FRANKFURT
UNIVERSITY
OF APPLIED SCIENCES

Forschungsgruppe für
Netzwerksicherheit,
Informationssicherheit
und Datenschutz

Fachbereich 2
Prof. Dr. Martin Kappes

IT Security
December 2021

Exam

Family Name, First Name:

Mat. No.:

I hereby confirm that,
1. I have written the presented exam alone without using any illicit tools or help,
2. I am healthy and able to conduct the exam. I understand that the exam will be considered taken and graded after the exam questions were received.

(Signature)

Question	1	2	3	4	5	Sum	Grade
max. Points	15	20	25	20	20	100	
achieved							

Please note:

1. This exam consists of 13 pages including cover sheets with five questions, totaling a score of 100.
2. To pass the exam, you need at least 50% of the total score.
3. The duration of the exam is 90 minutes.
4. Your answers should be clear, comprehensible and legible.
5. If the answer to a question requires calculations, do not just state the solution, but also its derivation in detail.
6. You are not allowed to use any resources except for a non-programmable pocket calculator.
7. Write your solutions solely within the space provided on the exam sheets. If necessary, use the back side. Mark all sheets with your name and Mat. No.

Good luck!

Task 1 (15 Points):

Answer the following questions with 2-3 sentences each:

(1.A) What is a Certificate? Which components does it contain?

(1.B) What is a Certificate Authority and what does it do exactly?

(1.C) In an X.509 Certificate, how do I recognize a Root Cerfiticate?

(1.D) Name two advantages of using Certificates.

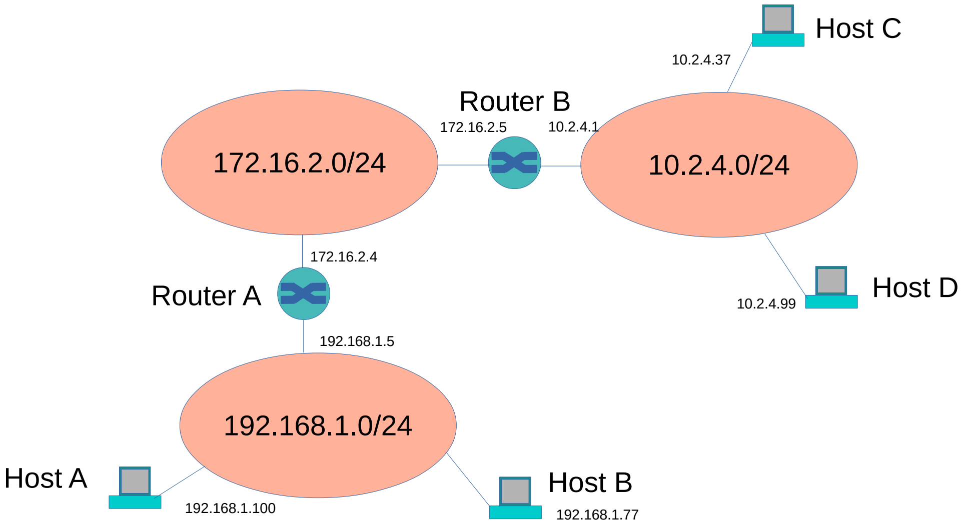
(1.E) What is Certificate Revocation and when do I need it? How can a user find out if a Certificate was revoked?

(1.F) What is OCSP, how does it work and why is it needed?

(1.G) What is a Certificate Signing Request? Which keys of the subject does the Signing Request contain?

Task 2 (20 Points):

Please consider the following network:



Hosts C and D are running Web Servers on Port 80.

(2.A) What is SSH?

(2.B) A user successfully starts an ssh connection from Host A using the command

```
ssh -L 8888:10.2.4.37:80 -g 10.2.4.99
```

What is the IP Address of the SSH Client?

(2.C) What is the IP Address of the SSH Server?

(2.D) A Web Browser on Host B contacts Host A on Port 8888. Which Web Server would answer the request?

(2.E) From the Web Server's perspective, where is the request coming from (Source IP address?)

(2.F) What does the -g-option in the command do?

