Exam number:

IT-Security, 2023

Department of Computer Science (DIKU)
Practice Exam

1 True or False (about 10 minutes)

For each statement, answer True or False. (Put one "X" in each.)	True	False
a) Availability is similar to the principle of complete mediation		
b) Multi-factor authentication is an effective measure to achieve non-repudiation		
c) Risk is calculated as a function of 'severity' and 'urgency'		
d) HTTPS is the standard to secure online browsing		
e) Proper use of AES does not require an underlying public key infrastructure		
f) If malware successfully opens a listener on port 80 on an infected computer, then anyone on the Internet may connect to it		
g) It is advisable to store passwords using at least data encoding		
h) Rootkits cannot exist in kernel mode		

Exam number:

2 Short Answer Questions (about 15 minutes)

Answer the following with just a few sentences.

Short Answer Questions, 2.1: How is 'amplification' used in DDoS attacks?

(Maximum 5 lines.)

Short Answer Questions, 2.2: How does memory layout randomization help protect against buffer overflow attacks?

(Maximum 5 lines.)

Short Answer Questions, 2.3: Which of IPsec and TLS encrypts most of the packet?

(Maximum 5 lines.)

Short Answer Questions, 2.4: Why do you think that phishing continues to be such a heavily used technique by attackers?

(Maximum 5 lines.)

3 Software updates (about 30 minutes)

Suppose a software company `xyz.com` sells a product P and wants to distribute a software update U. The company wants to ensure that its clients only install software updates published by the company. They decide to use the following approach:

- The company places the update U on its web server and designs the product P to periodically check this server for updates over HTTPS.

Software updates, 3.1: Explain what can go wrong if P downloads U over HTTP.

(Maximum 5 lines.)

Software updates, 3.2: To enable HTTPS downloads the company buys a public-key certificate for its web server from a CA. Explain what checks P should apply to the server's certificate to defeat a network attacker.

(Maximum 10 lines.)

Software updates, 3.3: The company worries that an attacker will break in and steal the web server's secret key. How would you design the software update system so that it can recover from such an event?

(Maximum 10 lines.)

Exam number:

4 Ransomware (about 30 minutes)

Ransomware is a type of malware that encrypts files on infected computers and demands a ransom for decrypting the files.

Ransomware, 4.1: Suppose you come across a piece of ransomware that encrypts the files the following way:

```
# generate random AES key
aes_key = generate_aes_key()

# for each file
for file in found_files:
    # encrypt the file with the key
    encrypt_file(file, aes_key)

# save to disk AES key
write_to_disk(aes_key)

# deallocate AES key from memory
delete_aes_key(aes_key)
```

When the victim pays the ransom, the ransomware will open the file with the AES key stored on disk and start decrypting the files.

Using this encryption approach, could victims expect to recover their files without paying the ransom?

(Maximum 10 lines.)

Ransomware, 4.2: Suppose you come across a new piece of ransomware that encrypts the files the following way:

```
# generate new RSA key pair
client_public_key = generate_public_key()
client_private_key = generate_private_key()

# generate random AES key
aes_key = generate_aes_key()

# for each file
for file in found_files:
    # encrypt the file with the key
    encrypt_file(file, aes_key)

#encrypt AES key with RSA public key
encrypted_aes_key = encrypt_aes_key(aes_key, client_public_key)

# save to disk encrypted AES key
write_to_disk(encrypted_aes_key)

# send to ransomware operator the RSA private key
send_to_server(client_private_key)

# deallocate AES key from memory
delete_aes_key(aes_key)
```

Using this encryption approach, could victims expect to recover their files without paying the ransom?

(Maximum 10 lines.)

Ransomware, 4.3: In general what would you advise in order to prevent ransomware infections and limit their impact?

(Maximum 15 lines.)

Exam number:

5 Email Security (about 30 minutes)

The email protocol (SMTP) has no authentication by default, so a sender can pretend to originate a message apparently from any email address. Sender Policy Framework (SPF) is a simple email validation system designed to detect email spoofing.

It works as follows: a site like `gmail.com` publishes in its DNS record an SPF entry specifying all the IP addresses that can send email on behalf of Gmail. When an email server, say `mail.diku.dk`, receives an email claiming to be from Gmail, the `mail.diku.dk` server looks up the SPF record for `gmail.com` and rejects the incoming email if the sender IP address is not in the list of authorised IP addresses who can send email on behalf of Gmail.

Email Security, 5.1: With SPF, how much is the risk of spearphishing lowered, if at all?

(Maximum 10 lines.)

Another spoofing defense called DKIM has Gmail digitally sign every outgoing email. Gmail publishes its public verification key in the `gmail.com` DNS record. When `mail.diku.dk` receives an email claiming to be from Gmail it first fetches Gmail's public key from DNS, verifies the signature on the incoming email, and accepts the email only if the signature verifies.

Email Security, 5.2: Does DKIM prevent a network attacker from sending mail on behalf of Gmail users? If so explain why, if not explain why not. Recall that a network attacker only attacks the network links, but does not attack any endpoints.

(Maximum 10 lines.)

Email Security, 5.3: A few years ago it was discovered that some organisations had set up DKIM in such a way that emails were signed with 512-bit RSA keys. Such keys were explicitly allowed in the DKIM standard. Explain why this is a problem.

(Maximum 10 lines.)