The Common Criteria make up an international standard for computer security certification and testing.

Question 1 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 2**(1 point)

*Saved*

Which of the following is a common defensive device found in defense-in-depth designs?

Question 2 options:

|  |  |
| --- | --- |
|  | intrusion prevention system (IPS) |
|  | demilitarized zone (DMZ) |
|  | wireless access point (WAP) |
|  | storage area network (SAN) |

**Question 3**(1 point)

*Saved*

Which of the following provides standards and a technical framework from the National Security Agency?

Question 3 options:

|  |  |
| --- | --- |
|  | Common Criteria (CC) |
|  | Internet Engineering Task Force (IETF) |
|  | IT Infrastructure Technical Framework (ITITF) |
|  | Information Assurance Directorate (IAD) |

**Question 4**(1 point)

*Saved*

When considering C-I-A in the context of defense in depth, which of the following is true?

Question 4 options:

|  |  |
| --- | --- |
|  | The more you protect confidentiality, the harder it becomes to provide provable integrity. |
|  | The more you protect confidentiality, the easier it becomes to provide provable integrity. |
|  | The more you protect integrity, the harder it becomes to provide effective technical controls. |
|  | The more you protect integrity, the easier it becomes to provide effective technical controls. |

**Question 5**(1 point)

*Saved*

System administrator privileges are one of the most heavily protected and monitored assets in any successful defense-in-depth design.

Question 5 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 6**(1 point)

*Saved*

DoD Instruction 8500.01E specifically addresses defense in depth.

Question 6 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 7**(1 point)

*Saved*

In traditional information security operations, security professionals can guarantee their employers that there are many ways to be perfectly secure.

Question 7 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 8**(1 point)

*Saved*

Security policies and procedures are found in which layer of the US-CERT's defense-in-depth strategy?

Question 8 options:

|  |  |
| --- | --- |
|  | network |
|  | security risk |
|  | operational |
|  | host |

**Question 9**(1 point)

*Saved*

Device integrity helps to ensure that attackers have not modified or changed systems and devices.

Question 9 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 10**(1 point)

*Saved*

The concept of providing defense in depth by layering protective capabilities has been in use for thousands of years.

Question 10 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 11**(1 point)

*Saved*

Layered defenses make it more likely that a single attack can completely compromise a network or system.

Question 11 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 12**(1 point)

*Saved*

The National Security Agency's (NSA's) people-based strategy is based on a framework that includes which of the following?

Question 12 options:

|  |  |
| --- | --- |
|  | management training, periodic employee credit checks, and biometric authentication |
|  | policies and procedures, training and awareness, and system administration |
|  | key management, public key infrastructure (PKI), and intrusion detection |
|  | validating configurations, ensuring that patching occur, and network monitoring |

**Question 13**(1 point)

*Saved*

Some of the biggest problems with defense in depth result from tradeoffs it creates simply because of the way it must be implemented.

Question 13 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 14**(1 point)

*Saved*

When designing defense in depth, which of the following is one of the hardest challenges to defend against?

Question 14 options:

|  |  |
| --- | --- |
|  | administrative change |
|  | operational change |
|  | technological change |
|  | managerial change |

**Question 15**(1 point)

*Saved*

The term *self-replicating network* implies that the network is able to respond to attacks by changing rules, modifying how it is configured, and otherwise responding to problems.

Question 15 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 16**(1 point)

*Saved*

Which of the following ensures that information has not been modified by unauthorized users or systems, and remains accurate and consistent?

Question 16 options:

|  |  |
| --- | --- |
|  | authentication |
|  | nonrepudiation |
|  | encryption |
|  | integrity |

**Question 17**(1 point)

*Saved*

Defense in depth has disadvantages for those who are defending a network because complex, more expensive defenses are required in each layer.

Question 17 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 18**(1 point)

*Saved*

Which of the following is the ability to validate that the system or user is who he or she claims to be?

Question 18 options:

|  |  |
| --- | --- |
|  | authentication |
|  | nonrepudiation |
|  | encryption |
|  | integrity |

**Question 19**(1 point)

*Saved*

Which of the following could result during an attack when there isn't sufficient internal defense?

Question 19 options:

|  |  |
| --- | --- |
|  | The firewalls will not block an attack. |
|  | The DMZ will allow malicious traffic. |
|  | The attackers can pivot, attacking other systems. |
|  | The employees will lose all Internet connectivity. |

**Question 20**(1 point)

*Saved*

Which of the following areas of the National Security Agency's (NSA's) Information Assurance and defense in-depth conceptual model emphasizes the need to defend in multiple places at once?

Question 20 options:

|  |  |
| --- | --- |
|  | operation-based strategy |
|  | administration-based strategy |
|  | integrity-based strategy |
|  | technology-based strategy |

**Question 21**(1 point)

*Saved*

Authentication codes are cryptographic functions that take a block of data and perform operations on it to produce a fixed-length string of characters.

Question 21 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 22**(1 point)

*Saved*

Self-defending systems are intended to adapt to prevent attacks by monitoring systems, users, and network traffic.

