



Answer



Copy

Explain it

Summarise

Translate

Grammar checker

Disable



Disable until next visit

Disable for this page

Disable for this website

Disable globally

You can re-enable in setting

**New Year 2025 Offer. Valid till Midnight. Prices Slashed 50%. Get Additional
25% OFF on enrolling in 2 or more courses. Use Code : SAVINGS25**

[Skip to content](#)



SKILLCERTPRO

IT CERTIFICATION TRAININGS



Products search

[All Courses](#)

[Contact Us](#)

[MY ACCOUNT](#)



SKILLCERTPRO

IT CERTIFICATION TRAININGS

[Cart/\\$0.00](#)

[Main Menu](#)

[/ Information Security](#) / [By SkillCertPro](#)

Practice Set 2

Your results are here!! for" CISSP Practice Test 2 "

0 of 58 questions answered correctly

Your time: 00:00:07

Your Final Score is : 0

You have attempted : 0

Number of Correct Questions : 0 and scored 0

Number of Incorrect Questions : 0 and Negative marks 0

Average score	<div><div></div></div> 65.61%
Your score	<div><div></div></div> 0%

You can review your answers by clicking view questions.

Important Note : Open Reference Documentation Links in New Tab (Right Click and Open in New Tab).

[\[Restart Test\]](#) [\[View Answers\]](#)

1
2
3
4
5
6
7
8
9
10
11
12
13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53


54

55

56

57

58

 Answered

 Review

[Review question]

[Pause]

[Summary]

1. Question

In a new implementation we have chosen to use Redundant Array of Independent Disks (RAID) 0 on a server, what does tell us about the disk configuration?

Striping without parity.

Mirror set: 2 identical hard disks.

Mirroring with parity.

Striping with parity.

Unattempted

RAID 0: Striping without mirroring or parity; no fault tolerance; only provides faster read write speed; requires at least 2 disks

2. Question

We are choosing a site to build a new data center and offices in. Which of these would NOT be a valid security concern?

How pretty the area is.

How good the utilities are.

Whether the area is prone to flooding.

Crime in the area.

Unattempted

Site Selection: Greenfield: Not built on yet; undeveloped land. Topography: the physical shape of the landscape – hills, valleys, trees, streams. Most often used

in military sites where they can leverage (sometimes by altering) the topology for higher security. Utilities: How reliable is the power, the internet in the area? Crime: How high are the crime rates in the area? How close are the police?

3. Question

We are using DAC (Discretionary Access Control) in our organization. What is DAC based on?

The discretion of the object owner.

Labels and clearance.

The job role of the user.

IF/THEN statements.

Unattempted

DAC (Discretionary Access Control): Often used when Availability is most important. Access to an object is assigned at the discretion of the object owner. The owner can add, remove rights, commonly used by most OS'. Uses DACL's (Discretionary ACL), based on user identity.

4. Question

We are building a new data center, and we will use the new site for real-time backups of our most critical systems. In the conduits between the demarc and the new server room, there are a lot of power cables. Which type of networking cables would be the BEST to use between the demarc and the server room?

Fiber Ethernet.

Wireless.

Coax copper.

Copper Ethernet.

Unattempted

Fiber Optic Cables are not susceptible to EMI, so the cables can be run next to power cables with no adverse effects.

5. Question

There are many types of financial motivated attacks. Which of these attacks is normally not of them?

Ransomware attacks.

Stealing trade secrets.

Distributed Denial Of Service (DDOS) attacks.

Phishing attacks.

Unattempted

Distributed Denial Of Service (DDOS) normally does not benefit an attacker financially, the motivation is often revenge, disagreement with a decision or just to prove the attacker can.

6. Question

Attackers are using Distributed Denial Of Service (DDOS) attacks on our organization using UDP flood. How does that type of Distributed Denial Of Service (DDOS) attack work?

Sends many IP addresses to a router.

Sends many ethernet frames, each with different media access control addresses.

Sends many user datagram protocol packets.

Opens many TCP sessions but never replies to the ACK from the host.

