Congratulations! You passed!
TO PASS 80% or higher

Keep Learning

GRADE 100%

System Hardening

TOTAL POINTS 10

1. What is an attack vector? — 1 / 1 point

- ○ The direction an attack is going in
- ◉ A mechanism by which an attacker can interact with your network or systems
- ○ The classification of attack type
- ○ The severity of the attack

Correct
Nice job! An attack vector can be thought of as any route through which an attacker can interact with your systems and potentially attack them.

2. Disabling unnecessary components serves which purposes? Check all that apply. — 1 / 1 point

- ☐ Making a system harder to use
- ☑ Closing attack vectors

Correct
Right on! Every unnecessary component represents a potential attack vector. The attack surface is the sum of all attack vectors. So, disabling unnecessary components closes attack vectors, thereby reducing the attack surface.

- ☐ Increasing performance
- ☑ Reducing the attack surface

Correct
Right on! Every unnecessary component represents a potential attack vector. The attack surface is the sum of all attack vectors. So, disabling unnecessary components closes attack vectors, thereby reducing the attack surface.

3. What's an attack surface? — 1 / 1 point

- ○ The total scope of an attack
- ◉ The combined sum of all attack vectors in a system or network
- ○ The payload of the attack
- ○ The target or victim of an attack

Correct
Yep! The attack surface describes all possible ways that an attacker could interact and exploit potential vulnerabilities in the network and connected systems.

4. A good defense in depth strategy would involve deploying which firewalls? — 1 / 1 point

- ○ Network-based firewalls only
- ◉ Both host-based and network-based firewalls
- ○ No firewalls
- ○ Host-based firewalls only

Correct
You got it! Defense in depth involves multiple layers of overlapping security. So, deploying both host- and network-based firewalls is recommended.

5. Using a bastion host allows for which of the following? Select all that apply. — 1 / 1 point

- ☐ Running a wide variety of software securely
- ☑ Having more detailed monitoring and logging

Correct
Woho! Bastion hosts are special-purpose machines that permit restricted access to more sensitive networks or systems. By having one specific purpose, these systems can have strict authentication enforced, more firewall rules locked down, and closer monitoring and logging.

- ☑ Applying more restrictive firewall rules

Correct
Woho! Bastion hosts are special-purpose machines that permit restricted access to more sensitive networks or systems. By having one specific purpose, these systems can have strict authentication enforced, more firewall rules locked down, and closer monitoring and logging.

- ☑ Enforcing stricter security measures

Correct
Woho! Bastion hosts are special-purpose machines that permit restricted access to more sensitive networks or systems. By having one specific purpose, these systems can have strict authentication enforced, more firewall rules locked down, and closer monitoring and logging.

6. What benefits does centralized logging provide? Check all that apply. — 1 / 1 point

- ☑ It allows for easier logs analysis.

Correct
Yes! Centralized logging is really beneficial, since you can harden the log server to resist attempts from attackers trying to delete logs to cover their tracks. Keeping logs in place also makes analysis on aggregated logs easier by providing one place to search, instead of separate disparate log systems.

- ☐ It blocks malware infections.
- ☐ It prevents database theft.
- ☑ It helps secure logs from tampering or destruction.

Correct
Yes! Centralized logging is really beneficial, since you can harden the log server to resist attempts from attackers trying to delete logs to cover their tracks. Keeping logs in place also makes analysis on aggregated logs easier by providing one place to search, instead of separate disparate log systems.

7. What are some of the shortcomings of antivirus software today? Check all that apply. — 1 / 1 point

- ☑ It can't protect against unknown threats.

Correct
Awesome! Antivirus software operates off a blacklist, blocking known bad entities. This means that brand new, never-before-seen malware won't be blocked.

- ☐ It only protects against viruses.
- ☐ It's very expensive.
- ☐ It only detects malware, but doesn't protect against it.

8. How is binary whitelisting a better option than antivirus software? — 1 / 1 point

- ○ It has less performance impact.
- ○ It's cheaper.
- ◉ It can block unknown or emerging threats.
- ○ It's not better. It's actually terrible.

Correct
That's right! By blocking everything by default, binary whitelisting can protect you from the unknown threats that exist without you being aware of them.

9. What does full-disk encryption protect against? Check all that apply. — 1 / 1 point

- ☑ Tampering with system files

Correct
Excellent job! With the contents of the disk encrypted, an attacker wouldn't be able to recover data from the drive in the event of physical theft. An attacker also wouldn't be able to tamper with or replace system files with malicious ones.

- ☐ Malware infections
- ☑ Data theft

Correct
Excellent job! With the contents of the disk encrypted, an attacker wouldn't be able to recover data from the drive in the event of physical theft. An attacker also wouldn't be able to tamper with or replace system files with malicious ones.

- ☐ IP spoofing attacks

10. What's the purpose of escrowing a disk encryption key? — 1 / 1 point

- ○ Providing data integrity
- ◉ Performing data recovery
- ○ Protecting against unauthorized access
- ○ Preventing data theft

Correct
Yep! Key escrow allows the disk to be unlocked if the primary passphrase is forgotten or unavailable for whatever reason.