System Hardening
Application Hardening
Graded Assessments
Quiz: Defense in Depth
10 questions

Congratulations! You passed!

Grade received 97.50%

Latest Submission Grade 97.50%

To pass 80% or higher

Go to next item

Defense in Depth

Quiz • 40 min

Submit your assignment

Due Jun 25, 11:59 PM +08 Attempts 3 every 24 hours

Receive grade

To Pass 80% or higher

Your grade 97.50%

View Feedback

We keep your highest score

Try again

1. What is the co[illegible]tors in a corporate network? **1 / 1 point**

- The Access Control List (ACL)
- The attack surface
- The risk
- The antivirus software

Correct

Like Dislike Report an issue

2. Which of these host-based firewall rules help to permit network access from a Virtual Private Network (VPN) subnet? **1 / 1 point**

- Active Directory
- Group Policy Objects (GPOs)
- Secure Shell (SSH)
- Access Control Lists (ACLs)

Correct

3. When looking at aggregated logs, you are seeing a large percentage of Windows hosts connecting to an Internet Protocol (IP) address outside the network in a foreign country. Why might this be worth investigating more closely? **1 / 1 point**

- It can indicate what software is on the binary whitelist
- It can indicate a malware infection
- It can indicate log normalization
- It can indicate ACLs are not configured correctly

Correct

4. What are the two main issues with antivirus software? Select all that apply. **1 / 1 point**

- [x] They depend on antivirus signatures distributed by the antivirus software vendor.

  Correct

- [x] They depend on the antivirus vendor discovering new malware and writing new signatures for newly discovered threats.

  Correct

- [ ] They depend on the IT support professional to discover new malware and write new signatures.
- [ ] There are no issues with antivirus software.

5. If a full disk encryption (FDE) password is forgotten, what can be incorporated to securely store the encryption key to unlock the disk? **1 / 1 point**

- Key escrow
- Application hardening
- Secure boot
- Application policies

Correct

6. What does applying software patches protect against? Select all that apply. **0.75 / 1 point**

- [ ] MITM attacks
- [x] Undiscovered vulnerabilities

  Correct

- [x] Data tampering

  This should not be selected

  Please review the video about software patch management

- [x] Newly found vulnerabilities

  Correct

7. When installing updates on critical infrastructure, it's important to be what? **1 / 1 point**

- Careful
- Fast
- Patient
- Calm

Correct

8. Why is it risky if you wanted to make an exception to the application policy to allow file sharing software? **1 / 1 point**

- The software can shrink attack vectors
- The software can normalize log data
- The software could be infected with malware
- The software could disable full disk encryption (FDE)

Correct

9. What is a defining characteristic of a defense-in-depth strategy to IT security? **1 / 1 point**

- Encryption
- Confidentiality
- Multiple overlapping layers of defense
- Strong passwords

Correct

10. Ideally, an attack surface is ___ **1 / 1 point**

- as small as possible.
- frequently updated.
- open and defended.
- as large as possible.

Correct