Question 22 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 23**(1 point)

*Saved*

Unlike traditional warfare, cyberwarfare is fought only defensively.

Question 23 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 24**(1 point)

*Saved*

The National Security Agency's Information Assurance Directorate (IAD) provides an extensive, detailed guide intended to provide guidance on how to counter attacks by non-nation-states.

Question 24 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 25**(1 point)

*Saved*

Defense in depth is the idea that defenses should have more than a single layer of protection between an attacker and the protected systems, data, or networks.

Question 25 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 26**(1 point)

*Saved*

Which of the following best describes dynamic defense?

Question 26 options:

|  |  |
| --- | --- |
|  | Defense that remains constant no matter what risk or threat arises |
|  | Defense-in-depth components that are updated by the vendor regularly |
|  | Defense strategy changes that can be approved in a short period of time |
|  | Defense that can change in reaction to threats and new risks |

**Question 27**(1 point)

*Saved*

Which of the following is true of endpoints, such as laptops, tablets, and mobile devices?

Question 27 options:

|  |  |
| --- | --- |
|  | Infected endpoint devices cannot infect the network because they only connect wirelessly. |
|  | Security for these devices can be incredibly complex due to the wide variety of devices. |
|  | Security for these devices is extremely simple because there are only a few operating systems. |
|  | Endpoint devices do not need to be secured because they have their own security. |

**Question 28**(1 point)

*Saved*

A certificate authority that issues and verifies certificates is part of which of the following?

Question 28 options:

|  |  |
| --- | --- |
|  | public key infrastructure (PKI) |
|  | demilitarized zone (DMZ) |
|  | disaster recovery plan (DRP) |
|  | Password Authentication Protocol (PAP) |

**Question 29**(1 point)

*Saved*

Which of the following best describes a network enclave?

Question 29 options:

|  |  |
| --- | --- |
|  | The perimeter defenses that protect the internal network of an organization |
|  | A separated portion of a network that isolates systems based on rules or purpose |
|  | A separated, publically available network that contains an organization's Web servers |
|  | A physically separated area of an organization that holds the networking equipment |

**Question 30**(1 point)

*Saved*

Many of the controls on the SANS Top 20 Critical Security Controls list match those on the National Security Agency's Information Assurance Directorate (IAD) list.

Question 30 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 31**(1 point)

*Saved*

Key management and public key infrastructure are a part of which of the following strategy?

Question 31 options:

|  |  |
| --- | --- |
|  | authentication |
|  | authorization |
|  | encryption |
|  | obfuscation |

**Question 32**(1 point)

*Saved*

Damage containment ensures that credentials are not exposed or misused.

Question 32 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 33**(1 point)

*Saved*

DoD Instruction 8500.01E requires which of the following?

Question 33 options:

|  |  |
| --- | --- |
|  | Limitation and control of network ports, protocols, and services |
|  | Inventory of authorized and unauthorized software |
|  | Implementation of antiexploitation features to help prevent buffer overflow and other attacks |
|  | The ability of technology components to self-defend and optimize with minimal human intervention |

**Question 34**(1 point)

*Saved*

The daily activities of a defense-in-depth strategy occur in the technology portion of the National Security Agency's defense-in-depth conceptual model.

Question 34 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 35**(1 point)

*Saved*

Which of the following is the first step in computer network defense (CND) strategies?

Question 35 options:

|  |  |
| --- | --- |
|  | Implementing security polices |
|  | Enumerating the organizational threats |
|  | Evaluating the organizational risks |
|  | Identifying the likely attackers |

**Question 36**(1 point)

*Saved*

The National Security Agency (NSA) C-I-A triad consists of which of the following principles?

Question 36 options:

|  |  |
| --- | --- |
|  | confidentiality, integrity, and availability |
|  | communication, interaction, and agreement |
|  | cryptology, integration, and authentication |
|  | collection, investigation, and apprehension |

**Question 37**(1 point)

*Saved*

Which of the following best describes application whitelisting?

Question 37 options:

|  |  |
| --- | --- |
|  | An antivirus file reputation service that uses centralized antivirus company data |
|  | A secure and available transport method that allows data to be sent without being compromised |
|  | A technological solution that uses known, allowed programs to run on trusted systems |
|  | A built-in operating system feature that helps prevent buffer overflows |

**Question 38**(1 point)

*Saved*

The US-CERT's defense-in-depth strategy for protecting individual systems against a sample attack contains which of the following layers?

Question 38 options:

|  |  |
| --- | --- |
|  | administrative, security risk, and physical |
|  | operational, network, and security risk |
|  | technical, host, and network |
|  | operational, technical, and administrative |

**Question 39**(1 point)

*Saved*

The Department of the Navy computer network defense (CND) defense-in-depth strategy combines elements at the host, network, network edge, and policy layer.

Question 39 options:

|  |  |
| --- | --- |
|  | True |
|  | False |

**Question 40**(1 point)

*Saved*

Using technological factors to attack systems was an important part of the Stuxnet malware attack on Iranian nuclear facilities.

Question 40 options:

|  |  |
| --- | --- |
|  | True |
|  | False |