UNIVERSITETET I BERGEN

KANDIDAT

143

PRØVE

INF140 0 Introduksjon til datasikkerhet

Emnekode	INF140
Vurderingsform	Skriftlig eksamen
Starttid	01.12.2023 09:00
Sluttid	01.12.2023 12:00
Sensurfrist	--
PDF opprettet	31.05.2024 13:15

Information about the exam

Oppgave	Oppgavetype
ℹ	Informasjon eller ressurser

Overview of Cybersecurity

Oppgave	Oppgavetype
1	Flervalg (flere svar)
2	Sammensatt
3	Plasser i tekst
4	Plasser i tekst

Cryptographic Tools

Oppgave	Oppgavetype
5	Nedtrekk
6	Flervalg (flere svar)
7	Sammensatt
8	Flervalg
9	Fyll inn tall
10	Fyll inn tall
11	Flervalg (flere svar)
12	Plasser i tekst

User Authentication

Oppgave	Oppgavetype
13	Flervalg (flere svar)
14	Sant/usant
15	Flervalg (flere svar)
16	Plasser i bilde

Access Control

Oppgave	Oppgavetype
17	Flervalg
18	Sammensatt
19	Plasser i tekst

Network Protocols and Attacks

Oppgave	Oppgavetype
20	Flervalg
21	Flervalg (flere svar)
22	Sammensatt
23	Flervalg
24	Flervalg (flere svar)
25	Flervalg (flere svar)
26	Fyll inn tall

Security Protocols

Oppgave	Oppgavetype
27	Sammensatt

Malware

Oppgave	Oppgavetype
28	Flervalg
29	Flervalg
30	Flervalg
31	Flervalg (flere svar)

Intrusion Detection

Oppgave	Oppgavetype
32	Flervalg (flere svar)
33	Flervalg (flere svar)

Firewall

Oppgave	Oppgavetype
34	Flervalg (flere svar)
35	Langsvar

Mandatory Assignment

Oppgave	Oppgavetype
36	Langsvar

1 Which of the following properties belong to the NIST CIA triad?

Select one or more alternatives

- [ ] Authenticity
- [ ] Accountability
- [ ] Authorization
- [x] Availability
- [x] Confidentiality
- [x] Integrity

Maks poeng: 1

2 (i) What is a security breach?

Select one alternative

- (•) A loss of any security property in an information system
- ( ) A flaw in an information system
- ( ) An attack performed by a hacker
- ( ) A way to ensure CIA triad

(ii) Threat consequences describe

Select one alternative

- ( ) the likelihood of an attack
- (•) the effect that an attack has on security properties
- ( ) the vector used to carry out the attack
- ( ) the action taken by an attacker to breach a security property

Maks poeng: 1

3 Assign the correct name to each threat action.

Hjelp

Misuse | Falsification | Incapacitation | Interception | Obstruction

Exposure	Sensitive data is released to an unauthorized entity from within the information system.
Intrusion	An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

Maks poeng: 1

4 Assign the correct name to each threat consequence.

Hjelp

Usurpation | Disruption | Deception

Corruption	A circumstance or event that may result in an authorized entity receiving false data and believing it to be true
Unauthorized Disclosure	A circumstance or event that results in control of system services or functions by an unauthorized entity.

Maks poeng: 1

5 Suppose the Playfair cipher use the following encryption matrix from the keyword **CRYPTO**

C	R	Y	P	T
O	A	B	D	E
F	G	H	I	K
L	M	N	Q	S
U	V	W	X	Z

(i) What is the ciphertext for the plaintext **SECURITY**? ZKOCPGCP (ZKODAZPC, ZKOCPGCP, ZKOCGPPC, KTULPGPR)

(ii) What is the plaintext for the ciphertext **PFYIAT**? CIPHER (ICONIC, CIPHER, CINEMA, ICEBOX)

Maks poeng: 1

6 Which of the following statements are correct for secure Hash functions?

Select one or more alternatives

- [ ] A secure hash function with 256-bit output should provide 256-bit security
- [ ] A secure Hash function shoud have good avalanche effect, namely, a single bit change in input leads to roughly 50% bit changes in the output
- [x] A secure hash function should be pre-image resistant
- [x] A secure hash function should be collision-free

Maks poeng: 1

7 Suppose you have a document of sensitive data, named sensitive_data.xls, and you need to ensure the confidentiality/secrecy and integrity of the data.