Unattempted

UDP (User datagram protocol) floods are used frequently for larger bandwidth Distributed Denial Of Service (DDOS) attacks because they are connectionless and it is easy to generate UDP messages from many different scripting and compiled languages.

7. Question

When, in telecommunications, we talk about the Demarc, what are we referring to?

You ensure all of the other tenants have full access to your network equipment.

The ISP terminates their line and your network begins.

You place all your routers and switches.

The servers are places to ensure faster speeds.

Unattempted

Demarc – Point of Demarcation (POD): Where the ISP (Internet Service Provider) terminates their phone/internet lines and your network begins; most buildings only have one.

8. Question

When an attacker can guess a URL they don't know about, from another similar logical URL, what is that called?

Under protected API's

CSRF.

Insecure direct object reference.

Unvalidated redirects.

Unattempted

2013 A4 Insecure direct object reference. Users can access resources they shouldn't, by guessing the URL or path, often if it is logical. If you have access to a report names ending in financials_may2017.pdf on your organization's network, you can try guessing other file names you should not have access to financials_August.pdf or financials_2017.pdf Mitigated by proper access control, using non-sequential names or monitoring file usage.

9. Question

Different types of memory are made for specific tasks and functions in our hardware. Which of these are types of nonvolatile memory? (Select all that apply).

PLD (Programmable logic devices)

DRAM (Dynamic RAM)

EEPROM (Electrically erasable programmable read only memory)

SRAM (Static RAM)

ROM (Read Only memory)

Unattempted

ROM (Read Only memory) is nonvolatile (retains memory after power loss).
EEPROM (Electrically erasable programmable read only memory) – These are electrically erasable, you can use a flashing program. This is still called read

only. The ability to write to the BIOS makes it vulnerable to attackers. PLD (Programmable logic devices) are programmable after they leave the factory (EPROM, EEPROM and flash memory). Not PROM.

10. Question

For us to ensure CONTINUAL clean power in our data center, we would use which of these?

Load balancing.

Uninterruptable Power Supply (UPS)

Power Distribution Unit (PDU)

Power Supply Unit (PSU)

Unattempted

An UPS (Uninterrupted Power Supply) contains a large battery bank that will take over in a power outage, it does also provide surge protection.

11. Question

In our physical access control, we use gates and fences to ensure what happens?

Allow employees to safely exit in an emergency.

Ensure entry and exit from our facility only happens through the gates.

Prevent employees from safely exiting in an emergency.

Allow easy entry and exit from our facility.

Unattempted

Fences (Deterrence, Preventative): Smaller fences such as 3ft. (1m) can be a deterrence, while taller ones, such as 8ft. (2.4m) can be a prevention mechanism. The purpose of the fences is to ensure that entrances/exits from the facility happen through only a few entry points (doors, gates, turnstiles). Gates (Deterrence, Preventative): Placed at control points at the perimeter. Used with the fences to ensure that access only happens through a few entry points.

12. Question

Without using anything to trick our systems, an unauthorized individual is allowed access using our biometric authentication. This is an example of what?

FRR.

CRR.

CER.

FAR.

Unattempted

FAR (False accept rate) Type 2 error: Unauthorized user is granted access. This is a very serious error.

13. Question

6 months ago, we had an attacker trying to gain access to one of our servers. The attack was not successful, and the authorities were able to find the attacker using our forensics. In court, the attacker claims we used entrapment. Which of these options describes entrapment?

Legal and unethical.

Not a solid legal defense strategy for the attacker.

Something we can do without consulting our legal department.

A solid legal defense strategy for the attacker; entrapment is illegal and unethical.

Unattempted

Entrapment (illegal and unethical): When someone is persuaded to commit a crime they had no intention to commit and is then charged with it. Openly advertising sensitive data and then charging people when they access them.

Entrapment is a solid legal defense.

14. Question

Which of these should NOT be part of our proper hardware disposal procedures?

Deleting all files on the hard drive.

Disk crushing.

Overwriting all bits on the disks with 0s.

