ℹ To pass the exam you need to get points from most sections, and approximately 2/3 of the possible total score.

☑ **You may not ask for, or receive, help from other people when answering the exam.**

You should answer the exam individually, and answer the questions on your own. It is OK to read the course material and other resources, but not to ask a friend, your group, or an online forum etc, for help.

By handing in the exam, you certify that you have followed these rules.

Select all options

□ I confirm that I will not seek assistance from anyone else to answer the exam questions.

□ I confirm that I will not use unauthorized resources to answer the exam questions.

1 If there is a vulnerability with respect to *authenticity* (the security property), the following is true:

Select one alternative:

○ Signing the hashes is a good choice for prevention

○ A reasonable protection must involve encryption/decryption

○ A trojan could reduce the accountability

○ Botnets are sometimes used for attacking this vulnerability

○ The threat must be controlled by proper access control

Maximum marks: 1

2 If there is a vulnerability with respect to *integrity,* the following is true:
Select one alternative:

○ The threat must be controlled by proper access control

○ Botnets are often used for attacking this vulnerability

○ A trojan could reduce the accountability

○ A reasonable protection must involve encryption/decryption

○ Signing the hashes is a good choice for prevention

Maximum marks: 1

3 If there is a vulnerability with respect to *availability* (the security property), the following is true:
Select one alternative:

○ Botnets are sometimes used for attacking this vulnerability

○ A reasonable protection must involve encryption/decryption

○ Signing the hashes is a good choice for prevention

○ A trojan could reduce the accountability

○ The threat must be controlled by proper access control

Maximum marks: 1

4 In a shell injection attack, which is **true**?

Select one alternative:

○ The attack can be avoided by the use of *parameterized queries*

○ The attack injects data which is interpreted as shell commands

○ If shell comment characters and boolean expressions are filtered, shell attacks are impossible

○ The attacker can inject machine code in the shell command through a stack overflow

○ Race conditions are fundamentally important to protect against shell injections

Maximum marks: 1

5 The following is **FALSE** regarding XSS (cross-site scripting) and CSRF (cross-site request forgery) attacks:

Select one alternative:

○ If CSRF attacks are made impossible, XSS attacks are still possible

○ If Javascript is disabled, all CSRF attacks are stopped

○ CSRF attacks are possible even if you follow the HTML5 standard

○ An XSS attack can be used to perform a CSRF attack

○ If all input is properly treated as data, XSS attacks can be stopped

Maximum marks: 1

6 To protect against a CSRF (cross-site request forgery) attack, which method is **most** effective?
Select one alternative:

○ To never use the "Basic" authentication scheme

○ To trust only web servers that use using TLS rather than SSL

○ To use nonces in web forms to make them unpredictable

○ To make sure that the web server follows the HTML5 standard

○ To make sure that the web server uses the latest version of MySQL

Maximum marks: 1

7 In one of the labs, you used S/MIME certificates for secure email. Which of the following is correct?
Select one alternative:

○ Digitally encrypting an email requires the certificate of the sender

○ Sending a digitally encrypted email requires the certificate of the recipient

○ Verifying a digitally signed email requires the certificate of the recipient

○ Sending a digitally signed email requires the certificate of the recipient

○ Decrypting a digitally encrypted email requires the certificate of the sender

Maximum marks: 1

8 A simple protocol for detecting modifications of a message **m** while transported between **A** and **B**, is to attach a hash code **H(m)** to the message:

1. **A** sends both **m** and **H(m)** to **B**
2. when **B** receives the two parts (call them **x** and **y**), **B** can compute **H(x)** and check that it matches **y**.

What if the following is **FALSE**?

Select one alternative:

○ The protocol does not work, in the sense that an attacker can modify **x** (replacing the message) and modify **y** (the hash code) to match it, and this is not detected by **B**.

○ An attacker **C** can fabricate data which is accepted by **B** by simply creating a new message **n** and sending it with its hash code **H(n)** to **B**.

○ The protocol can be fixed by using a fresh random nonce **n** in step 1, sending the three parts **m**, **H(m+n)**, and **n**, and in step 2 verifying that **y** is **H(x+z)** where **z** is the third part of the received message.

○ The protocol can be fixed by using a shared key **k** known only by **A** and **B**, which is hashed together with **m** in step 1 (when sending) and step 2 (when checking), i.e. using **H(m+k)** in place of **H(m)**.

○ The protocol can be fixed by using a digital signature **S(m,sk$_A$)** in place of **H(m)** in step 1, and signature verification **V(y,pk$_A$)** in step 2, where **(sk$_A$,pk$_A$)** is the key pair of **A**.

Maximum marks: 1

9 A common mechanism to detect integrity attacks is using cryptographic hash values.
What is **most** important for cryptographic hash algorithms?