(i). In order to ensure its confidentiality, you choose to encrypt the file to a ciphertext file sensitive_data.enc and store the ciphertext file only.

Which of the following can correctly and securely realise your goal?

Select one alternative

- ( ) openssl enc -aes-256-cbc -in sensitive_data.enc -out sensitive_data.xls -k "Qq942&%*%dsa_#@" -pbkdf2
- ( ) openssl enc -aes-256-ecb -in sensitive_data.xls -out sensitive_data.enc -k "Norway" -pbkdf2
- (•) openssl enc -aes-256-cbc -in sensitive_data.xls -out sensitive_data.enc -k "Qq942&%*%dsa_#@" -pbkdf2
- ( ) openssl enc -aes-256-cbc -in sensitive_data.xls -out sensitive_data.enc -k "1234" -pbkdf2

(ii). In order to ensure its integrity, you choose to calculate the hash of the document, output it to a file sensitive_data.hash, and store the hash file in a secure disk separately.

Which of the following can correctly and securely achieve your goal?

Select one alternative

- (•) openssl dgst -sha256 senstive_data.xls > sensitive_data.hash
- ( ) openssl dgst -md5 senstive_data.xls >sensitive_data.hash
- ( ) openssl dgst -sha256 sensitive_data.hash > senstive_data.xls
- ( ) openssl dgst -sha256 senstive_data.xls -output sensitive_data.hash

Maks poeng: 1

8 (i) Which of the following statements on symmetric ciphers, cryptographic Hash functions and MAC is wrong?

Select one alternative

- Sender and receiver need to use pre-shared key for using symmetric ciphers and MAC
- MAC algorithms should be reversible since the receiver needs to verify the integrity of received data
- Secure design of symmetric ciphers, Hash functions and MAC should have the "avalanche effect"
- When a cryptographic Hash function is used in combination of a block cipher, the hash output should double length of the cipher's secret for achieving same security level

(ii) Which of the following statements on MAC and digital signature is wrong?

Select one alternative

- Digital signature ensures non-repudiation
- MAC algorithm uses one secret key
- MAC algorithm protects data integrity
- MAC algorithm should be reversible

Maks poeng: 1

9 Suppose RSA cryptosystem chooses the following private key and public key:

- private key (p, q, d) = (13, 7, 29)
- public key (n, e) = (91, 5)

(i) For the plaintext m=4, what is the ciphertext? 23

(ii) For the plaintext m=8, what is the ciphertext? 8

Maks poeng: 1

10 Suppose Alice and Bob use the Diffie-Hellman key exchange scheme to share key.
They use the global parameters (p, g) = (11, 2) and proceed as follows:

1. Alice chooses a private key PriKey_a = 7 and sends her public key PubKey_a = g^{PriKey_a} mod p to Bob
2. Bob chooses a private key Prikey_b = 5 and sends his public key PubKey_b = g^{PriKey_b} mod p to Alice
3. Alice and Bob use their private key and the received public key to calculate the common key