Degaussing.

Unattempted

Deleting a file just removes it from the table. Everything is still recoverable.

Crushing, degaussing and overwriting should all be non-recoverable.

15. Question

What would be a reason to do misuse case testing on our software?

To expose the system to normal user traffic and use.

To see how well the software installs on certain hardware systems.

To ensure all exposed interfaces are tested.

Because attackers do not act like normal users, we need to test against that.

Unattempted

Misuse Case Testing: Executing a malicious act against a system, attackers won't do what normal users would, we need to test misuse to ensure our application or software is safe.

16. Question

We are building a new data center and the walls must be slab-to-slab. What does that mean?

The wall is from the real floor to the real ceiling.

The wall is from the real floor to the sub ceiling.

The wall is from the top of the subfloor to the sub ceiling.

The wall is made of slabs.

Unattempted

Walls should be "slab to slab" (from the REAL floor to the REAL ceiling); if subflooring or sub ceilings are used, then they should be contained within the slab to slab walls.

17. Question

When a penetration tester is doing a black box test, how much knowledge do they have about their target?

All of these.

Full knowledge and privileges access to systems.

Partial knowledge, user or vendor access level.

No knowledge other than what is publicly available.

Unattempted

Black box Pen testing (Zero Knowledge): The attacker had no knowledge about the organization other than publicly available information. They start from the point an external attacker would.

18. Question

When an attacker is using a brute force attack to break a password, what are they doing?

Trying every possible key to, over time, break any encryption.

Trying to recover the key without breaking the encryption.

Looking at common letter frequency to guess the plaintext.

Looking at the hash values and comparing it to thousands or millions of pre-calculated hashes.

Unattempted

Brute Force: Using the entire key space (every possible key); with enough time, any plaintext can be decrypted. Effective against all key-based ciphers except the one-time pad; it would eventually decrypt it, but it would also generate so many false positives that the data would be useless.

19. Question

In which type of access control does subjects have clearance and object labels?

Role-Based Access Control (RBAC)

Discretionary Access Control (DAC)

Rule-Based Access Control (RUBAC)

Mandatory Access Control (MAC)

Unattempted

MAC (Mandatory Access Control): Often used when confidentiality is most important. Access to an object is determined by labels and clearance. This is often used in the military or in organizations where confidentiality is very important.

20. Question

Our Disaster Recovery Plan (DRP) is a subplan of our Business Continuity Plan (BCP), and the DRP lifecycle has 4 distinct phases. What are those 4 phases? (Select all that apply).

Mitigation.

Preparation.

Failback.

Response.

Recovery.

Action.

Unattempted

DRP has a lifecycle of Mitigation, Preparation, Response and Recovery.

Mitigation: Reduce the impact, and likeliness of a disaster. Preparation: Build programs, procedures and tools for our response. Response: How we react in a disaster, following the procedures. Recovery: Reestablish basic functionality and get back to full production.

21. Question

Looking at the governance of our organization, we can use policies, standards, procedures, or other frameworks. Which of these characteristics would BEST describe our policies?

Non-specific, but can contain patches, updates, strong encryption.

Specific, all laptops are W10, 64 bit, 8GB memory, etc.

Low level step-by-step guides.

Recommendations.

Unattempted

Policies – Mandatory: High level, non-specific. They can contain “Patches, Updates, strong encryption”, they will not be specific to “OS, Encryption type, Vendor Technology”

22. Question

In the software capability maturity model, at which level are some processes “possibly repeatable with consistent results”?

Level 1.

Level 3.

Level 4.

Level 2.

Unattempted

Level 2: Repeatable This level of maturity that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

23. Question

Which of these would be part of our Disaster Recovery Plan (DRP)?

Specific names of who does what in an incident.

What to do if our staff goes on strike.

Which teams and roles does what in an incident.

What to do if our staff is hit by a pandemic like the flu.

Unattempted

Our DRP (Disaster Recovery Plan) should answer at least three basic questions: What is the objective and purpose. Who will be the people or teams who will be responsible in case any disruptions happen. What will these people do (our procedures) when the disaster hits.