Select one alternative:

○ That the hash algorithm has predictable collisions

○ That the hash algorithm is slow, to make hacking it take more time

○ That the hash algorithm is only known to the implementers, to make it harder for the attacker to hack it

○ That the hash algorithm is fast, so the user doesn't have to wait

○ That the hash algorithm has unpredictable collisions

Maximum marks: 1

10 Sandboxing is more and more often used in e.g. web browsers.
Which of the following design principles (by Saltzer et al) is **most specifically** addressed by sandboxing?

Select one alternative:

○ Economy of mechanism

○ Psychological acceptability

○ Complete mediation

○ Least common mechanism

○ Defense in depth

Maximum marks: 1

11 The terms sandboxing and virtualization can be easy to confuse. What is **false** of the following?
Select one alternative:

○ Virtualization can allow a macOS computer to run Windows, or vice versa

○ Sandboxing is (mainly) a software feature, and not helped much by hardware support

○ Virtualization abstracts underlying components

○ Sandboxing can lead to large overheads in execution time

○ Virtualization can protect the system against viruses

Maximum marks: 1

12 You should of course *never* store passwords in plain text, at any time. Instead, always use *salted hashing*. How does this work - what of the following is **true**?
Select one alternative:

○ When checking an input password, you compare its hash value with the stored salt value

○ The salt is hashed together with the password and the result is stored together with the salt

○ The salt is a nonce, and should never be saved after using it

○ It is efficient and secure to use the same salt for all your passwords as long as you keep the salt a secret

○ The size of the salt varies, and is used to make all passwords in the system the same length

Maximum marks: 1

13 Compare the entropies of different locks: a standard 3-digit combination lock, a standard 4-digit combination lock, and the Birthday lock.

Assume the following:

- the birthday lock can be set for years 00-99, months Jan-Dec, and dates 00-99.
- 3- and 4-digit locks have random codes, while Birthday locks use the birthdate of their owner,
- but you do not know who is the owner of the Birthday lock.

Which of the following is **FALSE**?

Select one alternative:

○ The entropy of the 3-digit lock is lower than the entropy of the Birthday lock.

○ The entropy of the 4-digit lock is less than 4 bits higher than that of the 3-digit lock.

○ The entropy of the 4-digit lock is approximately 3.5 bits higher than the entropy of the Birthday lock.

○ The difficulty of breaking the code of the Birthday lock is about the same as that of breaking the code of the 4-digit lock.

○ For well-contructed locks, it takes about 10 times more time to break the code of the 4-digit lock than that of the 3-digit lock.

Maximum marks: 1

14 The access control matrix can be implemented using Capability Lists (CL) or Access Control Lists (ACL). Which is better, when?

Select one alternative:

○ ACLs are better for settings where objects have owners, who can quickly see who has access to their objects

○ CLs always have a more compact representation than ACLs

○ CLs are better when the owner of an object often needs to revoke access rights to it

○ ACLs are better when subjects often need to have their rights to all objects revoked

○ ACLs often allow delegation of rights between subjects

Maximum marks: 1

15 Mandatory Access Control (MAC) differs from Discretionary Access Control (DAC). What of the following is **TRUE**?

Select one alternative:

○ "Classic" Linux file protection always supports MAC

○ Role-Based Access Control is typically DAC

○ On a Linux system with MAC, the root user can read and write any file

○ When using DAC, all objects typically have a specific owner

○ In a DAC system, central policies define the access rights

Maximum marks: 1

16 In Lab 3, you used Metasploit to attack the different systems. For a successful attack, you needed a *vulnerability*, an *exploit* and a *payload*.

Which of the following is **true** about those?

Select one alternative:

○ The exploit is used to stop the payload from being executed

○ The vulnerability always depends on the exploit

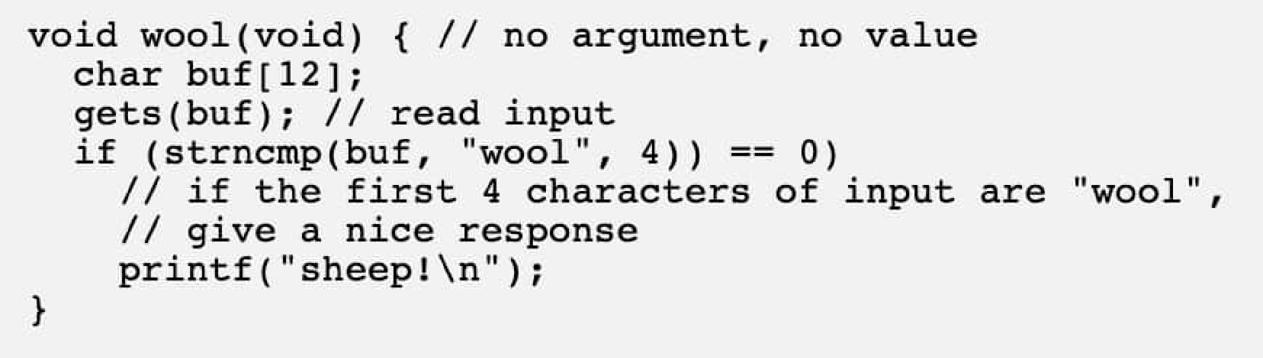
○ The payload enables the exploit, allowing the vulnerability to act