(i). What is the public key of Alice in Step 1? 7

(ii). What is the common key shared between Alice and Bob in Step 3? 10

Maks poeng: 1

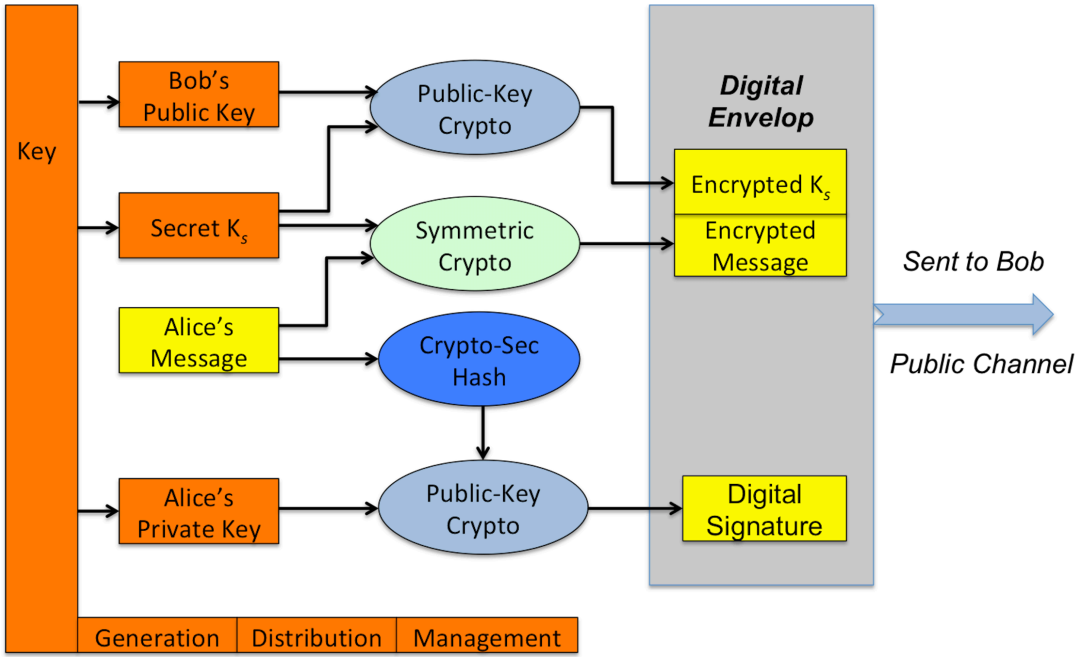
11 Which of the following properties can be provided by digital signature?

Select one or more alternatives:

- [ ] Non-repudiation
- [x] Integrity
- [x] Authenticity
- [ ] Confidentiality

Maks poeng: 1

12



The above figure is a typical usage of cryptographic primitives in hybrid manner to enable secure communications through an insecure channel.

At the sender side, suppose Alice uses Bob's RSA public key, AES with 256-bit key in CBC mode, and her own RSA private key in the above figure. This combination will provide confidentiality, integrity of the message and the sender's authenticity.

What are the steps Bob will go through in sequence when he receives such an envelop from Alice?

Hjelp

Encrypt the data with the key Ks

Verify the signature with the private key of Alice by comparing the hashes

Decrypt the encryption key Ks with his public key

Step 1. Decrypt the encryption key Ks with his private key

Step 2. Decrypt the data with the key Ks

Step 3. Calculate the Hash of the decrypted message

Step 4. Verify the signature with the public key of Alice by comparing the hashes

Maks poeng: 1

13

Which of the following are possession-based credentials?

Select one or more alternatives

- [x] smart card
- [ ] Face recognition
- [ ] PIN
- [x] software token

Maks poeng: 1

14 (i) Biometric credentials are easy to replace in case of theft

Select an alternative

- ○ True
- ◉ False

(ii) Multi-factor authentication can use different means of authentication

Select an alternative

- ◉ True
- ○ False

Maks poeng: 1

15 In a Linux system, suppose a user's password is stored in **/etc/shadow** as:

Password:5IM97wGbU5S.Funda$8HxX3gD5UjdwnXD7mHu7Foh9s6w.NCn5cxifoki7pr0m01Re5VG/yad86LjKmpJuXB/66ks1Y7T5y6cjV6.351:18313:0:9

Which of the following statements about the above file are correct?

Select one or more alternatives:

- [ ] there is no login name in the file
- [ ] '5' indicates the number of bytes in the salt
- [x] '18313' indicates the number of hash iterations in the file
- [x] 'Password' is the user name
- [x] '5' indicates the hash type used in the calculation

Maks poeng: 1

16 The European Union wants to centralize the digital identity solutions of the member states.

Each member state is still going to be responsible for registering residents and issuing their credentials. Residents must be provided a digital ID consisting of a smart card, and a PIN associated to it.