24. Question

What is the ISO 27002 standard focused on?

Risk management.

Information Security Management System (ISMS).

Health Insurance Portability and Accountability Act (HIPAA)

Protecting Protected Health Information (PHI).

Unattempted

ISO 27002: (From BS 7799, 1/2, ISO 17799) Provides practical advice on how to implement security controls. It focuses on Information Security Management Systems (ISMS).

25. Question

Which of these is NOT a type of open-source software licensing?

Oracle.

GNU.

BSD.

Apache.

Unattempted

Open source software can be protected by a variety of licensing agreement. GNU (General Public License), BSD (Berkeley Software Distribution) and Apache are all examples of this.

26. Question

We have tested our software and we have found over 10,000 flaws. What should our next steps be?

Rate them on likelihood of exploit and impact and address all the issues.

Fix them all.

Leave them alone, 10,000 is too many to fix.

Rate them on likelihood of exploit and impact and address the critical issues.

Unattempted

Now that we have completed our tests, just like on our log reviews, we need to use it and analyze the data we got from the testing. It can be huge amounts of data, and we need to prioritize what we act on first, what is acceptable and what is not. Think of the qualitative risk analysis, if it is low likelihood and low impact we may leave it alone and focus on higher priority items.

27. Question

As part of our data disposal process, we overwrite all of the disk's multiple times with random 0s and 1s. Sometimes that is NOT an option. When would that be?

When it involves SSD drives.

When the disk is still in the system.

When it involves spinning disk hard drives.

When the disk is damaged.

Unattempted

Overwriting is done by writing 0s or random characters over the data. As far as we know, there is no tool available that can recover even single pass overwriting (not possible on damaged media).

28. Question

When we list the Minimum Operating Requirements (MOR) for a system in our business impact analysis (BIA), what should it contain?

The required time to fully configure a system.

The maximum tolerable downtime.

How long is the maximum organizational redundancy.

Minimum specs for the system to function.

Unattempted

Minimum Operating Requirements (MOR) (Minimum Operating Requirements): The minimum environmental and connectivity requirements for our critical systems to function, can also at times have minimum system requirements for DR sites. We may not need a fully spec'ed system to resume the business functionality.

29. Question

When using the formal approval process, what is required to access data?

Higher clearance than the object requires and data owner approval.

Appropriate clearance.

Permission from the data owner.

Appropriate clearance and data owner approval.

Unattempted

Formal Access Approval: Document from the data owner approving access to the data for the subject. Subject must understand all requirements for accessing

the data and the liability involved if compromised, lost or destroyed. Appropriate Security Clearance is required as well as the Formal Access Approval.

30. Question

As part of a security audit, we have found some security flaws. The IT Security team has been asked to suggest mitigation strategies using the OSI model. Which of these would address layer 7 issues?

Access Lists.

Shut down open unused ports.

Start using application firewalls.

Installing UPSes in the data center.

Unattempted

Application layer firewalls are on the 7th OSI Layer. The key benefit of application layer firewalls is that they can understand certain applications and protocols. They see the entire packet; the packet isn't decrypted until layer 6; any other firewall can only inspect the packet, but not the payload. They can detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port, or detect if a protocol is being used any malicious way.

31. Question

As part of our authentication process, we have issued our staff TOTP tokens. How do they work?

Generates a new password often.

Sends us a new password when we request it, but never when we don't.
Does not need the clocks of the token and the server to be synchronized.
Generate a password that is valid until it is used.

Unattempted

Something you have – Type 2 Authentication: TOTP (Time-based One-Time Password): Time based with shared secret, often generated every 30 or 60 seconds, synchronized clocks are critical.

32. Question

Using the OSI model, which of these are COMMON layer 5-7 threats?

SYN floods.

Eavesdropping.

Ping of death.

Worms.

Unattempted

Of the options provided, **Eavesdropping** and **Worms** are commonly associated with threats at the Layer 5-7 (Session, Presentation, and Application) levels of the OSI model.

