Exam number:

SAMPLE Exam in IT-Security

Department of Computer Science (DIKU)

1 True or False (about 10 minutes)

For each statement, answer True or False. (Put one "X" in each.)	True	False
a) Denial of service attacks threaten the security goal of availability		
b) Privacy and availability are related but not the same		
c) Cryptographic checksums are used to combat malicious integrity violations		
d) RSA and Diffie-Hellman are used for data encryption in TLS		
e) A browser's trusted certificate store starts out empty and is populated by the user		
f) A worm is a piece of malware that consumes memory and/or CPU resources to reduce system performance on a host		
g) A stateful packet filter keeps track of payload data using specialized programs for a pre-determined set of applications		
h) A signature-based IDS detects zero-day exploits with lowest false positive rate		

Exam number:

2 Short Answer Questions (about 10 minutes)

Answer the following with just a few sentences.
Short Answer Questions, 2.1: If you have an effective firewall at the enterprise perimeter, why would you still recommend host-based firewalls?

(Maximum 5 lines.)

Short Answer Questions, 2.2: What is hybrid encryption?

(Maximum 5 lines.)

Short Answer Questions, 2.3: What is stored XSS?

(Maximum 5 lines.)

Exam number:

3 Security Principles (about 10 minutes)

Security Principles, 3.1: Suppose you have a network access control in place at your company that requires all computers that connects to your network to present a certificate that is signed by your company's Certificate Authority before being allowed access. Which security design principle is being followed here?

(Maximum 8 lines.)

Security Principles, 3.2: Your company enforces a password policy such that when users fail to log on for three consecutive attempts, their accounts are locked for 10 minutes. Which security design principle is being followed here?

(Maximum 8 lines.)

Security Principles, 3.3: If you browse the internet using an administrator account, you are breaking which security principle?

(Maximum 8 lines.)

Exam number:

4 Passwords and Password Managers (about 20 minutes)

Passwords and Password Managers, 4.1: Consider a password manager that stores and retrieves passwords as a means to cope with overwhelming numbers of passwords. Instead of remembering many passwords, a user remembers one master password to the password manager. It provides access to the others.

Consider these password manager approaches.

a. (Saving passwords in your browser). When you log into your online accounts, your browser will offer to save them for you. If you accept, your browser securely stores the password, and the master password is the password of the user account currently logged on to the computer, you are browsing from.

b. (Saving passwords in a standalone password manager application). In this case you locally on your computer install a password manager application. To open the password manager application, you must supply the master password. After this, you can create and store passwords and later retrieve them when you need to log into your online accounts.

c. (Saving passwords in a cloud-based password manager service). A cloud-based password manager service works in the same way as a standalone password manager application, but stores the passwords on the service's website, and you can access the password manager by supplying your username and password for the cloud-based password manager service.

Summarize strengths and weaknesses of the different approaches, as you view them.

(Maximum 20 lines.)

Passwords and Password Managers, 4.2: Suppose your password manager of choice, for added security, in addition to storing your online account's username and password, also stores the domain at which these credentials are valid, e.g., (username:bob, password:hash(il0vealice), domain:heste-nettet.dk). How could this approach help protect you against phishing scams against, in this case, heste-nettet.dk?

(Maximum 10 lines.)

Exam number:

5 Transport Layer Security (TLS) (about 20 minutes)

Transport Layer Security (TLS), 5.1: You browse to https://heste-nettet.dk, log in by entering your Heste-Nettet username and password, update your credit card number associated with your account, and make a purchase - all through Heste-Nettet's website.

Which of the following could an attacker that can passively eavesdrops on all your communication to and from heste-nettet.dk deduce? Briefly explain.

a. The approximate size of the HTTPS requests from your browser

b. Your Heste-Nettet username but not password

c. Your Heste-Nettet username and password

d. Your credit card

e. The fact that you are visiting heste-nettet.dk

f. The session cookie for the connection

g. The TCP sequence numbers transmitted for the connection

(Maximum 20 lines.)

Exam number:

Transport Layer Security (TLS), 5.2: Suppose that you are confident that your browser and operating system have not been tampered with, but you believe a user-level process has been infected and is running malware. Permissions on your system allow the user-level process to read your files (which includes the browser executable) but not to write them. The user-level process is also allowed by the operating system to "sniff" packets received or sent by your system's network interface card. Can the malware-infected user-level process extract your username and password when you log on to https://heste-nettet.dk? Explain why or why not.

(Maximum 10 lines.)

Exam number:

6 Intrusion Detection (about 20 minutes)

A new hacking campaign has been uncovered and indicators of compromise (IOCs) – that is, data or artifacts that if present is indicative of similar intrusions – has been published by security researchers.

You are given the following IOCs:

a. The MD5 hash value of the main malware component:
68b329da9893e34099c7d8ad5cb9c940

b. The IP address of the C2 server to which infected hosts communicate:
130.226.237.80

c. The domain name associated with the C2 server:
vinupdater.com

Intrusion Detection, 6.1: For each of the above IOCs, briefly discuss how you would use it to detect infections in your network. Be specific about what you would search for and where. Comment on the robustness of your detection strategy, or conversely, the ease of which the attackers could adjust their attacks to avoid being detected by the IOCs / your detection strategy.

(Maximum 20 lines.)

Exam number:

Intrusion Detection, 6.2: The main malware component looks up the vinupdater.com domain name every hour, connects to the C2 server and sends an update back to the C2 server. Suppose you deploy a network intrusion detection system to detect malware infections that exhibit the same pattern. Which intrusion detection approach would you use – signature-based, specification-based, or anomaly-based? Explain your answer.

(Maximum 10 lines.)