However, the EU wants to introduce a European Identity Database, EID, to collect all the identities so that they can be seamlessly used around the block. When submitting an application to a PA office, a resident in any of the states must present its card and input the PIN in a terminal.

Follow the E-authentication model in Figure 3.1 and fill the gaps in the figure below

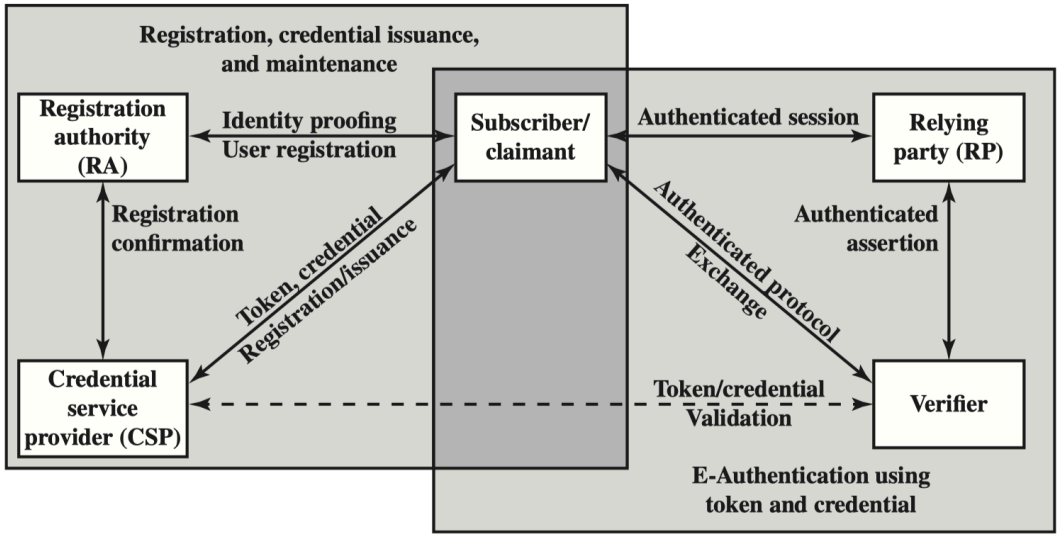
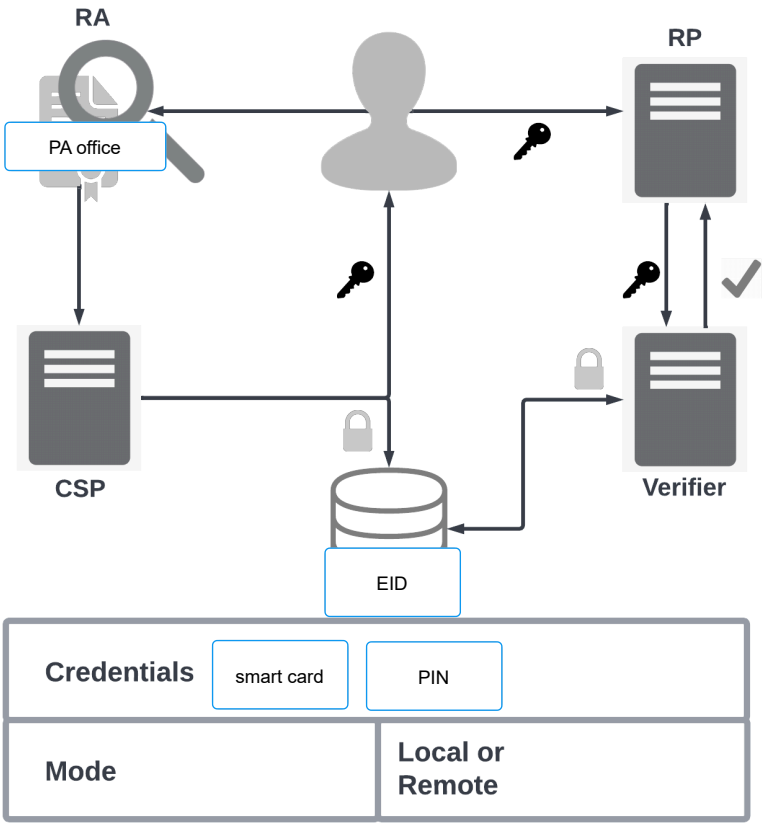


