GUIDELINES TO RESPOND TO QUESTIONS 1 AND 2

 **Selecting an answer**

 **Cancelling an answer**

You can only change your mind to cancel an answer. Once an answer has been canceled you cannot uncancel it.
To leave a question unresponded either do not circle any option, or cancel all the answers. Ambiguous answers will be considered wrong. If in doubt, ask a TA.

There is ONLY ONE correct response per question. Responses with more than one circled answer will be considered wrong!

The questions do NOT require justification, any justification will be disregarded.

Question 1 Circle the correct answer
[15pts] [+1 per correct answer; -0.5 per wrong answer]

1.1. Malware. [5 pts]

1.1.1. Eliminating buffer overflows would completely prevent the problem of backdoors.

A) True
B) False

1.1.2. An example of ransomware is malware that threatens to destroy a computer's content unless the owner pays an economical compensation.

A) True
B) False

1.1.3. Only expert hackers can use malware to do malicious actions.

A) True
B) False

1.1.4. Viruses can spread to systems even if they have no Internet connectivity.

A) True
B) False

1.1.5. A star topology with one command and control station connected to all bots enables perfect control over the bots. Therefore it is a robust choice to configure a botnet.

A) True
B) False

Lastname: **Firstname:** **SCIPER:**

1.2. Privacy. [5 pts]

1.2.1. Offering easy default privacy preferences for users does not guarantee that the users' privacy is protected from the service provider.

A) True
B) False

1.2.2. Having privacy when using digital services is important for individuals, but not for corporations or governments.

A) True
B) False

1.2.3. Encrypting communications is enough to provide privacy with respect to an adversary that can observe all Internet traffic.

A) True
B) False

1.2.4. In order to provide anonymity it is necessary that all nodes in a Tor path are owned by different people in different countries.

A) True
B) False

1.2.5. Attribute based credentials allow users to authenticate in a manner such that they are unlinkable across contexts.

A) True
B) False

1.3. Principles and basics. [5 pts]

1.3.1. The adversary's capabilities to attack a system are called vulnerabilities.

A) True
B) False

1.3.2. To comply with the principle of open design a company can release the binary code for the piece of software they sell.

A) True
B) False

1.3.3. The trusted computing base comprises all the elements in the system on which the security policy relies.

A) True
B) False

1.3.4. Following the least privilege principle implies that principals should only be given access to assets on a need-to-know basis.

A) True
B) False

1.3.5. When making a security argument about a system the threat model is not relevant.

A) True
B) False

Lastname: **Firstname:** **SCIPER:**

Question 2: <u>Circle</u> the correct answer
[18pts] [+2 per correct answer, -1 per wrong answer]

2.1 Security policies. Consider a University which uses classification labels:

```
student < professor < dean < president
```

for its documents. The process of upgrading a document from student to president is called:

A) Declassification
B) BIBA
C) Bell La Padula
D) Sanitization

2.2 Authentication. When designing a password-based authentication system, which of the following mechanisms should you use to mitigate the impact of offline attacks when the adversary gets access to the database:

A) Requiring knowledge of a nonce (random number) that has just been sent to the principal authenticating before accepting a password
B) Concatenating a salt with the password before hashing
C) Using a fast hash function
D) Store the hash of the password together with the hash of a random salt

2.3 Trusted computing. Tamper resistance, which ensures that a secure device cannot be physically opened, is a very important property to ensure:

A) Attestation
B) Isolation
C) Sealing
D) Sanitization

2.4 Malware. A honeypot is a computer which, on purpose, has vulnerabilities that can be exploited remotely so that it gets attacked. This is useful for:

A) Better understanding how malware, in particular botnets, works
B) Stopping worms from spreading
C) Amplifying the effect of viruses
D) Separating the intranet from the demilitarized zone

2.5 Access control. Consider the following program, owned by Alice, that raises an alarm whenever the temperature in a room is too low.

```
void alarm(int degrees, int hot) {
  if (degrees < 17) {
    file = open("logalarm.txt","a"); // open temperature log in append mode
    write("Freezing at %d degrees \n", degrees,file);  // log temperature
    close(file);                     // close messages log
  } else {
    hot += 1;                        // increase the count of hot days
  }
  exit;
}
```

Which of the following permission configurations will allow Bob to correctly execute the function alarm while assuring Alice that the alarm log cannot be tampered.

A) `-rwx--x--x  Alice Alice+Bob alarm`
`-rwxrw----  Alice Alice+Bob logalarm`

B) `-rws--x--x  Alice Alice+Bob alarm`
`-rwx-w----  Alice Alice+Bob logalarm`

C) `-rws--x--x  Alice Alice+Bob alarm`
`-rwxr-----  Alice Alice+Bob logalarm`

D) `-rwx-w---x  Alice Alice+Bob alarm`
`-rw-r-x---  Alice Alice+Bob logalarm`

2.6 Network security. Deep packet inspection is a firewall filtering technique that:

A) Inspects each packet header in isolation and rejects/allows depending on certain rules
B) Works equally well when traffic is sent in the clear, and when traffic is sent encrypted
C) Inspects the content of the packets and rejects/allows depending on certain rules
D) Never works

2.7 Software security. Data execution prevention (DEP):

A) Ensures that a memory page that can be read from cannot be executed
B) Ensures that a memory page that can be written to cannot be executed
C) Ensures that the stack canary is not modified
D) Is a well known fuzzing technique

Lastname: **Firstname:** **SCIPER:**

2.8 Network Security. The lack of security mechanisms in network protocols enables adversaries to change the origin of packets. This in turn enables:

A) Rerouting packets by changing the cost of routes in the BGP protocol
B) DNS hijacking attacks in which an adversary changes the content of a DNS response
C) Providing fake MAC addresses in response to an ARP request to bootstrap a man in the middle attack
D) The creation of VPNs that provide confidentiality and integrity for packets traversing the Internet

2.9 Access Control. Consider a system in which Alice can read and write to the file `xxx.sys`, can read the file `yyy.sys`, and can execute the file `zzz.sys`. Bob can read and write to `yyy.sys`, and cannot access `zzz.sys` or `xxx.sys`. Charlie can execute `yyy.sys`, can write and read `xxx.sys` and only write `zzz.sys`.

The Access Control List for this system would be:

A) xxx.sys = {Alice={read,write}, Bob={}, Charlie={read,write}}
yyy.sys = {Alice={read}, Bob={read,write}, Charlie={execute}}
zzz.sys = {Alice={execute}, Bob={}, Charlie={write}}

B) Alice = {xxx.sys={read,write},yyy.sys={read},zzz.sys={execute}}
Bob = {yyy.sys={read,write}}
Charlie = {xxx.sys={read,write},yyy.sys={execute},zzz.sys={write}}

C) xxx.sys = {Alice={read,write},Bob={read},Charlie={execute}}
yyy.sys = {Bob={read,write}}
zzz.sys = {Alice={read,write},Bob={execute},Charlie={write}}

D) None of the previous