**Part 1: Multiple-choice questions**
Mark the correct answer by *completely* filling in the corresponding square (■).
There is **only one** correct answer per question.
Each correct answer earns +1 point. Incorrect answers have a penalty of -0.25 points each. No answer neither adds nor subtracts points. Multiple marked answers are considered incorrect and will result in -0.25 points.
Use white-out fluid to change (delete) an answer (other deletion methods yield -0.25).
Read the answers carefully; the template may split the answers across columns.

**Question 1** **[Authentication]** Gru decides to build a homemade authentication system for his minions. Gru wants to try alternative approaches to passwords and listed four substitutes. Minions are very friendly, and tend to hang out in big groups to party and eat bananas. Which authentication method provides Gru with the *least* assurance of the identity of a Minion?

- [ ] User's behaviour
- [ ] Biometric
- [X] User's social ties
- [ ] Smart cards

**Question 2** **[Attacks]** A system implements Data Execution Prevention, Stack Canaries, and Address Space Layout Randomization. This guarantees that software running in this system will not contain exploitable vulnerabilities. This statement is:

- [ ] True, as these defenses eliminate control flow attacks.
- [X] False, no existing defense guarantees absence of bugs.
- [ ] False, that only happens if the system is also checked using fuzzing.
- [ ] False, that only happens if the system also implements Safe exception handlers.

**Question 3** **[Access Control]** The office Boss keeps a log of when employees enter work. To indicate they have arrived, employees must execute the script `update`. Assume that the Boss sets the permissions as follows:

```
-rwx--x---  Boss Employees update
-r-x------  Boss Employees entrylog
```

The Boss asks you whether the configuration will ensure that all arrivals get logged and employees cannot delete them. Which of the following would be a correct answer:

- [X] No, the employees cannot delete logs, but they cannot add new entries
- [ ] No, the employees cannot delete the logs, but they can add fake entries
- [ ] Yes, this configuration achieves the goal
- [ ] No, the employees can delete logs

**Question 4** **[Security Principles]** Which of the following approaches is NOT defense in depth:

- [ ] Checking a password and a code sent via SMS to access a web
- [ ] Having a bastion host behind a firewall
- [ ] Using two antivirus from different companies to analyze suspicious files
- [X] Checking the PIN and 9999 – PIN to unlock the phone, where PIN is a 4-digit number input by the user

**Question 5** **[Access Control]** Which of the following security violations is NOT caused by a confused deputy?

- [ ] A hacker performs Cross-site Request Forgery to gain access to a user's social network account
- [ ] A virus infects an email client to send spam
- [ ] A journalist tricks a banker into revealing the bank statements of a famous singer
- [X] A detective leaks information to a criminal using a covert channel

**Question 6** **[Network Security]** Alice wants to post a photo on instagram.com while at work, but she does not want her company's IT team to learn about her activities. She uses DNSSEC to obtain the IP address for instagram.com, and HTTPS to connect to the website. With this configuration, which of the following statements is true?
*Note: Assume that Alice's Instagram account is protected/private.*

- [ ] The IT team will know that Alice is trying to visit instagram.com and may prevent this by spoofing the DNS record returned to Alice.
- [ ] The IT team will not know that Alice is visiting instagram.com, since DNSSEC and HTTPS provide confidentiality.
- [ ] The IT team will know that Alice visited instagram.com, and also which photo she posted.
- [X] The IT team will know that Alice visited instagram.com, but will not know which photo she posted.

**Question 7** **[Privacy]** In which scenario does encryption of communication help?

- [ ] Hiding which record you are retrieving from the database provider
- [X] Hiding the identity of the receiver from the Internet Service Provider when sending an email via your Gmail account
- [ ] Hiding who you are calling from the Telco provider when making a phone call
- [ ] Hiding the message receiver from Telegram when using Telegram's secret chat

**Question 8** **[Security Policies]** Assume that a university uses the Bell-LaPadula model. The classification labels are public $<$ limited $<$ confidential, and the categories are {teaching, research, admin}. Which of the following statements is true:

- [ ] A principal with the security level (confidential, {teaching}) can read a file with the level (public, {admin}).
- [X] The security level that gives the most privileges for writing is {public, {}}.
- [ ] A principal with the security level (confidential, {teaching}) write to a file with the level (public, {admin}).
- [ ] The security level that gives the most privileges for writing is {public, {teaching, research, admin}}.

**Question 9** **[Malware]** Which of the following malware types is self spreading and does not require a host program?

- [ ] Trojan
- [ ] Keylogger
- [ ] Virus
- [X] Worm

**Question 10** **[Access Control]** Simon is the owner of Color OS, a simple OS that has 4 files: `red`, `yellow`, `green`, and `blue`. Simon says that a user Harry can read the file `red`, can write `yellow`, and can read and execute `blue`.
What is the capability that Simon should give to Harry?