- **Eavesdropping:** This involves intercepting communication between two parties, often by capturing network traffic. It's particularly relevant at higher layers where sensitive data like passwords or credit card information might be transmitted.

- **Worms:** These are self-replicating malware that can spread across networks, often exploiting vulnerabilities in applications or operating systems.

Why the other options aren't as directly linked to Layers 5-7:

- **SYN Floods:** While disruptive, SYN floods primarily target the Transport Layer (Layer 4) by overwhelming a server with connection requests.
- **Ping of Death:** This attack involves sending oversized ICMP packets, which can crash some older systems. It's more closely associated with the Network Layer (Layer 3).

In summary: While the boundaries between layers can sometimes be blurred, Eavesdropping and Worms are generally considered higher-level threats that can impact data integrity and confidentiality at the Session, Presentation, and Application layers.

33. Question

On which layer of the OSI model would we consider physical security?

4

1

3

2

Unattempted

Layer 1: Physical Layer: wires, fiber, radio waves, hub, part of NIC, connectors (wireless).

34. Question

In which of these protocols, is IPSEC built into and NOT added on later?

PGP.

HMAC.

IPv6.

IPv4.

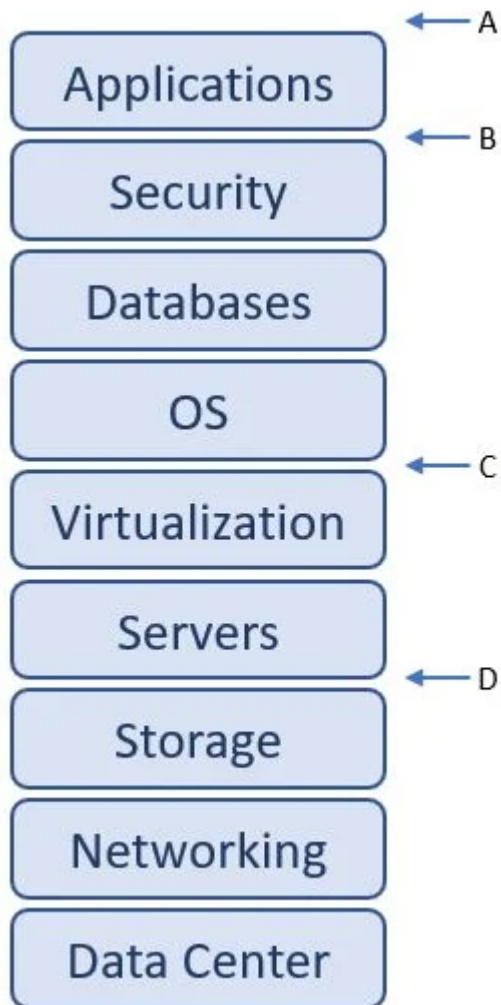
Unattempted

IPSEC (Internet Protocol Security): Set of protocols that provide a cryptographic layer to IP traffic; for IPv4, it is bolted on. For IPv6, it is designed into the protocol.

35. Question

We have just signed a contract with a vendor for a Software as a Service (SaaS) implementation. Where does our responsibility start, and the vendor's

responsibility stop?



D: Between storage and servers.

B: Between security and application.

A: After the application.

C: Between virtualization and OS.

Unattempted

In Software as a Service (SaaS), the vendor provides everything including the applications and programs. We would provide the data for the applications.

36. Question

In our fuzz testing, we analyze data and change the fuzz input iteratively. What is this called?

Mutation fuzzing.

Mutilation fuzzing.

Migration fuzzing.

Mitigation fuzzing.

Unattempted

Fuzzing (Fuzz testing): Testing that provides a lot of different inputs, to try to cause unauthorized access or for the application to enter unpredictable state or crash. If the program crashes or hangs the fuzz test failed. The Fuzz tester can enter values into the script or use pre-compiled random or specific values.

Mutating fuzzing – The tester analyses real info and modify it iteratively.

37. Question

We are doing security audits and we test against published standards. Which of these is NOT one of the standards we would test against?