Figure 3.1 The NIST SP 800-63-3 E-Authentication Architectural Model

Drag the correct text block to each gap. **Gaps for credential follow alphabetic order** Hjelp

EID	PIN	keycard
EU	PA office	smart card
Multi factor authentication	continuous authentication	local
remote	Member state	



Maks poeng: 2

17 (i) Which of the following statements is correct?

Select one alternative

- In DAC an owner of a resource can delete it. In MAC this is not possible
- MAC is concerned with Messages AC. DAC is concerned with Data AC
- In DAC the owner of an object are allowed to edit access rights.
- In MAC access rights for a file can be edited by its owner

(ii) What is a Role in RBAC?

Select one alternative:

- A well defined set of access rights
- An entity asking for access to a resource
- A job function common to many users
- A policy used to determine access to a resource

Maks poeng: 1

18 (i) Suppose a file in Linux system has the permission rwxr-xr--. What is the numeric representation of this file? 754

(ii) Suppose a text file Linux system has the permission 766. What is the letter representation of this file?

rwxrw-rw-

Maks poeng: 1

19 Suppose in a system, User 1 can read and write File 1, File 2, and can execute File 3. User 2 can read, write, execute File 1, and can read and execute File 3. User 3 can read File 2 and File 3.

According to the above description, fill the following Access Matrix with the correct access right

- Read (R), Write (W), Execute (X), or
- a combination of them (RX, RW, RWX, ...), or
- 'None' if the user has no access rights to the file.

Then complete the remaining statements.

Hjelp

ACL	WX	None	Authorization Table	R	
RWX	Capability Ticket	X	RW	W	
RX					

Access Matrix

	File 1	File 2	File 3
User 1	RW	RW	X
User 2	RWX	None	RX
User 3	None	R	R

The following is the ACL for File 1.

File 1	User 1: RW	User 2: X

Maks poeng: 5

20 (i) Which of the following protocol is used to find the MAC address of a device for a given IP address in a LAN?

Select one alternative:

- Dynamic Host Configuration Protocol
- Address Resolution Protocol
- Network Address Translation
- Domain Name System

(ii) Which of the following protocol is used to find the uniform resource locator (URL) for a given IP address in a WAN?

Select one alternative

- Address Resolution Protocol
- Domain Name System
- Transmission Control Protocol
- Dynamic Host Configuration Protocol

Maks poeng: 1

21 When a device connects to a network and sends a DHCP request to the DHCP server, which of the following IP addresses will be typically included in the DHCP response from the server?

Select one or more alternatives:

- IP address of google.com
- IP address of the DNS server in the LAN
- IP address for the new device in the LAN
- IP address for the gateway router in the LAN

Maks poeng: 1

22 Fill in the 5 layers of TCP/IP stack in the first column **from top to down**, and assign relevant protocols for each layer in the right column.

Application (Application, Transport, Physical, Data Link, Network)	DHCP (ARP, ARP, DHCP, TLS)
Transport (Network, Physical, Application, Transport, Data Link)	TCP
Network (Application, Data Link, Network, Physical, Transport)	IP
Data Link (Physical, Data Link, Transport, Network, Application)	ICMP (NAT, DNS, ARP, ICMP)
Physical Layer	

Maks poeng: 3

23 (i) 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
- ARP spoofing
- DHCP spoofing
- SYN spoofing

(ii) In the _____„ an attacker sends a forged IP address to the client which it requested for a domain name.

Select one alternative

- DNS spoofing
- ARP spoofing
- ICMP spoofing
- SYN spoofing

Maks poeng: 1

24 In which of the following attacks, the IP address of the packet from an attacker towards the target network or system is spoofed?

