

I5020 Computer Security

Quizz 4: Malware and protection

This assessment evaluates the following competencies:

- *CS201 – Understand software protections that can be installed on a computer system*
- *CS206 – Explain techniques that can be used to protect a system against malware*

Three affirmations are given for each assessed competency. For each of them, you have to decide whether it is true or false. To get a star for the competency, you must have the correct answer for the three affirmations.

CS201	True	False
An anti-malware system can become the source of a DoS attack on the system.	<input type="checkbox"/>	<input type="checkbox"/>
It is possible to use encryption techniques to detect if a file has been corrupted and therefore probably infected by a virus or any other malware.	<input type="checkbox"/>	<input type="checkbox"/>
It is possible to monitor the system calls to detect some kinds of viruses or other malwares.	<input type="checkbox"/>	<input type="checkbox"/>

CS206	True	False
Network communications sniffing can help detecting malware, namely by identifying signatures of their operations.	<input type="checkbox"/>	<input type="checkbox"/>
A technique to prevent malware is to block some operations on a host and ask the user if he/she is the initiator or these “critical” operations.	<input type="checkbox"/>	<input type="checkbox"/>
Checking the values of each pixel of the screen to detect patterns revealing the operations of a malware is a relevant and efficient malware detection technique.	<input type="checkbox"/>	<input type="checkbox"/>