1. What are the purposes of performing a patch update for security hardening? Select all that apply.

1 / 1 point

☐ Requiring a user to verify their identity to access a system or network.

☐ Preventing malicious actors from flooding a network.

☑ Fixing known security vulnerabilities in a network or services.

✓ **Correct**

☑ Upgrading an operating system to the latest software version.

✓ **Correct**

2. When performing security hardening, what is the goal with regards to the attack surface?

1 / 1 point

○ Hide the attack surface

○ Mirror the attack surface

◉ Reduce the attack surface

○ Augment the attack surface

✓ **Correct**

3. Fill in the blank: Installing security cameras is an example of a _____ security hardening practice.

1 / 1 point

◉ physical

○ software-based

○ network-focused

○ virtual

✓ **Correct**

4. A company's executive team approves a proposal by the security director. The proposal involves security professionals simulating an attack on the company's systems in order to identify vulnerabilities. What does this scenario describe?

1 / 1 point

◉ Penetration testing

○ A Distributed Denial of Service (DDoS) attack

○ Packet sniffing

○ The Ping of Death

✓ **Correct**

5. Which of the following statements accurately describe OS hardening tasks? Select three answers.

1 / 1 point

☑ OS hardening is a set of procedures that maintain and improve OS security.

✓ **Correct**

☑ Some OS hardening tasks are performed at regular intervals, while others are performed only once.

✓ **Correct**

☐ Multi-factor authentication is a security measure requiring users to change passwords every month.

☑ When disposing of software, it is a best practice to delete any unused applications.

✓ **Correct**

6. Fill in the blank: A/An _____ is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates

1 / 1 point

◉ baseline configuration

○ virtual private network installation

○ internet control message protocol update

○ network segment

✓ **Correct**

7. Multi-factor authentication (MFA) is an example of which type of hardening practice?

0 / 1 point

- ○ OS hardening
- ◉ Network hardening
- ○ Attack surface
- ○ Network log analysis

> ⊗ **Incorrect**
> Please review the video about OS hardening ↗.

8. In what way might port filtering be used to protect a network from an attack?

1 / 1 point

- ○ To create isolated subnets for different departments in an organization
- ○ To increase the attack surface in a network
- ◉ To disable unused ports in order to reduce the attack surface
- ○ To inspect, analyze, and react to security events based on their priority

> ⊘ **Correct**

9. A security team considers the best way to handle the different security zones within their network. They prioritize protecting the restricted zone by separating from the rest of the network and ensuring it has much higher encryption standards. What does this scenario describe?

1 / 1 point

- ○ Cloud hardening
- ○ Patch updating
- ◉ Network segmentation
- ○ Penetration testing

> ⊘ **Correct**

10. What is one key similarity between regular web servers and cloud servers?

1 / 1 point

- ○ In both, all applications are stored together, regardless of their age.
- ◉ They both require proper maintenance and security hardening.
- ○ In both, all data and application are stored together, regardless of their service category.
- ○ They both use baseline images stored in the cloud to compare data.

> ⊘ **Correct**