Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

Retake the assignment in **7h 54m**

GRADE

100%

Module 1 Quiz

LATEST SUBMISSION GRADE

100%

1. A malicious worm program is characterized by the following fundamental attribute:

1 / 1 point

○ Local installation with expert system administration

○ Multi-stage provisioning based on simple tools

● Auto-propagation without human intervention

○ Simpler design than a Trojan horse program

○ All the above

✓ **Correct**

Correct! A worm program is characterized by the ability to propagate automatically without the assistance of a human being.

2. Embedding a trap door into a login program results in which of the following:

1 / 1 point

○ A trap door program with the potential to lock out authorized users

● A Trojan horse

○ A compliant version of the code with respect to some process frameworks

○ An improved version of the login program with enhanced secret access

○ A login program that requires encryption support

Correct

✓ Correct! A trap door turns a login program into a Trojan horse.

3. Learning the incredibly easy, but devastatingly effective techniques for hacking an old soda machine is instructive, because it exemplifies which of the following properties of cyber security?

1 / 1 point

● Simple attacks might prompt complex redesigns

○ Security fixes might be simple and effective

○ Security physical systems are simpler than you would think

○ No system can ever be secure

✓ **Correct**

Correct! The simplicity of old soda machine hacks contrasted with the ultimate fix, which was a total redesign of how vending machines operate.

4. Which of the following statements is true?

1 / 1 point

○ Dirty compilers are always written from clean code.

○ Dirty compilers never produce clean code.

● Dirty code is sometimes produced by clean compilers.

○ Clean code has no real difference from dirty code.

○ Dirty code is always produced by dirty developers.

✓ **Correct**

Correct! Developers might write dirty source code which would result in dirty code from a clean compiler.

5. Cyber adversary motivation does not include which of the following:

1 / 1 point

○ Curiosity

○ Money

○ Politics

○ Fame

● None of the above

✓ **Correct**

Correct! All the listed examples are clearly found as motivations for cyber adversaries.

6. Remote exploitation of an unaltered vehicle by hackers is enabled by which of the following design decisions:

1 / 1 point

○ Being careless about the so-called “on-board bus architecture”

○ Not enforcing separation between on-board entertainment and safety systems

○ Using older, unsafe programming languages

● All of the above

✓ **Correct**

Correct! Each of the vehicle design decisions listed contribute to the vulnerabilities exploited by hackers.

7. Which of the following is a reasonable conclusion that one might draw by studying Unix kernel attacks such as the old IFS exploit?

1 / 1 point

○ Open source code cannot help in the design of an attack

○ Set-uid-to-root should be used more extensively in OS design

● Seeing open source code might help one design an attack.

○ Setting variables by users of an OS should be encouraged

○ The object code for an OS runtime system cannot be understood

Correct

✓ Correct! The ability to freely peruse the source code of an OS kernel can be valuable in the design of an effective attack.

8. The root cause of some discovered cyber security vulnerability might reasonably be which of the following: **1 / 1 point**

● The developers didn’t invest enough money during development

○ The designers had too much technical training

○ The government regulators were smarter than the developers expected

○ It was hidden and therefore acceptable to leave in place

○ All of the above

✓ **Correct**

Correct! As simple as it sounds, not investing enough money in the development can result in security errors.

9. Buffer overflow attacks might best be avoided by which of the following preventive approaches: **1 / 1 point**

○ Picking better variable names

● Using languages with strong type enforcement

○ Improving in-line comments

○ Replacing call-by-value with call-by-name

○ None of the above

✓ **Correct**

Correct! Strong type enforcement reduces the likelihood that declared variables might be stuffed with values that do not fit the defined type.

10. The integrity threat can be exemplified by which of the following scenarios: **1 / 1 point**

○ Every customer record is stolen by hackers

○ Every customer record is exposed by nation states

● Customer records were hidden, but one might have been slightly garbled

○ The entire company database was posted to the Internet

○ None of the above

✓ **Correct**

Correct! If any data has its correctness or validity degraded in any way, then an integrity threat has been realized.