SOC-2 type 1.

RBAC.

SOC 2 type 2.

PCI-DSS.

Unattempted

RBAC is role based access control, not a security audit standard. SOC 2 and PCI-DSS are standards we audit against.

38. Question

We are adding random data to our password hashes, to prevent attackers from successfully using rainbow table and dictionary attacks. What are we adding to the hash function?

Key stretching.

Nonce.

Clipping levels.

Salting.

Unattempted

Salting is random data that is used as an additional input to a one-way function that hashes a password or passphrase.

39. Question

We are implementing new networking infrastructure in our organization. The new infrastructure is using Carrier-sense multiple access with collision detection (CSMA/CD). What are we implementing?

Extranet.

Wireless.

Internet.

Ethernet.

Unattempted

CSMA/CD (Carrier Sense Multiple Access Collision Detection): Used for systems that can send and receive at the same time, like Ethernet. If two clients listen at the same time and see the line is clear, they can both transmit at the same time, causing collisions; CD is added to help with this scenario. Clients listen to see if the line is idle, and if idle, they send; if in use, they wait a random amount of time (milliseconds). While transmitting, they monitor the network. If more input is received than sent, another workstation is also transmitting, and they send a jam signal to tell the other nodes to stop sending, and wait for a random amount of time before starting to retransmit.

40. Question

We need to ensure we are compliant with all the laws and regulations of all the states, territories, and countries we operate in. How are the security breach notification laws in the US handled?

Federal.

Mandatory for states to have.

Handled by the individual organizations.

Handled by the individual states.

Unattempted

Security Breach Notification Laws. NOT Federal. 48 states have individual laws. Know the one for your state (none in Alabama and South Dakota). They normally require organizations to inform anyone who had their PII compromised. Many

states have an encryption clause where lost encrypted data may not require disclosure.

41. Question

As part of our annual security audit we hired a pen testing company. What could be some of the tools they would use?

Social engineering.

Cutting power cables.

Access control lists.

Force against employees.

Unattempted

Social engineering is often the easiest way for pen testers to get the initial foothold on our network.

42. Question

What could be a type of physical access control that we would use, to prevent cars and vans from entering our perimeter?

Cameras.

Lights.

Bollards.

Motion sensors.

Unattempted

Bollards (Preventative): Used to prevent cars or trucks from entering an area while allowing foot traffic to pass. Often, shops use planters or similar; it looks prettier, but achieves the same goal. Most are static heavy duty objects, but some cylindrical versions can also be electronically raised or lowered to allow authorized traffic past a “no traffic” point. Some are permanent fixtures and can be removed with a key or other unlock function.

43. Question

We have, for many years, used dogs as part of our physical security. However, we are considering implementing other physical security measures and stop using dogs. Which of these could be the reason we would consider NOT using dogs more?

It is expensive.

They are always friendly.

They are not very good at deterring.

They can cause liability issues.

Unattempted

Dogs (Deterrent, Detective, Compensating): Most often used in controlled, enclosed areas. Liability can be an issue. Dogs are trained to corner suspects and attack someone who’s fleeing. People often panic when they encounter a dog and run. Even if they’re in a secure area, the organization may still be liable for injuries.

44. Question

In a new data center implementation, we are wanting to use IPv6 addresses. Which of these statements are TRUE about IPv6 addresses? (Select all that apply).

They are 128 bit binary.

They use the fe80: prefix for link local addresses.

They use broadcast addresses.

They can use EUI/MAC48 addresses, by adding fffe in the middle of the mac address.

They are 32-bit binary.

Unattempted

IPv6 is 128-bit binary, often expressed in hexadecimal numbers (using 0-9 and a-f); for Link Local addresses we add the fe80: prefix to an address, and for EUI/MAC48 addresses we add “fffe” to make it an EUI/MAC64 address.

45. Question

When attackers are war dialing, what are they trying to do?

Driving around trying to gain access to unsecured or weak security wireless access points.

Use a modem to call different numbers, looking for an answer with a modem carrier tone.