○ Which payload to select always depends on the vulnerability

○ The exploit depends on the vulnerability

Maximum marks: 1

17



```
void wool(void) { // no argument, no value
  char buf[12];
  gets(buf); // read input
  if (strncmp(buf, "wool", 4)) == 0)
    // if the first 4 characters of input are "wool",
    // give a nice response
    printf("sheep!\n");
}
```

Above is the definition of the program procedure **wool**, which is vulnerable to a stack overflow attack.

What is the main problem with the procedure, which causes the vulnerability?

Select one alternative:

○ The stack overflow is caused by the "void" argument declaration, and if **wool** is called with a suitable argument the attacker can inject arbitrary code.

○ Allocating only 12 bytes for the "buf" variable, when it should be 4 times the length of the string "wool", i.e. 24.

○ The "printf" procedure is used, which is known to have format string vulnerabilities. Instead, "puts" should have been used.

○ The "gets" procedure is used, which is known to be unsafe. Instead, "fgets" should have been used.

○ The problem is the use of "strncmp" with the argument 4, which is off-by-one since strings in C are terminated by a null character. Given a longer input can still perform a stack overflow attack.

Maximum marks: 1

18 Having security mechanisms in more than one layer is a good choice. What is **true** of the following?

Select one alternative:

○ Using "ssh tunnels" to connect to web services is preferable to using https

○ When Wifi is protected by WPA2 and the network cables are physically protected, no additional encryption is necessary

○ It is often a good idea to combine TLS with SSL in the transport layer, and WPA2 with WEP for Wifi.

○ When S/MIME is used to encrypt all email, you must still consider confidentiality attacks from the layers above

○ Protecting both the network layer and the transport layer (e.g. using both IPsec and TLS) always gives enough protection

Maximum marks: 1

19 Protecting against DDoS (distributed denial of service) attacks *based on address spoofing* can be very hard. What is **most often** an efficient protection?

Select one alternative:

○ Strictly implementing IPsec at DNS servers

○ All endpoint routers filter packets with spoofed addresses when they enter the local network, as they arrive from the Internet

○ Upgrading from IP version 4 to version 6

○ All endpoint routers filter packets with spoofed addresses when they exit the local network, as they enter the Internet

○ Upgrading your network interface to handle more incoming traffic

Maximum marks: 1

20 One of your friends takes part in a medical study at a university hospital. The data collected in the studio is going to be publicly available after it finishes, but in a *k*-anonymous database. Your friend isn't sure what this means - please help! What is true?

Select one alternative:

○ A *k*-anonymous database does not allow to identify individuals at all

○ One can identify maximally *k* many individuals in a *k*-anonymous database

○ With additional information about a person, it may be possible to identify the person in the collected data

○ A person can be identified in the data only if at least *k*-many different properties about the person are known

○ If *k* is sufficiently large, *k*-anonymity ensures that even with additional information about the persons in the data, we cannot learn anything new about them from the database

Maximum marks: 1

21 The course dealt with two types of formal anonymity/privacy: k-anonymity and differential privacy (ε-DP for some $\varepsilon \geq 0$, or simply DP).

Which of the following does **NOT** hold?

Select one alternative:

○ Anonymity is quantified, and thus limited, in both *k*-anonymity and DP

○ *k*-anonymity always has fewer privacy guarantees than DP

○ Any kind of data can be made *k*-anonymous (for some *k*) or differentially private (ε-DP for some $\varepsilon \geq 0$)

○ *k*-anonymity and DP both provide *forward secrecy*

○ Combined with additional information, differentially private data can still reveal information

Maximum marks: 1

22 In July 2020, the British newspaper The Guardian, and 16 other media organizations and Amnesty International, revealed an investigation into an advanced surveillance system developed by the NSO Group (an Israeli surveillance company) - **see https://www.theguardian.com/news/series/pegasus-project for more details**. The system, called **Pegasus**, allows remote control over both Android and iPhone units, including using the microphone, camera and GPS of the smartphone without the owner detecting it. It can also read email and other messages, photos etc. (Recall, again, the importance of "defense in depth"!)

