.4.8:50345

Fill in your answer here

part 1:

question	source	destination	protocol	action
(i) rule1	1.1.1.*:*	4.4.4.7:22	tcp	drop
(i) rule2	2.2.2.*:*	4.4.4.7:22	tcp	drop
(ii) rule1	4.4.4.8:*	1.1.1.*:80	tcp	drop
(ii) rule2	4.4.4.8:*	1.1.1.*:443	tcp	drop
(iii) rule1	2.2.2.3:*	3.3.3.6:*	icmp	accept
(iii) rule2	2.2.2.*:*	3.3.3.6:*	icmp	drop

part 2: (question iv)

source	destination	state
3.3.3.6:40123	2.2.2.3:25	established

4.4.4.8:50345	1.1.1.1:443	established
3.3.3.5:50789	1.1.1.2:80	established

question (v):

segment 1 is accepted because there is an established connection between the source and destination with those ports

segment 2 is accepted for the same reason as segment 1

segment 3 is not in the spi table, and since the firewall only has a rule from node 4 to node 1 with port 80 (not from node 1 to node 4) it will be dropped and a connection will not be established in the spi table

Ord: 137

Maks poeng: 7

36 This question is intended for collecting points in the two mandatory assignments.

Provide your marks for the two mandatory assignments here in the form: Total = (A1+A2)/4, e.g, 44 = (90+86)/4. (Your mark will be checked)

Maks poeng: 52.5