Disrupt our wireless access points by transmitting noise on the wireless channels we use.

Calling our dispatch trying to get information through social engineering.

Unattempted

War dialing: Uses modem to dial a series of phone numbers, looking for an answering modem carrier tone, the penetration tester then attempts to access the answering system. Not really done anymore, but know it for the exam.

46. Question

We can use smart cards, tokens, passports, and IDs for which type of authentication?

Type 2.

Type 5.

Type 3.

Type 1.

Unattempted

Something you have – Type 2 Authentication: ID, passport, smart card, token, cookie on PC; these are called Possession factors.

47. Question

As part of our fault tolerance strategy we are using remote journaling. What does that do?

Sends an exact database or file copy to another location.

Sends transaction log files to a remote location, not the files themselves.

Sends copies of the database to backup tapes.

Using a remote backup service, sends backups off-site at a certain time interval.

Unattempted

Remote journaling: Sends transaction log files to a remote location, not the files themselves. The transactions can be rebuilt from the logs if we lose the original files.

48. Question

What is the PRIMARY reason we would implement clipping levels?

To allow users a few tries when they fat finger their password.

To prevent administrative overhead.

To prevent password guessing.

To allow users to unlock their own account when they mistype their password too many times.

Unattempted

The PRIMARY reason we would implement clipping levels is:

To prevent password guessing.

Explanation:

- **Clipping Levels:** These are security measures that limit the number of unsuccessful login attempts within a specific timeframe.
- **How they prevent password guessing:** By limiting the number of attempts, clipping levels make it much harder for attackers to use

automated tools to systematically try different passwords (brute-force attacks) to gain unauthorized access to an account.

- **Other benefits:**

- **Reduced risk of account lockout:** While clipping levels help prevent account lockouts due to legitimate user errors, they primarily focus on thwarting malicious attempts.
- **Improved security posture:** They enhance overall account security by making it more difficult for attackers to compromise accounts.

In summary: The primary purpose of clipping levels is to significantly increase the difficulty and time required for attackers to successfully guess passwords, thereby enhancing the security of user accounts.

49. Question

What can Redundant Array of Independent Disks (RAID) protect us against, if we are using RAID with fault tolerance?

Attackers gaining access to our data.

Data loss if a single disk fails.

Hardware failures.

Multiple disk failures happening at the same time.

Unattempted

Redundant Array of Independent Disks (RAID) can protect our data if we have a single disk failure, as default not against more than one. It can however be configured to support multi disk failure, but is rarely done and is expensive.

50. Question

All of these are examples of Distributed Denial Of Service (DDOS) attacks, except one. Which of these is NOT a Distributed Denial Of Service (DDOS) attack?

UDP flood.

SYN flood.

MAC flood.

IPSec flood.

Unattempted

There are many different types of Distributed Denial Of Service (DDOS) attacks, there is no such thing as an IPSec flood. UDP, SYN and MAC floods are all Distributed Denial Of Service (DDOS) attacks.

51. Question

When is it appropriate to install and use backdoors and maintenance hooks?

Never.

When it makes it easier for the administrators to use the software.

When the code is still in development.

When it is easier for the users to use the software.

Unattempted

A. Never.

Correct. In the context of security best practices, backdoors and maintenance hooks should **never** be installed or used in production environments. They introduce significant security risks, such as unauthorized access or exploitation by attackers. Even during the development phase, the use of backdoors is discouraged because they might be forgotten or inadvertently left in the final production code, creating vulnerabilities.

Backdoors and maintenance hooks introduce significant security risks and vulnerabilities. They can be exploited by malicious actors, leading to unauthorized access and potential system compromises. Therefore, it's never appropriate to install and use them.

Backdoors can create significant security vulnerabilities if left in production code, allowing unauthorized access to systems. Best practices in software development advocate for the removal of such mechanisms before deployment to mitigate potential risks associated with exploitation by malicious actors

B. When it makes it easier for the administrators to use the software.

Incorrect. While backdoors may offer convenience for administrators, they compromise the security posture of the system. Security takes precedence over ease of use, and alternative secure methods should be implemented to facilitate administrative tasks.