(2.G) Name Source IP, Destination IP, Ports and Transport Protocol of the connection carrying the traffic in network 172.16.2.0/24

(2.H) After shutting down the SSH connection, a new connection is successfully established from Host A using the command `ssh -g -D 9999 10.2.4.37`. How is this feature of SSH called?

(2.I) A Web Browser on Host B wants to contact Host A on Port 9999 in order to connect to the Web Server on Host C. How would the Browser need to get configured?

(2.J) What address line would the user need to put into the browser?

Task 3 (25 Points):

Answer the following questions with one or two words each:

(3.A) In which mode and protocol is IPSec used when facilitating a VPN?

(3.B) What does DoS stand for?

(3.C) Which of the CIA-principles can usually not be achieved by cryptograhpic means?

(3.D) What is the name for the ability to prove that a given message was sent and by whom to a third party not involved in communication?

(3.E) What does AES stand for?

(3.F) What is the size of the password domain if only numbers are allowed and the size of the passwort is at least 1 and at most 5 digits?

(3.G) The three possible factors for authenticaton are what you are, what you have and what you

(3.H) What is the name for the feature of an OS to hide complicated details from users and applications which otherwise had to be dealt with?

(3.I) How is a maliciously injected script which is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc calles which the victim retrieves from server when it requests information?

(3.J) What is an alternative name for DNS-Spoofing?

(3.K) Name a security mechanism on the Data Link Layer.

(3.L) On which layer does SSH work?

(3.M) How is the translation of a private to a public IP address called?

(3.N) Where would you typically place a server in a company network which must be reachable from the public Internet?

(3.O) How are Firewall components called which work above the Transport Layer?

(3.P) Which protocol is used in OpenVPN to encrypt the data between two endpoints?

(3.Q) Which virtual interface is used in OpenVPN for a site-to-site connection?

(3.R) Which protocol is used for the proxy in ssh in dynamic port forwarding?

(3.S) What is the first message in an SSL/TLS handshake?

(3.T) How is an exploit called which is not yet publicly known?

(3.U) What is the result when decrypting the ciphertext 0000 1111 0101 with one time pad 0110 0101 0011 ?

(3.V) The TLS record protocol may contain records of four different protocols. The ClientHello message is part of which ot these protocols?

(3.W) Define the term Confidentiality in one sentence.

(3.X) What does CBC stand for?

Task 4 (20 Points):

In the following, we consider a router connecting the networks 10.1.1.0/24 and 192.168.5.0/24 with a static packet filter. All packets are processed against a chain with the following rules:

Nr.	IP Source Address	IP Destination Address	Protocol	set Flags	considered Flags	Action
1	10.1.1.0/24	192.168.5.1	TCP	SYN	SYN	DROP
2	10.1.1.9	192.168.5.0/24	TCP	SYN ACK	SYN ACK	DROP
3	10.1.1.0/24	192.168.5.2	TCP	SYN ACK	SYN ACK	ACCEPT
4	10.1.1.7	192.168.5.0/24	TCP	SYN ACK	SYN ACK	DROP
5	192.168.0.0/16	10.1.1.8	TCP	ACK	ACK	DROP
Default: ACCEPT						

Assuming typical behavior (i.e. each TCP segment is transmitted in one IP packet), analyze whether a TCP connection setup between the following hosts is successful or not.
For every packet sent during connection setup, specify which of the rules is applied to the packet.

(4.A) TCP connection setup from 10.1.1.5 to 192.168.5.9

(4.B) TCP connection setup from 192.168.5.1 to 10.1.1.7

(4.C) TCP connection setup from 192.168.5.16 to 10.1.1.8

(4.D) TCP connection setup from 192.168.5.2 to 10.1.1.7

(4.E) TCP connection setup from 192.168.5.3 to 10.1.1.7

(4.F) TCP connection setup from 192.168.5.2 to 10.1.1.4

(4.G) TCP connection setup from 192.168.5.16 to 10.1.1.8

Task 5 (20 Points):

Answer the following questions with 2-3 sentences each:

(5.A) What are threats to anonymity on the Network Layer?

(5.B) What is a Pharming Attack?

(5.C) What is a Buffer Overflow?

(5.D) What is SSH Port Forwarding?

(5.E) What is the difference between Authentication and Nonrepudiation?