Congratulations! You passed!

Grade received 100% | Latest Submission Grade 100% | To pass 80% or higher

Go to next item

1. In the Payment Card Industry Data Security Standard (PCI DSS), what are the requirements for the "regularly monitor and test networks" objective? Select all that apply 1 / 1 point

- [x] Track and monitor all access to network resources and cardholder data
  - Correct
- [x] Regularly test security systems and processes
  - Correct
- [ ] Encrypt the transmission of cardholder data across open public networks
- [ ] Develop and maintain secure systems and applications

2. What tools can be used to discover vulnerabilities or dangerous misconfigurations in systems and networks? 1 / 1 point

- ( ) Bastion hosts
- ( ) Antimalware software
- ( ) Firewalls
- (•) Vulnerability scanners
  - Correct

3. _____ is the practice of attempting to break into a system or network for the purpose of verifying the systems in place. 1 / 1 point

- ( ) Network probing
- ( ) Security assessment
- ( ) Vulnerability scanning
- (•) Penetration testing
  - Correct

4. Which of the following devices are considered a risk when storing confidential information? 1 / 1 point

Select all that apply.

- [ ] Encrypted portable hard drives
- [ ] Limited access file shares
- [x] USB sticks
  - Correct
- [x] CD drives
  - Correct

5. Which of the following are bad security habits commonly seen amongst employees in the workplace? Select all that apply. 1 / 1 point

- [x] Password on a post-it note
  - Correct
- [ ] Lock desktop screen
- [x] Leave laptop logged in and unattended
  - Correct
- [ ] Log out of website session

6. Which of the following are ways to prevent email phishing attacks against user passwords? Select all that apply. 1 / 1 point

- [x] User education
  - Correct
- [x] Spam filters
  - Correct
- [ ] Virtual private network
- [ ] Cloud email

7. What is a quick way of evaluating a third party's security? 1 / 1 point

- ( ) A manual evaluation of all security systems
- ( ) A signed contract

- (selected) A security assessment questionnaire
- ( ) A comprehensive penetration testing review

Correct

8. What are some things that are generally included on a third party security assessment report? Select all that apply — 1 / 1 point

- [x] Third party security audit results

Correct

- [ ] User reviews
- [ ] Customer feedback scores
- [x] Penetration testing results

Correct

9. Management wants to build a culture where employees keep security in mind. Employees should be able to access information freely and provide feedback or suggestions without worry. Which of these are great ideas for this type of culture? Select all that apply. — 1 / 1 point

- [x] Designated mailing list

Correct

- [x] Posters promoting good security behavior

Correct

- [ ] Desktop monitoring software
- [ ] Bring your own device

10. Once the scope of the incident is determined, the next step would be _____. — 1 / 1 point

- (selected) containment
- ( ) escalation
- ( ) documentation
- ( ) remediation

Correct