Select one or more alternatives:

- [ ] Amplification attack
- [ ] ARP spoofing
- [x] Reflection attack
- [x] DNS spoofing

Maks poeng: 2

25 Which of the following attacks can be enabled by ARP spoofing?

Select one or more alternatives:

- [ ] Denial of Service
- [ ] Ping Flooding
- [x] Packet Sniffing
- [x] Man-In-The-Middle (MITM) attack

Maks poeng: 1

26 In order to implement a classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization.

Question: Consider an attack using ICMP echo request (ping) packets that are 400 bytes in size (ignoring framing overhead). What is the minimum number of such packets per second must the attacker send to flood a target organization using a 32-Mbps link?

Answer: The attacker needs to send at least 1000000 packets per second to flood the link.

Maks poeng: 1

27 In order to achieve secure communication, security protocols are needed at different layers.

At transport layer, the protocol [TLS/SSL] (TLS/SSL, WPA, SSH, HTTPS) is typically used to provide security support for communication protocols at application layer. For instance, in HTTPs, the client will first validate the server by verifying its [X509 public key certificate] (X509 public key certificate, Hash, URL, public key) issued by [a certificate authority] (a state authority, a certificate authority, a root certificate authority, a local authority) to the organisation. After this step, the client and server can agree on certain ciphersuite to protect their subsequent communications.

For instance, a ciphersuite TLS_AES_256_GCM_384 uses AES_256 to protect the [communication] to the data with expected [256] -bit security level.

At the physical link layer, the protocol [SSH] (SSH, WPA2, WEP, IPSec) is used to ensure robust wireless security, which realises secure communication between mobile devices and the wireless hot spot. The original version of such a protocol in 1990s was insecure, because the protocol misused the cipher [Velg alternativ] (RSA, AES, DES, RC4) and it didn't use strong cryptographic scheme to protect the [integrity] of the data in communication.

Maks poeng: 4

28 (i) Which of the following stands alone and exploits computer networks and security holes to reproduce itself?

Select one alternative:

- Trojan horse
- Virus
- Remote Access Exploit
- Worm

(ii) A _____ is a method in which a computer security mechanism is bypassed untraceable for accessing the computer or its information.

Select one alternative

- key-logging
- backdoor
- session hijacking
- clickjacking

Maks poeng: 1

29 (i) _____ can automate an action or attack so that repetitive tasks are done at a faster rate.

Select one alternative:

- Botnets
- Robots
- Cookie-bots
- Remote Access Tool

(ii) _____ is a type of code specific to certain unknown vulnerability, or a set of unknown vulnerabilities in a system

Select one alternative

- Zero-day exploit
- Backdoor
- Rootkit
- Remote Access Tool

Maks poeng: 1

30 (i) _____ is a type of virus that uses macro or scripting code; it is typically embedded in a document and when triggered, it runs and replicates itself into other such documents.

Select one alternative

- Multipartite virus
- Macro virus
- File infector
- Boot virus

(ii) _____ is a type of virus that creates copies during replication that are functionally equivalent but have slightly different bit patterns, in order to defeat programs that scan for viruses

Select one alternative

- Encrypted Virus
- Polymorphic virus
- Metamorphic virus
- Stealth virus

Maks poeng: 1

31 Which of the following are typical features that a computer virus and a trojan horse have in common?

Select one or more alternatives:

- [ ] silently open a backdoor to external attackers
- [ ] sending message to a remote controller
- [ ] replicating itself in the infected system and network
- [x] residing in a software
- [x] be active when certain condition is triggered

Maks poeng: 1

32 Which of the following are practices of intruders in the phases of information gathering and initial access?

Select one or more alternatives:

- [ ] Use various techniques to crack passwords
- [ ] Use NMAP to scan the target network
- [x] Send phishing emails to key personnel of the target organization
- [x] Use RAT to cover intrusion tracks

Maks poeng: 1

33 Which of the following statements about IDS are correct?

Select one or more alternatives:

- [ ] IDS introduces much overhead to the network as it always analyses all incoming traffic before letting them into the internal network
- [ ] IDS has the same functionality as firewall, so only one of them needs to be present in a network
- [x] IDS assumes that system activities and incoming traffic are observable
- [x] IDS assumes legitimate activities and intrusive activies can be distinguished