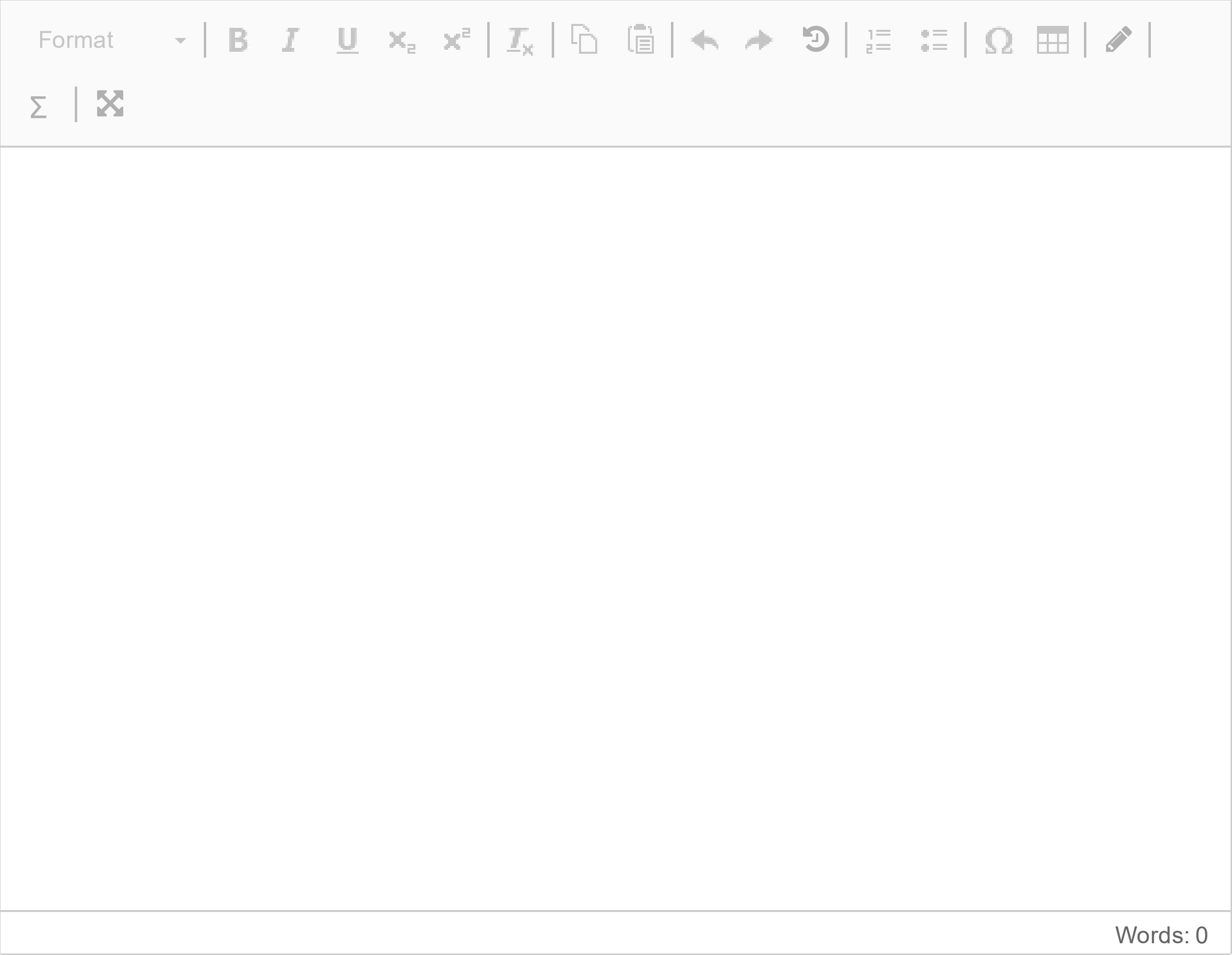
The system was allegedly developed for law enforcement and anti-terrorism, and only sold to "vetted" governments. However, it turned out to be used also for spying on pro-democracy activists and journalists investigating corruption, as well as political opponents and government critics.

Read about the case, and make an ethical analysis of it. What arguments can you find to the benefit of the Pegasus system, and what arguments can you find against it? Under what circumstances is the system permissible, and under what circumstances not?

Analyse the issue **ethically** by applying **more than one** ethical aspect (e.g. consequences, duties, virtues, freedom, fairness, or relations). **Do not** simply state "this is what I think" without referring to ethical principles.

For 1 point, you need to show reflection and use basic ethical argumentation. **For 2 points**, you need to argue showing (relevant) understanding of ethical principles. Just stating "this is what I/the writer think(s)" is not enough for any score at all. Only applying one ethical aspect (e.g. only egoism and utilitarianism which both deal with consequences) gives at most **half the score**.

Fill in your answer here



Maximum marks: 2

☑ By handing in the exam, I certify that

Select all options

□ I have answered the questions on my own.

□ I have not received help from other people

□ I have answered the exam individually

If you have any comments on the exam, please write them below:

Write here