- [ ] red: {(Harry, read, no write/execute)}, yellow: {(Harry,write, no read/execute)}, blue: {(Harry, read/execute, no write)}.
- [ ] red: {(Harry, read)}, yellow: {(Harry,write)}, blue: {(Harry, read/execute)}.
- [ ] Harry: {(red, read), (yellow,write), (green,"), (blue, read/execute)}.
- [X] Harry: {(red, read), (yellow,write), (blue, read/execute)}.

**Question 11** **[Privacy]** A VPN can hide the destination of your communication against an adversary looking at your local traffic. What would be the advantage of using Tor if a VPN can already do that?

- [X] To prevent trust centralization
- [ ] To reduce latency
- [ ] To eliminate traffic analysis attacks
- [ ] To protect against weak cryptographic keys

**Question 12** **[Authentication]** Consider the following authentication exchange in which Spock uses his password 'LongAndProsper' to prove his identity to Kirk:

```
Spock ----    (Spock, 'I want to login')     ----> Kirk
Spock <---         Hash(Spock)               ----- Kirk
Spock ---- Enc('LongAndProsper', Hash(Spock)) ----> Kirk
```

Which of the following statements is correct?

- [X] Hash(Spock) is not a good challenge because it will be used every time
- [ ] Hash(Spock) is not a good challenge because anyone can compute it
- [ ] The protocol is bad because the login is sent on the first message
- [ ] Hash(Spock) is a good challenge because hashes output random numbers

**Question 13** **[Security Policies]** Alice and Bob work for a company with a Chinese Wall security policy with clients in the following companies (each group indicates competing companies):

- Apple, Facebook, Microsoft
- HBO, Netflix, Disney
- Prada, Armani
- Lindt, Frey

Alice has previously worked on cases for Frey and Microsoft, while Bob works with Facebook and Prada. Alice is ready for a new assignment. According to the policy, which options are available to her:

- [X] Armani, Frey
- [ ] Prada, Armani
- [ ] Armani, Facebook
- [ ] Prada, Frey

**Question 14** **[Network Security]** Alice subscribed to a digital diary site. She is worried that her roommate might try to read her diary. She went through the COM-301 material to learn what attacks her roommate could launch. She made a shortlist of worrisome attacks and asked you to confirm. Which attack would you remove from the list?

- [X] BGP hijacking
- [ ] Looking over the shoulder
- [ ] ARP poisoning
- [ ] DNS hijacking

**Question 15** **[Network Security]** Alice has designed a private file-sharing protocol over HTTPS (on the same port as typical applications). Which of the following firewall types can block the file-sharing connections without impacting other protocols over HTTPS?

- [ ] Stateless
- [ ] Both stateful and stateless
- [ ] Stateful
- [X] Neither stateful nor stateless

**Question 16** **[Attacks]** Which of the following approaches does NOT help to ensure that you do not run adversarial code in the Trusted Computing Base?

- [ ] Make sure code updates are signed.
- [ ] Sanitize the compiler code before compiling updates.
- [X] Only accept updates encrypted with your public key.
- [ ] Check for new updates using an antivirus.

**Question 17** **[Software Security]** Alice has used two test cases {a = -1, b = -1},{a = 1, b = 1} to test the following program. What is the maximum level of coverage that this test achieves?

```
1. int test(int a, int b) {
2.      if(a < 0)
3.          b += 1;
4.      if(b == 1)
5.          return 0
6.      else
7.          return 1;
8. }
```

- [ ] Path coverage
- [ ] Statement coverage
- [X] Branch coverage
- [ ] Method coverage

**Question 18** **[Applied cryptography]** CBC encryption mode can not achieve:

- [X] Parallel encryption
- [ ] Limiting error propagation in transmission
- [ ] Parallel decryption
- [ ] Confidentiality

**Question 19** **[Security Principles]** Dany and Jorah decide to hide a dragon egg inside a crypt. The crypt has two locks and can be opened only if both locks get unlocked. Dany has the key to one lock and Jorah has the key to the other. What security principle did Dany and Jorah follow to decide on this mechanism?

- [ ] Least common mechanism.
- [ ] Least privilege.
- [ ] Complete mediation.
- [X] Separation of privilege.

**Question 20** **[Security Policies]** David and Robert are co-workers. They have started dating and they don't want the people in their office to know about their relationship, including the system administrators that inspect the network traffic and the corporate email server to avoid information leaks. What is a good *covert channel* to agree on the time for their next date:

- [ ] Sending the meeting time in an email through Tor
- [ ] Writing the meeting time on the door of the restroom
- [X] Encoding the meeting time in whitespaces added to the corporate emails they send to each other for work
- [ ] Sending the meeting time in an encrypted corporate email