Maks poeng: 1

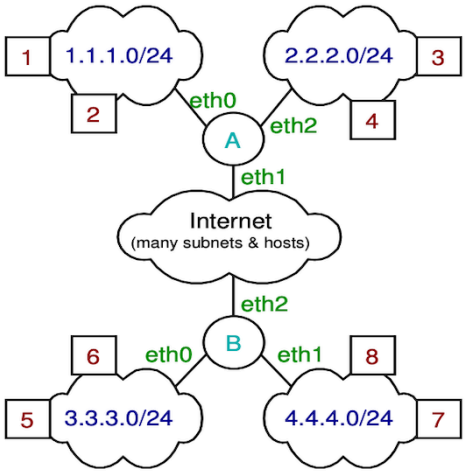
34 Which of the following statements about firewall are correct?

Select one or more alternatives:

- [ ] A proper configuration in firewall can prevent IP address spoofing
- [x] As a design goal, all traffic between an internal network and external networks must pass through the firewall
- [ ] A packet filtering firewall can inspect the MAC address, IP address and port number of an incoming traffic
- [x] A firewall may not protect fully against internal threats

Maks poeng: 1

35



The above figure displays a network topology, where

- 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 3 in network 2.2.2.0/24 has IP address 2.2.2.3.

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 you 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 in the “Source” and “Destination” columns. For instance, use the format “4.4.4.4:25” to show IP address is 4.4.4.4 and port number 25.

For each question, assume the firewall table has been flushed, indicating that there is no existing rule in the table. Thus your answer in Question (ii) has nothing to do with your answer in Question (i).

(i) Block all hosts on networks 1.1.1.0/24, 2.2.2.0/24 from SSHing host 7 in 4.4.4.0/24;

(ii) Block host 6 in 3.3.3.0/24 from visiting HTTPS webpages hosted at any web server in 2.2.2.0/24

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)				
Default	*.*.*.*:*	*.*.*.*:*	Any	Accept

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:*	1.1.1.1:443	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 3.3.3.6:1234 and destination 2.2.2.4:25
- Segment 2 arrived on interface eth1 with source 4.4.4.8:2345 and destination 1.1.1.2:443

(iii) What will happen to the above two TCP segments?
Create a stateful packet inspect (SPI) table as follows.

Source IP: Source Port	Destination IP: Destination Port	Connection State

(iv) According to your SPI table from the answer above. Explain what will happen for the following segments that arrive at Router B later. Justify your answer.

- Segment 1 arrives on interface eth2 with source 1.1.1.1:80 and destination 4.4.4.8:2345
- Segment 2 arrives on interface eth2 with source 2.2.2.4:25 and destination 3.3.3.6:1234

Fill in your answer here with question numbers (i), (ii), (iii), (iv).

(i)

question	source	destination	protocol	action
(i)	1.1.1.0/24:*	4.4.4.7:22	TCP	drop
(i)	2.2.2.0/24:*	4.4.4.7:22	TCP	drop
(ii)	3.3.3.6:*	2.2.2.0/24:80	TCP	drop
(ii)	2.2.2.0/24:*	3.3.3.6:443	TCP	drop

(iii)

Source IP:source port	Destination IP: destintaion port	connection State
3.3.3.6:1234	2.2.2.4:25	ACCEPT
4.4.4.8:2345	1.1.1.2:443	DENY

(iv)

Segment 1 will be dropped, dropped since there is no syn/ack falg since it got denied in (iii). Segment 2 wil arrive with a syn/ack flag since it is the return packet from segment 2 in (iii) so this will connect if the Firewall is configured to allow syn/ack falgs. if not it will be dropped since there is no condition that meets source from 2.2.2.2:25.

Ord: 109

Maks poeng: 5

36 This part is for collecting the points for your mandatory assignments. I will take care of this part and you can just ignore it.
In case you would like to have more explanations for some of your answers, leave your explanation/comments here

Ord: 0

Maks poeng: 50