C. When the code is still in development.

Incorrect. Backdoors and maintenance hooks might sometimes be used during the development phase for debugging purposes, but this is a **poor security practice**. These mechanisms can be unintentionally left in the codebase, leading

to potential security breaches in production environments. Secure debugging methods should be utilized instead.

D. When it is easier for the users to use the software.

Incorrect. Backdoors designed to enhance user convenience are a major security risk. They bypass authentication and other security controls, exposing the system to exploitation. Security measures should be implemented in a way that balances usability and protection.

52. Question

When we are talking about data remanence, what does that refer to?

Files saved locally and not on a remote storage device.

Data we are actively using and therefore can't encrypt.

All the data on our systems.

Data left over after normal removal and deletion.

Unattempted

Data Remanence: Data left over after normal removal and deletion of data.

53. Question

Which type of access control could we use to limit access outside of regular work hours?

Context-based access control.

Discretionary access control.

Content-based access control.

Role-based access control.

Unattempted

Context-based access control: Access to an object is controlled based on certain contextual parameters, such as location, time, sequence of responses, access history.

54. Question

Which project management methodology uses a linear approach where each phase leads into the next and you can't go back to a previous phase?

Waterfall.

Agile.

Sashimi.

Spiral.

Unattempted

Waterfall: Very linear, each phase leads directly into the next. The unmodified waterfall model does not allow us to go back to the previous phase.

55. Question

A pen tester is calling one of our employees. The pen tester explains to the employee the company will be hit with a lawsuit if he won't do what he is told. Which type of social engineering is the pen tester using?

Scarcity.

Authority.

Intimidation.

Familiarity.

Unattempted

Social engineering uses people skills to bypass security controls. Intimidation (If you don't bad thing happens) – Virus on the network, credit card compromised, lawsuit against your company, intimidation is most effective with impersonation and vishing attacks.

56. Question

We use the CIA triad as a logical model for IT Security and the protection profile our organization wants. What does the A stand for in the CIA triad?

Accountability.

Authorization.

Availability.

Authentication.

Unattempted

The CIA (Confidentiality, Integrity, Availability) Triad: Availability – We ensure authorized people can access the data they need, when they need to.

57. Question

We are using the OSI model to categorize attacks and threats. Which of these are COMMON layer 2 threats?

ARP spoofing.

SYN floods.

Ping of death.

Eavesdropping.

Unattempted

ARP spoofing is an attack where an attacker sends a fake ARP (Address Resolution Protocol) messages over a local area network. This results in associating the attacker's MAC address with the IP address of an authorized computer or server on our network.

58. Question

We are using RAID-5 (Redundant Array of Independent Disks) on a one of our servers, that uses at least how many disks?

1

3

4

2

Unattempted

RAID 5: Block level striping with distributed parity, requires at least 3 disks.
Combined speed with redundancy.

**Use Page numbers below to navigate to other
practice tests**

Pages: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#)
[33](#) [34](#) [35](#)

Post navigation

[← Previous Post](#)

[Next Post →](#)

We help you to succeed in your certification exams

We have helped over thousands of working professionals to achieve their certification goals with our practice tests.

Skillcertpro

Instagram



Twitter



LinkedIn-in



Facebook-f



Quick Links

[ABOUT US](#)

[FAQ](#)

[BROWSE ALL PRACTICE TESTS](#)

[CONTACT FORM](#)

Important Links



[POLICY](#)

[REFUND](#)



REFUND

REQUEST

TERMS & CONDITIONS

PRIVACY POLICY

[Privacy Policy](#)



⌘K



QuestionAI



Chat AI

Hello! Is there any question I can help you with?

Which city is known as the “Big Apple” in the United States?

What is the highest peak in the United States?

Capture



Study Tools

Ask AI 

Please select your level

You can get more accurate solutions!

☐ Middle School ☐ High School ☐ University ☐ Community College ☐ Others