Back **Defense in Depth**
Graded Quiz • 40 min

Due Jun 25, 11:59 PM +08

System Hardening

Application Hardening

Graded Assessments

✓ **Quiz:** Defense in Depth
10 questions

Congratulations! You passed!

Grade received 97.50% **Latest Submission Grade** 90% **To pass** 80% or higher

Retake the assignment in **23h 53m**

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

Try again

Retake the quiz in **23h 53m**

Receive grade

To Pass 80% or higher

Your grade
97.50%

View Feedback

We keep your highest score

Like Dislike Report an issue

1. What is a class of vulnerabilities that are unknown before they are exploited? **1 / 1 point**

○ ACLs

○ Attack Surfaces

○ Attack Vectors

● Zero-day

✓ **Correct**

2. A core authentication server is exposed to the internet and is connected to sensitive services. What are some measures you can take to secure the server and prevent it from getting compromised by a hacker? Select all that apply. **0.5 / 1 point**

□ Designate as a bastion host

☑ Secure firewall

✓ **Correct**

☑ Access Control Lists (ACLs)

✓ **Correct**

☑ Patch management

☒ **This should not be selected**
Please review the video about host based firewalls

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 log normalization

○ It can indicate what software is on the binary whitelist

● It can indicate a malware infection

○ 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**

□ They depend on the IT support professional to discover new malware and write new signatures.

□ There are no issues with antivirus software.

☑ They depend on antivirus signatures distributed by the antivirus software vendor.

✓ **Correct**

☑ They depend on the antivirus vendor discovering new malware and writing new signatures for newly discovered threats.

✓ **Correct**

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**

○ Secure boot

○ Application policies

● Key escrow

○ Application hardening

✓ **Correct**

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

☑ Undiscovered vulnerabilities

✓ **Correct**

□ MITM attacks

□ Data tampering

☑ Newly found vulnerabilities

✓ **Correct**

7. How can software management tools like Microsoft SCCM help an IT professional manage a fleet of systems? Select all that apply **0.75 / 1 point**

☑ Confirm update installation

✓ **Correct**

☑ Detect and prevent malware on managed devices

☒ **This should not be selected**
Please review the video about software patch management

☑ Analyze installed software across multiple computers

✓ **Correct**

☑ Force update installation after a specified deadline

✓ **Correct**

8. What is the best way to avoid personal, one-off software installation requests? **1 / 1 point**

○ A strict no-installation policy

● A clear application whitelist policy

○ An application honor code policy

○ An accept-all application policy

✓ **Correct**

9. Securely storing a recovery or backup encryption key is referred to as _______. **1 / 1 point**

○ Key obfuscation

○ Key backup

● Key escrow

○ Key encryption

✓ **Correct**

10. Which of the following are potential attack vectors? Select all that apply **0.75 / 1 point**

☑ Network interfaces

✓ **Correct**

☑ Passwords

☒ **This should not be selected**
Please review the video about disabling unnecessary components

☑ Network protocols

✓ **Correct**

☑ Email attachments

✓ **Correct**